Your network device (commonly referred to as a "router") has an **internal network**. The internal network connects the internal physical(=hardware):

- switch
- wireless access point

with the:

- network processors default internal device network and services.

Contents

- 1 Modifying internal network
- 2 Internal network services
- 3 Software network interfaces
- 4 Examples of changed internal network

Modifying internal network

Via the user interface you can modify how the hardware is logically interconnected with each other and with your software services.

> **Note**: It is easy to lock yourself out of your network device and if/when this happens (use the waiting time checking the PC's ip settings - try release/renew the dhcp lease if not ok):
>
> ◊ First: Wait some minutes - it might just be a temporary glitz.
> ◊ Second: Try to restart the device, because it might just be a device service that need to be restarted.
> ◊ Last resort: Restore to the firmware defaults by resetting the device.

Internal network services

The software services are serviced by the network processor (ARM, MIPS...). Please note that the possibilities are limited by the software implementation and hardware.

List of non-exhaustive internal software services:

- Network traffic services:
  - ♦ OSI layer 2 interconnection - ethernet address routing; a (software) **bridge** or **switch** - Definition: A two port switch is a bridge - a traditional bridge has two ends - not three or more ;-).
  - ♦ OSI layer 3 interconnection - ip address routing; a (software) **router**
  - ♦ OSI layer 2 interconnection and 2-4 moderation, ethernet **transparent/bridging firewall**
  - ♦ OSI layer 3 interconnection and 2-4 moderation; ip **packet filtering firewall**
  - ♦ Please note that the (above) (DD-WRT) firewall normally inspects higher OSI layers. Iptables can refer to modules that can do that:
    - ◊ OSI layer 2-4 moderation; ip **statefull firewall**

        ◊ OSI layer 2-7 moderation; **proxying/application/deep packet inspection firewall**
    - ♦ Quality of Service
    - ♦ NAT - Network Address Translation
    - ♦ Transparent web proxy
- (Inter)network client or server services:
    - ♦ Tunneling
    - ♦ PPPoE
- Network related server services:
    - ♦ DHCP server, client
    - ♦ DNS server
- Management server services:
    - ♦ Telnet and SSH
    - ♦ Web interface via the WEB server
    - ♦ Monitoring
- Other server services:
    - ♦ FTP
    - ♦ Printer Sharing

Software network interfaces

The software network services is connected by you, to physical or logical network interfaces. The interfaces might be a:

- physical interfaces might be labelled eth0, eth1...
- logical might be a bridge (=switch) labelled br0, br1...
- logical vlan labelled vlan0, vlan1....

and maybe:

- teql0 - load sharing device I believe this is used for the "Link Aggregation on Ports 3 & 4" option on the Setup/Vlans page.
- imq0,1 - QOS device or IMQ Device

Refer to the DD-WRT Wiki Page **default internal device networks** for illustrations of current and pre-N device mappings and a more in-depth description of vLan, port and bridge assignments.

.

Examples of changed internal network

There are examples of how to move the wireless acces point on a separate vlan, so it can be separately firewalled:

- Separate LAN and WLAN (GUI)
- V24: WLAN separate from LAN, with independent DHCP
- WLAN separate from LAN, with independent dhcp, etc

There are examples of how to assign a wired LAN port to some vlan different from the rest of the LAN ports:

- VLAN Detached Networks (Separate Networks With Internet Access)
- VLAN Detached Networks (Separate Networks With Internet)

There are examples of how to have more than one ssid on the wireless acces point:

- Multiple WLANs
- Dual SSID isolated

Combinations of the above:

- VLAN Detached Networks each with Wireless and Internet
- Dual SSID one for public network