3. HARDWARE & SOFTWARE USATI PER LA REALIZZAZIONE DELLA WAN

In questo capitolo presentiamo brevemente l'hardware ed i moduli software usati durante lo svolgimento della tesi per la creazione della rete wireless. Questo capitolo si avvale di Appendici in cui sono state raccolte informazioni più dettagliate riguardo i protocolli in uso. L'utilizzo delle Appendici soddisfa contemporaneamente due esigenze: permette di non tediare con inutili dovizie di particolari il lettore già esperto dell'argomento, e mentre, d'altro canto, di informare più dettagliatamente il lettore meno informato.

3.1 HARDWARE

La rete ad-hoc è stata predisposta utilizzando 1 PC fisso, 3 PC portatili e 2 palmari, tutti dotati di scheda per l'interconnessione alla rete wireless. Di seguito sono riportate le loro caratteristiche tecniche.

a) 3 PC PORTATILI
Modello: TravelMate 220
Sistema Operativo: Debian Linux
Processore e Core Logic: Mobile Intel® Celeron® M fino a 1.33 GHz con 256Kb di cache 133MHz System Bus
Memoria fino a 256MB SDRAM espandibile a 1024MB
HDD 20GB Ultra ATA/100 HDD
Networking & Communication: Modem/Fax 56Kbps e scheda 10/100 Base-T Ethernet, Wake on-Lan integrata
Interfacce: 1slot PCMCIA CardBus a 32bit tipo II o 1 tipo III, 1 × RJ-11 per modem, 1 x RJ-45 per Ethernet

b) 2 PALMARI
Modello: iPAQ 3900
Sistema operativo: Microsoft Pocket PC 2002
Dimensioni: 133 mm x 80 mm x 16 mm
Peso: 180 grammi
Processore: Intel PXA250 XScale a 400Mhz
Memoria: ROM:32MBRAM:64MB
Interfacce: Microfono incorporato Speaker Ingresso Cuffie Porta infrarossi (10m)USB Seriale Ingresso alimentazione
Display: Transflective240 x 3203.8" LCD65.536 colori
Slot integrati: Secure Digital I/O MMCard
Keypad: Tastierino di navigazione a 5 funzioni Tastierino di registrazione5 tasti con funzioni personalizzabili
Batteria ricaricabile: 1400 mAh polimeri di litio

Modello: Zaurus 3500
CPU: StrongARM(1) SA-1110, 206MHz[1]
Platform: Linux based embedded OS (Embedix) Qtopia, Personal Java[4]
Display: Reflective TFT LCD with Front Light 3.5" with 240x320 pixel, 65,536 colors
Memory: 64MB SDRAM 16MB FLASH ROM
Input Device: Touch Panel, QWERTY keyboard with a slide cover
Card Slot: 1 compact Flash Card[5] slot, 1 SD card slot
I/O Port: Serial/USB, IR port
Sound: Stereo headphone jack included, Audio input

c) 1 PC FISSO
Modello: Athlon 1800
Sistema operativo: Windows 98
Processore AMD Athlon da 1,6 Ghz
Scheda madre: formato ATX, Bus AGP 4x, Front Side Bus da 266 MHz e controller UDMA/100;
Memoria centrale: 256 MByte di RAM,
Unità disco fisso: Capacità di 40 GB di tipo Ultra DMA/100;
Scheda grafica: 32 MByte di memoria video su bus AGP;
Porta parallela: ECP/EPP;
Coppia di porte seriali: UART 16550; 2 porte USB;

Scheda per l'aggancio alla rete wireless

La scheda utilizzata per l'aggangio alla rete wireless è una Linksys WPC11. È un adattatore a 11 Mbps per Wireless LAN (WLANs) conforme allo standard 802.11b con chipset integrato Intersils PRISM2 da inserire in uno slot PCMCIA di tipo II. È costituito da un'antenna integrata a da due led verdi indicatori di potenza e di connessione alla rete.
La scheda Linksys WPC11 lavora nella banda di frequenza tra 2,4 – 2,4835 GHz con tecnica di modulazione Direct Sequenze Spread Spectrum (DSSS) e usa una tecnica di encryption 64/128-bit WEP (Wired Equivalent Privacy) per una connessione di rete più sicura. Può trasmettere dati a 11, 5,5, 2 o 1 Mbps per canale e tale valore può essere settato secondo le esigenze. Il raggio massimo di copertura dichiarato è di 100 metri indoor e 500 outdoor.
L'adattatore PCMCIA usato può lavorare sia in modalità ad-hoc sia in modalità Infrastructure ed in questo caso il terminale può essere connesso alla rete esistente tramite un access point.
Nella pagina seguente sono brevemente descritte le specifiche tecniche dell'adattatore.

Modello: WPC11 ver. 3.0
Standard: IEEE 802.11b
Tipi di adattatore PCMCIA Type II or III Slot
Canali: 11 Channels (US, Canada)
13 Channels (Europe)
14 Channels (Japan)
Campo di azione: Indoors: fino a 300' (91 m)
Outdoors: fino a 1500' (457 m)
Velocita' di trasmissione: fino a 11Mbps (con Automatic Scale Back)
LEDs: Link, Transmit

Caratteristiche fisiche
Dimensions: 4.5" x 2.13" x 0.3" (115 mm x 54 mm x 7.5 mm)
Unit Weight: 1.65 oz. (.047 kg.)
Power: 3.3V or 5V DC, 275mA Tx, 225mA Rx,20mA Standby
Certifications: FCC Class B, CE Mark
Operating Temp: 32ºF to 131ºF (0ºC to 55ºC)
Storage Temp: -4ºF to 158ºF (-20ºC to 70ºC)
Operating Humidity: 0% to 90% Non-Condensing
Storage Humidity: 0% to 95% Non-Condensing

E' doverosa una nota sul *perché abbiamo scelto di usare il sistema operativo Linux GNU/Debian* con kernel 2.4.20. La scelta di tale sistema è giustificata da diversi fattori quali:

Codice sorgente

Chi vuole sviluppare software apprezzerà il fatto che ci sono centinaia di strumenti di sviluppo e linguaggi, oltre a milioni di linee di codice nel sistema di base. Tutto il software nella distribuzione principale soddisfa i criteri delle Linee Guida Debian per il Software Free (DFSG). Ciò significa che si può liberamente usare il codice per studiarlo o incorporarlo in nuovi progetti software liberi. Inoltre ci sono moltissimi strumenti e codice disponibili anche per software proprietario.

Aggiornamenti facili

A causa del sistema di impacchettamento, aggiornarsi a una nuova versione di Debian è una operazione semplicissima. Basta eseguire apt-get update ; apt-get dist-upgrade e potremmo aggiornare da CD nel giro di pochi minuti, oppure si può far puntare apt ad uno dei 150 mirror Debian e fare l' aggiornamento attraverso la rete.

Stabilità

Ci sono molti casi di macchine che hanno funzionato più di un anno senza dover riavviare il sistema. Anche in quel caso, vengono riavviate solo a causa di mancanza di continuità nella alimentazione o di un aggiornamento hardware. Si confronti questa caratteristica con quella di altri sistemi che vanno in crash più volte al giorno.

Queste, come detto, sono le principali (ma non uniche) ragioni per cui abbiamo scelto come Sistema Operativo il GNU/Debian. Per gli interessati, in Appendice A di questo stesso capitolo e' fornita una breve descrizione sulla nascita e l'evoluzione della filosofia "open source".

3.2 SOFTWARE UTILIZZATO PER LA MISURA DELLE PRESTAZIONI DEL TRAFFICO SU IEEE 802.11b

3.2.1 L'applicativo NETPERF

Netperf è stato sviluppato dalla Hewlett-Packard agli inizi degli anni '90 come uno strumento che potesse essere usato per *misurare vari aspetti delle prestazioni di reti IP* [5]. Netperf prova a saturare il cammino e restituisce il valore del throughput determinato in questo modo. Così facendo determina il throughput che un'applicazione avrebbe potuto ottenere se fosse stata utilizzata al momento della misura.
Netperf deve essere installato su entrambi gli estremi del path del quale si vogliono misurare le caratteristiche [6]. Funziona sulla base del modello client-server. Il server deve essere messo in funzione per primo e per default ascolta sulla porta 12685. Quando il client richiede di effettuare una misura, una connessione TCP di controllo viene stabilita per passare le informazioni di configurazione e, alla fine della misura, i risultati. Immediatamente dopo che le informazioni di configurazione sono state scambiate, una ulteriore connessione viene aperta per realizzare la misura e nessun traffico viene generato sulla connessione di controllo. Il trasferimento della quantità di dati per la misura (bulk transfer) avviene per un tempo di durata configurabile tramite linea di comando. Quando il bulk transfer è concluso, i risultati della misura vengono spediti attraverso la connessione di controllo e sono mostrati sia dalla parte client dell'applicazione che da quella server.
In Appendice B di questo capitolo, il lettore interessato troverà delle specifiche dei test con Netperf ed altre informazioni relative a questo applicativo.

3.2.2 L'applicativo IPERF

Iperf è stato sviluppato dal National Laboratory for Applied Network Research (NLANR) ed è attivamente supportato al momento [7]. Le sue caratteristiche sono molto simili a quelle di Netperf ma, in aggiunta, supporta avanzate funzionalità come, ad esempio, la possibilità di scegliere la grandezza delle finestre TCP (window size) e flussi multipli di traffico (multiple streams), mentre, con il traffico UDP, riporta la banda, il ritardo, il jitter e la perdita di dati. Iperf è costituito da un unico eseguibile che una volta compilato funziona in modalità client-server semplicemente mediante l'utilizzo o meno di un flag.
Lo scopo primario di Iperf è semplificare la configurazione delle connessioni TCP su un particolare percorso. Un parametro fondamentale è la dimensione della window TCP, che determina le prestazioni dell'algoritmo di controllo e prevenzione della congestione (congestion control e avoidance). Se questa è troppo piccola, il

trasmettitore avrà basse prestazioni. Il valore teorico da utilizzare per settare la dimensione della finestra è il risultato del prodotto della banda massima disponibile (bottleneck bandwidth) e del round trip time.

3.3 APPLICAZIONI MULTIMEDIALI

Le recenti ricerche, tese a sviluppare tools di videoconferenza basati su IP Multicast, hanno condotto alla realizzazione di applicazioni multimediali. Dal momento che la maggior parte di dette applicazioni è stata sviluppata appoggiandosi su MBone di Internet, questo paragrafo comincia con una descrizione di IP Multicast e di Mbone.
Il metodo Unicast fornisce una comunicazione punto punto, in cui sia l' host che la destinazione sono specificati ed unici. Con il Broadcast possiamo supplire a trasmissioni verso destinazioni multiple e quindi questa tecnica è ampiamente scalabile quando si presenti il caso di un gran numero di ricevitori; con tale metodo tutti gli hosts su una determinata rete ricevono una copia dei pacchetti inviati. Con la tecnica nota come Multicast il traffico IP è inviato a tutti gli hosts che sono in ascolto su un determinato indirizzo che identifica il gruppo multicast stesso. Unico per ogni gruppo, questo appartiene agli indirizzi IP di classe D: quindi un gruppo multicast non è altro che un certo numero di hosts che vogliono ricevere datagrammi con quello specifico indirizzo di classe D. I gruppi sono dinamici: i membri possono prendere parte al gruppo o abbandonarlo tramite specifici messaggi indirizzati ai Router multicast che si incaricano di generare l' albero di distribuzione dei pacchetti verso i ricevitori interessati.
Il Multicast Backbone di Internet, ovvero MBone, implementa la tecnica sopra descritta. È una tecnica di recente sviluppo che non è ancora stata estesa a tutti gli hosts e i router della rete internet. Un host può trasmettere pacchetti senza neppure sapere a chi sono indirizzati dal momento che l' indirizzo di destinazione sul pacchetto IP è di classe D, ovvero multicast, e quindi è compito degli interessati ricevere quei pacchetti notificare ai router multicast la loro disponibilità a ricevere pacchetti. Per limitare loop indefiniti ci si riferisce al valore del campo Time To Live nell' intestazione dei pacchetti; il TTL è decrementato ogni volta che il pacchetto viene ricevuto da un router: una volta che a raggiunto il valore zero, il pacchetto viene scartato. Per convenzione un valore di TTL compreso tra 1 e 16 limita la distribuzione del datagramma ad una singola sottorete, mentre un valore di 127 permette una distribuzione a livello mondiale.
Nel nostro progetto ciascun flusso di dati mediatici è gestito separatamente da una specifica applicazione. Requisiti come il controllo di conferenza, il prendere parte o l' abbandonare la conferenza stessa, l' avviare o lo spegnere i tools necessari sono delegati a un controllore esterno (connector). Ciascun agente mediatico può facilmente essere rimpiazzato e riusato in nuove applicazioni; la pecca più grande di questo tipo di approccio è che una volta avviato un tool mediatico questo sfugge al controllo del gestore; questo significa che l' utente deve impiegare, per ogni applicazione, un' interfaccia con l' effetto negativo che tutte sono coinvolte in parti di compiti comuni

come iniziare o terminare un servizio o mostrare la lista dei membri di una sessione. Un membro della sessione che contribuisce ai flussi audio e video compare quindi in tre differenti interfaccie delle applicazioni in esecuzione e a volte succede anche che i nomi non coincidano. Un' altra e ben più severa pecca è la mancanza di vera interazione tra i vari tools: è molto difficile infatti costruire delle applicazioni monolitiche che nascondano la molteplicità dei flussi mediatici e che appaiano all' utente tramite un' unica interfaccia con la quale sia possibile gestire l' intera sessione a cui sta prendendo parte.

Media tools
I tools di videoconferenza, per inviare o ricevere flussi che chiameremo “mediatici” possono essere applicazioni indipendenti o possono essere integrati in un sistema più ampio per la gestione della videoconferenza. I flussi mediatici includono audio video e spazi di lavoro condivisi nei quali i partecipanti possono scrivere o disegnare. La distribuzione di questi flussi avviene tramite IP multicast creando così all' interno della rete Internet dei gruppi contraddistinti da indirizzi di classe D in cui tutto ciò che è inviato da un host è ricevuto da tutti gli altri nello stesso gruppo.
Nel seguito di questo paragrafo esamineremo Vic, Rat prodotti dal Lawrence Berkeley National Laboratori (USA). Ciascuno dei suddetti tools utilizza il protocollo RTP (Real Time Protocol). Ancora una volta, il lettore interessato trovera’ dettagliate informazioni sul protocollo RTP nell’Appendice C alla fine di questo capitolo.

3.4 VIC (VIDEO CONFERENCING TOOL)

Vic è una applicazione prevalentemente sviluppata in linguaggio C e Tcl/Tk che gestisce i flussi video all’interno della videoconferenza. Come tutti i tools per applicazioni multicast va avviato con un indirizzo multicast ed un numero di porta che, insieme, specificano una determinata conferenza all' interno del gruppo indicato nell' indirizzo. Vic si compone principalmente di tre tipi di pannello: il primo mostra, in modalità *thumbnails*, cosa i vari membri stanno trasmettendo insieme a brevi informazioni sulla velocità del frame e la velocità di trasmissione, nonché un bottone di “mute” che permette, in modo rapido, di escludere la ricezione dei pacchetti di quello specifico membro. Le immagini, in modalità thumbnails, possono essere ingrandite semplicemente cliccandoci sopra (figura 3.1 e 3.2).

Figura 3.1 Finestra principale di Vic

Il nome del generatore del flusso video ricevuto è contenuto nel file $HOME/.RTPdefaults
E' possibile anche visualizzare le immagini in bianco e nero tramite l' opzione *no color* che figura accanto ad ogni thumbnails.
Il pulsante Menu, indicato sul pannello ove sono listati i differenti membri della conferenza, permette di accedere alle informazioni più dettagliate sui parametri relativi al modo in cui noi stessi inviamo flussi video nel gruppo multicast di cui facciamo parte (figura 3.3).
Il pannello visualizzato in figura 3.3 è chiamato "pannello di controllo" e consente di modificare i parametri che sono stati configurati in precedenza. Come si può vedere, il pannello è diviso in tre parti che, anche logicamente, si riferiscono a tre aspetti differenti dell' applicazione che sta girando sulla nostra macchina. La prima sezione attiva o meno la trasmissione tramite il pulsante "transmit", e, con le due barre a scorrimento, si possono controllare il framerate e la banda che vogliamo impiegare nella trasmissione. La seconda sezione permette di scegliere il dispositivo da cui prelevare le immagini da inviare in multicast, tramite il pulsante "device". È anche possibile scegliere il formato di codifica. Infatti H.261 e MPEG hanno lo svantaggio che contengono dei punti di sincronizzazione ad esempio ogni 10 frames. Ciò implica che la perdita di un pacchetto, in realtà, provoca la perdita di tutti i pacchetti fino al nuovo punto di sincronizzazione, e questo può essere inaccettabile a basse velocità. In VIC sono state elaborate delle modifiche su H.261 che hanno aggirato il problema senza degradare sensibilmente le prestazioni della codifica. Questa decodifica è stata denominata intra-H.261.

Figura 3.2 Ingrandimento del thumbnail

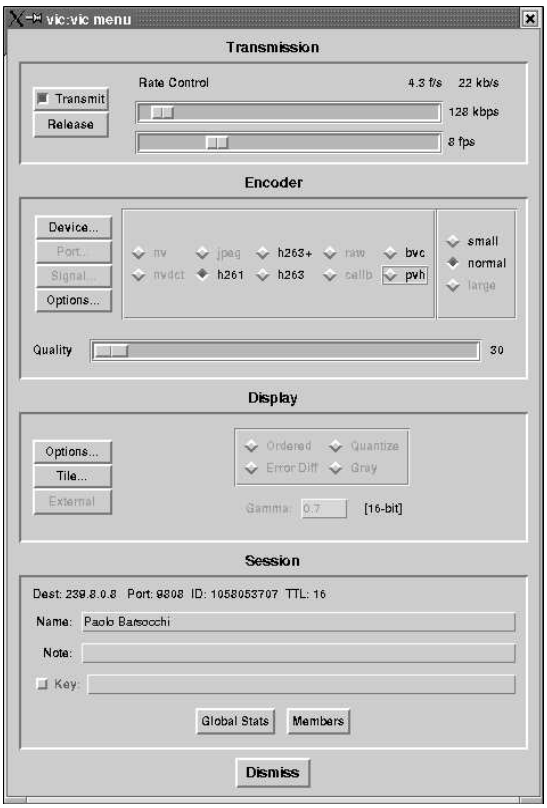


Figura 3.3 Menù di controllo di Vic

Nella sezione finale sono mostrate le informazioni relative al partecipante selezionato. Le immagini che vengono ricevute non portano purtroppo informazioni su cosa stia dicendo la persona in quello specifico momento. Queste sono gestite dal programma RAT, con cui VIC collabora.
Infine l' opzione "*members*", che si vede in fondo al pannello di figura 3.3 permette di vedere le persone che stanno partecipando alla conferenza grazie alle funzionalità di RTCP.

3.5 RAT (ROBUST AUDIO TOOL)

RAT è un tool per la gestione dell'audio in una conferenza, è quindi un'applicazione che permette di partecipare a una conferenza audio su una internet. Questa può essere una conferenza punto-punto via unicast o multipunto via multicast. RAT usa un'interfaccia utente (come mostrata in figura 3.4) realizzata con il Tcl/Tk che richiama delle procedure C che gestiscono la comunicazione ed il rendering audio.

Come possiamo vedere compare sul fondo dall'applicativo RAT un tasto di opzioni. Una volta premuto questo tasto compare una nuova schermata (fig. 3.5) nella quale possiamo scegliere di cambiare i dati personali inseriti la prima volta che si è lanciato RAT, oppure cambiare il tipo di codifica usata in trasmissione, la qualità e il delay in ricezione, visualizzare la qualità del suono che riviamo, e molte altre opzioni.

Figura 3.4 Schermata principale di RAT

RAT implementa RTP ed usa un interessante tipo di payload (vedi RFC 2198). Qui vengono infatti sfruttati il principio delle trasmissioni ridondanti e dell'interleaving.

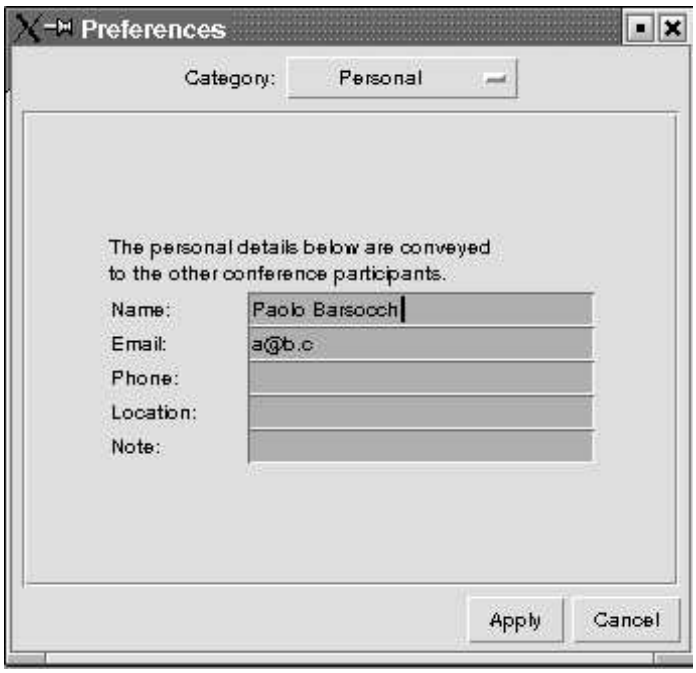


Figura 3.5 Preference

La trasmissione ridondante (fig. 3.6) significa che in un pacchetto, oltre che includere la codifica audio di un certo intervallo temporale, viene inserita anche una copia del precedente intervallo, pesantemente compressa. Ciò vuol dire che la perdita di un pacchetto possa essere "rattoppata" con una copia compressa del pacchetto successivamente arrivato.

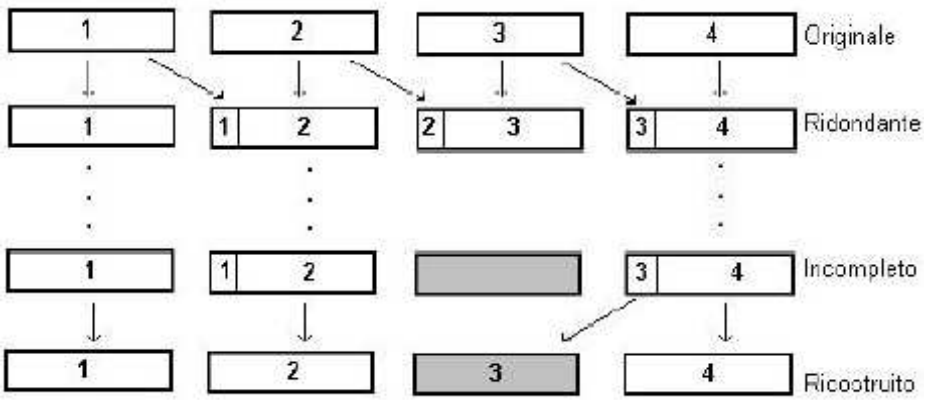


Figura 3.6 Esempio di trasmissione ridondante

Con *interleavin*g (fig. 3.7) s'intende la dispersione di un intervallo temporale su diversi pacchetti. Per questo, invece di mettere 20ms audio su un unico pacchetto, vengono inseriti quattro segmenti di 5ms ciascuno provenienti da intervalli diversi. Così la perdita di un pacchetto provoca effetti che si disperdono su un intervallo.

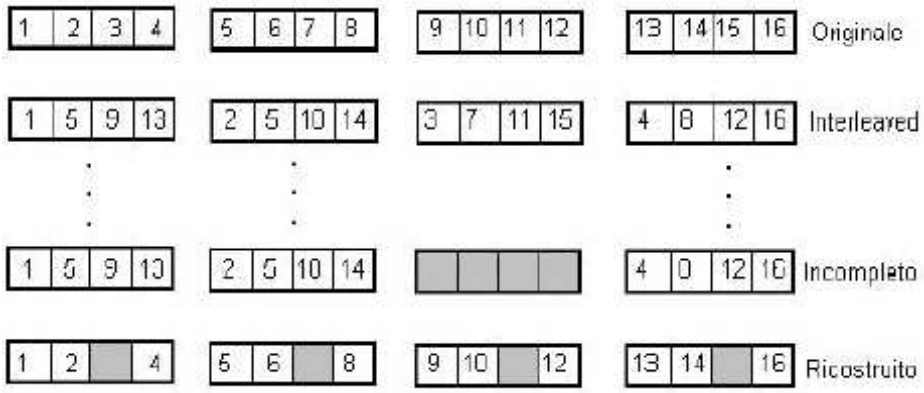


Figura 3.7 Esempio di una trasmissione con interleaving

Il difetto di questa tecnica è che introduce un maggiore delay. Il pregio è che al contrario della ridondanza non richiede una maggiore banda. Questi sono due esempi della flessibilità di RTP.
Le tecniche di ricovero implementate da RAT (nel caso non si usi la ridondanza) sono tre:

- **Silence substituation**: la perdita di un pacchetto è sostituita con il silenzio. Questa è la tecnica più semplice e meno efficace.
- **Packet repetition**: la perdita dl pacchetto è rimpiazzata dal pacchetto precedentemente ricevuto. Questa è una soluzione semplice e abbastanza efficace.
- **Pattern matching repair**: viene prodotta una interpolazione fra il pacchetto precedente e quello successivo a quello perso. Questa è la soluzione più "pesante" ma che dà anche i migliori risultati.

3.6 CONNECTOR

Il software per la gestione della videoconferenza, che ci permette di creare un tunnel IP con Toulouse per usare (in remoto) la sua stazione trasmittente su satellite, e quindi di poter trasmette i segnali audio-video sul satellite, è il *connector*. Una volta lanciato, apparirà una schermata (fig 3.8), nella quale è possibile selezionare in che modo vogliamo il ritorno del segnale.
Di default non è selezionato il ritorno satellitare ma, se vogliamo, premendo sulla scritta "satellite return" possiamo selezionarlo (fig 3.9). In questo modo il segnale che

noi trasmettiamo tramite l'interfaccia ethernet verrà ricevuto dal reflector a Toulouse e trasmesso sul canale satellitare. Il segnale verrà quindi ricevuto da un computer dotato di interfaccia satellitare e, tramite un mini router, rispedito su un'altra interfaccia scelta dall'utente. Ed è proprio per quest'ultimo motivo che dobbiamo indicare al connector su quale interfaccia ci aspettiamo il ritorno satellitare (fig. 3.9). Per attivare la connessione basterà poi premere il tasto start sul fondo dell'interfaccia.

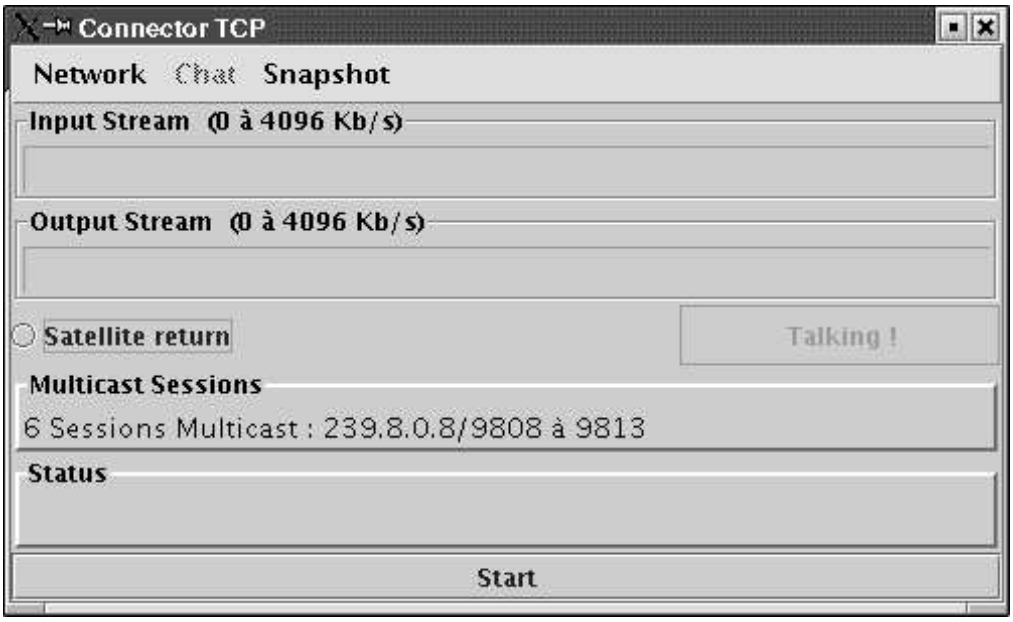


Figura 3.8 Schermata principale del Connector TCP

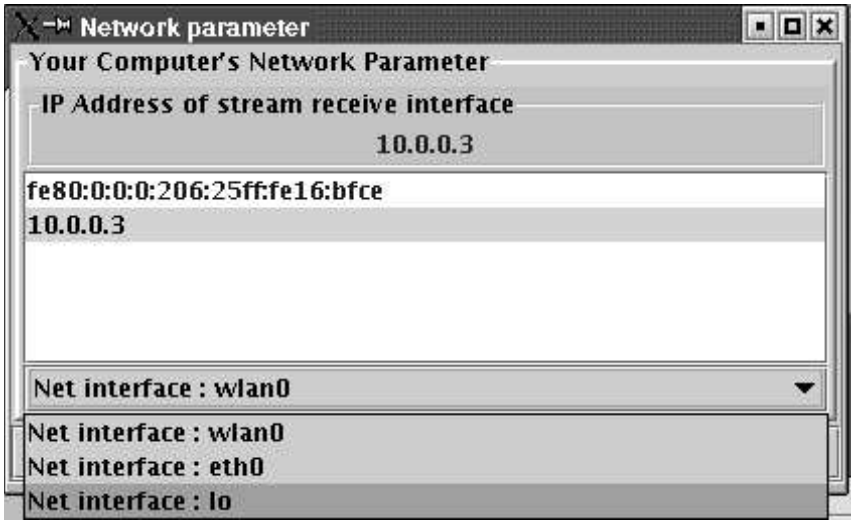


Figura 3.9 Network parameter

Una volta lanciato, il Connector esegue diverse operazioni:

- Verifica se esiste qualche altro connector attivo nella rete locale spedendo un "multicast probe message" ed aspettando la risposta di altri connector attivi.
- Se dopo un tempo di time-out il connector appena lanciato non riceve risposta significa che non esistono altri connector attivi sulla rete locale e quindi lui si elegge Connector primario, questo significa che apre il tunnel TCP con il reflector di Toulouse.
- Se invece viene ricevuta risposta allora significa che il tunnel TCP è già aperto da un altro connector e quindi i miei dati vengono inviati in multicast all'indirizzo 239.8.0.8. Sarà compito poi del connector primario catturarli e ritrasmetterli a Toulouse.

Dopo questi preliminari controlli il Connector lancia Vic, Rat e Chat (applicativo utilizzato per spedire messaggi) come mostrato in figura 3.10.

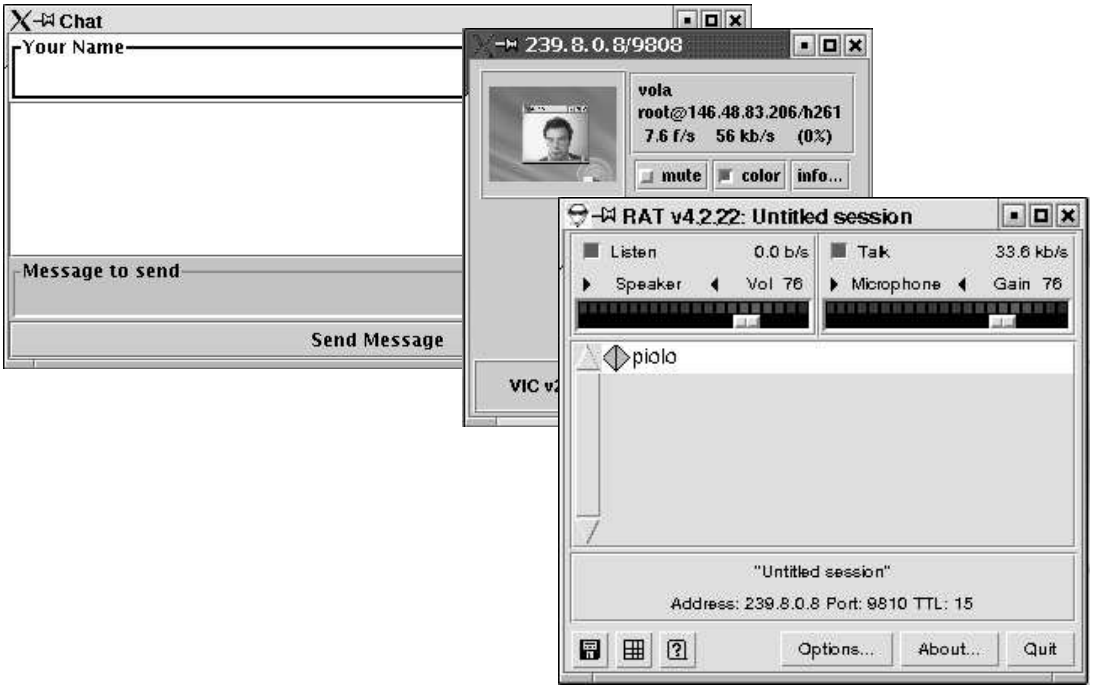


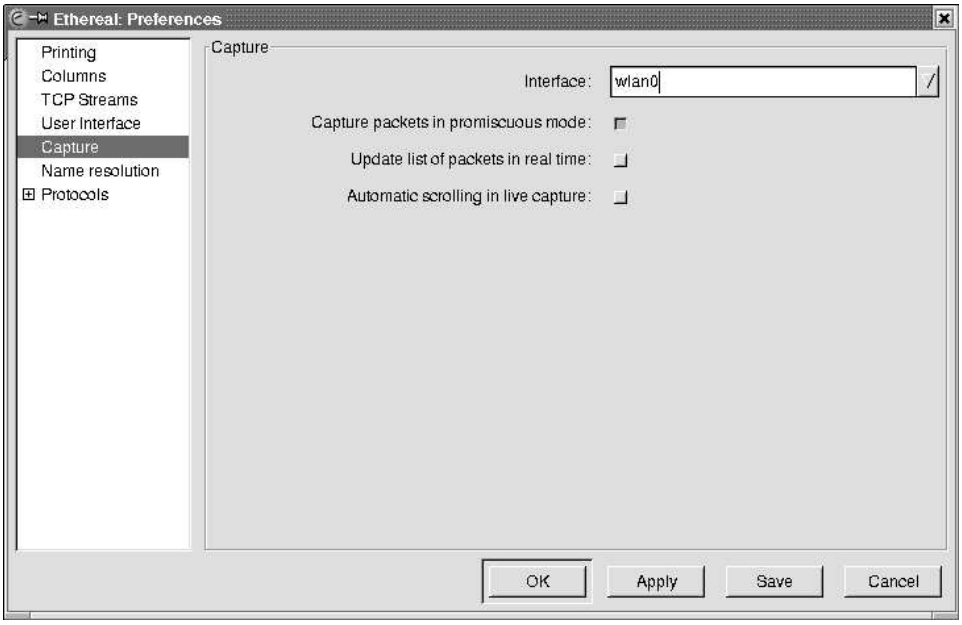
Figura 3.10 Come si presenta il desktop dopo aver lanciato il connector

In effetti, se il Connector non è il primario, le funzioni si limitano a lanciare questi applicativi. Quindi potremmo anche farne a meno, e lanciare manualmente VIC e RAT all'indirizzo multicast 239.8.0.8 rispettivamente sulle porte 9808 e 9810, sulle quali il Connector primario si aspetta di trovare traffico.

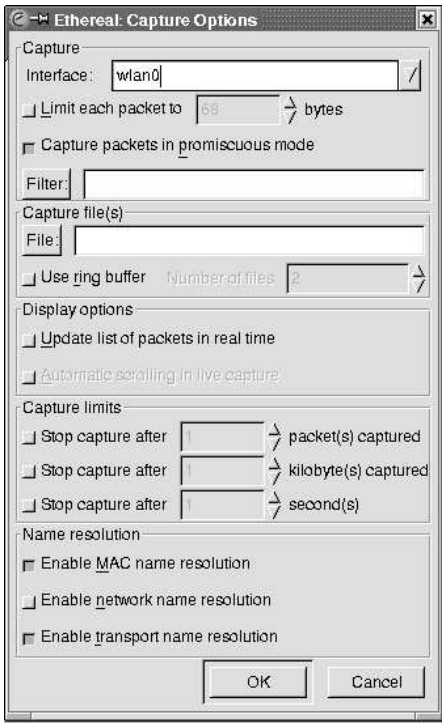
3.7 ETHEREAL

Ethereal è un programma per l' analisi del traffico di rete, che agisce fino al livello due del modello ISO-OSI (collegamento dati), riuscendo a riconoscere all' interno di questo una serie di protocolli al livello tre e quattro del modello ISO-OSI (rete). In particolare, individua correttamente molti protocolli collegati a IPv4 e IPv6.
È pensato principalmente per accumulare il traffico intercettato, allo scopo di consentirne un' analisi dettagliata in un momento successivo; nello stesso modo è predisposto per accedere a informazioni di questo genere accumulate da programmi diversi, così come è in grado di esportare i propri dati in formati alternativi. Ethereal consente anche una visualizzazione in tempo reale del traffico in corso, in modo analogo a quanto fa IPTraf, con la differenza che le informazioni fornite sono molto più chiare. In questo senso, Ethereal è un ottimo strumento didattico per lo studio delle reti. Ethereal viene usato normalmente attraverso il sistema grafico X e deve funzionare con i privilegi dell' utente root, per poter accedere direttamente all' interfaccia di rete da sondare. L' eseguibile da avviare **è***thereal* **[***opzioni***].**
Mostriamo qui il funzionamento di Ethereal in modo interattivo, senza l' uso di opzioni nella riga di comando.

Ethereal avviato senza opzioni, rimane in attesa prima di iniziare la sua analisi.



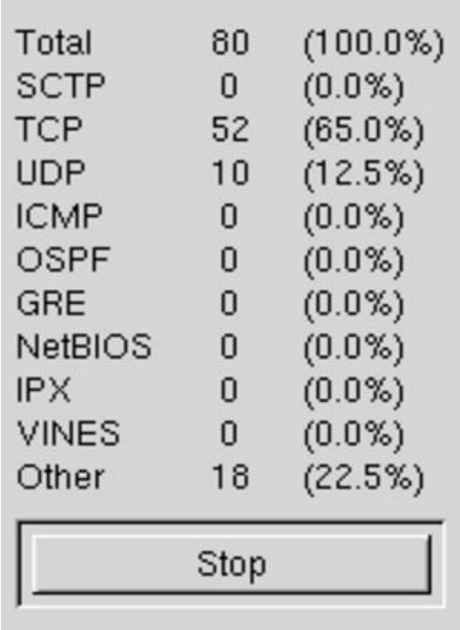
La finestra di configurazione di Ethereal per quanto riguarda la selezione dei pacchetti catturati.



La finestra che appare quando si chiede di iniziare la cattura dei pacchetti

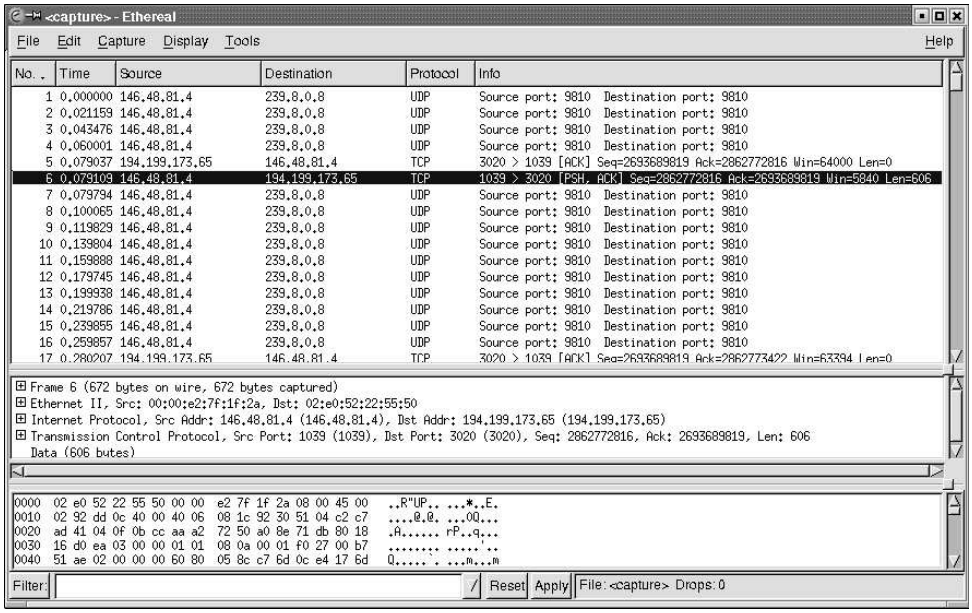
Una volta avviato l' eseguibile ethereal, per ottenere un' analisi del traffico in tempo reale può essere necessario controllare la configurazione. Si trova la voce {Preferences} nel menù {Edit}:
La figura mostra in particolare la selezione della modalità promiscua, con cui si intercettano tutti i pacchetti che l' interfaccia di rete selezionata è in grado di osservare.

Una volta definita la configurazione e selezionata l' interfaccia di rete di interesse, si può passare alla cattura dei pacchetti, selezionando la voce {Start} dal menù {Capture}. Si ottiene una finestra da cui è possibile aggiustare le opzioni relative alla cattura.



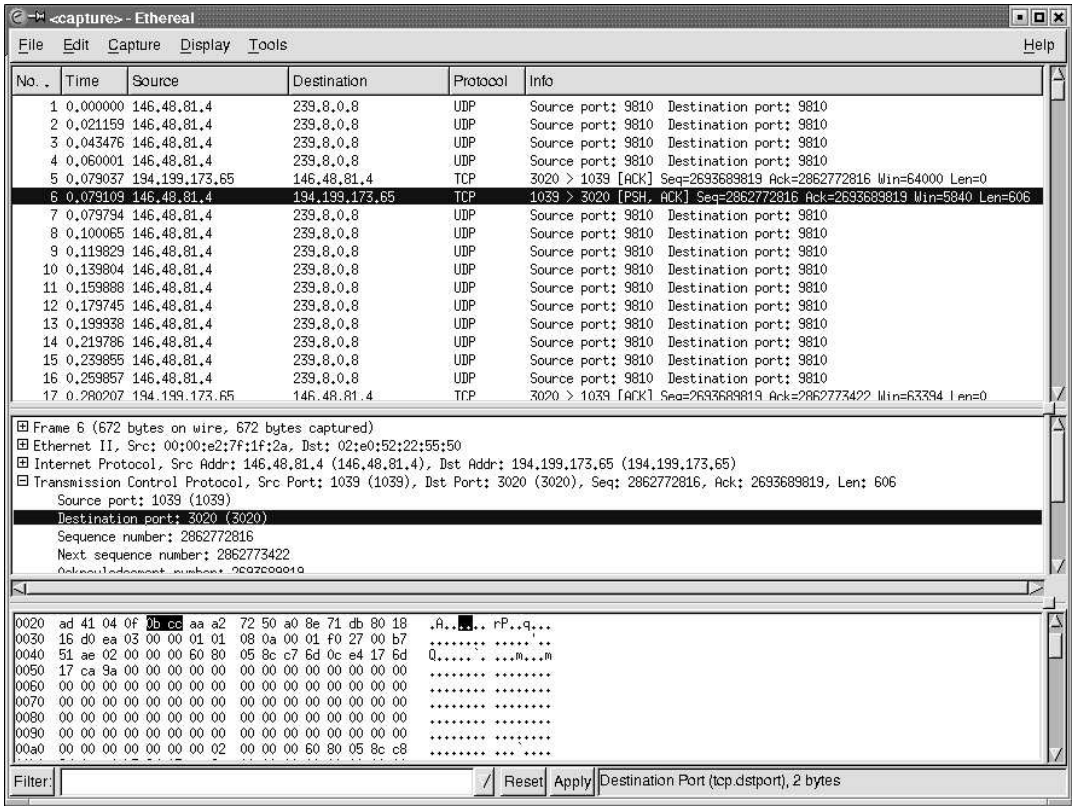
Statistiche visualizzate durante la cattura dei pacchetti

Durante la cattura dei pacchetti viene visualizzata una statistica sull' avanzamento di questo lavoro, e appare un pulsante grafico che consente di fermare l' accumulo dei dati. Se era stata richiesta la visualizzazione in tempo reale delle informazioni relative alla cattura, anche il contenuto dei pacchetti viene visualizzato nella finestra principale di Ethereal.
La finestra principale di Ethereal si divide in tre parti: in quella superiore appare l' elenco dei pacchetti intercettati con una descrizione essenziale del loro contenuto; selezionando un pacchetto nella parte superiore, in quella centrale appare un elenco ad albero di componenti del pacchetto stesso; selezionando una voce nell' elenco del riquadro centrale, appare in quello inferiore l' evidenziamento della porzione di pacchetto che lo riguarda. La figura seguente mostra pacchetti UDP in transito dall'indirizzo 146.48.81.4 all'indirizzo multicast 239.8.0.8 e il tunnel TCP, aperto una volta lanciato il connector, con il reflector (194.199.173.65).



Tunnel TCP aperto con il reflector (194.199.173.65)

Nella figura successiva, si analizzano i dati TCP dello stesso pacchetto, mostrando in particolare dove si colloca l' informazione sulla porta di destinazione:



Porta di destinazione TCP del pacchetto inviato al reflector

3.8 COMPILAZIONE DEL KERNEL

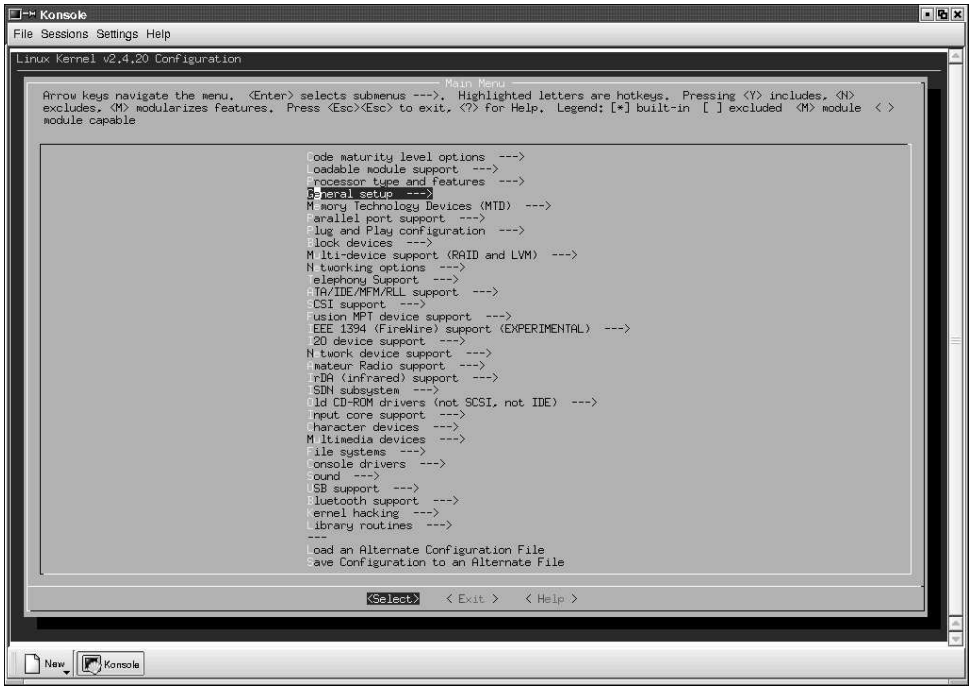
Per riuscire a "far vedere" la scheda PCMCIA al kernel è stato necessario ricompilare il kernel utilizzato (2.4.20). La procedura per la compilazione del kernel e dei moduli per la distribuzione GNU/Debian mette a disposizione uno strumento accessorio, molto utile, per facilitare questa operazione, passando per la creazione di un pacchetto Debian vero e proprio. Il pacchetto in questione è denominato *Kernel-package* e per questo scopo può essere usato direttamente senza bisogno di alcuna configurazione. È sufficiente procedere nel modo seguente:

cd directory_iniziale_dei_sorgenti

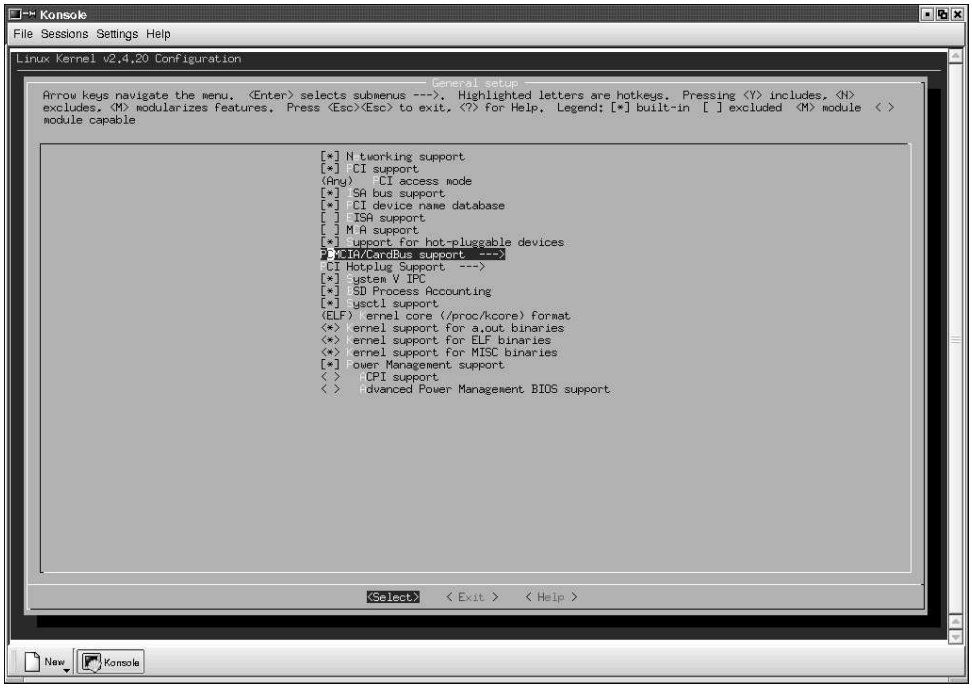
con cui ci spostiamo nella directory iniziale della sorgente del kernel;

make menuconfig

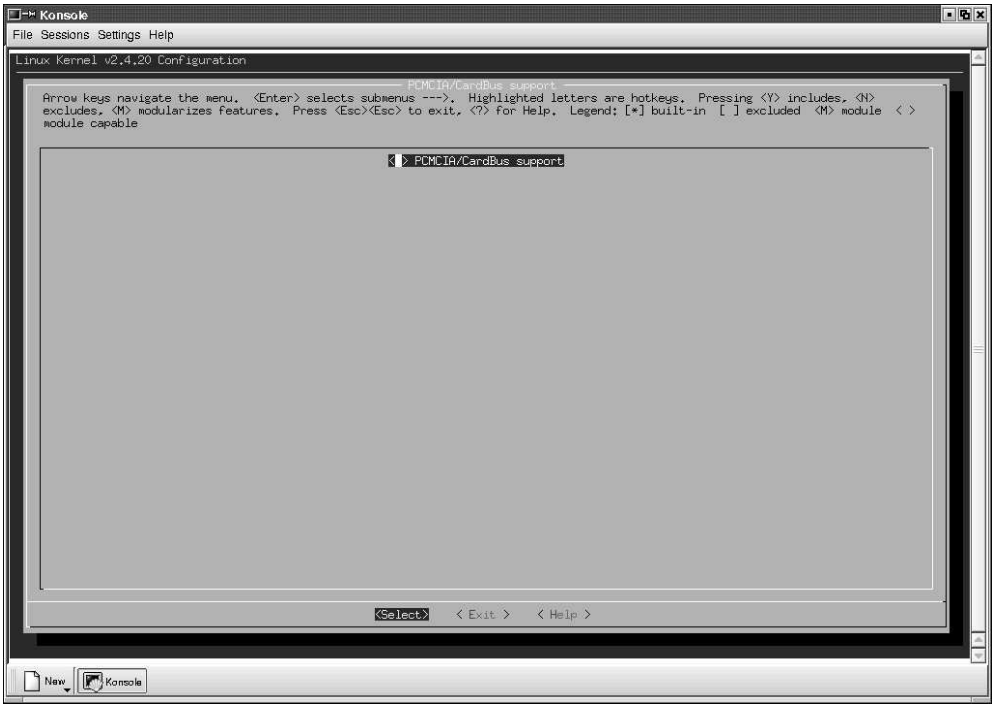
Eseguito il comando, si ottiene una schermata simile alle figure seguenti. Abbiamo quindi proceduto con la configurazione del kernel che si vuole ottenere. Nel nostro caso, volevamo configurare correttamente la scheda PCMCIA; per far questo inizialmente è stato disabilitato il supporto PCMCIA, selezionando General Setup



All'interno è apparsa la successiva schermata



Per disabilitare il supporto PCMCIA è bastato selezionare PCMCIA/CardBus support e, come si può vedere nella figura seguente, digitare il tasto n.



Fatto questo, digitando exit, usciremo dalla schermata grafica e, per eseguire la compilazione generando l'archivio Debian corrispondente nella directory precedente, basterà digitare:

make-kpkg clean

con il quale si prepara alla compilazione ed infine

make-kpkg –revision=versione Kernel_image

L'esempio seguente si riferisce alla sequenza di comandi eseguiti per compilare il kernel 2.4.20 (compresi gli eventuali moduli) collocato nella directory /usr/src/linux

 # cd /usr/src/linux
 # make menuconfig
 # make-kpkg clean
 # make-kpkg –revision=custom.1.0 kernel_image

Al termine si ottiene l'archivio kernel-image-2.4.20-custom.1.0-i386.deb, collocato nella directory precedente a quella da cui è stato ottenuto. Per installarlo è bastato procedere come segue:

 # dpkg -i ../kernel-image-2.4.20_custom.1.0_i386.deb

Successivamente il pacchetto Debian pcmcia-cs è stato scaricato, compilato e installato eseguendo il comando:

make config

make all && make install

Infine è stato installato il pacchetto wlan-ng, necessario alla maggior parte delle schede wireless. Questo pacchetto infatti contiene i moduli prism2 che permettono il riconoscimento della PCMCIA inserita.

3.9 CONFIGURAZIONE DELLA RETE

Passiamo quindi alla configurazione della nuova scheda wireless. Il file di configurazione che ci interessa è **/etc/pcmcia/wlan-ng.opts**. Le voci importanti per la nostra configurazione sono fondamentalmente due: **SSID="nome rete" CHANNEL=numero canale.** Il "nome rete" rappresenta il nome della rete wireless a cui vogliamo collegarci; deve essere lo stesso che abbiamo impostato sull' Access Point. Il "numero canale" è un numero e rappresenta il canale su cui eseguiremo le comunicazioni; anche in questo caso deve essere lo stesso impostato nel Access Point. Adesso basta verificare che il nostro modulo venga correttamente visto dal sistema nel file **/etc/modules.conf**; dovrà comparire la riga: **alias wlan0 prism2_cs**. Facendo ripartire la sezione relativa al pcmcia con il comando **/etc/init.d/pcmcia restart**, due beep ci avvisano del corretto riconoscimento della scheda PCMCIA con l'avvenuto caricamento dei moduli specifici per quella particolare scheda e dell'avvenuta configurazione della rete. La configurazione IP viene editata nel file /etc/pcmcia/network.opts come mostrata nelle figure seguenti.
Come si può notare, avevo a disposizione due schede PCMCIA. Ad una (MAC Address 00:06:25:16:C1:14) ho associato l'indirizzo della rete privata (ad-hoc), mentre l'altra (MAC Address 00:06:25:16:BF:CE) è stata utilizzata per una rete ad infrastruttura. Come possiamo vedere dalle figure, a quest'ultima scheda è stato attivato il DHCP e quindi non è necessario specificare un indirizzo perché questo viene dato direttamente dall'AP.

Un utile tool è il Wireless Extensions [8], un'estensione dell'interfaccia network di Linux. Implementata da Jean Tourrilhes, permette di configurare i devices delle WLAN in un modo standard ed uniforme e di ottenere da essi specifiche statistiche wireless. E' composta da tre parti complementari:

- interfaccia d'uso (Wireless Tools): tool capace di manipolare le Wireless Extensions;
- moduli: software che modificano il kernel di Linux per supportare e definire le estensioni;
- interfaccia hardware: implementata per ogni driver, mappa le estensioni con l'effettiva interfaccia di rete.


emacs@ala.cnuce.cnr.it
Buffers Files Tools Edit Search Mule Help
case "$ADDRESS" in
,,*,00:06:25:16:BF:CE)
INFO="Sample private network setup"
# Transceiver selection, for some cards -- see 'man ifport'
IF_PORT=""
# Use BOOTP (via /sbin/bootpc, or /sbin/pump)? [y/n]
BOOTP="n"
# Use DHCP (via /sbin/dhcpcd, /sbin/dhclient, or /sbin/pump)? [y/n]
DHCP="y"
# If you need to explicitly specify a hostname for DHCP requests
DHCP_HOSTNAME=""
# Use PPP over Ethernet (via the pppoe package)? [y/n]
PPPOE="n"
# Use WHEREAMI (via the whereami package)? [y/n]
WHEREAMI="n"
# Host's IP address, netmask, network address, broadcast address
IPADDR=""
NETMASK=""
NETWORK=""
BROADCAST=""
# Gateway address for static routing
GATEWAY=""
# Things to add to /etc/resolv.conf for this interface
DOMAIN=""
SEARCH=""
# The nameserver IP addresses specified here complement the
# nameservers already defined in /etc/resolv.conf. These nameservers
# will be added to /etc/resolv.conf automatically when the PCMCIA
# network connection is established and removed from this file when
# the connection is broken.
DNS_1=""
DNS_2=""
DNS_3=""
# NFS mounts, should be listed in /etc/fstab
MOUNTS=""
# If you need to override the interface's MTU...
MTU=""
# For IPX interfaces, the frame type and network number
IPX_FRAME=""
IPX_NETNUM=""
# Run ipmasq? [y/n] (see the Debian ipmasq package)
IPMASQ="n"
--:** network.opts (Fundamental)--L36-- 9%
Konsole
emacs@ala.cnuce.cnr.it
16 04
20/5/2003
emacs@ala.cnuce.cnr.it
Buffers Files Tools Edit Search Mule Help
IPMASQ="n"
# Extra stuff to do after setting up the interface
start_fn () { return; }
Extra stuff to do before shutting down the interface
stop_fn () { return; }
# Card eject policy options
NO_CHECK=n
NO_FUSER=n
#KEY="1808960000"
;;
#Per una configurazione Ad-hoc
,,*,00:06:25:16:C1:14)
ESSID="piolo"
MODE="Ad-hoc"
RATE="11M"
IPADDR="10.0.0.2"
NETMASK="255.255.255.0"
NETWORK="10.0.0.0"
BROADCAST="10.0.0.255"
GATEWAY="10.0.0.1"
;;
#Per una Ethernet
#*,*,*,00:40:F4:1B:C9:F4)
IPADDR="146.48.82.233
NETMASK="255.255.252.0"
NETWORK="146.48.80.0"
BROADCAST="146.48.83.255"
GATEWAY="146.48.80.1"
#DOMAIN=""
#SEARCH="isti.cnr.it cnuce.cnr.it"
DNS_1="146.48.80.130"
DNS_2="194.119.192.34"
DNS_3="146.48.127.2"
;;
esac
This tries to use Debian's network setup in /etc/network/interfaces
if no settings are given higher up in this file. You can delete it
--:** network.opts (Fundamental)--L60--57%
Konsole
emacs@ala.cnuce.cnr.it
16 05
20/5/2003

Wireless Tools, la cui sintassi generale è: comando [<interfaccia >] [<espressione>], è composta da tre comandi:

iwconfig: permette di configurare tutti i parametri wireless specifici del driver e dell'hardware. E' un clone di ifconfig, usato per la configurazione dei device standard. I parametri modificabili sono per esempio, il nome della rete, la frequenza o il canale di comunicazione, l'encryption etc. Nel caso specifico di rete 802.11 anche la soglia per attivare o meno il meccanismo di RTS/CTS è configurabile.

iwspy: serve a testare il supporto per il Mobile IP, permettendo all'utilizzatore di settare nel driver una lista di indirizzi di rete.

iwpriv: permette di settare alcuni parametri extra supportati da alcuni driver.

3.10 PROBLEMI RISCONTRATI

Oltre al problema già affrontato relativo alla ricompilazione del kernel, i problemi affrontati sono stati diversi:

1) all'inserimento della scheda PCMCIA, i relativi moduli software non venivano caricati
2) l'impossibilità di lavorare sul portatile quando era attiva la scheda wireless. Infatti, proprio per l'architettura di rete utilizzata, i pacchetti persi risultavano essere molti, dovuto al fatto che il kernel mi segnalava continuamente, quando non si era in modalità grafica, l'avvenuta perdita mediante la seguente scritta eth0: Unknown Rx error (0x3). Frame dropped

Per lettori particolarmente interessati, in Appendice D "Soluzioni", sono riportate le soluzioni adottate.