



Configurazione WL-R220L

ELSIST S.r.l.
Sistemi in elettronica

*Via G. Brodolini, 15 (Z.I.)
15033 CASALE M.TO
ITALY*

*Internet: <http://www.elsist.it>
Email: elsist@elsist.it*

*TEL. (39)-0142-451987
FAX (39)-0142-451988*

INDICE

1 Configurazione WL-R220L Router 4G LTE OpenWrt con I/O.....	2
1.1 Come configurare il router.....	2
1.2 Riconfigurare il router a default.....	2
Pag. 10/10.....	2
2 Connessione alla rete cellulare.....	3
3 Configurazione firewall.....	4
4 Upgrade firmware.....	4
5 Installazione applicazioni.....	5
6 Installazione ZeroTier.....	6
6.1 File “/etc/config/network”.....	6
6.2 File “/etc/config/firewall”.....	7
6.3 File “/etc/config/dhcp”.....	10

1 Configurazione WL-R220L Router 4G LTE OpenWrt con I/O

Il [WL-R220L 4G OpenWrt](#) è un router cellulare industriale M2M (Machine to Machine) che può funzionare su rete cellulare 4G/3G per fornire connettività wireless affidabile, sicura e ad alta velocità con I/O e VPN supportati. Si tratta di un dispositivo industriale potente e programmabile con prestazioni elevate e involucro robusto progettato per la gestione remota, la telemetria, il monitoraggio delle condizioni, CCTV, bancomat, distributori automatici e altre applicazioni M2M.

OpenWrt è una distribuzione Linux per router; offre un gestore di pacchetti software integrato che consente di installare il pacchetto da un repository software. Il router viene configurato utilizzando un'interfaccia web (LuCI). I clienti possono personalizzare il dispositivo per adattarlo alle proprie necessità.



1.1 Come configurare il router

Inserire la SIM 2 (A router spento), per iniziare meglio che la SIM non abbia alcun PIN, eventualmente inserirla in un telefono ed eliminare il PIN. Accendere il router che ha di default ha indirizzo 192.168.1.1 ed il server DHCP attivo, connettendosi in ethernet (Porta LAN) con un PC, digitando da browser l'indirizzo IP (192.168.1.1), si verrà reindirizzati alla pagina di login. Le credenziali di accesso di default sono utente "root" nessuna password. Nella pagina Status->Overview sono riportate le informazioni sulla versione del software.

System	
Hostname	OpenWrt
Model	Mediatek MT7628AN evaluation board
Architecture	MediaTek MT7628AN ver:1 eco:2
Firmware Version	OpenWrt 18.06.9 r8077-7cbbab7246 / LuCI openwrt-18.06 branch (git-21.041.07147-20b3600)
Kernel Version	4.14.206

E' possibile connettersi anche in SSH o da porta seriale RS232, il router implementa l'interfaccia BusyBox un semplice tool, che permette di gestire tutti i comandi e gli strumenti più utili del mondo Unix. Per un elenco dei comandi possibili rimando alla documentazione OpenWrt reperibile su Internet.

1.2 Riconfigurare il router a default

Per riconfigurare il router a default dalla pagina System->Backup agire sul tasto Perform reset. Da connessione SSH o seriale è possibile eseguire il comando jffs2reset, che eseguirà la cancellazione e riformattazione dell'intera partizione jffs2, creandola nuovamente.

```
umount /overlay && jffs2reset && reboot now
```

To restore configuration files, you can upload a previously generated backup

Reset to defaults:

2 Connessione alla rete cellulare

Verificare se nella pagina delle interfacce è presente l'interfaccia LTE in caso contrario occorre definirla.

1. Con il tasto Add new interface creare la nuova interfaccia.
2. Definire il nome dell'interfaccia (Esempio LTE) di tipo QMI Cellular.
3. Selezionare il dispositivo /dev/cdc-wdm0 e l'autenticazione PAP/CHAP.
4. Dopo avere salvato le impostazioni, eseguire il reboot del router e verificare se l'interfaccia è configurata.
5. Eseguire un ping per verificare la connessione alla rete.

Screenshot 1: Shows the 'Interfaces' section of the OpenWrt configuration interface. It lists three interfaces: LAN (br-lan), WAN (eth0.2), and WAN6 (eth0.2). The LAN interface is highlighted with a red box. Below the interface list is a button labeled 'Add new interface...'.

Screenshot 2: Shows the 'Create Interface' form. The 'Protocol of the new interface' dropdown is set to 'QMI Cellular'. The 'Name of the new interface' dropdown is set to 'LTE'. The 'Authentication Type' dropdown is set to 'PAP/CHAP (both)'. At the bottom are 'Save & Apply', 'Save', and 'Reset' buttons.

Screenshot 3: Shows the 'Interfaces - LTE' configuration page. It displays the 'Common Configuration' section with fields for 'Protocol' (QMI Cellular), 'Modem device' (/dev/cdc-wdm0), 'APN', 'PIN', 'PAP/CHAP username', and 'PAP/CHAP password'. A status box shows details for the 'Device: wwan0' interface. Below the configuration are 'General Setup', 'Advanced Settings', and 'Firewall Settings' tabs.

Screenshot 4: Shows the 'Interfaces' section again, but now includes a new interface entry for 'LTE' (wwan0). Other interfaces listed are 'WAN' (eth0.2) and 'WAN6' (eth0.2).

Screenshot 5: Shows the 'Diagnostics' section with the 'Network Utilities' tab selected. A 'Ping' button is highlighted with a red box. The results of a ping to 'openwrt.org' are displayed, showing 5 packets transmitted, 0% packet loss, and round-trip times.

3 Configurazione firewall

Per permettere ai dispositivi connessi al router l'accesso ad Internet occorre configurare il firewall.

1. Con il tasto Add definire una nuova zona.
2. Definire il nome alla zona (Esempio Ite), ed impostarne le opzioni aggiungendo alla zona il dispositivo LTE.
3. Definire tramite i pulsanti Edit le regole di forwarding tra le zone.

The figure consists of three screenshots of the OpenWrt web interface, labeled 1, 2, and 3, illustrating the steps to configure a new firewall zone:

- Screenshot 1:** Shows the "Firewall - Zone Settings" page. A red box highlights the "Add" button at the bottom left.
- Screenshot 2:** Shows the "Firewall - Zone Settings - Zone 'newzone'" page. A red box highlights the "Name" field set to "lte". A dropdown menu under "Covered networks" shows "LTE" selected. A red box highlights the "Forward" dropdown set to "reject".
- Screenshot 3:** Shows the "Zones" table. It lists three zones: "lan" (forwarding to "wan" with "accept" rules), "wan" (forwarding to "lan" with "reject" rules), and "lte" (forwarding to "lan" with "accept" rules). A red box highlights the "Forward" dropdown for the "wan" zone set to "reject".

4 Upgrade firmware

OpenWRT è una distribuzione Linux specifica per dispositivi embedded, si hanno sempre nuove versioni disponibili. Per poter utilizzare le nuove versioni occorre eseguire l'upgrade del firmware, l'operazione si esegue semplicemente da pagina web.

Consiglio di mettere il tick sulla voce Keep settings per mantenere tutte le impostazioni, durante l'upgrade del firmware occorre garantire l'alimentazione attiva.

The figure shows the "Actions" menu open, with "Configuration" selected. Under "Configuration", a red box highlights the "Backup / Restore" option. The "Backup / Restore" section includes fields for "Restore backup" (with "Choose File" and "Upload archive...") and "Flash new firmware image" (with "Keep settings" checked, "Image" field, and "Flash image" button).

5 Installazione applicazioni

Il vantaggio di utilizzare OpenWRT è di poter disporre di una enorme libreria di programmi eseguibili (Ad oggi sono più di 6000). La gestione dei pacchetti può essere fatta semplicemente da pagina web, dal menù Software è possibile gestire i pacchetti installati eseguendone l'upgrade o la disinstallazione, oppure installare nuovi pacchetti.

Naturalmente come tutti i sistemi Linux la manutenzione del software è possibile anche da linea di comando, accedendo dalla console SSH. Il comando:

- opkg update Esegue l'aggiornamento dai repository delle applicazioni disponibili.
- opkg install packagename Esegue l'installazione di un pacchetto software (Applicazione).
- opkg remove packagename Esegue la disinstallazione di un pacchetto software (Applicazione).

	Package name	Version	Size (.ipk)	Description
Install	acl	20160519-1	17239	Access control list support This package chacl - getfacl - setfacl
Install	acme	1.6-3	36082	A client for issuing Letsencrypt certificate
Install	zerotier	1.2.4-2	356990	ZeroTier creates a global provider-indepe

6 Installazione ZeroTier

ZeroTier interconnette tramite Internet dispositivi dislocati geograficamente, permettendone l'accesso con un proprio indirizzo IP come se virtualmente connessi alla propria rete ethernet.

Sul router WL-R220L andremo ad installare il client per OpenWRT, l'installazione è estremamente semplice accedere al menù System -> Software, se non è già stata eseguito eseguire il comando Update lists che si collega al repository ed aggiorna tutti i pacchetti che è possibile installare sul router. Nel TAB Available packages alla lettera "Z" è possibile trovare il client zerotier cliccando sulla voce install verrà installato. Terminata l'installazione trovare il pacchetto all'interno del TAB Installed packages. Ora occorre editare il file di configurazione, da connessione SSH con vi /etc/config/zerotier definendo l'ID di rete.

```
list join 'xxxxxxxxxxxxxxxxxxxx'
```

Definito l'ID di rete occorre eseguire il restart del servizio con il comando /etc/init.d/zerotier restart, ora è possibile verificare dal portale ZeroTier tramite la dashboard di rete l'avvenuta connessione rilevando l'IP assegnato al dispositivo.

Di seguito riporto un esempio dei files di configurazione da trasferire sul router, i files si trovano nella cartella /etc/config, per trasferirli sul router occorre utilizzare una connessione in SFTP (Personalmente utilizzo MobaXterm). Prima di trasferirli occorre eseguire le modifiche per adattarli alle proprie esigenze.

6.1 File “/etc/config/network”

```
# -----
# GLOBAL CONFIGURATION
# -----


config globals 'globals'
    option ula_prefix 'fd87:9c82:8292::/48'

# -----
# INTERFACE CONFIGURATION
# -----


config interface 'loopback'
    option ifname 'lo'
    option proto 'static'
    option ipaddr '127.0.0.1'
    option netmask '255.0.0.0'

# Definire indirizzo IP che si vuole assegnare alla porta ethernet del router.

config interface 'lan'
    option type 'bridge'
    option ifname 'eth0.1 eth1'
    option proto 'static'
    option ipaddr '192.168.1.1'
    option netmask '255.255.255.0'
    option ip6assign '60'

# Definire APN del gestore di telefonia utilizzato.

config interface 'wan'
    option proto '3g'
    option service 'umts'
    option ipv6 'auto'
    option device '/dev/ttyUSB3'
    option apn 'apn.fastweb.it'

config interface 'wan6'
    option ifname 'eth0.2'
    option proto 'dhcpv6'
```

```
config interface 'zerotier'
    option proto 'dhcp'
    option ifname 'zt0'
```

```
# -----
# SWITCH CONFIGURATION
# -----
```

```
config switch
    option name 'switch0'
    option reset '1'
    option enable_vlan '1'
```

```
config switch_vlan
    option device 'switch0'
    option vlan '1'
    option vid '1'
    option ports '0t 1 2 5'
```

6.2 File “/etc/config/firewall”

```
# -----
# DEFAULT CONFIGURATION
# -----
```

```
config defaults
    option syn_flood '1'
    option input 'ACCEPT'
    option output 'ACCEPT'
    option forward 'REJECT'
# Uncomment this line to disable ipv6 rules
#     option disable_ipv6 1
```

```
# -----
# ZONE CONFIGURATION
# -----
```

```
config zone
    option name 'lan'
    option network 'lan'
    option input 'ACCEPT'
    option output 'ACCEPT'
    option forward 'ACCEPT'
    option masq '1'
```

```
config zone
    option name 'wan'
    option network 'wan wan6'
    option input 'REJECT'
    option output 'ACCEPT'
    option forward 'REJECT'
    option mtu_fix '1'
```

```
config zone
    option name 'zerotier'
    option network 'wan wan6 zerotier'
    option input 'ACCEPT'
    option output 'ACCEPT'
    option forward 'ACCEPT'
    option device 'zt0'
    option mtu_fix '1'
```

```
# -----
# FORWARDING
# -----



config forwarding
    option src 'lan'
    option dest 'wan'

config forwarding
    option src 'lan'
    option dest 'zerotier'

config forwarding
    option src 'zerotier'
    option dest 'lan'

# -----
# FIREWALL RULES
# -----
# Firewall rule definitions.



config rule
    option name 'Allow-DHCP-Renew'
    option src 'wan'
    option proto 'udp'
    option dest_port '68'
    option target 'ACCEPT'
    option family 'ipv4'

config rule
    option name 'Allow-Ping'
    option src 'wan'
    option proto 'icmp'
    option icmp_type 'echo-request'
    option family 'ipv4'
    option target 'ACCEPT'

config rule
    option name 'Allow-IGMP'
    option src 'wan'
    option proto 'igmp'
    option family 'ipv4'
    option target 'ACCEPT'

config rule
    option name 'Allow-DHCPv6'
    option src 'wan'
    option proto 'udp'
    option src_ip 'fc00::/6'
    option dest_ip 'fc00::/6'
    option dest_port '546'
    option family 'ipv6'
    option target 'ACCEPT'

config rule
    option name 'Allow-MLD'
    option src 'wan'
    option proto 'icmp'
    option src_ip 'fe80::/10'
    list icmp_type '130/0'
    list icmp_type '131/0'
```

```
list icmp_type '132/0'
list icmp_type '143/0'
option family 'ipv6'
option target 'ACCEPT'

config rule
    option name 'Allow-ICMPv6-Input'
    option src 'wan'
    option proto 'icmp'
    list icmp_type 'echo-request'
    list icmp_type 'echo-reply'
    list icmp_type 'destination-unreachable'
    list icmp_type 'packet-too-big'
    list icmp_type 'time-exceeded'
    list icmp_type 'bad-header'
    list icmp_type 'unknown-header-type'
    list icmp_type 'router-solicitation'
    list icmp_type 'neighbour-solicitation'
    list icmp_type 'router-advertisement'
    list icmp_type 'neighbour-advertisement'
    option limit '1000/sec'
    option family 'ipv6'
    option target 'ACCEPT'

config rule
    option name 'Allow-ICMPv6-Forward'
    option src 'wan'
    option dest '*'
    option proto 'icmp'
    list icmp_type 'echo-request'
    list icmp_type 'echo-reply'
    list icmp_type 'destination-unreachable'
    list icmp_type 'packet-too-big'
    list icmp_type 'time-exceeded'
    list icmp_type 'bad-header'
    list icmp_type 'unknown-header-type'
    option limit '1000/sec'
    option family 'ipv6'
    option target 'ACCEPT'

config rule
    option name 'Allow-ESP-Forward'
    option src 'wan'
    option dest 'lan'
    option proto 'esp'
    option target 'ACCEPT'

config rule
    option name 'Allow-L2TP/IPSec-Forward'
    option src 'wan'
    option dest 'lan'
    option dest_port '500 4500'
    option proto 'udp'
    option target 'ACCEPT'

# -----
# FIREWALL USER CONFIGURATION
# -----
# Include a user configuration

config include
    option path '/etc/firewall.user'
```

6.3 File “/etc/config/dhcp”

```
config dnsmasq
    option domainneeded '1'
    option boguspriv '1'
    option filterwin2k '0'
    option localise_queries '1'
    option rebind_protection '1'
    option rebind_localhost '1'
    option local '/lan/'
    option domain 'lan'
    option expandhosts '1'
    option nonegcache '0'
    option authoritative '1'
    option readethers '1'
    option leasefile '/tmp/dhcp.leases'
    option resolvfile '/tmp/resolv.conf.auto'
    option localservice '1'

config dhcp 'lan'
    option interface 'lan'
    option start '100'
    option limit '150'
    option leasetime '12h'
    option dhcpcv6 'server'
    option ra 'server'

config dhcp 'wan'
    option interface 'wan'
    option ignore '1'

config odhcpd 'odhcpd'
    option maindhcp '0'
    option leasefile '/tmp/hosts/odhcpd'
    option leasetrigger '/usr/sbin/odhcpd-update'
```