ROOT TIM HUB DGA4132 E GUI ANSUEL - VERSIONE AGTHP 2.3.3

La presente guida è stata concepita per avere un punto di riferimento semplice e immediato in caso si voglia procedere con l'abilitazione dell'utenza root del modem router TIM HUB DGA4132 (di seguito "router") e della successiva installazione della GUI Ansuel. Tutti i passaggi sono stati presi e adattati dai siti web riportati nel paragrafo sottostante, successivamente raggruppati in questa pagina e impostati nell'ordine corretto.

Questa guida è disponibile nei seguenti formati:

- Markdown (`TIM_HUB_guide_IT.md`)
- PDF (`TIM_HUB_guide_IT.pdf`)
- HTML (`TIM_HUB_guide_IT.html`)

SITI WEB

- Hacking Technicolor Gateways: Material for MkDocs
- IlPuntoTecnico GUI Ansuel
- GitHub GUI Ansuel
- GitHub AutoFlashGUI
- WinSCP

FILE UTILI

Il file `autoflashgui-master_timhub.zip` contiene la versione `16.02.2018` del tool AutoFlashGUI sviluppato da Mark Smith (mswhirl). Una volta estratto, all'interno della cartella *autoflashgui-master/firmware* è possibile trovare i seguenti file necessari a questa guida:

- `AGTHP_1.0.3_CLOSED.rbi.torrent`: file torrent per avviare il download della versione AGTHP 1.0.3 del firmware scaricato dal sito web "Hacking Technicolor Gateways: Material for MkDocs". Una volta completato il download, spostare il file nella cartella *autoflashgui-master/firmware*
- `AGTHP_2.3.3_CLOSED.rbi.torrent`: file torrent per avviare il download della versione AGTHP 2.3.3 del firmware scaricato dal sito web "Hacking Technicolor Gateways: Material for MkDocs". Una volta completato il download, spostare il file nella cartella *autoflashgui-master/firmware*
- `GUI.tar.bz2`: versione stabile 9.6.65 della GUI Ansuel scaricata dalla repository GitHub `gui-dev-build-auto` di Ansuel. Per favore, controllare la presenza di nuove versioni prima di procedere

---

GUIDA - PARTE 1

- Aggiornare il router alla versione 2.3.3 (è possibile effettuare questa operazione tramite l'applicazione per smartphone "TIM Modem" disponibile per Android e iOS)
- Dalla prima scheda *Gateway* nella GUI web, se necessario, eseguire backup configurazione in `.bin` tramite il pulsante *Esporta*. Verrà scaricato un file denominato "config.bin"
- Eseguire reset router tramite il pulsante *Ripristina*
- Al riavvio, login nella pagina web (`admin/admin`), non cambiare la password e attivare la modalità *Configurazione estesa*

> ATTENZIONE: Per abilitare la Configurazione estesa è necessario cliccare su una scheda che compare SOLO al primo login subito dopo un reset. Se si esegue il logout dalla GUI web o si chiude la finestra del browser, sarà necessario procedere con un ulteriore reset del router per ottenere nuovamente il prompt Configurazione estesa. Inoltre, il router NON deve essere in alcun modo collegato a Internet: scollegare quindi il cavo RJ11, il cavo Ethernet nella porta WAN oppure la connessione in FTTH.

- Per rifare il login nella GUI, la password è la **ACCESS KEY** sull'etichetta posta alla base del router (sotto l'ultimo codice a barre nella colonna a sinistra)
- Entrare nella prima scheda *Gateway* ed eseguire dalla terza tab il downgrade alla versione 1.0.3. Per fare ciò, caricare il file `AGTHP_1.0.3_CLOSED.rbi` cliccando su *Scegli il file* e poi su *Aggiorna* nella sezione *Aggiornamento firmware*
- Al riavvio, non sarà possibile fare il login. Eseguire reset router dal tasto sul retro (tenere premuto per **10-12 sec.**)
- Al secondo riavvio, login nella pagina web (`admin/admin`) senza cambiare la password
- Eseguire il programma `autoflashgui.exe` contenuto nella cartella *autoflashgui-master*

AUTOFLASHGUI.EXE

Impostare i seguenti parametri con i rispettivi valori

- Load default: *Generic (Advanced DDNS)*
- Target IP: ip router
- Username: user GUI web
- Password: password GUI web
- **NON** selezionare *Firmware File Name* e la spunta *Flash firmware?*
- Attivare *Split the given command on semicolons [...]* se non selezionato
- Lasciare invariato il resto delle impostazioni
- Cliccare su *Run*
- Attendere risultato sulla shell
- Chiudere il programma (non sarà più necessario)
- Collegarsi in SSH al router e provare ad autenticarsi con `root/root`

GUIDA - PARTE 2

- Dalla shell root del router abilitare la Serial Console Port
  - `sed -i -e 's/#//' -e 's#askconsole:.*\$#askconsole:/bin/ash#' /etc/inittab`
- Verificare lo stato delle bank
  - `find /proc/banktable -type f -print -exec cat {} ';' -exec echo ';'`
- Prendere nota dei seguenti parametri

```
...
/proc/banktable/booted
<take note of this>
proc/banktable/active
```

```
<take note of this>
...
```

- Per raggiungere il nostro scopo, è necessario che il risultato del comando precedente diventi come segue

```
/proc/banktable/active
bank_1
/proc/banktable/activeversion
Unknown
/proc/banktable/booted
bank_2
```

- Proseguire quindi al passaggio successivo per impostare come active il `bank_1` per poi cancellarlo e fare in modo che vada in boot il `bank_2`

SCRIPT

- Creare con il comando `vim` uno script con i seguenti comandi

```
# Ensure two banks match in sizes
[ $(grep -c bank_ /proc/mtd) = 2 ] && \
[ "$(grep bank_1 /proc/mtd | cut -d' ' -f2)" = \
"$(grep bank_2 /proc/mtd | cut -d' ' -f2)" ] && {
# Clone and verify firmware into bank_2 if applicable
[ "$(cat /proc/banktable/booted)" = "bank_1" ] && {
mtd -e bank_2 write /dev/$(grep bank_1 /proc/mtd | cut -d: -f1) bank_2 && \
mtd verify /dev/$(grep bank_1 /proc/mtd | cut -d: -f1) bank_2 || \
{ echo Clone verification failed, retry; exit; } }
# Make a temp copy of overlay for booted firmware
cp -rf /overlay/$(cat /proc/banktable/booted) /tmp/bank_overlay_backup
# Clean up jffs2 space by removing existing old overlays
rm -rf /overlay/*
# Use the previously made temp copy as overlay for bank_2
cp -rf /tmp/bank_overlay_backup /overlay/bank_2
# Activate bank_1
echo bank_1 > /proc/banktable/active
# Make sure above changes get written to flash
sync
# Erase firmware in bank_1
mtd erase bank_1;
# Emulate system crash to hard reboot
echo c > /proc/sysrq-trigger; }
# end
```

- Lanciare il seguente comando per renderlo eseguibile
    - `chmod +x script.sh`

- Eseguire lo script appena creato
  - `./script.sh`

GUIDA - PARTE 3

- Adesso è possibile proseguire con l'upgrade del firmware per tornare alla versione 2.3.3
- Aprire WinSCP (o software simile) e collegarsi con protocollo SCP al router con credenziali `root/root`
- Caricare nella directory `/tmp` del router il file `AGTHP_2.3.3_CLOSED.rbi` rinominandolo in `new.rbi`
- Eseguire da shell il seguente comando
  - `cat "/tmp/new.rbi" | (bli_parser && echo "Please wait..." && (bli_unseal | dd bs=4 skip=1 seek=1 of="/tmp/new.bin"))`
- E' necessario procedere con un clean-up di file e configurazioni
- Creare un backup con il seguente comando e salvarlo sul proprio PC tramite WinSCP
  - `tar -C /overlay -cz -f /tmp/backup-$(date -I).tar.gz $(cat /proc/banktable/booted)`
- Eseguire il comando seguente per cancellare completamente l'overlay della bank attualmente bootata
  - `rm -rf /overlay/$(cat /proc/banktable/booted)`
- Cambiando versione del firmware il root potrebbe andare perso. NON riavviare e procedere quindi con il passaggio successivo

PRESERVARE ACCESSO ROOT

- Eseguire tramite SSH il blocco di comandi seguente per preparare uno script che andrà eseguito una volta sola al boot successivo per garantire l'accesso con root

> COPIA E INCOLLA NEL TERMINALE. PREMERE INVIO PER ESEGUIRE L'ULTIMO COMANDO.

```
mkdir -p /overlay/$(cat /proc/banktable/booted)/etc
chmod 755 /overlay/$(cat /proc/banktable/booted) /overlay/$(cat
/proc/banktable/booted)/etc
echo -e "echo root:root | chpasswd
sed -i 's#/root:.*\$#/root:/bin/ash#' /etc/passwd
sed -i -e 's/#//' -e 's#askconsole:.*\$#askconsole:/bin/ash#' /etc/inittab
uci -q set \$(uci show firewall | grep -m 1 \$(fw3 -q print | \
egrep 'iptables -t filter -A zone_lan_input -p tcp -m tcp --dport 22 -m comment --
comment \"!fw3: .+\" -j DROP' | \
sed -n -e 's/^iptables.\+fw3: \(.\+\)\".\+/\1/p') | \
sed -n -e \"s/\(.\+\).name='.\+'$/\1/p\").target='ACCEPT'
uci add dropbear dropbear
uci rename dropbear.@dropbear[-1]=afg
uci set dropbear.afg.enable='1'
uci set dropbear.afg.Interface='lan'
uci set dropbear.afg.Port='22'
uci set dropbear.afg.IdleTimeout='600'
uci set dropbear.afg.PasswordAuth='on'
uci set dropbear.afg.RootPasswordAuth='on'
uci set dropbear.afg.RootLogin='1'
uci set dropbear.lan.enable='0'
uci commit dropbear
```

```
/etc/init.d/dropbear enable
/etc/init.d/dropbear restart
rm /overlay/\$(cat /proc/banktable/booted)/etc/rc.local
source /rom/etc/rc.local
" > /overlay/$(cat /proc/banktable/booted)/etc/rc.local
chmod +x /overlay/$(cat /proc/banktable/booted)/etc/rc.local
sync
```

- Se la password di root è stata cambiata, questa verrà resettata a `root/root`
- Il gateway adesso è pulito. L'accesso con root tramite SSH verrà abilitato di nuovo permanentemente al boot successivo

FLASHING DEL FIRMWARE

- Eseguire uno alla volta i seguenti comandi per scrivere il file `/tmp/new.bin` nella bank booted e per provocare un hard reboot
  - `mtd -e $(cat /proc/banktable/booted) write "/tmp/new.bin" $(cat /proc/banktable/booted)`
  - `echo c > /proc/sysrq-trigger`

CONSOLIDARE L'ACCESSO OTTENUTO

- Eseguire i seguenti comandi nel terminale SSH per prevenire che il router perda inaspettatamente la possibilità di accesso con root

> COPIA E INCOLLA NEL TERMINALE. PREMERE INVIO PER ESEGUIRE L'ULTIMO COMANDO.

```
# Disable CWMP
uci delete cwmpd.cwmpd_config
uci delete firewall.cwmpd
uci del_list watchdog.@watchdog[0].pidfile='/var/run/cwmpd.pid'
uci del_list watchdog.@watchdog[0].pidfile='/var/run/cwmpevents.pid'
uci commit
/etc/init.d/watchdog-tch reload
/etc/init.d/cwmpd disable
/etc/init.d/cwmpd stop
/etc/init.d/cwmpdboot disable
/etc/init.d/cwmpdboot stop
/etc/init.d/zkernelpanic disable
/etc/init.d/zkernelpanic stop

# Disable CWMP - extra, in case you think it may resurrect
uci set cwmpd.cwmpd_config.state=0
uci set cwmpd.cwmpd_config.acs_url='https://127.0.1.1:7547/'
uci set cwmpd.cwmpd_config.use_dhcp=0
uci set cwmpd.cwmpd_config.interface=loopback
uci set cwmpd.cwmpd_config.enforce_https=1
uci commit cwmpd

# Disable Telstra monitoring
```

```
uci delete tls-vsparc.Config
uci delete tls-vsparc.Passive
uci delete autoreset.vsparc_enabled
uci delete autoreset.thor_enabled
uci delete wifi_doctor_agent.acs
uci delete wifi_doctor_agent.config
uci delete wifi_doctor_agent.as_config
uci commit

# Disable Telstra Air/Fon WiFi
/etc/init.d/hotspotd stop
/etc/init.d/hotspotd disable
uci delete dhcp.hotspot
uci delete dhcp.fonopen
uci commit

# Remove any default SSH pubkey
echo > /etc/dropbear/authorized_keys
# Disable SSH access over wan
uci set dropbear.wan.enable='0'
uci commit dropbear

# Free space for gateways with small flash
find /rom/usr/lib/ipk -type f |xargs -n1 basename | cut -f 1 -d '_' |xargs opkg --
force-removal-of-dependent-packages remove
```

- Se ricevi uno o più messaggi di errore dall'esecuzione di questi comandi, è possibile ignorarli: significa che il comando non era necessario per la tua versione del firmware

INSTALLAZIONE GUI ANSUEL

- Collegarsi con WinSCP al router come descritto in precedenza
- Copiare il file `GUI.tar.bz2` nella directory `/tmp`
- Collegarsi in SSH al router con root
- Eseguire il seguente comando per estrarre la GUI
  - `bzcat /tmp/GUI.tar.bz2 | tar -C / -xvf - && /etc/init.d/rootdevice force`
- Attendere fino al termine della procedura. Se necessario il router potrebbe riavviarsi da solo. Ignorare gli ultimi messaggi di errore
- In caso di *Errore 9* riavviare il router e il problema sarà risolto

CAMBIARE PASSWORD ROOT E GUI

- Eseguire il comando `passwd` nel terminale per cambiare la password di accesso dell'utente root. Questa procedure è fortemente consigliata
- Una volta installata la GUI Ansuel, username e password saranno nuovamente `admin/admin`. E' consigliato cambiare anche questa password in modo tale da prevenire accessi non autorizzati alla pagina web di amminsitrazione. Per fare ciò, dopo essere entrati nella GUI web, cliccare sul pulsante *Avanzate* in alto a destra accanto al nome utente *admin* e poi su *Impostazioni profilo*

FINE

Ora si dispone di un modem router TIM HUB DGA4132 aggiornato alla versione AGTHP 2.3.3 con i permessi di root abilitati e la GUI Ansuel.