Cambio firmware su Fonera FON2100 fw 0.7.2 r3 (ottobre 2009)

La sostituzione del firmware del fonera non riguarda la sostituzione di un solo file,
ma sono coinvolti una serie di operazioni, e per chi non conosce l'ambiente Linux
avrà maggiori difficoltà, in quanto il fonera è un mini sistema operativo somigliante a Linux,
difatti all'interno sono presenti delle cartelle nello stile Linux, 4 sono gli stadi da superare:

1) downgrade del firmware se superiore al 0.7.1 r1
2) accesso al fonera con putty_ssh, e modifiche ad alcuni file
3) Abilitazione RedBoot: caricare una versione modificata del kernel compatibile con il firmware della Fonera che permetta la scrittura nella partizione che contiene la configurazione di RedBoot,
per poi caricare una configurazione di RedBoot che ci permetta di collegarci via telnet.
4) Flashare la fonera con DD-WRT tramite l'utility Access Point-51

File necessari

fonera_0.7.1.1.fon (1,980 KB - firmware)
due file htm con il codice descritto nella parte 2
putty_ssh.exe (444 KB - programma)
hfs.exe (560 KB - programma)
openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma (512 KB - kernel compatibile)
WinPcap_4_0_2.exe (538 KB – librerie x ap51)
ap51-flash-fonera-gui-1.0-42.exe (3,796 KB - programma)
root.fs (2,748 KB - fw)
vmlinux.bin.l7 (768 KB - fw)

....1)

Per facilitare il cambio di fw è necessario riportare il fonera al firmware 0.7.1 r1
Ci sono due vie possibili.
Provare con reset, o scaricare fw e caricarlo direttamente da fonera.

- Reset. E' il metodo più semplice:
  disconnettere La Fonera da Internet (cavo Ethernet)
  premere e tener premuto il pulsante di reset (posto sotto il router)
  per più di 15 secondi
  riavviare il router scollegando e ricollegando l'alimentazione
  connettersi all'interfaccia http della Fonera senza connettere La Fonera stessa ad Internet (si può fare via wireless o con un cavo crossed utilizzando sul PC l'indirizzo 169.254.255.2/24 per trovare La Fonera all'indirizzo http://169.254.255.1/) e verificare che il firmware sia quello giusto (7.1.1).
- Downgrade via http.
  disconnettere La Fonera da Internet (cavo Ethernet)
  scaricare sul PC il firmware 7.1.1, fonera_0.7.1.1.fon
  collegarsi alla Fonera via wireless oppure con cavo cross (169.254.255.2/24 sul PC, Fonera all'indirizzo 169.254.255.1)
  aprire l'interfaccia di amministrazione della Fonera, andare in firmware upgrade e caricare il firmware 7.1.1
  molto probabilmente il router non accetterà il downgrade a 7.1.1 dandovi il seguente output (messaggio di errore),
- …. Ma, nonostante questo errore, il firmware dovrebbe essere installato,
  riavviare La Fonera e controllare che sia così

....2)

Riusciti a riportare il fw al 0.7.1.1 bisogna accedere all'interno del fonera per cambiare delle impostazioni,
per questo passaggio bisogna sbloccare le porte ssh e accedere con il client SSH sull'indirizzo del fonera
Per sboccare ssh creare un file html (ad es. primo.html) sul PC con il contenuto seguente:
(Controllare che l'indirizzo IP coincida con quello del fonera)

- <html>
- <head></head><body>
- <form method="post" action="http://169.254.255.1/cgi-bin/webif/
- connection.sh" enctype="multipart/form-data">
- <input name="username" value="$(/usr/sbin/iptables -I INPUT 1 -p tcp
- --dport 22 -j ACCEPT)" size="68" />
- <input type="submit" name="submit" value="Submit" />
- </form>
- </body></html>

creare un'altro file html (ad es. secondo.html) con il contenuto seguente:

- <html>
- <head></head><body>
- <form method="post" action="http://169.254.255.1/cgi-bin/webif/
- connection.sh" enctype="multipart/form-data">

- <input name="username" value="$(/etc/init.d/dropbear)" size="68"
- ><input type="submit" name="submit" value="Submit" />
- </form>
- </body></html>

aprire il primo file html, cliccare su "Submit", verranno chieste le credenziali di accesso alla Fonera, inserirle (se non le si è modificate sono username admin, password admin)
aprire il secondo file html, cliccare su "Submit", verranno chieste le credenziali di accesso alla Fonera, inserirle
in questo modo, tramite il post dei due form contenuti nei file html abbiamo iniettato i comandi

- /usr/sbin/iptables -I INPUT 1 -p tcp --dport 22 -j ACCEPT
- /etc/init.d/dropbear

per, rispettivamente, aprire la porta 22 (SSH) nel firewall della Fonera e lanciare il daemon SSH (Dropbear)

Avviare il programma "putty_ssh.exe" di 444 KB (client SSH)
sull'indirizzo della Fonera 169.254.255.1 (se è questo)
loggarsi come root, stessa password di prima
dare il comando

- mv /etc/init.d/dropbear /etc/init.d/S50dropbear

il daemon SSH ora partirà automaticamente all'avvio.

dare

- vi /etc/firewall.user

e editare il file /etc/firewall.user che contiene le regole che il firewall carica all'avvio, trovare le linee

- # iptables -t nat -A prerouting_rule -i $WAN -p tcp –dport 22 -j ACCEPT
- # iptables -A input_rule -i $WAN -p tcp –dport 22 -j ACCEPT

e decommentarle togliendo il "#" e lo spazio
Per salvare tutto, premete sulla tastiera "shift" e il tasto ":" e poi scrivete "wq" confermate con invio

....3)

Abilitazione RedBoot:
Entrare nella modalità RedBoot ci darà la possibilità di inviare in remoto dei comandi a La fonera, come se avessimo una tastiera collegata direttamente col nostro dispositivo.

- Apriamo il programma HFS (560 KB), cliccate col tasto destro sull'icona con la casa, e dal menù contestuale scegliete AddFiles…, selezionate i file openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma e out.hex.
- Nella barra degli indirizzi, impostate l'IP 169.254.255.2 e la porta 80, come da immagine: (controllare nome file, e indirizzo ip)

Aprite Putty, selezionate SSH, nel campo Hostname scrivetel'IP 169.254.255.1 (controllare) e poi cliccate su Open. Si aprirà, dopo qualche secondo, una finestra con un messaggio che vi avvisa del pericolo in cui incorrete nel proseguire, cliccate su yes.
Dopo aver cliccato verrà aperta un ulteriore finestra uguale in tutto e per tutto ad una shell linux, inserite come nome utente root e come password admin, una volta loggati avrete la possibilità di digitare i comandi per dialogare direttamentecon la Fonera.
La prima cosa da fare e abilitare permanentemente la connessione SSH, per fare ciò copiamo ed incolliamo nel terminale il comando:

- mv /etc/init.d/dropbear/ etc/init.d/S50dropbear

Fatto ciò digitiamo il comando per scaricare ed installare, dentro la memoria de La Fonera, il file openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma, aggiunto precedentemente attraverso il programma HFS, ed il comando per il riavvio del dispositivo:

- cd /tmp
- wget http://169.254.255.2/openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma
- mtd-e vmlinux.bin.l7 write openwrt-ar531x-2.4-vmlinux-CAMICIA.lzma vmlinux.bin.l7 (controllare nomi file)

....4)

http://www.nabuk.org/f/index.php?topic=1075.0

- Flashare la fonera con DD-WRT tramite l'utility Access Point-51 senza errori!

Ciao a tutti leggendo qua è la nei vari forum ho trovato una guida per flashare la fonera con il firmware AP-51 senza che si verifichi il blocco su Creating nvram problema che si verifica sulla fonera modello 2200,
questa procedura e valida anche per ripristinare fonere brikkate:
1) Scaricate questo pacchetto che contiene l'utility AP-51, i file del firmware versione RC6 e l'utility WinPcap:http://rapidshare.com/files/95640845/pack.zip.html
2) se non l'avete gia fatto in precedenza installate Wincap e riavviate il pc
3) Disattivate eventuali antivirus e firewall impostate la scheda di rete per ottenere automaticamente l'indirizzo IP (DHCP) e disattivate tutti i protocolli lasciando solo TCP/IP nelle proprieta della scheda di rete.

4) Staccate l'alimentazione dalla fonera e collegatela al pc con il cavo fornito in dotazione.
5) Aprite AP-51 e caricate i due file del firmware root.fs e vmlinux.bin.l7, spuntate l'opzione "create nvram partition" e selezionate la vostra scheda di rete dal menu a discesa
6) Premete il pulsante GO e attendete fino a quando non vedrete la scritta "No packet"
7) Premete il pulsante reset sulla fonere e collegate l'alimentazione continuando a premerlo
8) Aspettate 5 secondi e lasciate il pulsante reset
9) Attendete senza fare nulla che il processo sia terminato a questo punto la fonera si riavviera automaticamente e assegnera un indirizzo IP al vostro PC
10) Attendete che tutti i led si siano accesi e accedete alla fonera sull'indirizzo
(l'operazione dura diversi minuti, sui 20. con processore al 100%)

Link consultati
http://www.ninux.org/LaFoneraDallaScatolaAOpenWrt
http://marcopulvirenti.wordpress.com/2009/05/19/installare-firmware-dd-wrt-su-la-fonera/
http://www.wifi-ita.com/index.php?option=com_content&task=view&id=143&Itemid
http://www.napoliwireless.net/doku/doku.php?id=hack:fonera
http://www.wifi-ita.com/index.php?option=com_content&task=view&id=168&Itemid=51

su nabuk
http://www.nabuk.org/f/index.php?topic=1075.15

Fon2201 è un testa dura?
http://www.nabuk.org/f/index.php?topic=2590.msg24057

Ho comperato un fonera, speravo mi arrivasse qualcosa già ben conosciuto, è arrivato un Fon 2201A.
Ho iniziato a documentarmi, ma mi pare di aver capito di avere a che fare con un testa dura.
Ho provato un po di reset consigliati ma è rimasto al Firmware Version: 1.1.1 r2, di scendere alla 0.ecc. niente.

La precedente esperienza con il Fon 2100A dopo qualche mese sono riuscito a portarla a termine,
abituato e fossilizzato al D-Link 900 usato come client, passare al Fonera (client) con DD-WRT è un'altro pianeta.

Vi chiedo: Mettere il DD-WRT sul Fon 2201 (senza seriale) è più difficile del 2100?
Forse ho sbagliato acquisto?
In quale access point è più facile mettere il DD-WRT, e che non ha prestazioni inferiori al Fonera?

Ritiro quanto detto prima
E' stato molto facile

spunti presi da
http://www.gbcnet.net/showthread.php?4006-La-Fonera-2201-Plus-FonSpot-2200-2100-aggiornamento-firmware-facile-e-veloce.
http://finallevel.forumcommunity.net/?t=19572554
ovvero.

Scaricare e decomprimete in una cartella l'AP-51, i file del firmware (root.fs e vmlinux.bin.l7) e l'utility WinPcap:
Installate ora Wincap e poi riavviate il pc
Deselezionate tutti i protocolli meno che il TCP/IP e nelle proprieta della scheda di rete del pc scrivete :
192.168.1.2
255.255.255.0
192.168.1.1

Fare una verifica.
http://www.hwupgrade.it/forum/showpost.php?p=30160703&postcount=508
Aprire una finestra dos (windows) con il comando "cmd"
digitare il comando ping 192.168.1.1 -t
alimentare il fonera e avviare il comando ping
Il tempo per il quale è attiva questa risposta di difault è di 2 sec
Procedura utile per avere la conferma che il fonera è raggiungibile
Fine verifica.

Connettere SOLO con il cavo di rete la fonera al pc
Lanciate AP-51 e caricate i due file del firmware root.fs e vmlinux.bin.l7, selezionate l'opzione "create nvram partition"

e anche la vostra scheda di rete (menu a tendina)

Ciccate sul tasto GO e aspettate la comparsa della scritta "No packet"

Premete e tenete premuto il pulsantino reset del fonera (sta nel retro ed è di colore rosso) e alimentatelo

Passati circa 10 secondi rilasciate il tastino reset

Inizia ora la scrittura sul fonera

Aspettate che finisca e il 2201 avrà il riavvio in automatico e assegnera un indirizzo ip al pc

Infine quando vedete che tutti i led sono accesi potete entrare nel fonera x la configurazione
che fa per voi tramite l'indirizzo 192.168.1.1