Guida per resuscitare un WRT54G con EJTAG

Autore: HairyDairyMaid (a.k.a. lightbulb) (hairydairymaid@yahoo.com)
Tradotto da: ac3bf1 (ac3rent.it - ac3bf1@gmail.com) for ninux.org (23/05/2006)

Chiarimenti:

1) Se utilizzate l'EJTAG o qualsiasi forma di JTAG, lo fato ***ESCLUSIVAMENTE A VOSTRO RISCHIO***.
2) Ne l'autore, ne la Linksys, possono essere tenuti responsabili per danni causati a qualsiasi oggetto utilizzando questa guida (includendo il router). [se volete lamentarvi con la Broadcom per non aver rilasciato le specifiche del chip siete benvenuti]
3) Queste procedure annulleranno la garanzia del WRT. (ovviamente pero se avete gia aperto il coperchio, la garanzia è scaduta).
4) Odio scrivere documentazione – quindi non chiedetemi un'altra guida.

Introduzione

Suppongo che starete leggendo questa guida perche avete un wrt da resuscitare, o perche altri modi per flashare il chip Intel non hanno funzionato fino ad ora.

Beh io sfortunatamente mi sono trovata in questa posizione... cercando di aggiornare il firmware e crashava, e non riuscivo a recuperarlo con nulla. Quindi ho pensato che non dovevo essere l'unico in questa situazione, e che ci sarebbe bisogno di un recovery utilizzando JTAG sulla flash. Ho iniziato a seguire questo progetto e ho subito scoperto che Broadcom era il peggior fabbricatore di chip nel rilasciare informazioni sui loro prodotti, a meno che si firmasse una NDA, e si giurava di non divulgare informazioni relative a Broadcom. (I loro chip sono ok – ma la loro natura "proprietaria" è terribile)

Comunque – dato che Broadcom non aveva voglia di cooperare nel rilasciare il file della Boundary Scan Definition Language (BSDL), e/o le specifiche del chip per il bcm4712, c'era solo una alternativa, ovvero EJTAG. EJTAG utilizzerebbe la stessa porta del JTAG Boundary Scan. Fortunatamente la Broadcom ah inserito il supporto per l'EJTAG 2.0 a chip bcm4712 utilizzando nel router WRT54G v2. Questo è quello che ho deciso di utilizzare. Io comunque non ho condiviso pienamente tutto quello che il EJTAG ha da offrire.

Dato il fatto che l'obiettivo di questo progetto è SOLAMENTE quello di recuperare/reflashare una cattiva flash (alcune o tutte le sue parti) o di fare copie di backup della flash (alcune o tutte le sue parti) – Ho solo scritto questa guida utilizzando il minimo indispensabile di EJTAG per parlare con la flash utilizzando delle routines DMA su EJTAG.
Detto questo andiamo avanti...

Requisiti

Per far resuscitare la flash del tuo router WRT54g v2 utilizzando EJTAG/JTAG hai bisogno solo di due cose:

1) UN cavo parallelo JTAG. Ho costruito il mio per pochissimo utilizzando pezzi di scarto. Altrimenti puoi comprarne uno chiamato “Xilinx III parallel JTAG cable” o possibilmente uno stile “Wiggler.”
2) Software per fare la comunicazione e parlare con la flash. Io ho scritto il mio che rilascio sotto la licenza GPL. (download)

Costruire il cavo JTAG

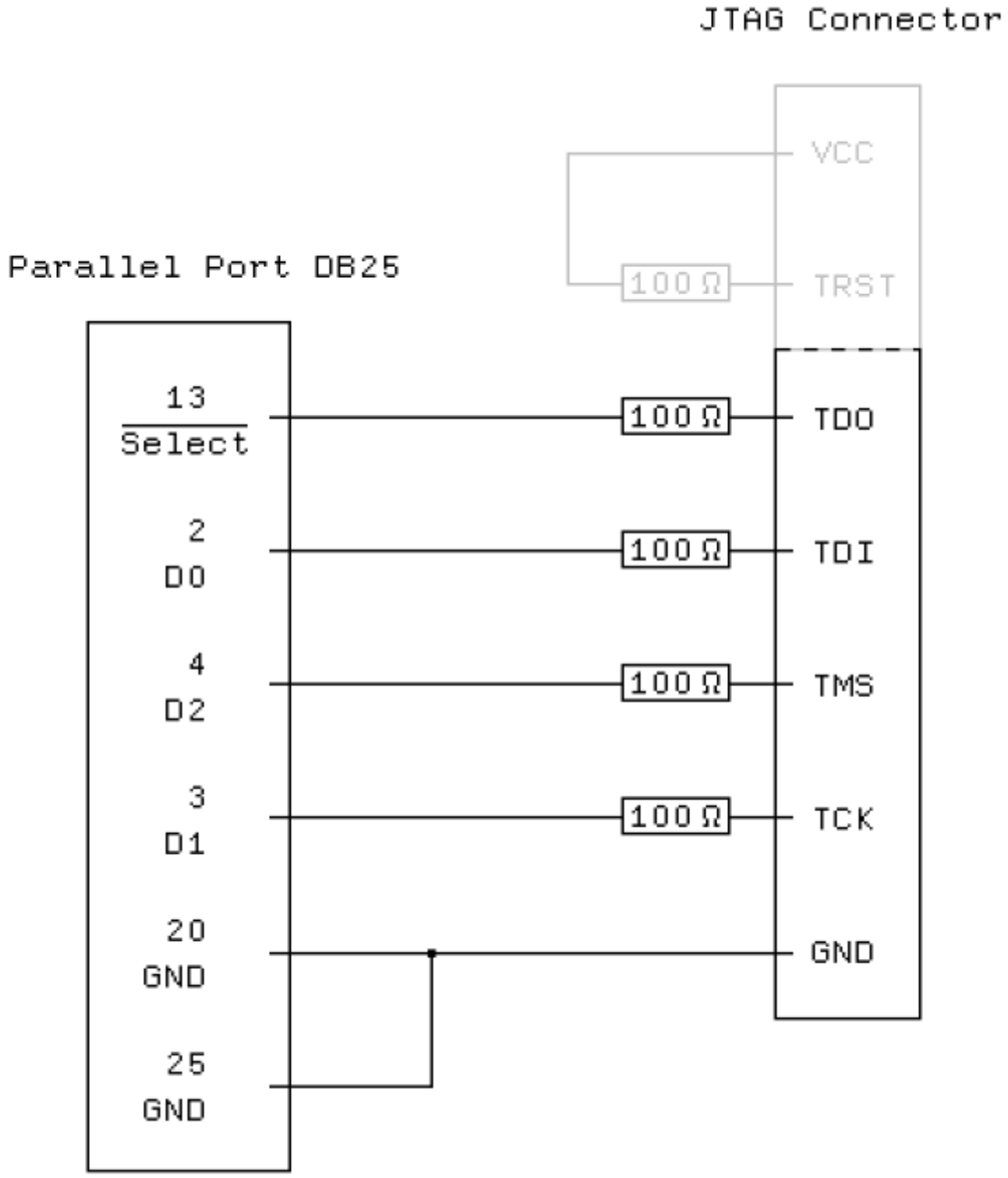
Il cavo JTAG puo essere di vari tipi; comunque, ho deciso di usare uno tipo quello della Xilinx, dato che sono molto facili da costruire, per un costo irrisorio, o nullo. Puoi comunque utilizzare un cavo JTAG di tipo Wiggler. Dato che il va Xilinx l’ho fatto da solo, questo è quello che descriverò:

<u>Parti necessarie:</u>

1) Un connettore parallelo DB25 con i pin saldabili
2) Quattro resistenze da 100-ohm
3) Un vecchio pezzo di cavo da 12 o 14 pin con un connettore ad una estremità (da una vecchia PC card) o puoi usare il cavo che vuoi e saldare le tue parti.
4) Un connettore a 12 pin maschio (da saldare sulla piastra)

Non scriverò una spiegazione molto dettagliata, dato che le foto renderanno il tutto piu semplice.

Ecco uno schema semplice per come fare il connettore parallelo e dove mappano i segnali.



Nota:

Non hai bisogno dei pin VCC e TRST sull'interfaccia: il TRST è gia incluso (?) sul WRT54G, ecco perche non c'è (il bisogno di avere) il pin TRST sulla board. Ma forse vorrai fare un cavo JTAG generico che funzioni anche con altri apparati (come ho fato io – ma non ce ne + bisogno), anche se hanno un pin TRST. Dato che questo è solo un cavo passivo, fai attenzione a non farlo troppo lungo. 75 cm hanno funzionato per me.

Mi è stato detto che questo tipo di cavo potrebbe non funzionare con tutti i tipi di porte parallele in mercato. Puoi trovare dei link a degli schemi per vari tipi di cavi sul sito JTAG-tools (link?). Comunque, il cavo passivo ha funzionato bene per me ed è probabilmente sufficiente per la maggior parte delle persone.

Sull'altro lato del cavo:

CONFIGURING THE EJTAG CONNECTION

The VisionIce JTAG connector has fourteen (14) pins whereas the EJTAG block (J10) has only twelve (12). A twelve-pin jumper block may be needed to mount the VisionIce connector onto the BCM94710AP. Note that pins 13-14 of the VisionIce adapter remain unconnected. The pinout for the EJTAG block (J10) is described in the following table.

Table 8: EJTAG Connections

J10 Pin number	*EJTAG SIGNAL*
1	JTAG_TRST_L
3	JTAG_TDI
5	JTAG_TDO
7	JTAG_TMS
9	JTAG_TCK
11	SW1 RESET[a]
2, 4, 6, 8, 10, 12	GROUND

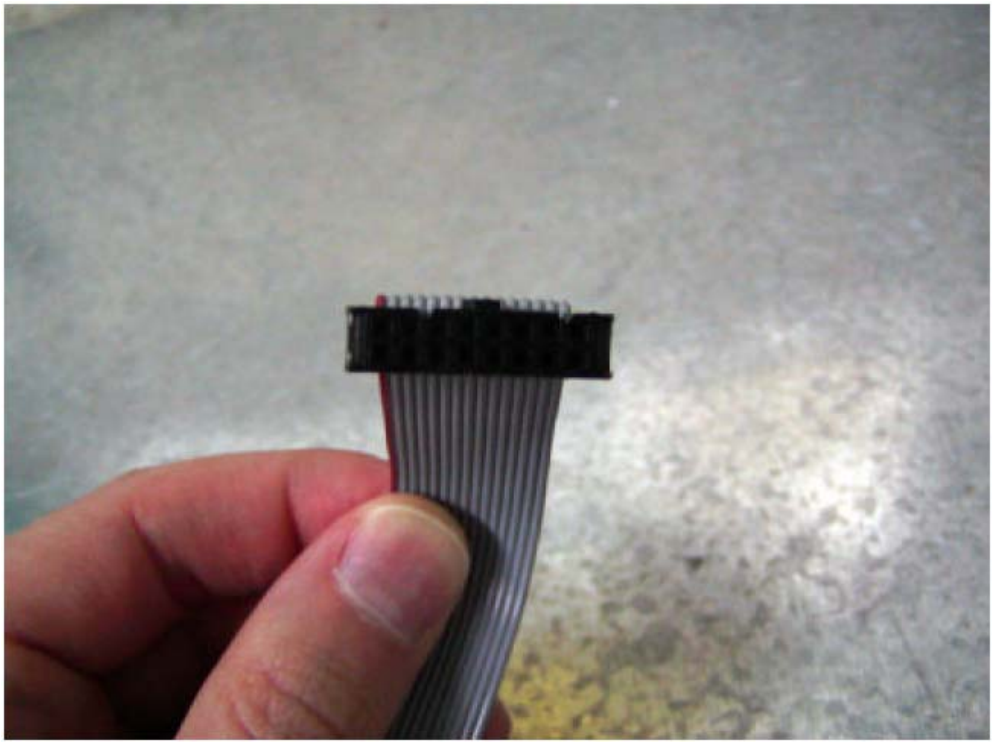
a. Pin 11 is connected to the hardware reset switch (SW1) of the BCM94710AP.

(Questo è stato preso dalla guida della Broadcom per il BCM47XX)

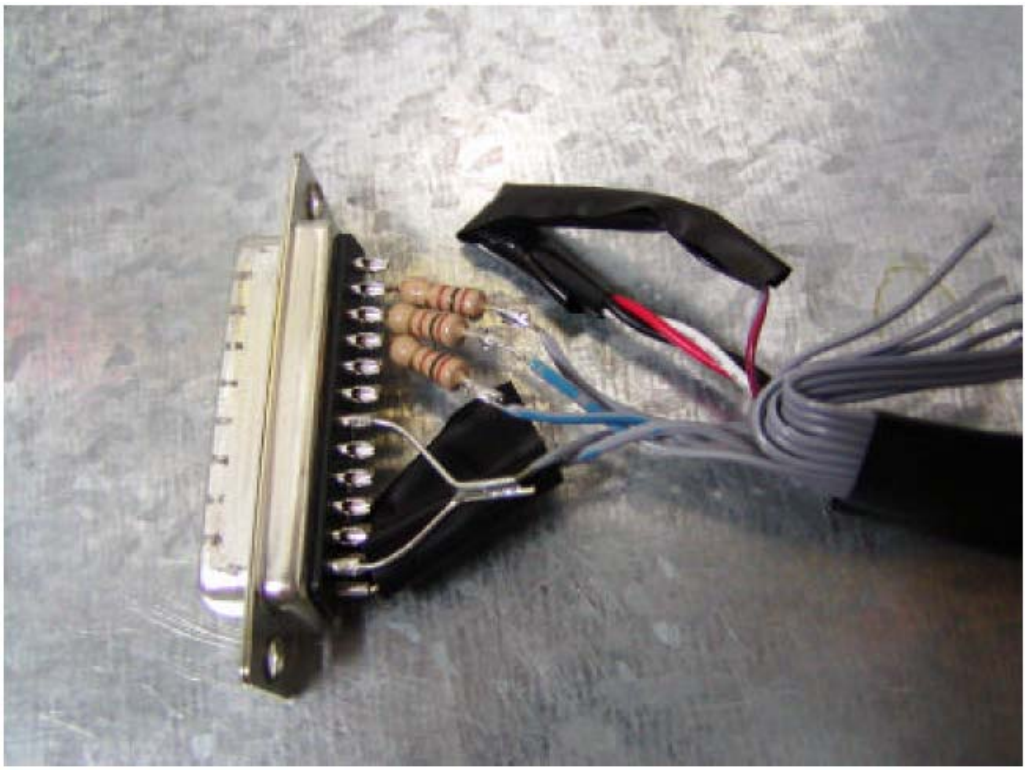
Non preoccupatevi per il collegamento del pin 1(TRST) o del pin 11 (RESET) dato che funziona anche senza di quelli. Io li ho collegati me non li ho usati per il WRT54G v2.

Ecco alcune foto del mio cavo parallelo JTAG Xilinx:

(Il cavo piccolo non è necessario)

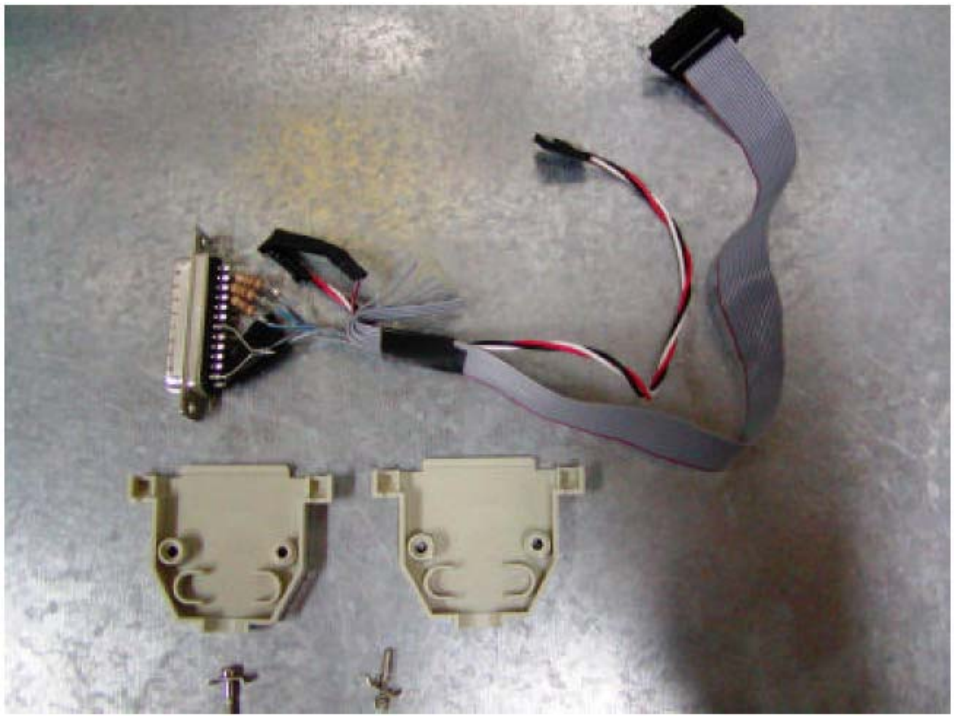


La parte del connettore JTAG (da una vecchia PC card)



La Parte del connettore DB25 (notate il modo economico con il quale ho collegato le resistenze direttamente al connettore)

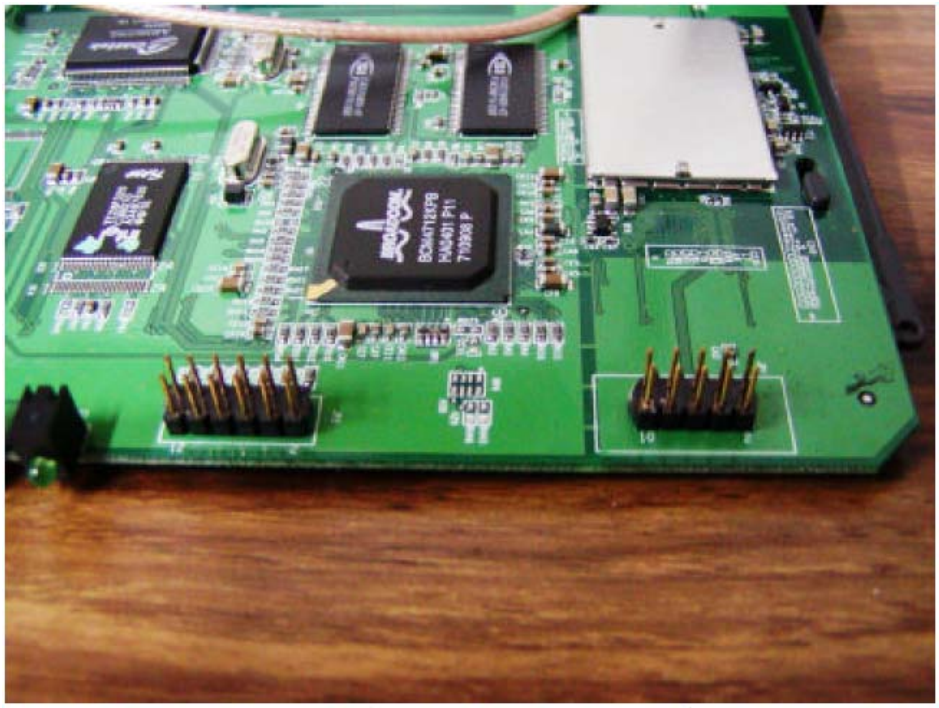
Un’altra foto (un po mossa - scusate)



Giusto prima di richiudere il connettore DB25

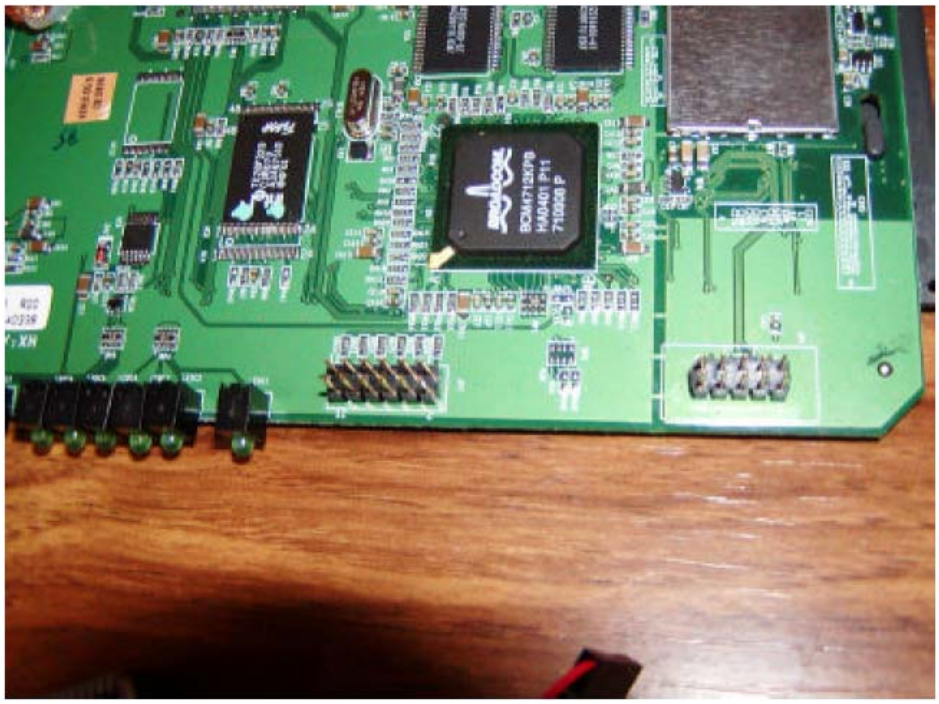
OK – questo dovrebbe bastare – (*Odio* scrivere documentazione)

Una volta che avete il cavo assemblato dovrete saldare un maschio da 12 pin sulla board del WRT54G v2. La mia board aveva i buchi delle saldature gia pieni, quindi ho dovuto dissaldarli e aspirare le saldature. Una volta fatto cio, è stato facile saldare il maschio da 12 pin al suo posto.



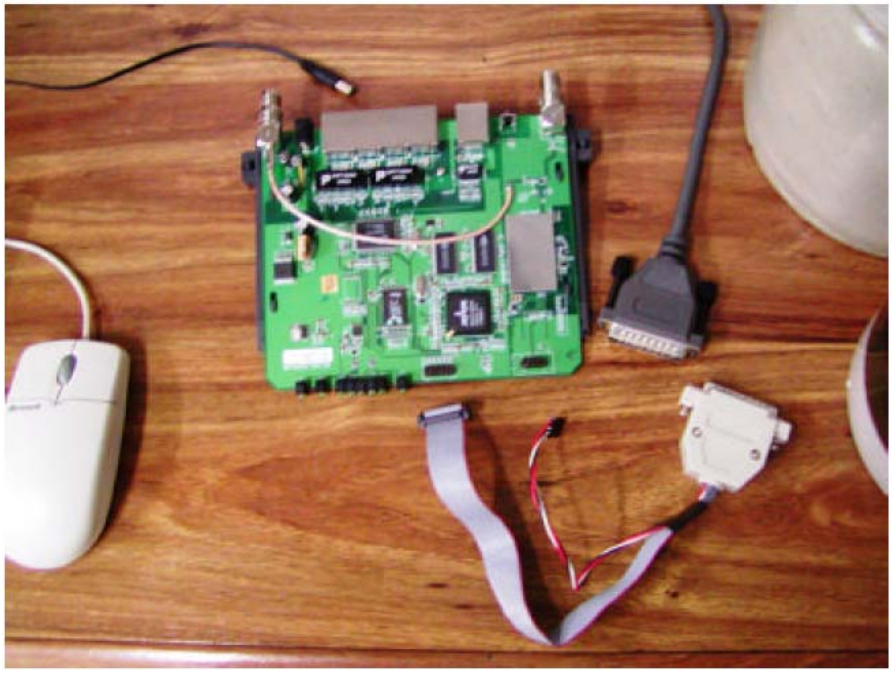
JP2 – è il connettore maschio JTAG (sinistra)

JP1 – è il maschio seriale (destra – da un altro progetto)

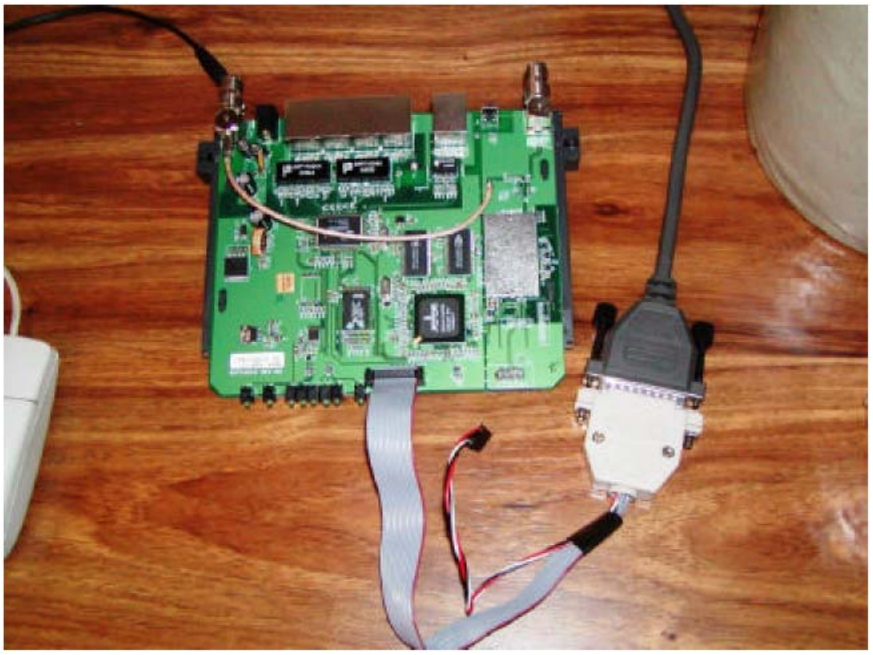


Un’altra foto del connettore JTAG saldato (sinistra)

Una volta che il cavo è stato fatto, e il connettore JTAG è saldato al suo posto, sei pronto per collegare il tutto. Ecco un paio di foto mie:



WRT54G v2 & cavo JTAG pronti all'uso



Ecco il mio cavo JTAG Xilinx collegato e pronto all'uso sul WRT54G v2 (nota: il cavo piccolo non collegato trasporta il segnale / VCC TRST che non serve sul WRT54G v2 ed è per questo che no è collegato)

Il Software

Una volta che il cavo è stato fatto (od è stato comprato) ed è pronto all'uso, allora il software + l'ultimo pezzo. Ho scritto io il mio software che parla sulla porta JTAG via lo standard EJTAG 2.0.

Una cosa da annotare è che JTAG (almeno su parallela) è abbastanza lento. Questa è una cosa molto importante da ricordare dato che potrebbe impiegarci molto tempo per flashare l'intero chip in una volta o addirittura l'immagine del kernel. Suggerisco di flashare la CFE (come si voglia) e la NVRAM, poi utilizzate il normale metodo tftp su ethernet per recuperare/riflashare un'altra immagine del kernel.

Ci sono due file sorgenti inclusi (qui e qui) scritti per essere compilati sotto linux:

- wrt54g.c
- wrt54g.h

Compila questi come compileresti qualsisi altro file sorgente sotto linux. Ho anche incluso un semplice makefile (qui). Una volta che questo è fatto, sei quasi pronto per utilizzare il software.

<u>Un paio di cose prima:</u>

1) Sii certo che la porta parallela sia "accessibile" – dai il comando "rmmod lp" se necessario.
2) Collega sempre il cavo alla parallela del pc e alla board del WRT PRIMA di alimentare il WRT
3) Sii furbo – fai un backup prima di flashare o eliminare qualsiasi cosa. (Non venire a piangere se non lo fai)
4) Di nuovo – flashare su parallela è un processo lento – (si molto piu lento che su ethernet) – non diventare impaziente.

Per eseguire il software scrivi:

`./wrt54g` <enter>

E vedrai quanto segue:

```
wrt54g: read/write flash memory via EJTAG
usage: wrt54g [option]
     -backup:cfe
     -backup:nvram
     -backup:kernel
     -backup:wholeflash
     -erase:cfe
     -erase:nvram
     -erase:kernel
     -erase:wholeflash
     -flash:cfe
     -flash:nvram
     -flash:kernel
     -flash:wholeflash
```

Queste sono le opzioni con le quali puoi far girare il programma. Facendo partire il programma con qualsisi delle opzioni lo farà eseguire immediatamente, e lo farà eseguire fino al completamento (quindi attento all'opzione scelta!)

Un paio di note:

- Fare il backup del Kernel o della WholeFlash impiegherà molto tempo (gia ho menzionato cio – no?)
- L'immagine da flashare deve risiedere nella stessa directory del programma
- L'immagine da flashare deve essere chiamata in uno dei seguenti modi: CFE.BIN, NVRAM.BIN, KERNEL.BIN, WHOLEFLASH.BIN
- Ogni volta che si esegue un backup l'immagine verrà salvata con uno di questi nomi: CFE.BIN.SAVED, NVRAM.BIN.SAVED, KERNEL.BIN.SAVED, WHOLEFLASH.BIN.SAVED
- Ogni volta che flashate una porzione della flash con questa utility, l'utility prima farà un erase di di quella parte della flash
- Eseguire un comando per flashare, NON farà automaticamente i backup di cio che è dentro la destinazione. E' compito tuo fare prima i backup.

Prendi il tempo per fare i backup di ogni sezione prima di fare qualsiasi altra cosa. Questa è una cosa intelligente da fare in caso si peggiori la situazione dopo; e magari ti conviene salvare quei backup in un posto sicuro. Credo che se mi ricordo bene, l'immagine CFE.BIN.SAVED (la porzione della CGE nella flash) contenga il MAC Address SPECIFICO del router.

OK – ora che avete visto le opzioni che bisogna conoscere, manca una cosa prima di eseguire il programma...

Devi scrivere il comando richiesto per intero e giusto prima di dare l'invio, collegare l'alimentazione al WRT54G. In altre parole prepara e collega il JTAG al pc e al router con l'alimentazione del router SCOLLEGATA, poi scrivi il comando desiderato, collega l'alimentazione al router e dai l'invio. Il comando dovrebbe inziare a lavorare e si potrà vedere il progresso sullo schermo.

***** NOTA IMPORTANTE *****

Ogni volta che rieseguite il programma, seguite le indicazioni sopra riportate – è importante dato che il WRT54G v2 ha un Watchdog Timer al suo interno che resetterà tutto in un momento inappropriato se non puo essere disabilitato dal software.

Un ultimo commento – se eliminate la NVRAM – molte volte è quanto basta per sbloccare (?) la flash; provate questo prima. Inoltre – se la CFE e il KERNEL sono intatti allora caricherà(?) una copia refreshata della NVRAM nel suo spazio una volta svuotato (al prossimo avvio).

E' un'ottima idea riavviare l'unità durante le operazioni (backup/eliminazione/flash) e svolgere i passi menzionati prima velocemente dopo aver collegato l'alimentazione al router.

OK – ne ho abbastanza di scrivere documentazione – quindi spero che sia stata utile! In bocca al lupo nel resuscitare il vostro router WRT54G v2.

Divertitevi!
- hairydairymaid (a.k.a. lightbulb)