ROUTER 4G

8D5858 _ Router 4G

Manuale Operativo

rev. 2.0 10/2017

ENGLISH ITALIANO

digicom

INDICE

PRECAUZIONI

Al fine di salvaguardare la sicurezza, l'incolumità dell'operatore e il funzionamento dell'apparato, devono essere rispettate le seguenti norme per l'installazione. Il sistema, compresi i cavi, deve venire installato in un luogo privo o distante da:

- Polvere, umidità, calore elevato ed esposizione diretta alla luce del sole.
- Oggetti che irradiano calore. Questi potrebbero causare danni al contenitore o altri problemi.
- Oggetti che producono un forte campo elettromagnetico (altoparlanti Hi-Fi, ecc.)
- Liquidi o sostanze chimiche corrosive.

CONDIZIONI AMBIENTALI
Temperatura ambiente da -10° a +60°C Umidità relativa da 20 a 80% n.c.
Si dovrà evitare ogni cambiamento rapido di temperatura e umidità.
PULIZIA DELL'APPARATO
Usate un panno soffice asciutto senza l'ausilio di solventi.
VIBRAZIONI O URTI
Attenzione a non causare vibrazioni o urti.

DICHIARAZIONE DI CONFORMITÀ UE SEMPLIFICATA

Il fabbricante, Digicom S.p.A., dichiara che il tipo di apparecchiatura radio **Router 4G** è conforme alla direttiva 2014/53/UE.
Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: www.digicom.it

ASSISTENZA E CONTATTI

La maggior parte dei problemi può essere risolta consultando la sezione Supporto > F.A.Q. presente sul nostro sito www.digicom.it. Se, dopo un'attenta lettura delle procedure ivi descritte, non riusciste comunque a risolvere il problema, vi invitiamo a contattare l'assistenza Digicom.

E-mail: support@digicom.it

È possibile stampare il modulo di "RICHIESTA ASSISTENZA" scaricandolo dal nostro sito Internet www.digicom.it nella sezione Supporto > Riparazioni e Garanzia, o prelevando il file PDF dal CD-ROM incluso nella confezione (ove presente).

INFORMAZIONI SULLA SICUREZZA

Leggete attentamente le istruzioni e norme qui riportate prima di accendere il dispositivo. Violare tali norme potrebbe essere illegale e creare situazioni di pericolo.
Per ognuna delle situazioni descritte è necessario fare riferimento alle disposizione e norme del caso. Il presente dispositivo è una radioricetrasmittente a bassa potenza. Quando è in funzione, invia e riceve energia a radiofrequenza (RF).
Il dispositivo produce campi magnetici, per questa ragione deve essere tenuto lontano da supporti magnetici quali dischetti, nastri, ecc.
Il funzionamento del dispositivo vicino a dispositivi elettrici ed elettronici quali radio, telefoni, televisioni e computer può causare interferenze.

INTERFERENZE

Il presente dispositivo, così come tutti i dispositivi senza fili, è soggetto a interferenze che possono influire sulle prestazioni del dispositivo.

UTILIZZO IN AUTO

Non utilizzate il dispositivo se siete alla guida. Nel caso di utilizzo su autovetture è necessario verificare se i dispositivi elettronici del veicolo siano protetti contro l'emissione RF. Non installate il dispositivo nello spazio che l'airbag occuperebbe gonfiandosi.

UTILIZZO IN AEREO

Spegnete il dispositivo quando siete in aereo. L'utilizzo di dispositivi GSM su aeromobili è illegale.

UTILIZZO ALL'INTERNO DEGLI OSPEDALI

Spegnete il dispositivo in prossimità di apparecchiature medicali; in particolare potrebbero verificarsi interferenze con stimolatori cardiaci e protesi acustiche. Ponete la massima attenzione nell'utilizzo del dispositivo negli ospedali e nei centri sanitari, in quanto è possibile che siano in uso dispositivi sensibili a segnali esterni di radiofrequenza. Nei centri sanitari, dove espressamente indicato, l'apparecchio va tenuto spento.

UTILIZZO IN PROSSIMITÀ DI MATERIALI ESPLOSIVI

Non utilizzate il dispositivo in depositi di carburante, impianti chimici o in aree caratterizzate dalla presenza di gas esplosivi o dove sono in corso operazioni con esplosivi. Sarà necessario rispettare le limitazioni e attenersi a qualunque norma o disposizione prevista.

MODALITÀ D'USO

Non utilizzate il dispositivo a contatto col corpo umano, e mantenete una distanza minima dall'apparato e dall'antenna di 20 cm. Utilizzate solo accessori approvati. Consultate i manuali di eventuali altri dispositivi da collegare al presente dispositivo. Non collegate dispositivi incompatibili.

INFORMAZIONE AGLI UTENTI

ai sensi dell'Art. 26 "Informazione agli utilizzatori" - **Decreto Legislativo 14 marzo 2014, n. 49 "Attuazione della direttiva 2012/19/UE sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE).".**

Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.
L'utente dovrà, pertanto, conferire l'apparecchiatura giunta a fine vita agli idonei centri di raccolta differenziata dei rifiuti elettronici ed elettrotecnici, oppure riconsegnarla al rivenditore al momento dell'acquisto di una nuova apparecchiatura di tipo equivalente, destinata ad un nucleo domestico, in ragione di uno a uno, ai sensi dell'articolo 11, comma 1 del suddetto Decreto Legislativo.
Inoltre, come previsto dell'articolo 11, comma 3 del suddetto Decreto Legislativo è previsto presso il punto vendita, il conferimento a titolo gratuito senza alcun obbligo di acquisto per i RAEE di piccolissime dimensioni, provenienti dai nuclei domestici.
L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile, contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute umana dovuti alla eventuale presenza di sostanze pericolose e favorisce il reimpiego e/o riciclo dei materiali di cui è composta l'apparecchiatura.
Lo smaltimento abusivo del prodotto da parte detentore, comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente.

1. INTRODUZIONE

1

Gentile Cliente,
grazie per la fiducia accordataci nell'acquistare un prodotto Digicom.

Il Router 4G 8D5858 è un dispositivo di Networking per applicazioni su rete su rete mobile LTE e 3G.
Dotato delle principali funzionalità e protocolli per l'interconnessione ad Internet, collegamenti protetti da VPN e funzionalità di Backup/ Fail-over e per la gestione remota del link è la soluzione ideale per i più comuni scenari applicativi professionali in ambito industriale e civile.

1.1. CARATTERISTICHE

- Tipo di rete mobile:
  4G/LTE-FDD bande 3/7/20 (1800/2600/800MHz) max Power 24 dBm
  HSPA+/UMTS/WCDMA banda 1 (2100MHz) max Power 23 dBm
- Velocità: 4G/LTE Download 150Mbps / Upload 50Mbps,
  HSPA+/UMTS/WCDMA Download 21.6Mbps / Upload 5.76Mbps
- Standard Wi-Fi: 802.11n 300Mbps a 2.4GHz max Power <20 dBm
- 3 porte LAN RJ45 10/100Mbps, Auto MDI-X
- 1 porta WAN RJ45 10/100Mbps, Auto MDI-X
- 1 Slot per SIM di qualsiasi operatore
- Connessione 4G/3G automatica e manuale
- Backup tra interfacce WAN/LTE automatico
- Security Wireless WEP, WPA/WPA2, WPA/WPA2-PSK
- Impostazione security automatica da tasto WPS
- Supporto DHCP Server, IP Reservation
- Supporto DDNS, Virtual Server e DMZ
- Supporto OpenVPN Client e Server
- Firmware aggiornabile
- Interfaccia di configurazione via Browser e Console SSH
- Gestione Connessione da remoto tramite SMS* per connessione, stato, disconnessione e reset
- Alimentazione 12VDC 1A con alimentatore di rete (nella versione standard)

* Richiede SIM con funzionalità Internet + SMS

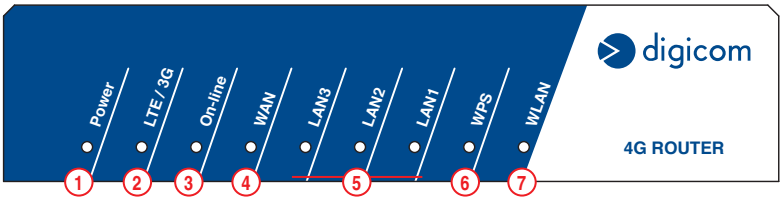
1.2. CONTENUTO DELLA CONFEZIONE

- 8D5858 Router 4G
- Alimentatore (solo in versione a 12VDC)
- Cavo Ethernet RJ45
- 2 Antenne 4G
- Guida Rapida

2. DESCRIZIONE HARDWARE

2.1. PANNELLO FRONTALE

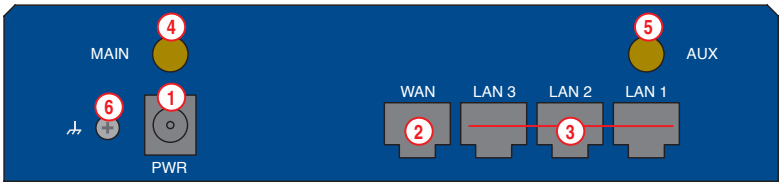
Indicatori Led



	LED	STATO	DESCRIZIONE
1	**Power**	Spento	Alimentazione non collegata
		Acceso	Alimentazione collegata
2	**LTE/3G**	Rosso	Livello segnale Scarso
	(Livello Segnale)	Arancio	Livello segnale Sufficiente
		Verde	Livello segnale Buono o Eccellente
3	**On-line**	Rosso	Connessione On-Line su WAN Ethernet
		Verde	Connessione On-Line su 3G/4G LTE
		Spento	Connessione Off-Line
4	**WAN**	Spento	La porta Ethernet WAN è disconnessa
		Acceso	La porta Ethernet WAN è connessa ad un Gateway
		Lampeggiante	Dati trasmessi sulla porta Ethernet WAN
5	**LAN3 - LAN1**	Spento	La porta è disconnessa
		Acceso	La porta è connessa ad un dispositivo di rete
		Lampeggiante	Dati trasmessi sulla porta
6	**WPS**	Spento	Nessuna procedura WPS in corso
		Lampeggiante	Procedura WPS in corso
7	**WLAN**	Spento	Interfaccia Wi-Fi disattivata
		Acceso	Interfaccia Wi-Fi attiva
		Lampeggiante	Dati trasmessi su Wi-Fi

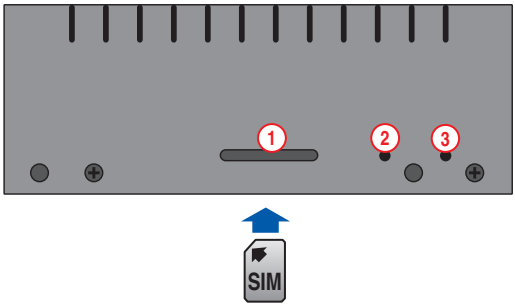
2.2. PANNELLO POSTERIORE

Porte e connettori



		DESCRIZIONE
1	**PWR**	Connettore per l'alimentatore
2	**WAN**	Porta UTP RJ45 di WAN per connessione con Gateway esterni, Autosensing 10/100Mbps 2 Auto MDI/MDI-X
3	**LAN1 - LAN3**	Porte UTP RJ45 per la connessione di computer o altri dispositivi di rete LAN, tutte Autosensing 10/100Mbps e Auto MDI/MDI-X
4	**MAIN**	Antenna 4G/3G MAIN (principale) removibile su connettore SMA
5	**AUX**	Antenna 4G/3G AUX (diversity) removibile su connettore SMA
6	**Terra**	Morsetto di collegamento elettrico di Terra

2.3. PANNELLO LATERALE

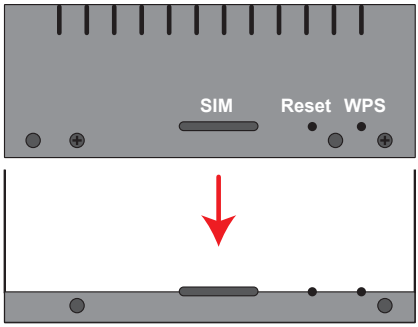


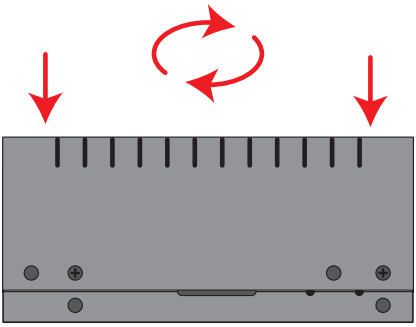
		DESCRIZIONE
1	**SIM**	Slot per inserimento SIM, da effettuare a dispositivo spento
2	**Riavvio** **Reset al default di fabbrica**	Premere il pulsante interno con un oggetto appuntito - 3 secondi per riavviare il Router - più di 10 secondi per ripristinare le impostazioni di fabbrica Attendere per circa 1 minuto il riavvio completo del dispositivo
3	**WPS**	Premere il pulsante interno con un oggetto appuntito per 2 secondi per avviare la procedura WPS.

Per una più agevole installazione della SIM, è possibile rimuovere il coperchio che può essere rimontato in modo da proteggere ed evitare l'accesso allo slot.

2.3.1. Protezione slot di inserimento SIM e pulsanti di Reset/WPS

E' possibile **proteggere lo slot di inserimento SIM ed i pulsanti di Reset al default di fabbrica e attivazione WPS** da manomissioni indesiderate, semplicemente montando il coperchio superiore della meccanica in modo che feritoia e fori di accesso stiano sulla sinistra del dispositivo, rendendoli in questo modo inaccessibili.





3. CONFIGURAZIONE

Il Router dispone di due diverse modalità di configurazione; da **Browser Web Interface** e da **Command Line Interface** testuale (SSH CLI).
Alcune funzioni di base sono configurabili solamente da CLI.

3.1. IMPOSTAZIONI DA COMMAND LINE INTERFACE (CLI)

La comandistica disponibile via CLI permette di configurare le funzioni per la gestione della rete cellulare tra cui modalità di rete, modalità di connessione, backup, monitoring e riavvii schedulati.

3.1.1. Accesso alla console CLI

La console CLI è di tipo SSH ed è attiva all'indirizzo IP di LAN del Router, protocollo TCP, porta 22.
Per accedere alla console CLI utilizzare un comune programma che metta a disposizione una sessione SSH come, ad esempio, PuTTY o Teraterm.

3.1.2. Sintassi dei comandi CLI

I comandi devono essere digitati in MAIUSCOLO.
Possono essere presenti uno o più parametri, separati da virgola, da digitare in minuscolo o maiuscolo.

I parametri sono separati dal carattere virgola.
In caso di parametri multipli un (o più) parametro può essere omesso lasciandone la posizione vuota.

Lo stato dei parametri di un comando può essere interrogato tramite il carattere ?.
Il carattere ? per l'interrogazione dello stato del comando è anche esso gestito come parametro e pertanto deve essere preceduto da uno spazio.

Un parametro descritto di seguito tra < > è definito come **mandatorio**. Se omesso genera una condizione e risposta di ERRORE.

Un parametro descritto di seguito tra [ ] è definito come **facoltativo**. Se omesso **va lasciato vuoto**.
Se dichiarato va a modificare l'impostazione della rispettiva funzione.
Se omesso non viene modificata l'impostazione della rispettiva funzione.

Esempi:
SETDIALMODE *99#,,,,auto
SETSREBOOT 23,59,0
SETWANBKP ?

3.1.3. SETAPN

Impostazione APN per connessione 3G/4G.

Struttura comando	SETAPN <apn>
Esempio comando	SETAPN ibox.tim.it
Parametri	apn stringa alfanumerica min. 8, max. 32 caratteri
Risposta al comando	OK
	ERROR (in caso di errore di sintassi, assenza o troppi parametri)
Interrogazione	SETAPN ?
Esempio Risposta	APN: ibox.tim.it
Factory Default	Ibox.tim.it

3.1.4. SETMOBILE

Impostazione modalità di registrazione alla rete cellulare 3G/4G e Roaming.

Struttura comando	SETMOBILE **<netmode>, [roaming]**
Esempio comando	SETMOBILE 3G,roam
Parametri	**netmode** = Modalità rete • 3G • 4G • auto = selezione automatica 4G/3G **roaming** = Roaming • noroam = Roaming disabilitato • roam = Roaming abilitato
Risposta al comando	OK ERROR (in caso di errore di sintassi, assenza o troppi parametri)
Interrogazione	SETMOBILE ?
Esempio Risposta	MOBILE: 4g,noroam
Factory Default	SETMOBILE auto,noroam

3.1.5. SETDIALMODE

Impostazione dei parametri di chiamata 3G/4G e modalità di connessione.

Struttura comando	SETDIALMODE **<num>,[user],]pwd],[auth],[mode]**
Esempio comando	SETDIALMODE *99#, user1,pass1,chap,auto SETDIALMODE *99#,,,,auto
Parametri	**num** = Numero da chiamare **user** = Username di autenticazione (max. 32 caratteri) **pwd** = Password di autenticazione (max. 32 caratteri) **auth** = Autenticazione • none = nessuna autenticazione • pap = autenticazione PAP • chap = autenticazione CHAP **mode** = Modalità • auto = connessione automatica Always on • manual = connessione attivata da SMS o CLI
Risposta al comando	OK ERROR (in caso di errore di sintassi, assenza o troppi parametri)
Interrogazione	SETDIALMODE ?
Esempio Risposta	DIALMODE: *99#,,,none,auto
Factory Default	SETDIALMODE *99#,,,none,auto

3.1.6. SETCONNECTION

Forzatura connessione o disconnessione 3G/4G.

Struttura comando	SETCONNECTION **<mode>**
Esempio comando	SETCONNECTION up
Parametri	**mode** = stato connessione • up = attiva connessione • down = forza disconnessione, il Router rimane offline fino a successivo comando di connessione o reboot (se SETDIAL mode diverso da auto).
Risposta al comando	OK ERROR (in caso di errore di sintassi, assenza o troppi parametri)
Interrogazione	SETCONNECTION ?
Esempio Risposta	CONNECTION up

NOTA: A fronte di un comando SETCONNECTION up o down la console potrebbe essere non utilizzabile fino a 30 secondi, tempo durante il quale id Router effettua delle reinizializzazioni delle interfacce.

3.1.7. SETWANBKP

Impostazione dell'interfaccia di connessione primaria e abilitazione funzione di Backup.

Struttura comando	SETWANBKP **<Main_IF>, <BKP_en>**
Esempio comando	SETWANBKP ETH,0 SETWANBKP LTE,1
Parametri	**Main_if** = interfaccia primaria • ETH = Interfaccia WAN Ethernet • LTE = Interfaccia 3G/4G **BKP_en** = abilitazione della funzione di WAN Backup • 1 = abilitata • 0 = disabilitata **NOTA: l'interfaccia di Backup è quella non definita come primaria**
Risposta al comando	OK ERROR (in caso di errore di sintassi, assenza o troppi parametri)
Interrogazione	SETWANBKP ?
Esempio Risposta	WANBKP: ETH,1
Factory Default	SETWANBKP LTE,0

3.1.8. SETPINGMON

Impostazioni parametri di monitoraggio della connessione per la funzione di Backup.
Vedere anche Funzione di Backup automatico.

Struttura comando	SETPINGMON **<PPI>,<PRT,<MF>,<DH1>,<DH2>**
Esempio comando	SETPINGMON 300,60,3,195.103.9.66,8.8.8.8
Parametri	**PPI** = Intervallo di tempo, in secondi, che intercorre tra un invio di Ping Sequence (PS) e l'altro **PRT** = Intervallo di tempo, in secondi, tra una sequenza PS e l'altra **MF** = Numero di volte per cui la sequenza PS deve fallire per innescare un riavvio **DH1**= Indirizzo IP del primo host di cui verificare la raggiungibilità. **DH2**= Indirizzo IP del secondo host di cui verificare la raggiungibilità.
Risposta al comando	OK ERROR (in caso di errore di sintassi, assenza o troppi parametri)
Interrogazione	SETPINGMON ?
Esempio Risposta	PINGMON: 120,30,3,8.8.8.8,8.8.4.4
Factory Default	SETPINGMON 120,30,3,8.8.8.8,8.8.4.4

NOTE:
La connettività è considerata assente se entrambi gli host DH1 e DH2 sono irraggiungibili.
Se i parametri PPI, PRT e MF sono tutti a zero, la funzione NPC è disabilitata.

3.1.9. SETSREBOOT

Impostazioni per riavvio schedulato.

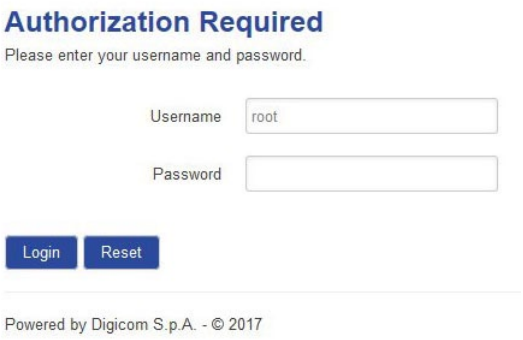
Struttura comando	SETSREBOOT <RH>,<RM>,<RE>
Esempio comando	SETSREBOOT 0,0,600 SETSREBOOT 23,59,0
Parametri	**RH** = Ora dell'orario a cui effettuare il riavvio forzato **RM** = Minuto dell'orario a cui effettuare il riavvio forzato **RE** = Intervallo di tempo, in minuti, tra un riavvio forzato e l'altro
Risposta al comando	OK ERROR (in caso di errore di sintassi, assenza o troppi parametri)
Interrogazione	SETSREBOOT ?
Esempio Risposta	SREBOOT: 0,0,0
Factory Default	SREBOOT 0,0,0

NOTA:
Se RE è a zero oppure RM e RH entrambi a zero, la funzione SREBOOT è disabilitata.
I due metodi sono alternativi uno all'altro. Il metodo Orario del giorno prevale sul metodo Intervallo definito in minuti (se entrambi configurati).

3.2. IMPOSTAZIONI DA WEB INTERFACE

L'interfaccia WEB permette la configurazione della quasi totalità delle impostazioni del Router.
Per accedere all'interfaccia Web digitare l'indirizzo URL http://192.168.1.1 in un browser ed inserire le credenziali di accesso:

- Username: **root**
  Password: lasciare vuoto
- Cliccare su **Login**



- Una volta effettuato il login apparirà la pagina di **Status Overview**.
- Verrà richiesto di **impostare o modificare la password** di default, dal menu **System – Administrator**.

3.2.1. Status - Overview

La pagina riporta una serie di indicazioni sullo stato corrente ed alcune impostazioni di funzionamento del Router.

System

Hostname	Hostname per il Router
Model	Modello Digicom del dispositivo (8D5858)
Firmware Version	Versione e data di build del firmware a bordo del Router
Kernel Version	Versione del kernel del Router
Local Time	Data e Ora di sistema corrente
Uptime	Tempo di funzionamento del Router in ore, minuti, secondi
Load Average	Indicazioni di carico operativo della CPU

Mobile Network

Sim Status	Stato operativo della SIM
Iccid	ICCID della SIM
Imei	IMEI del modulo 3G/3G
Signal Level	Livello del segnale 3G/4G ricevuto in percentuale
Rssi	Livello in dbm del segnale 3G/4G ricevuto
Network Mode	Modalità 3G,4G
Registered Status	Stato di registrazione alla rete 3G/4G
Registered Network	Rete 3G,4G registrata e modalità
Apn	APN impostato
Apn User	Credenziale di accesso all'APN
Apn Password	Credenziale di accesso all'APN
Apn Authentication Mode	Autenticazione di accesso all'APN
Roaming	Stato di Roaming

Network

IPv4 WAN Status Parametri e tempistiche di connessione dell'interfaccia IPV4 corrente, ad esempio:

eth1

Type: dhcp
Address: 2.194.64.53
Netmask: 255.255.255.0
Gateway: 2.194.64.202
DNS 1: 10.206.56.132
DNS 2: 10.207.43.46
Expires: 23h 40m 56s
Connected: 0h 19m 4s

IPv6 WAN Status Parametri dell'interfaccia IPV6 corrente

Active Connections Numero di sessioni attive

Wireless

Generic 802.11bgn Wireless Controller (radio0) Parametri dell'interfaccia WIFI, ad esempio:

100%

SSID: Digicom4G_07f4
Mode: Master
Channel: 11 (2.462 GHz)
Bitrate: ? Mbit/s
BSSID: 00:A0:A2:AC:07:F4
Encryption: WPA2 PSK (CCMP)

Associated Stations Informazioni sugli host connessi all'interfaccia Wi-Fi

DHCP Leases

DHCPv6 Leases

Informazioni sugli host che hanno ricevuto un indirizzo IP dal DHCP server del Router.

Memory

Informazioni sull'occupazione dinamica della memoria di sistema

Dynamic DNS

Informazioni sullo stato di registrazione della funzione DDNS.

3.2.2. Status - Routes

La pagina di mostra le informazioni relative ad:

ARP

Informazioni ARP sugli host connessi al Router.

Informazioni ARP sulle interfacce in uso.

Routes

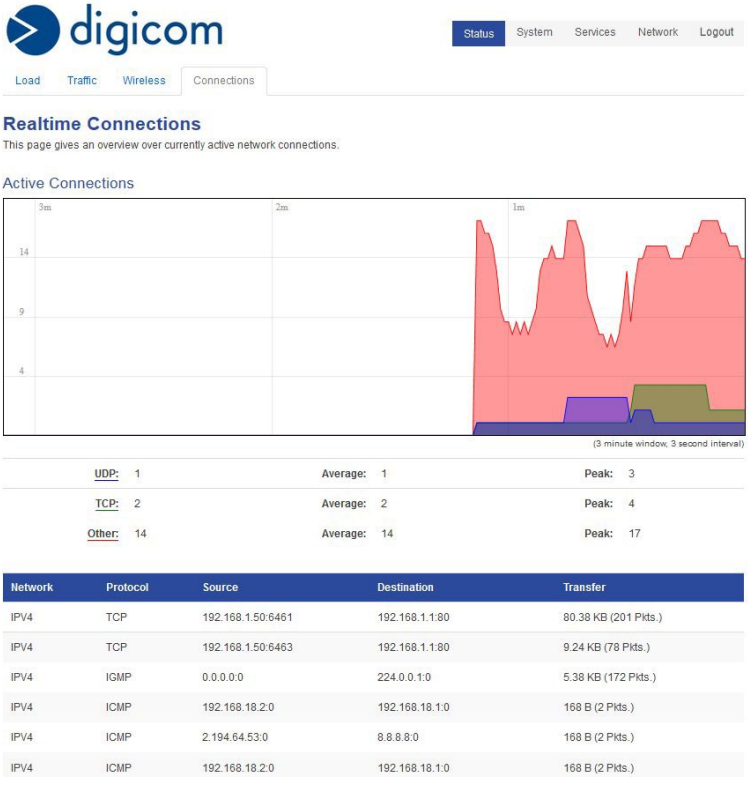
Informazioni sugli instradamenti in essere.

3.2.3. Status – System Log

La pagina mostra il log di sistema.

3.2.4. Status – Realtime Graphs

La pagina mostra grafici in tempo reale sullo stato di occupazione, carico, protocolli e traffico sulle interfacce del Router.



3.3. SYSTEM – SYSTEM

3.3.1. System Properties - General Settings

Local Time	Mostra la data e ora di sistema corrente.
Sync with Browser	Cliccare per impostare la data/ora corrente del computer in uso.
Hostname	Nome Host per il Router. Imposta anche il Prompt name in CLI.
Timezone	Imposta il Timezone per il fuso orario locale.

3.3.2. Time Synchronization

Enable NTP client	Attiva il client NTP per l'acquisizione di data/ora da Internet.
Provide NTP server	Attiva la funzione NTP server per redistribuire la propria data/ora.
NTP server candidates	Lista di server NTP da cui acquisire data/ora. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.3.3. System Properties - Logging

System log buffer size	Dimensione in KB del buffer dedicato al log di sistema.
External system log server	Indirizzo IP del Syslog server in rete.
External system log server port	Porta del Syslog server in rete.
External system log server protocol	Protocollo in uso dal Syslog server in rete.
Write system log to file	Percorso del file log di sistema.
Log output level	Livello di output del log di sistema.
Cron Log Level	Livello di cron del log di sistema.

3.3.4. System Properties – Language and Style

Menu con parametri di sola lettura.

3.4. SYSTEM – ADMINISTRATOR

3.4.1. Router Password

Password	Digitare la password per l'account di amministrazione.
Confirmation	Ridigitare la password per l'account di amministrazione per conferma.

3.4.2. SSH Access

Interface	Selezionare l'interfaccia sulla quale permettere l'accesso alla console CLI via SSH. Selezionare unspecified per abilitare su tutte le interfacce. Cliccare su **Delete** e **Save & Apply** per disabilitare l'accesso SSH.
Port	Porta per la console SSH.
Password authentication	Richiede autenticazione per l'accesso SSH.
Allow root logins with password	Richiedi all'utente root di accedere con autenticazione.
Gateway ports	Permetti a gateway esterni di accedere a porte SSH inoltrate.
SSH-Keys	Campo di inserimento delle chiavi di autenticazione pubbliche (una per riga).

3.5. SYSTEM – FLASH / BACKUP FIRMWARE

3.5.1. Backup / Restore

3.5.2. Salvare le impostazioni del Router

Download backup	Cliccare per scaricare il file archivio contenente le impostazioni del Router.

3.5.3. Caricare una configurazione salvata

Restore backup	Cliccare su **Sfoglia** per selezionare il file/immagine di aggiornamento del firmware.
Upload archive…	Cliccare per **caricare** il file archivio contenente le impostazioni del Router. Cliccare su **Proceed** una volta che il file è stato calcolato e verificato il checksum MD5 del file. Cliccare su **Cancel** per non effettuare il caricamento.

3.5.4. Ripristinare le impostazioni di fabbrica

Reset to defaults	Cliccare su **Perform reset** per ripristinare le impostazioni di fabbrica del Router.

3.5.5. Aggiornare il firmware del Router

Image	Cliccare su **Sfoglia** per selezionare il file/immagine di aggiornamento del firmware.
Flash image…	Cliccare per avviare il caricamento del file/immagine di aggiornamento del firmware.
Keep Settings	Selezionare per non cancellare la configurazione attuale al termine dell'aggiornamento. Può generare incongruenze di funzionamento in caso di firmware molto differenti in termini di funzioni e features. Deselezionare per non mantenere le impostazioni attuali.

3.6. SYSTEM – REBOOT

Perform Reboot	Cliccare per effettuare un riavvio (reboot) del Router. Non verranno modificate le impostazioni salvate ed applicate.

3.7. SERVICES - OPENVPN

Sono supportate sessioni OpenVPN di tipo Client e Server.

- Cliccare su **Edit** per modificare un profilo esistente.
- Cliccare su **Add** per creare un profilo OpenVPN dopo aver selezionato la tipologia Client o Server ed assegnato un nome mnemonico.
- Cliccare su **Delete** per cancellare un profilo OpenVPN.

Enable	Selezionare per abilitare il profilo.
Start/Stop	Cliccare per attivare la sessione del profilo. La colonna Started indicherà Yes(id sessione) una volta avviata la sessione. Se la sessione non si avvia a fronte della pressione di Start il profilo potrebbe contenere errori di impostazione o configurazione.

3.7.1. OpenVPN Client

Overview - Basic configuration

verb	Livello di verbosità da inserire nei log di sistema.
tun_ipv6	Selezionare per permettere il protocollo IPv6.
nobind	Selezionare per non forzare la sessione all'indirizzo dell'interfaccia in uso (float).
comp_lzo	Selezionare il tipo di compressione LZO.
proto	Selezionare il protocollo da utilizzare per la sessione (corrispondente al lato server).
client	Selezionare per forzare la sessione in modalità Client.
client_to_client	Selezionare per permettere comunicazioni tra client (solo per sessioni Server).
remote	Indirizzo del server OpenVPN remoto (su porta 1194). Se la porta remota è diversa da 1194 impostarla dopo aver caricato il campo aggiuntivo **port**.
Additional field	Selezionare il **campo aggiuntivo** e cliccare su **Add**.

ESEMPI:

Aggiunta dei campi tipici per sessioni TLS (autenticazione tramite Certificati)

- Selezionare **ca**, cliccare su **Add**.
- Comparirà l'opzione di selezione (Sfoglia) per il caricamento del file certificato CA (ad esempio ca.crt).
- Utilizzare **cert** per il certificato del client (ad esempio client.crt).
- Utilizzare **key** per la chiave per il client (ad esempio client.pem).
- Utilizzare **dh** per la chiave Diffie-Helman (ad esempio dh1024.pem).
- Una volta creati e caricati tutti i campi richiesti cliccare su **Save**. A caricamento avvenuto comparirà l'informazione **Uploaded File (x.xx KB)** per ogni file caricato valido.

Aggiunta dei campi tipici per autenticazione con PSK (sessioni non-TLS)

- Selezionare **secret**, cliccare su **Add**.
- Comparirà l'opzione di selezione (Sfoglia) per il caricamento del file contenente le password.

Overview - Advanced configuration

- Cliccare su **Switch to Advanced configuration** per accedere alle sezioni di configurazione avanzata specifica per i parametri inerenti **Service, Networking, VPN** e **Cryptography**.

3.7.2. OpenVPN Server

Overview - Basic configuration

verb	Livello di verbosità da inserire nei log di sistema.
port	Porta TCP/UDP utilizzata dal server.
tun_ipv6	Selezionare per permettere il protocollo IPv6.
server	Indirizzo della subnet virtuale su cui saranno allocate le sessioni client.
nobind	Selezionare per non forzare la sessione all'indirizzo dell'interfaccia in uso (float).
comp_lzo	Selezionare il tipo di compressione LZO.
keepalive	Tempistiche per i parametri ping e ping-restart.
proto	Selezionare il protocollo da utilizzare per la sessione (corrispondente al lato server).
client	Non selezionare (sessione in modalità Server).
client_to_client	Selezionare per permettere comunicazioni tra client.
Additional field	Selezionare il campo aggiuntivo e cliccare su Add.

ESEMPI:

Aggiunta dei campi tipici per sessioni TLS (autenticazione tramite Certificati)

- Selezionare **ca**, cliccare su **Add**.
- Comparirà l'opzione di selezione (Sfoglia) per il caricamento del file certificato CA (ad esempio ca.crt).
- Utilizzare **cert** per il certificato del client (ad esempio server.crt).
- Utilizzare **key** per la chiave per il client (ad esempio server.pem).
- Utilizzare **dh** per la chiave Diffie-Helman (ad esempio dh1024.pem).
- Una volta creati e caricati tutti i campi richiesti cliccare su **Save & Apply**. A caricamento avvenuto comparirà l'informazione **Uploaded File (x.xx KB)** per ogni file caricato valido.

Aggiunta dei campi tipici per autenticazione con PSK (sessioni non-TLS)

- Selezionare secret, cliccare su Add.
- Comparirà l'opzione di selezione (Sfoglia) per il caricamento del file contenente le password.

Overview - Advanced configuration

- Cliccare su **Switch to Advanced configuration** per accedere alle sezioni di configurazione avanzata specifica per i parametri inerenti **Service, Networking, VPN** e **Cryptography**.

Ad esempio, per aggiungere l'opzione 'push route 192.168.100 255.255.255.0'

- Selezionare **VPN**.
- Aggiungere il campo push.
- Cliccare su **Save**.
- Selezionare custom per l'opzione **push** e digitare route 192.168.100 255.255.255.0 all'interno del campo.
- Cliccare su **Save**.

3.8. SERVICES - DYNAMIC DNS

Sono supportati diversi provider di servizio Dynamic DNS.

- Cliccare su **Edit** per modificare un profilo esistente.
- Cliccare su **Add** per creare un profilo DDNS dopo aver digitato un nome nel campo 'Configuration'.
- Cliccare su **Delete** per cancellare un profilo DDNS.

3.8.1. Basic Settings

Enable	Selezionare per attivare il profilo configurato.
DDNS Service provider	Selezionare uno dei provider DDNS supportati. Cliccare su **Change provider** e visualizzare i parametri specifici del provider scelto.
Lookup Hostname	Digitare il nome del dominio impostato presso il provider DDSN, ad esempio router4g.dyndns.org
IP address version	Selezionare IPv4 o IPv6.
Domain	Digitare il nome del dominio impostato presso il provider DDSN, ad esempio router4g.dyndns.org
Username	Digitare la username delle credenziali di accesso al provider DDNS.
Password	Digitare la password delle credenziali di accesso al provider DDNS.
Use HTTP Secure	Selezionare per utilizzare una sessione HTTPS con il provider.

3.8.2. Advanced settings

IP address source	Selezionare la sorgente/interfaccia/porta sorgente per l'IP da registrare.
Force IP Version	Selezionare per forzare comunicazione unicamente in IPv4 o IPv6.
Proxy-Server	Digitare l'URL di accesso al proxy server, se utilizzato. E' ammesso il formato [user:password@] proxyhost:port
Log to Syslog	Livello di logging nel syslog di sistema.
Log to file	Se selezionato effettua logging su file di sistema.

3.8.3. Timer settings

Check Interval	Intervallo di verifica per eventuali cambi di indirizzo IP, in minuti (min. 5).
Force Interval	Intervallo forzato di aggiornamento dell'IP presso il provider DDNS.
Error Retry Counter	Contatore per terminare gli aggiornamenti IP in caso di continui errori.
Error Retry Interval	Intervallo per ripetizione dell'azione in caso di errore.

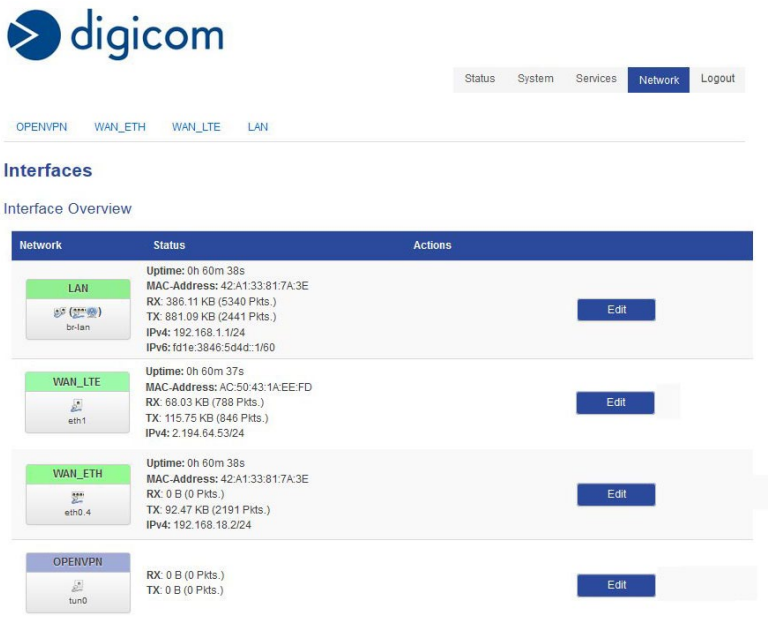
3.8.4. Log File Viewer

Visualizza il file di log.

3.9. NETWORK - INTERFACE

Mostra lo stato delle interfacce del Router, riportando tempistiche, indirizzi IP e MAC, volume di dati trasmessi.

- Cliccare su **Edit** per modificare le impostazioni di una interfaccia.



3.10. LAN

Edit	Cliccare per accedere ai paramentri di configurazione dell'interfaccia.
If up/ If down	Cliccare per attivare/disattivare l'interfaccia dal sistema.

3.10.1. General Setup

Protocol	Selezionare il tipo di protocollo/modalità e cliccare su **Switch Protocol**. **Nota: Non tutte le opzioni sono disponibili.**
Hostname to send when requesting DHCP	Permette di specificare un nome host per la richiesta DHCP (disponibile se protocol è DHCP Client).
IPv4 address	Indirizzo IP per l'interfaccia.
IPv4 netmask	Subnet Mask per l'interfaccia. Selezionare custom per maschere speciali.
IPv4 gateway	Indirizzo del Gateway per l'interfaccia (opzionale).
IPv4 broadcast	Indirizzo di broadcast per l'interfaccia (opzionale).
Use custom DNS servers	Indirizzi IP dei server DNS specifici. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
IPv6 assignment length	Lunghezza per la parte di indirizzo IPv6. Selezionare disabled per assegnare indirizzi statici.
IPv6 address	Indirizzo IPv6 per l'interfaccia.
IPv6 Gateway	Indirizzo del Gateway IPv6.
IPv6 routed prefix	Prefisso per l'indirizzo IPv6.
IPv6 assignment hint	ID per il sub-prefisso IPv6.
IPv6 suffix	Suffisso IPv6.

3.10.2. Advanced Settings

Bring up on boot	Selezionare per attivare l'interfaccia all'avvio del Router.
Use builtin IPv6-management	Selezionare per usare il protocollo IPv6 nativo.
Force link	Selezionare per attivare le impostazioni dell'interfaccia anche in assenza di link fisico.
Use broadcast flag	Selezionare in caso di specifica richiesta da parte dell'operatore (modalità DHCP Client).
Use default Gateway	Se selezionato imposta una **default route** per l'interfaccia (modalità DHCP Client).
Client ID to send when requesting DHCP	Permette di specificare un Client ID per le richieste DHCP (modalità DHCP Client).
Vendor Class to send when requesting DHCP	Permette di specificare un Vendor class per le richieste DHCP (modalità DHCP Client).
Override MAC address	Permette di specificare per l'interfaccia un MAC address definito dall'utente.
Override MTU	Permette di specificare un valore MTU specifico per l'interfaccia.
Usa gateway metric	Permette di impostare una metrica specifica per l'interfaccia.

3.10.3. Physycal Settings

Bridge interfaces	Selezionare per creare un 'bridge' tra interfacce specifiche
Enable STP	Selezionare per abilitare il protocollo Spanning Tree (in caso di bridging con loop)
Interface	Selezionare le interfacce da associare al bridge, ad esempio LAN e Wi-Fi.

3.10.4. Firewall Settings

Create / Assign firewall-zone	Permette di specificare la Firewall-zone alla quale l'interfaccia è assegnata.

3.10.5. DHCP Server - General Setup

No DHCP Server configured for this interface	Cliccare su **Setup DHCP Server** per attivare il server DHCP per l'interfaccia nel caso non fosse presente.
Ignore interface	Selezionare per **disabilitare** il DHCP server per l'interfaccia.
Start	Primo campo host dell'indirizzo IP da assegnare, ad esempio 100 per 192.168.1.100. Per controllare l'assegnamento degli indirizzi in sequenza oppure casuale impostare **Allocate IP sequentially** nel menu Network DHCP & DNS, Server Settings – Advances Settings.
Limit	Numero massimo di indirizzi IP da assegnare.
Lease time	Durata in ore prima della scadenza dell'assegnazione.

3.10.6. DHCP Server – Advanced Settings

Dynamic DHCP	Abilita assegnazione indirizzi dinamici. **Disabilitare** per assegnare unicamente indirizzi IP host configurati per **assegnamento statico**.
Force	Forza funzionamento DHCP Server anche se viene rilevata la presenza di un altro server in rete.
IPv4-Netmask	Subnet mask non standard da assegnare ai client.
DHCP-Options	Opzioni DHCP. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.10.7. DHCP Server – IPV6 Settings

Router Advertisement-Service	Selezionare il tipo di servizio advertisement (server/relay/hybrid)
DHCPv6-Service	Selezionare il tipo di servizio DHCP (server/relay/hybrid)
NDP-Proxy	Selezionare il tipo di servizio proxy (relay/hybrid)
DHCPv6-Mode	Selezionare la modalità DHCP (stateless/stateful/mista)
Always announce default Router	Selezionare per annunciare il Router come gateway anche in assenza di prefisso pubblico
Announced DNS servers	Lista di DNS server annunciati. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
Announced DNS domains	Lista di Domini DNS annunciati. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.11. WAN_LTE

Edit	Cliccare per accedere ai paramentri di configurazione dell'interfaccia.
If up/ If down	Cliccare per attivare/disattivare l'interfaccia dal sistema.

3.11.1. General Setup

Protocol	Selezionare il tipo di protocollo/modalità e cliccare su **Switch Protocol**. **Attenzione: Utilizzare unicamente Static address e DHCP Client.**
Hostname to send when requesting DHCP	Permette di specificare un nome host per la richiesta DHCP (disponibile se protocol è DHCP Client).
IPv4 address	Indirizzo IP per l'interfaccia.
IPv4 netmask	Subnet Mask per l'interfaccia. Selezionare custom per maschere speciali.
IPv4 gateway	Indirizzo del Gateway per l'interfaccia (opzionale).
IPv4 broadcast	Indirizzo di broadcast per l'interfaccia (opzionale).
Use custom DNS servers	Indirizzi IP dei server DNS specifici. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
IPv6 assignment length	Lunghezza per la parte di indirizzo IPv6. Selezionare disabled per assegnare indirizzi statici.
IPv6 address	Indirizzo IPv6 per l'interfaccia.
IPv6 Gateway	Indirizzo del Gateway IPv6.
IPv6 routed prefix	Prefisso per l'indirizzo IPv6.
IPv6 assignment hint	ID per il sub-prefisso IPv6.
IPv6 suffix	Suffisso IPv6.

3.11.2. Advanced Settings

Bring up on boot	Selezionare per attivare l'interfaccia all'avvio del Router.
Use builtin IPv6-management	Selezionare per usare il protocollo IPv6 nativo.
Force link	Selezionare per attivare le impostazioni dell'interfaccia anche in assenza di link fisico.
Use broadcast flag	Selezionare in caso di specifica richiesta da parte dell'operatore (modalità DHCP Client).
Use default Gateway	Se selezionato imposta una **default route** per l'interfaccia (modalità DHCP Client).
Client ID to send when requesting DHCP	Permette di specificare un Client ID per le richieste DHCP (modalità DHCP Client).
Vendor Class to send when requesting DHCP	Permette di specificare un Vendor class per le richieste DHCP (modalità DHCP Client).
Override MAC address	Permette di specificare per l'interfaccia un MAC address definito dall'utente.
Override MTU	Permette di specificare un valore MTU specifico per l'interfaccia.
Usa gateway metric	Permette di impostare una metrica specifica per l'interfaccia.

3.11.3. Physycal Settings

Bridge interfaces	Selezionare per creare un 'bridge' tra interfacce specifiche
Enable STP	Selezionare per abilitare il protocollo Spanning Tree (in caso di bridging con loop)
Interface	Selezionare le interfacce da associare al bridge, ad esempio LAN e Wi-Fi.

3.11.4. Firewall Settings

Create / Assign firewall-zone	Permette di specificare la Firewall-zone alla quale l'interfaccia è assegnata.

3.11.5. DHCP Server - General Setup

No DHCP Server configured for this interface	Cliccare su **Setup DHCP Server** per attivare il server DHCP per l'interfaccia nel caso non fosse presente.
Ignore interface	Selezionare per **disabilitare** il DHCP server per l'interfaccia.
Start	Primo campo host dell'indirizzo IP da assegnare, ad esempio 100 per 192.168.1.100. Per controllare l'assegnamento degli indirizzi in sequenza oppure casuale impostare **Allocate IP sequentially** nel menu Network DHCP & DNS, Server Settings – Advances Settings.
Limit	Numero massimo di indirizzi IP da assegnare.
Lease time	Durata in ore prima della scadenza dell'assegnazione.

3.11.6. DHCP Server – Advanced Settings

Dynamic DHCP	Abilita assegnazione indirizzi dinamici. **Disabilitare** per assegnare unicamente indirizzi IP host configurati per **assegnamento statico**.
Force	Forza funzionamento DHCP Server anche se viene rilevata la presenza di un altro server in rete.
IPv4-Netmask	Subnet mask non standard da assegnare ai client.
DHCP-Options	Opzioni DHCP. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.11.7. DHCP Server – IPV6 Settings

Router Advertisement-Service	Selezionare il tipo di servizio advertisement (server/relay/hybrid)
DHCPv6-Service	Selezionare il tipo di servizio DHCP (server/relay/hybrid)
NDP-Proxy	Selezionare il tipo di servizio proxy (relay/hybrid)
DHCPv6-Mode	Selezionare la modalità DHCP (stateless/stateful/mista)
Always announce default Router	Selezionare per annunciare il Router come gateway anche in assenza di prefisso pubblico
Announced DNS servers	Lista di DNS server annunciati. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
Announced DNS domains	Lista di Domini DNS annunciati. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.12. WAN_ETH

Edit	Cliccare per accedere ai paramentri di configurazione dell'interfaccia.
If up/ If down	Cliccare per attivare/disattivare l'interfaccia dal sistema.

3.12.1. General Setup

Protocol	Selezionare il tipo di protocollo/modalità e cliccare su **Switch Protocol**. **Nota: Non tutte le opzioni sono disponibili.**
Hostname to send when requesting DHCP	Permette di specificare un nome host per la richiesta DHCP (disponibile se protocol è DHCP Client).
IPv4 address	Indirizzo IP per l'interfaccia.
IPv4 netmask	Subnet Mask per l'interfaccia. Selezionare custom per maschere speciali.
IPv4 gateway	Indirizzo del Gateway per l'interfaccia (opzionale).
IPv4 broadcast	Indirizzo di broadcast per l'interfaccia (opzionale).
Use custom DNS servers	Indirizzi IP dei server DNS specifici. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
IPv6 assignment length	Lunghezza per la parte di indirizzo IPv6. Selezionare disabled per assegnare indirizzi statici.
IPv6 address	Indirizzo IPv6 per l'interfaccia.
IPv6 Gateway	Indirizzo del Gateway IPv6.
IPv6 routed prefix	Prefisso per l'indirizzo IPv6.
IPv6 assignment hint	ID per il sub-prefisso IPv6.
IPv6 suffix	Suffisso IPv6.

3.12.2. Advanced Settings

Bring up on boot	Selezionare per attivare l'interfaccia all'avvio del Router.
Use builtin IPv6-management	Selezionare per usare il protocollo IPv6 nativo.
Force link	Selezionare per attivare le impostazioni dell'interfaccia anche in assenza di link fisico.
Use broadcast flag	Selezionare in caso di specifica richiesta da parte dell'operatore (modalità DHCP Client).
Use default Gateway	Se selezionato imposta una **default route** per l'interfaccia (modalità DHCP Client).
Client ID to send when requesting DHCP	Permette di specificare un Client ID per le richieste DHCP (modalità DHCP Client).
Vendor Class to send when requesting DHCP	Permette di specificare un Vendor class per le richieste DHCP (modalità DHCP Client).
Override MAC address	Permette di specificare per l'interfaccia un MAC address definito dall'utente.
Override MTU	Permette di specificare un valore MTU specifico per l'interfaccia.
Usa gateway metric	Permette di impostare una metrica specifica per l'interfaccia.

3.12.3. Physycal Settings

Bridge interfaces	Selezionare per creare un 'bridge' tra interfacce specifiche
Enable STP	Selezionare per abilitare il protocollo Spanning Tree (in caso di bridging con loop)
Interface	Selezionare le interfacce da associare al bridge, ad esempio LAN e Wi-Fi.

3.12.4. Firewall Settings

Create / Assign firewall-zone	Permette di specificare la Firewall-zone alla quale l'interfaccia è assegnata.

3.12.5. DHCP Server - General Setup

No DHCP Server configured for this interface	Cliccare su **Setup DHCP Server** per attivare il server DHCP per l'interfaccia nel caso non fosse presente.
Ignore interface	Selezionare per **disabilitare** il DHCP server per l'interfaccia.
Start	Primo campo host dell'indirizzo IP da assegnare, ad esempio 100 per 192.168.1.100. Per controllare l'assegnamento degli indirizzi in sequenza oppure casuale impostare **Allocate IP sequentially** nel menu Network DHCP & DNS, Server Settings – Advances Settings.
Limit	Numero massimo di indirizzi IP da assegnare.
Lease time	Durata in ore prima della scadenza dell'assegnazione.

3.12.6. DHCP Server – Advanced Settings

Dynamic DHCP	Abilita assegnazione indirizzi dinamici. **Disabilitare** per assegnare unicamente indirizzi IP host configurati per **assegnamento statico**.
Force	Forza funzionamento DHCP Server anche se viene rilevata la presenza di un altro server in rete.
IPv4-Netmask	Subnet mask non standard da assegnare ai client.
DHCP-Options	Opzioni DHCP. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.12.7. DHCP Server – IPV6 Settings

Router Advertisement-Service	Selezionare il tipo di servizio advertisement (server/relay/hybrid)
DHCPv6-Service	Selezionare il tipo di servizio DHCP (server/relay/hybrid)
NDP-Proxy	Selezionare il tipo di servizio proxy (relay/hybrid)
DHCPv6-Mode	Selezionare la modalità DHCP (stateless/stateful/mista)
Always announce default Router	Selezionare per annunciare il Router come gateway anche in assenza di prefisso pubblico
Announced DNS servers	Lista di DNS server annunciati. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
Announced DNS domains	Lista di Domini DNS annunciati. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.13. OPENVPN

Interfaccia tun0 di sistema.
Non modificare le impostazioni di questa interfaccia pena il malfunzionamento del servizio OpenVPN.

3.14. NETWORK – WIRELESS

Permette di impostare l'interfaccia Wi-Fi del Router.

3.14.1. Wireless Overview

Mostra le informazioni di base dell'interfaccia Wi-Fi attiva.

Edit	Cliccare per modificare le impostazioni dell'interfaccia Wi-Fi.
Disable	Cliccare per disattivare l'interfaccia Wi-Fi. Per riabilitare l'interfaccia cliccare su **Edit** e poi su **Enable**.

3.14.2. Associated Stations

Mostra le informazioni di connessione relative ai client Wi-Fi attivi.

3.14.3. Device Configuration - General Setup

Wireless network is	Cliccare su **Disable** per disattivare l'interfaccia Wi-Fi. Cliccare su **Enable** per attivare l'interfaccia Wi-Fi.
Operating Frequency	Permette di selezionare Modalità, Canale e Larghezza di banda dell'interfaccia Wi-Fi.
Transmit Power	Permette di impostare la potenza di trasmissione, in dBm, dell'interfaccia Wi-Fi.

3.14.4. Device Configuration - Advanced Settings

Country Code	Permette di selezionare il paese in cui il Router è installato, adattandovi le impostazioni per l'interfaccia Wi-Fi.
Distance Optimization	Distanza in metri dal client più lontano (sperimentale).
Fragmentation Threshold	Permette di impostare un valore per F.T.
RTS/CTS Threshold	Permette di impostare un valore per RTS/CTS.T.

3.14.5. Interface Configuration - General Setup

ESSID	SSID (nome) per la rete Wi-Fi.
Mode	Modalità per l'interfaccia Wi-Fi. **Attenzione: non tutte le modalità sono disponibili.**
Network	rete di sistema al quale l'interfaccia Wi-Fi è associata. Non modificare.
Hide SSID	Selezionare per 'nascondere' la rete Wi-Fi.
WMM Mode	Selezionare per permettere la modalità Qos Wi-Fi per dispositivi multimediali.

3.14.6. Interface Configuration – Wireless Security

Encryption	Selezionare il protocollo di sicurezza. E' deprecato l'uso di WEP, molto insicuro.
Cipher	Selezionare il protocollo di cifratura.
Key	Digitare la password Wireless (min. 8, max. 63 caratteri). Modificarla per motivi di sicurezza. Cliccare su per visualizzarla.
802.11r Fast Transition	Selezionare per permettere il roaming Wireless.
802.11w Management Frame Protection	Funzione Non disponibile
Enable WPS pushbutton	Selezionare per abilitare o meno il pulsante WPS.
Radius-Authentication-Server	Indirizzo del server Radius per l'autenticazione.
Radius-Authentication-Port	Porta del server Radius per l'autenticazione.
Radius-Authentication-Secret	Password del server Radius per l'autenticazione (min. 8, max. 63 caratteri). Cliccare su per visualizzarla.

Radius-Accounting-Server	Indirizzo del server Radius per l'accounting.
Radius-Accounting-Port	Porta del server Radius per l'accounting.
Radius-Accounting-Secret	Password del server Radius per l'accounting (min 8, max. 63 caratteri). Cliccare su per visualizzarla.
NAS ID	ID per il Radius NAS.

3.14.7. Interface Configuration – MAC Filter

MAC-Address Filter	Selezionare **disable** per disattivare il filtro sui MAC address dei client Wi-Fi. Selezionare **Allow listed only** per definire una lista di accesso ristretto. Selezionare **All exept listed** per definire una lista di accesso rifiutato.
MAC-List	Inserire il MAC address dell'interfaccia Wi-Fi client. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.14.8. Interface Configuration – Advanced Settings

Isolate clients	Selezionare per impedire che i client Wi-Fi possano comunicare tra di loro.
Interface name	Permette di modificare il nome di sistema dell'interfaccia Wi-Fi (non l'SSID).

3.15. NETWORK - SWITCH

Permette di creare VLAN sulle porte fisiche dello Switch del Router.
Non modificare se non si hanno specifiche competenze in materia.

3.16. NETWORK – DHCP & DNS

3.16.1. Server Settings – General Setup

Domain required	Selezionare per inoltrare richieste DHCP solo se includono il DNS-Name.
Authoritative	Selezionare per imporre che il Router sia l'unico DHCP server sulla rete.
Local server	Dominio locale.
Local domain	Suffisso di dominio locale.
Log queries	Se selezionato inserisce le richieste DNS nel syslog di sistema.
DNS forwardings	Lista di DNS a cui inoltrare le richieste. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
Rebind protection	Selezionare per scartare risposte RFC1918 upstream.
Allow localhost	Selezionare per permettere risposte nel range 127.0.0.0/8.
Domain whitelist	Lista di domini per cui permettere risposte RFC1918. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
Local Service Only	Limitare il servizio DNS alle interfacce del Router.
Non-wildcard	Selezionare per associare il servizio solo a interfacce specifiche.
Listen Interfaces	Lista di interfacce su cui limitare l'ascolto e il loopback. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
Ecxlude Interfaces	Lista di interfacce da escludere dall'ascolto e loopback. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.16.2. Server Settings – Resolv and Host Files

Use /etc/ethers	Selezionare per utilizzare il file /etc/ethers per configurare il DHCP server.
Leasefile	File in cui vengono salvati le lease assegnate.
Ignore resolv file	Selezionare per ignorare il file DNS locale.
Resolve file	Percorso del file DNS locale.
Ignore /etc/hosts	Selezionare per ignorare il file hosts locale.
Additional Hosts files	Lista di file Hosts addizionali. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.

3.16.3. Server Settings – TFTP settings

Enable TFTP server	Selezionare per abilitare il servizio TFTP locale.
TFTP Server root	Percorso dei file per il server TFTP.
Network boot image	Nome file per la boot image servita ai clients.

3.16.4. Server Settings – Advances Settings

Suppress logging	Selezionare per non effettuare il logging di operazioni DHCP e DNS.
Allocate IP sequentially	Selezionare per allocare gli indirizzi IP in modo sequenziale e non random.
Filter private	Selezionare per non inoltrare reverse lookups per reti locali.
Filter useless	Selezionare per non inoltrare richieste che non possono essere servite.
Localise queries	Selezionare per localizzare gli hostname in base alla disponibilità di indirizzi IP della subnet richiesta.
Expand hosts	Selezionare per aggiungere il suffisso di dominio locale per nomi serviti dal file hosts locale.
No negative cache	Selezionare per non fare cache di risposte negative.
Additional servers file	Lista di server DNS addizionali.
Strict order	Selezionare per fare le query ai server DNS nell'ordine specificato nel file resolv.
Bogus NX Domain override	Lista di hosts per forniscono risultato Bogus NX. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
DNS Server port	Porta per le richieste DNS in ingresso.
DNS query port	Porta sorgente per le richieste DNS in uscita.
Max DHCP Leases	Numero massimo di Lease DHCP attive.
Max EDNS0 packet size	Dimensione massima per i pacchetti UDP EDNS.0.
Max concurrent queries	Numero massimo di query DNS concorrenti permesse.

3.16.5. Active DHCP Leases

Informazioni relative ai client DHCP associati al Router, come Nome, Indirizzo IP, MAC address e scadenza dell'assegnazione.

3.16.6. Static Leases

- Cliccare su **Add** per aggiungere un host alla lista degli assegnamenti DHCP statici.

Hostname	Digitare un nome host.
MAC address	Selezionare un MAC address dalla lista nota oppure selezionare **custom** per impostarne uno nuovo.
IPv4 address	Selezionare un indirizzo IP dalla lista nota oppure selezionare **custom** per impostarne uno nuovo.
Lease time	Impostare un Lease time, in ore.
IPv6-Suffix	Impostare un suffisso IPv6, in formato esadecimale.

3.17. NETWORK - HOSTNAMES

Permette di definire dei nomi host per i client di LAN.

- Cliccare su **Add** per aggiungere un host name.
- Cliccare su **Delete** per cancellare un host name.

Hostname	Digitare un nome host.
IP address	Selezionare un indirizzo IP dalla lista nota oppure selezionare **custom** per impostarne uno nuovo.

3.18. NETWORK – STATIC ROUTES

Permette di definire instradamenti statici.

- Cliccare su **Add** per aggiungere una route statica.
- Cliccare su **Delete** per cancellare una route statica.

Interface	Selezionare l'interfaccia per la quale si crea l'instradamento statico.
Target	Inserire l'indirizzo host o della rete di destinazione.
IP Netmask	Inserire la maschera di rete (in caso di rete).
IP Gateway	Indirizzo IP del gateway che instrada verso la destinazione.
Metric	Inserire una metrica per la route.
MTU	Inserire un valore MTU per il tipo di route.
Route type	Selezionare il tipo di advertising per la route.

3.19. NETWORK - FIREWALL

3.19.1. General Settings

Enable SYN-flood protection	Selezionare per abilitare la protezione da attacchi DDOS di tipo Syn-flood.
Drop invalid packets	Selezionare per abilitare il blocco di pacchetti considerate non validi.
Input	Selezionare la regola di base per i pacchetti in ingresso nelle zone del firewall.
Output	Selezionare la regola di base per i pacchetti in uscita dalle zone del firewall.
Forward	Selezionare la regola di base per i pacchetti di inoltro tra le zone del firewall.

3.19.2. Zones

Regole di inoltro tra le zone del firewall. Non modificare queste impostazioni.

3.19.3. Port Forwards

Permette di creare regole di Port Forwarding e fornire l'accesso a risorse e host di LAN da parte di computers esterni alla rete.

- Cliccare su **Add** per aggiungere una regola di Port Forwarding.
- Cliccare su **Delete** per cancellare una regola di Port Forwarding.
- Cliccare su **Edit** per modificare una regola di Port Forwarding.
- Selezionare **Enable** per abilitare la regola di Port Forwarding. Deselezionare **Enable** per disabilitare la regola di Port Forwarding. Cliccare su **Save** per confermare l'impostazione.
- Cliccare sul **pulsante di direzione** per spostare la regola in su o in giù nella lista (Sort).

Name	Inserire un nome mnemonico per la regola.
Protocol	Selezionare il protocollo in uso dal servizio.
External zone	Selezionare la zona o interfaccia esterna attraverso la quale dare accesso al servizio.
External port	Porta esterna attraverso la quale dare accesso al servizio.
Internal zone	Selezionare la zona o interfaccia interna su cui risiede il servizio.
Internal IP address	Selezionare l'indirizzo IP dell'host che fornisce il servizio. Selezionare custom per inserirne uno nuovo.
Internal port	Porta dell'host sulla quale è attivo il servizio.

NOTA: Una volta creata la regola di Port Forwarding è possibile personalizzarla ulteriormente (vedere parametri di Traffic Rules).

3.19.4. Traffic Rules

Permette di creare regole che sovraintendono al transito di pacchetti tra le varie zone del firewall, per restringere il traffico o aprire l'accesso a servizi sulle interfacce WAN.

- Cliccare su **Add** per aggiungere una regola.
- Cliccare su **Delete** per cancellare una regola.
- Cliccare su **Edit** per modificare una regola.
- Cliccare sul **pulsante di direzione** per spostare la regola in su o in giù nella lista (Sort).
- Selezionare **Enable** per abilitare la regola. Deselezionare **Enable** per disabilitare la regola. Cliccare su **Save** per confermare l'impostazione.

Open ports on Router

Permette l'ingresso di traffico proveniente dall'esterno, specificandone il protocollo e la porta.

Name	Digitare un nome mnemonico per la regola.
Protocol	Selezionare il protocollo.
External port	Porta esterna attraverso la quale dare accesso al servizio.

- Cliccare su **Add** per aggiungere una regola.

NOTA: Una volta creata la regola è possibile personalizzarla ulteriormente (vedere Parametri di personalizzazione delle regole).

New forward rules

Permette di inoltrare del traffico da una zona sorgente ad una di destinazione.

Name	Digitare un nome mnemonico per la regola.
Source zone	Selezionare la Zona di origine del traffico.
Destination zone	Selezionare la Zona di destinazione del traffico.

- Cliccare su **Add** and **Edit** per aggiungere una regola dopo averla eventualmente ulteriormente personalizzata (vedere Parametri di personalizzazione delle regole).

3.19.5. Source NAT

Permette di creare regole che modificano la sorgente dei pacchetti in uscita, per assegnare il traffico a zone o interfacce WAN in modo NATtato.

Name	Digitare un nome mnemonico per la regola.
Source zone	Selezionare la Zona di origine del traffico.
Destination zone	Selezionare la Zona di destinazione del traffico.
To source IP	Selezionare dalla lista l'indirizzo IP (che diventerà sorgente) sul quale rimappare il traffico in uscita. Selezionare custom per inserirne uno nuovo. Selezionare 'Do not rewrite' per non modificarlo.
To source Port	Inserire la porta (che diventerà sorgente) sulla quale rimappare il traffico in uscita. Lasciare in bianco per non modificarla.

- Cliccare su **Add** and **Edit** per aggiungere una regola dopo averla eventualmente ulteriormente personalizzata (vedere Parametri di personalizzazione delle regole).

Parametri di personalizzazione delle regole

Rule is enabled/disabled	Cliccare su **Enable/Disable** per abilitare/disabilitare la regola.
Name	Digitare un nome mnemonico per la regola.
Restrict to address family	Selezionare la versione di protocollo IP.
Protocol	Selezionare il protocollo.
Match ICMP type	Lista di pacchetti ICMP. Cliccare su **+** per aggiungere un elemento, cliccare su **X** per rimuovere un elemento.
Source zone	Selezionare la Zona di origine del traffico.
Source MAC address	Selezionare dalla lista il MAC address sorgente del traffico. Selezionare **custom** per inserirne uno nuovo.
Source address	Selezionare dalla lista l'indirizzo IP sorgente del traffico. Selezionare **custom** per inserirne uno nuovo.
Source port	Inserire la porta sorgente del traffico oppure **any** per qualsiasi.
Destination zone	Selezionare la Zona di destinazione del traffico.
Destination address	Selezionare dalla lista l'indirizzo IP di destinazione del traffico. Selezionare **custom** per inserirne uno nuovo.
Destination port	Inserire la porta di destinazione del traffico oppure **any** per qualsiasi.
SNAT IP address	Solo per Source NAT. Selezionare dalla lista l'indirizzo IP (che diventerà sorgente) sul quale rimappare il traffico in uscita. Selezionare **custom** per inserirne uno nuovo. Selezionare '**Do not rewrite**' per non modificarlo.
SNAT port	Solo per Source NAT. Inserire la porta (che diventerà sorgente) sulla quale rimappare il traffico in uscita. Lasciare in bianco per non modificarla.
Action	Selezionare l'azione per la regola, tra accept, reject, drop, don't track.
Extra arguments	Argomenti extra per iptable. Usare con cautela.
Week Days	Selezionare i giorni della settimana per cui la regola è attiva.
Month Days	Selezionare i giorni del mese per cui la regola è attiva.
Start Time (hh:mm:ss)	Inserire l'ora di inizio validità per la regola.
Stop Time (hh:mm:ss)	Inserire l'ora di fine per la regola.
Start Date (yyyy-mm-dd)	Inserire la data di inizio per la regola.
Stop Date (yyyy-mm-dd)	Inserire la data di fine per la regola.
Time in UTC	Selezionare per definire l'orario in formato UTC.

3.19.6. Custom Rules

Permette di eseguire comandi iptables arbitrari che non sono altrimenti coperti dal firewall.
I comandi sono eseguiti ad ogni riavvio del firewall, subito dopo il caricamento del set di regole di default.

- Cliccare su **Restart Firewall** per riavviare il firewall.

3.20. NETWORK - DIAGNOSTICS

Permette di eseguire delle verifiche diagnostiche di raggiungibilità, instradamento e risoluzione di indirizzi.

Ping	Selezionare il protocollo IPv4 o IPv6. Cliccare per avviare un PING all'indirizzo inserito.
Traceroute	Selezionare il protocollo IPv4 o IPv6. Cliccare per avviare un TRACEROUTE all'indirizzo inserito.
Nslookup	Selezionare il protocollo IPv4 o IPv6. Cliccare per avviare un NSLOOKUP dell'indirizzo inserito.

3.21. NETWORK – QOS

Permette di creare regole per la gestione prioritaria del traffico in base a porte, indirizzi e servizi.

3.21.1. Interfaces

- Cliccare su **Add** dopo aver inserito un nome mnemonico per aggiungere una nuova regola di priorità.
- Cliccare su **Delete** per cancellare una regola di priorità.
- Cliccare sul **pulsante di direzione** per spostare la regola in su o in giù nella lista (Sort).

3.21.2. WAN

Enable	Selezionare per abilitare la regola.
Classification group	Gruppo default.
Calculate overhead	Selezionare per calcolare anche l'overhead di protocollo.
Half-duplex	Selezionare per considerare solo il traffico in un senso.
Download speed (kbit/s)	Impostare la massima velocità di download.
Upload speed (kbit/s)	Impostare la massima velocità di upload.

3.21.3. Classification Rules

Target	Selezionare un livello di priorità per la regola tra Priority (massima), Express (alta), Normal (normale), Low (bassa).
Source host	Selezionare dalla lista l'indirizzo IP sorgente del traffico. Selezionare **custom** per inserirne uno nuovo. Inserire **all** per 'tutti'.
Destination host	Selezionare dalla lista l'indirizzo IP di destinazione del traffico. Selezionare **custom** per inserirne uno nuovo. Inserire **all** per 'tutti'.
Protocol	Selezionare dalla lista il protocollo del traffico. Selezionare **custom** per inserirne uno diverso. Inserire **all** per 'tutti'.
Ports	Selezionare dalla lista la porta utilizzata dal traffico. Selezionare **custom** per inserirne una o più diverse, separate da virgola. Inserire **all** per 'tutte'.
Number of bytes	Inserire la dimensione del pacchetto in bytes.
Comment	Inserire un commento mnemonico per la regola.
Sort	Cliccare sul **pulsante di direzione** per spostare la regola in su o in giù nella lista.

3.22. LOGOUT

- Cliccare per **terminare la sessione** di configurazione e tornare alla finestra di Login.

3.23. FUNZIONE DI BACKUP AUTOMATICO

Il Router può effettuare il backup automatico della connessione primaria in caso di sopravvenuta assenza di connettività di questa. Per assenza di connettività di definisce l'impossibilità di raggiungere degli host di cui viene impostato l'indirizzo IP attraverso il comando CLI SETPINGMON.
Il meccanismo che sovraintende alla funzione di Backup è denominato **Network PING Control (NPC)**.

3.23.1. Criteri di determinazione della connettività

Il meccanismo NPC effettua dei PING, con tempistiche e sequenze sotto definite, ad uno o più destinatari e ne controlla la risposta.

In caso di totale assenza di risposta può:
- Attivare un backup sull'interfaccia secondaria (vedere impostazioni SETWANBKP)
- Effettuare un riavvio (Reboot) del Router al fine di ripristinare il funzionamento da 'zero'.

Attivazione Backup (Fail-over) o riavvio

1. Ad intervalli regolari definiti dal paramento **Periodic Ping Interval** (PPI) il Router invia una serie di 4 PING (PS) al primo indirizzo destinatario definito dal parametro **Destination Host1** (DH1).

2. Se tutti i PING della sequenza PS falliscono il Router ne invia una sequenza al secondo indirizzo destinatario definito dal parametro **Destination Host2** (DH2).

3. Il Router a quel punto inizia ad inviare, con tempistica definita da **Ping Retry Timer** (PRT), sequenze PS a DH1 e DH2.

4. Se tutti i PING del punto 3 falliscono, per un numero di volte definito in **Maximum Failures** (MF), allora il Router, a seconda delle impostazioni del comando SETWANBKP) attiva l'interfaccia secondaria oppure effettua un riavvio.

Se almeno uno dei PING dei punti 1 o 2 vanno a buon fine, il ciclo ricomincia dal punto 1 e non viene intrapresa alcuna azione di backup o riavvio.

Ripristino interfaccia primaria (Fail-back)

Una volta attivato il backup sull'interfaccia secondaria il meccanismo NPC monitorizza l'eventuale ripristino della connettività dell'interfaccia primaria. Se questa si ripristina il Router effettua un Fail-back, ritornando sull'interfaccia primaria.

Mancata connettività sull'interfaccia secondaria al momento del Fail-over)

Se il meccanismo NPC rileva l'impossibilità di attivare l'interfaccia secondaria oppure l'assenza di connettività su quest'ultima, allora effettua un riavvio (Reboot).

3.24. FUNZIONE DI ATTIVAZIONE REMOTA E CONTROLLO VIA SMS

Il Router dispone della funzione di attivazione remota che permette, ad esempio, di attivare la connessione 3G/4G inviandogli un SMS contenente un testo opportunamente formattato.
Via SMS è anche possibile disattivare la connessione, richiederne lo stato attuale oppure forzare un riavvio del Router.
Per utilizzare la funzione di attivazione remota via SMS è necessario Impostare la **modalità Manuale** di connessione (vedere comando SETDIALMODE).
Il comando di connessione attiva la connettività 3G/4G ed in caso di inattività dati questa viene abbattuta automaticamente un **Timeout di 600 sec**.
I comandi disponibili sono:
- **<Codice SMS> connect** per richiedere (o prolungare) la connessione, ad esempio 1234 CONNECT
- **<Codice SMS> disconnect** per chiedere la disconnessione, ad esempio 1234 DISCONNECT
- **<Codice SMS> status** per chiedere lo stato attuale della connessione, ad esempio 1234 STATUS
- **<Codice SMS> reboot** per forzare il riavvio del Router, ad esempio 1234 REBOOT

NOTE:
- **Tra Codice SMS e comando c'è uno spazio.**
- **Il comando è Case Insensitive, può essere digitato sia maiuscolo che minuscolo.**
- **Se un SMS inviato al Router non inizia con un codice numerico di sole 4 cifre oppure il codice è errato l'SMS viene ignorato e non ci sarà alcuna risposta ad esso.**

Comandi disponibili

Connessione	**<Codice SMS> CONNECT**
Esempio comando	**1234 CONNECT**
Parametri	nessuno
Risposta al comando	Connected. WAN IP is x.x.x.x. Timeout is xxx sec. Connection failed! (se non connesso entro 120 sec)
Esempio Risposta	Connected. WAN IP is 2.93.69.251. Timeout is 258 sec.
Interrogazione	Vedere funzione **Stato** NOTA: Se il dispositivo è già connesso, alla ricezione del comando CONNECT il **Timeout** viene **reinizializzato** al valore massimo (600 sec).

Sconnessione	**<Codice SMS> DISCONNECT**
Esempio comando	**1234 DISCONNECT**
Parametri	nessuno
Risposta al comando	Disconnected
Esempio Risposta	Disconnected
Interrogazione	Vedere funzione Stato

Stato	**<Codice SMS> STATUS**
Esempio comando	**1234 STATUS**
Parametri	nessuno
Risposta al comando	Disconnected Connected. WAN IP is x.x.x.x. Timeout is xxx sec.
Esempio Risposta	Disconnected Connected. WAN IP is 2.93.69.251. Timeout is 258 sec.
Interrogazione	Non prevista

Riavvio	**<Codice SMS> REBOOT**
Esempio comando	**1234 REBOOT**
Parametri	nessuno
Risposta al comando	OK:REBOOT ERROR:REPOOT (errore sintattico oppure riavvio non possibile per cause di sistema)
Esempi Risposta	OK:REBOOT ERROR:REBOOT
Interrogazione	Non prevista

3.25. IMPOSTAZIONI DI FABBRICA (FACTORY DEFAULT)

Di seguito sono riportate le impostazioni di fabbrica dei parametri di funzionamento del Router.

Le impostazioni di fabbrica possono essere ripristinate in due modi:

- **Hardware**: Agendo sul pulsante di Reset (vedere capitolo Porte e Connettori)
- **Software**: Attraverso il menu **System/Backup Flash Firmware** dell'interfaccia di configurazione Web, cliccando su Reset to Defaults: **Perform Reset**

NETWORK	Descrizione / Note
IP LAN: 192.168.1.1	
SUBNET MASK: 255.255.255.0	
Login user: root	
Login password: nessuna	
Wi-Fi attivo: SI	
SSID: Digicom4G_xxxx	xxxx=ultimi 4 digit del MAC Address
WPA2 PSK: digicom4g	Modificare la PSK per motivi di sicurezza

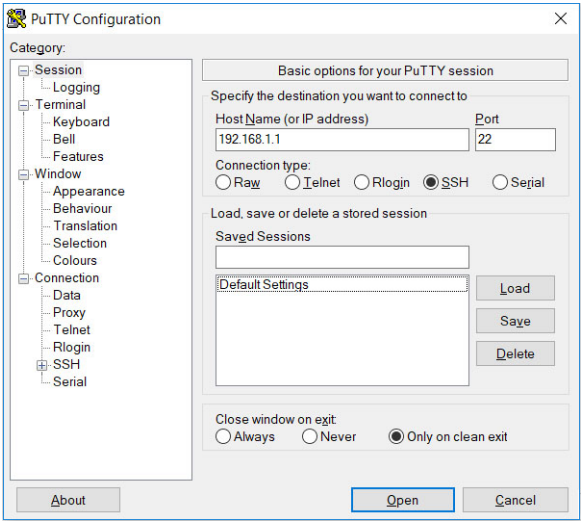
CONFIGURAZIONE	Descrizione / Note
Porta Web UI: 80	
Porta Console SSH: 22	
SSH attivo: solo LAN	

ATTIVAZIONE REMOTA	Descrizione / Note
Attivazione remota via SMS	Abilitata
Codice per SMS: 1234	
Connection Timeout per SMS: 600 sec	

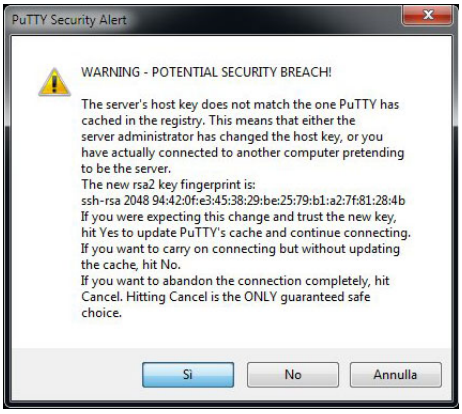
COMANDI	Descrizione / Note
SETAPN ibox.tim.it	TIM
SETDIALMODE *99#,,,none,auto	No autenticazione, always on
SETMOBILE auto,noroam	3G/4G, Roaming disabilitato
SETSREBOOT 0,0,0	Nessun reboot schedulato
SETPINGMON 120,30,3,8.8.8.8,8.8.4.4	PING monitor ogni 2 minuti, 3 tentativi
SETWANBKP LTE,0	Interfaccia principale LTE, Backup disattivo

Esempio di accesso alla console CLI SSH tramite PuTTY

- Lanciare l'applicativo **Putty**
- Impostare
  - Host Name -> **192.168.1.1** (oppure l'indirizzo IP di LAN del Router4G)
  - Port -> **22**
  - Connection Type -> **SSH**
  - Cliccare su **Open**

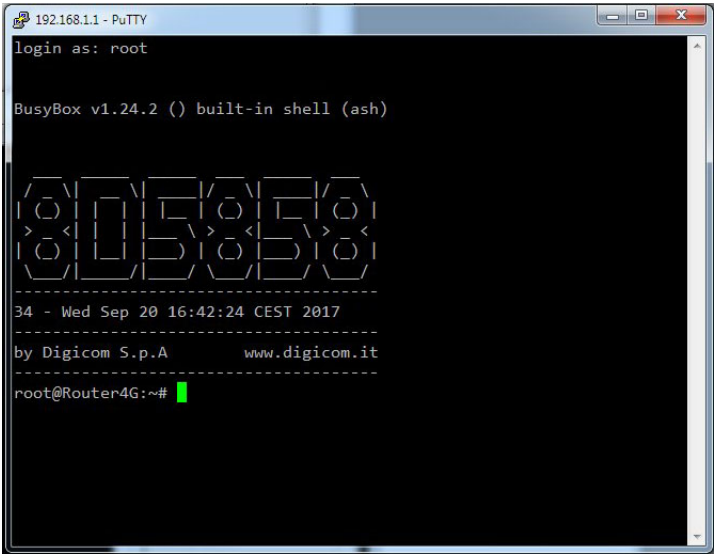


- Cliccare su **Si** per accettare la chiave di crittografia, se mostrata.



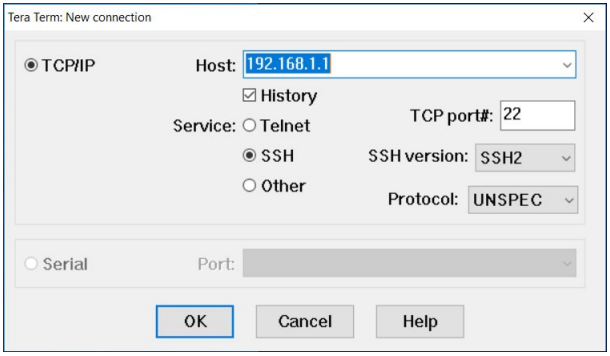
- Si aprira una finestra con la richiesta di immissione delle **credenziali per il login**.
- Digitare la **username** e la **password** e premere **Invio**.

- Apparirà il **messaggio di benvenuto** seguito dal **prompt**.

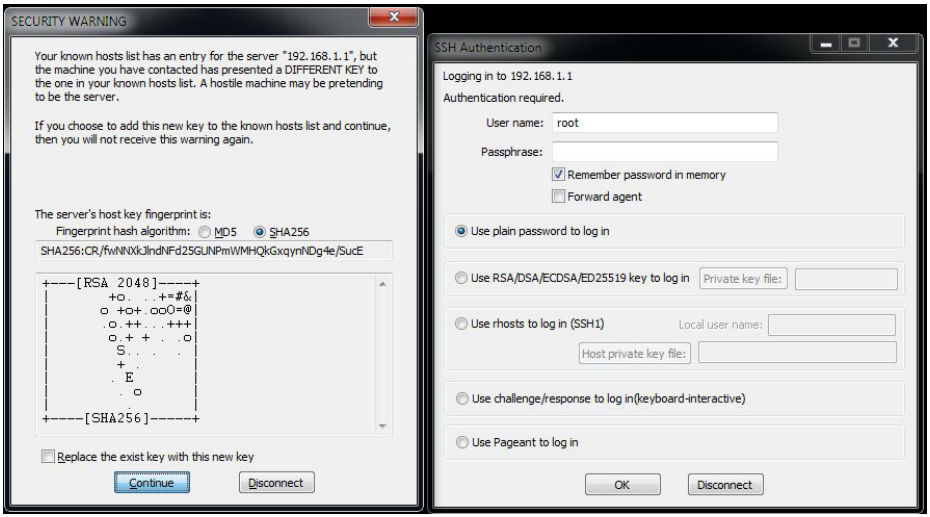


Esempio di accesso alla console CLI SSH tramite TeraTerm

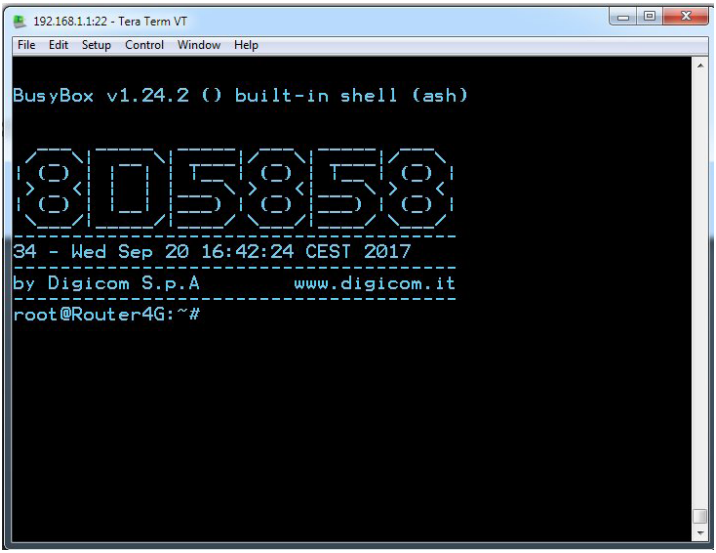
- Lanciare l'applicativo **TeraTerm**.
- Selezionare il menu **File, New Connection** ed impostare
  - TCP/IP
  - Host: -> **192.168.1.1** (oppure l'indirizzo IP di LAN del Router4G)
  - TCP Port# -> **22**
  - Service -> **SSH**
  - Cliccare su **OK**



- Nella finestra successiva digitare le credenziali **Username** e **Passphrase** di accesso al Router4G e premere cliccare su **OK**
- Cliccare su **Continue** per accettare la chiave di crittografia, se mostrata.
  (In caso di errore selezionare **Replace the existing key with this new key** e ripetere l'operazione.)



- Apparirà il **messaggio di benvenuto** seguito dal **prompt**.



4. SICUREZZA DELLA RETE

Ti sei ricordato di cambiare la password di accesso alla configurazione?

Lasciare la **password di fabbrica invariata**, sia che si tratti di quella di login alla configurazione piuttosto che di quella di accesso alla rete Wi-Fi, **può lasciarti esposto ad intrusioni malevole da parte di hackers o bot automatici** in circolazione su Internet che sfruttano attacchi standardizzati.
Se non lo hai ancora fatto mettiti subito al riparo da questo tipo di problemi modificando la password di admin, root o Wi-Fi.

Per le password di login scegline una sufficientemente complessa e difficile da indovinare; per le password Wi-Fi usa combinazioni di lettere, numeri e caratteri speciali; se non utilizzi servizi per l'accesso remoto alla tua rete o al tuo Router disattivali (WPS, HTTP, Telnet, SSH…).
Le tecniche di hacking sono in continua evoluzione ed ogni giorno più potenti e sofisticate ma questi piccoli accorgimenti basilari costituiscono la prima **linea di difesa per il tuo dispositivo** di comunicazione e la tua rete!

digicom

Digicom S.p.A.
Italy - Via Alessandro Volta 39
21010 Cardano al Campo -VA
Tel +39 0331 702611
Fax +39 0331 263733
http://www.digicom.it