

# Introduction :

I consider myself as a beginner in networking even-thought I am able to set up VPN using ZyWall, Fritz Box, OS X.

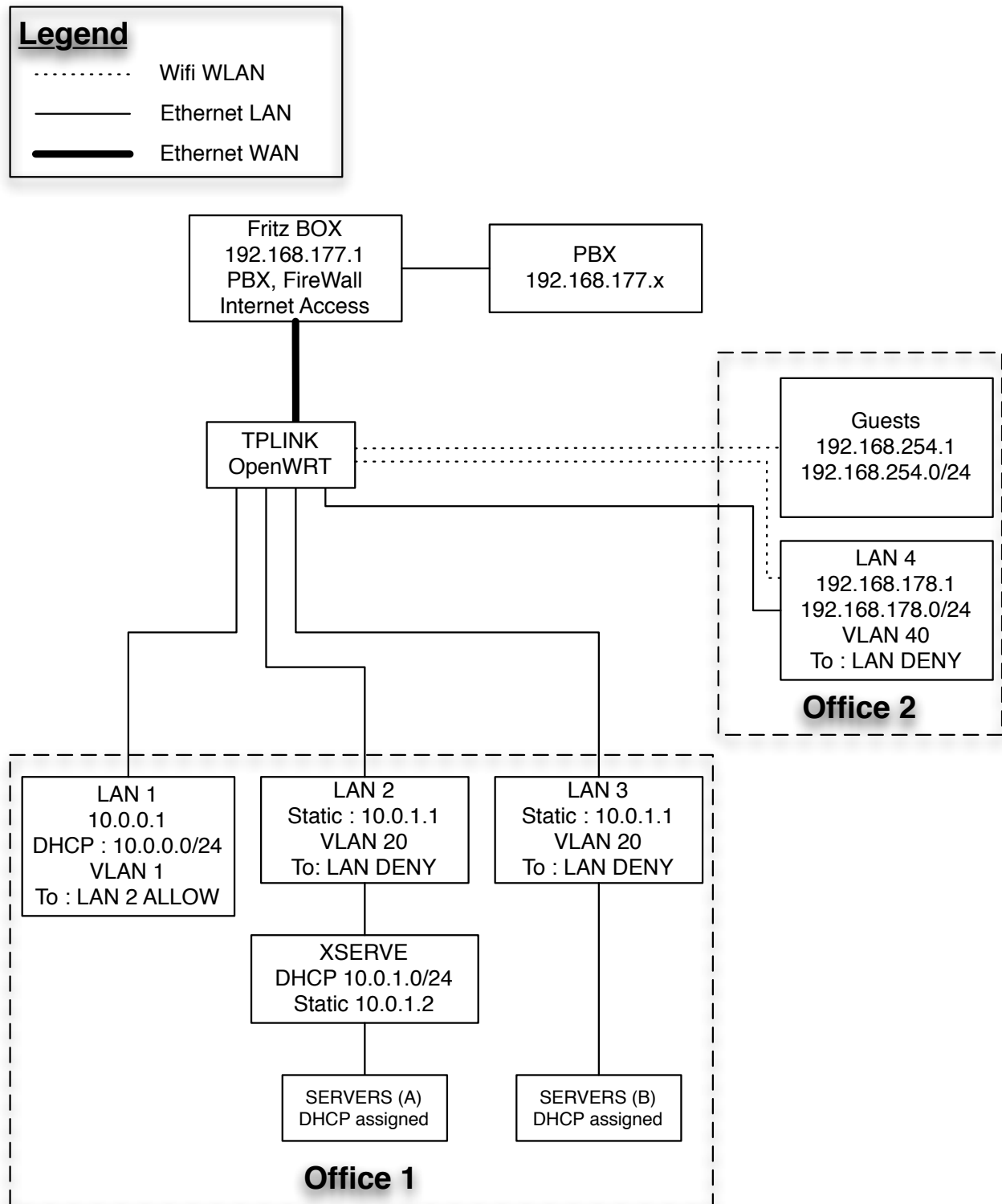
I have written this guide because I thought, I would ask the help of OpenWRT community. After many hours to understand how to set up :

- Multiple VLANs => LAN ;
- Multiple DHCP ;
- Reject or allow connections from some LANs to others ;

I am not sure every settings I have made are useful. Neither am I about the security perspective (don't think my WiFi isn't secure). If you'd like to point out stuff I should consider to help myself and others you're welcome to do so using

me.com email : lange.ludo+openwrt

# Network map :



## TP-Link :

**Model :** TL-WR1043ND

**OpenWRT :** Attitude Adjustment 12.09-beta2

# WiFi enabled :



**Generic 802.11bgn Wireless Controller (radio0)**

Channel: 11 (2.462 GHz) | Bitrate: ? Mbit/s

SSID: OpenWrt | Mode: Master

0% BSSID:XX:XX:XX:XX:XX:XX | Encryption: None

If it allows myself not to push like a dumb-head on the QSS button. Set my computer to static IP 192.168.1.2 and telnet 192.168.1.1 to write "firstboot" it's worth configure it first.

# LAN SERVERS :

## Interfaces :

### General Setup :

#### Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Status

eth0.20

Uptime: 0h 1m 6s  
MAC-Address:XX:XX:XX:XX:XX:XX  
RX: 0.00 B (0 Pkts.)  
TX: 0.00 B (0 Pkts.)  
IPv4: 10.0.1.1/24

Protocol	Static address
IPv4 address	10.0.1.1
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	

#### DHCP Server

No DHCP Server configured for this interface [Setup DHCP Server](#)

## Physical Settings :

**Common Configuration**

General Setup | Advanced Settings | **Physical Settings** | Firewall Settings

**Bridge interfaces**  ? creates a bridge over specified interface(s)

**Interface**

- Ethernet Switch: "eth0"
- VLAN Interface: "eth0.1" ([lan](#))
- VLAN Interface: "eth0.2" ([wan](#))
- VLAN Interface: "eth0.20" ([LAN\\_SERVERS](#))
- \_Wireless Network: Master "OpenWrt" ([lan](#))
- Custom Interface:

## Firewall Settings :

**Common Configuration**

General Setup | Advanced Settings | Physical Settings | **Firewall Settings**

**Create / Assign firewall-zone**

- LAN\_SERVERS:**
- lan:**
- wan:**
- unspecified -or- create:*

? Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

## Switch :

**VLANs on "rtl8366rb" (RTL8366RB)**

VLAN ID Port status:	Port 0 no link	Port 1 no link	Port 2 100baseT full-duplex	Port 3 100baseT full-duplex	Port 4 no link	CPU 100baseT full-duplex	
1	off	untagged	off	off	untagged	tagged	Delete
2	untagged	off	off	off	off	tagged	Delete
20	off	off	untagged	untagged	off	tagged	Delete

Add

# Firewall :

## General Settings :

We now create a / update the new zone :

### General Settings :

**Zone "LAN\_SERVERS"**

This section defines common properties of "LAN\_SERVERS". The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specifies which available networks are member of this zone.

General Settings | **Advanced Settings**

Name	LAN_SERVERS
Input	accept
Output	accept
Forward	reject
Masquerading	<input checked="" type="checkbox"/>
MSS clamping	<input type="checkbox"/>
Covered networks	<input checked="" type="checkbox"/> LAN_SERVERS: <input type="text"/> <input type="checkbox"/> lan: <input type="text"/> <input type="checkbox"/> wan: <input type="text"/> <input type="checkbox"/> create: <input type="text"/>

**Inter-Zone Forwarding**

The options below control the forwarding policies between this zone (LAN\_SERVERS) and other zones. Destination zones cover forwarded traffic **originating from "LAN\_SERVERS"**. Source zones match forwarded traffic from other zones **targeted at "LAN\_SERVERS"**. The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.

Allow forward to destination zones:

- lan: lan:
- wan: wan:

Allow forward from source zones:

- lan: lan:
- wan: wan:

### Advanced Settings :

We don't want another LAN DHCP to interfere with our new zone :

**Zone "LAN\_SERVERS"**

This section defines common properties of "LAN\_SERVERS". The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specifies which available networks are member of this zone.

General Settings | **Advanced Settings**

Restrict to address family	IPv4 and IPv6
Restrict Masquerading to given source subnets	10.0.1.0/24
Restrict Masquerading to given destination subnets	0.0.0.0/0
Force connection tracking	<input type="checkbox"/>
Enable logging on this zone	<input type="checkbox"/>

Our firewall general configuration will look like :

### General Settings :

wan: wan: <input type="text"/>	→ LAN_SERVERS	reject	accept	reject	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LAN_SERVERS: LAN_SERVERS: <input type="text"/>	→ wan	accept	accept	reject	<input checked="" type="checkbox"/>	<input type="checkbox"/>

## Traffic rules :

We'd like to forbid access to other subnets :

New Forward Rule :

### Firewall - Traffic Rules - LAN\_SERVERS-LAN

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled	<input checked="" type="checkbox"/> Disable
Name	LAN_SERVERS-LAN
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	<input type="radio"/> Any zone <input checked="" type="radio"/> LAN_SERVERS: LAN_SERVERS: <small>255</small> <input type="radio"/> lan: lan: <small>255</small> <small>255</small> <input type="radio"/> wan: wan: <small>255</small> <small>255</small>
Source MAC address	any
Source address	any
Source port	any
Destination zone	<input type="radio"/> Device (input) <input type="radio"/> Any zone (forward) <input type="radio"/> LAN_SERVERS: LAN_SERVERS: <small>255</small> <input checked="" type="radio"/> lan: lan: <small>255</small> <small>255</small> <input type="radio"/> wan: wan: <small>255</small> <small>255</small>
Destination address	any
Destination port	any
Action	reject
Extra arguments	<input type="text"/> <small>Passes additional arguments to iptables. Use with care!</small>

NB : You still have access to whole bunch of router IP address...

# LAN QBDESIGN :

## Interfaces :

### General Setup :

Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Status

eth0.40 **Uptime:** 0h 0m 0s  
**MAC-Address:** A0:F3:C1:CF:9C:EA  
**RX:** 0.00 B (0 Pkts.)  
**TX:** 17.69 KB (44 Pkts.)

Protocol: Static address

IPv4 address: 192.168.178.1

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers:

---

DHCP Server

General Setup | Advanced Settings

Ignore interface:  Disable DHCP for this interface.

Start: 200  
Lowest leased address as offset from the network address.

Limit: 50  
Maximum number of leased addresses.

Leasetime: 14h  
Expiry time of leased addresses, minimum is 2 Minutes (2m).

### Physical Settings :

Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Bridge interfaces:  creates a bridge over specified interface(s)

Interface:

- Ethernet Switch: "eth0"
- VLAN Interface: "eth0.1" (lan)
- VLAN Interface: "eth0.2" (wan)
- VLAN Interface: "eth0.20" (LAN\_SERVERS)
- VLAN Interface: "eth0.40" (LAN\_QBDESIGN)
- Wireless Network: Master "OpenWrt" (lan)
- Custom Interface:

### Firewall Settings :

Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Create / Assign firewall-zone

- LAN\_QBDESIGN: LAN\_QBDESIGN:
- LAN\_SERVERS: LAN\_SERVERS:
- lan: lan:
- wan: wan:
- unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.



# Switch :

VLANs on "rtl8366rb" (RTL8366RB)

VLAN ID Port status:	Port 0 100baseT full-duplex	Port 1 1000baseT full-duplex	Port 2 no link	Port 3 no link	Port 4 no link	CPU 1000baseT full-duplex	
1	off	untagged	off	off	off	tagged	Delete
2	untagged	off	off	off	off	tagged	Delete
20	off	off	untagged	untagged	off	tagged	Delete
40	off	off	off	off	untagged	tagged	Delete
Add							

# Firewall :

## General Settings :

Zone "LAN\_QBDESIGN"

This section defines common properties of "LAN\_QBDESIGN". The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specifies which available networks are member of this zone.

General Settings | Advanced Settings

Name	LAN_QBDESIGN
Input	accept
Output	accept
Forward	reject
Masquerading	<input checked="" type="checkbox"/>
MSS clamping	<input type="checkbox"/>
Covered networks	<input checked="" type="checkbox"/> LAN_QBDESIGN: <input type="text"/> <input type="checkbox"/> LAN_SERVERS: <input type="text"/> <input type="checkbox"/> lan: <input type="text"/> <input type="text"/> <input type="checkbox"/> wan: <input type="text"/> <input type="checkbox"/> create: <input type="text"/>

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (LAN\_QBDESIGN) and other zones. Destination zones cover forwarded traffic **originating from "LAN\_QBDESIGN"**. Source zones match forwarded traffic from other zones **targeted at "LAN\_QBDESIGN"**. The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.

Allow forward to destination zones:

- LAN\_SERVERS: LAN\_SERVERS:
- lan: lan:
- wan: wan:

Allow forward from source zones:

- LAN\_SERVERS: LAN\_SERVERS:
- lan: lan:
- wan: wan:



## Advanced Settings :

We forbid masquerading with our 10.0.x.x LAN by setting "Restrict Masquerading to given destination subnets" to "!10.0.1.0/24" and "!10.0.0.0/24" :

Zone "LAN\_QBDESIGN"

This section defines common properties of "LAN\_QBDESIGN". The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specifies which available networks are member of this zone.

General Settings | **Advanced Settings**

Restrict to address family	IPv4 and IPv6
Restrict Masquerading to given source subnets	192.168.178.0/24
Restrict Masquerading to given destination subnets	!10.0.1.0/24 !10.0.0.0/24
Force connection tracking	<input type="checkbox"/>
Enable logging on this zone	<input type="checkbox"/>

## Traffic Rules :

We also as previously explained set up Traffic Rules to reject traffic from this zone to the other LAN :

LAN_QBDESIGN- LAN_SERVERS	Any TCP+UDP From any host in LAN_QBDESIGN To any host in LAN_SERVERS	Refuse forward	<input checked="" type="checkbox"/>
LAN_QBDESIGN-LAN	Any TCP+UDP From any host in LAN_QBDESIGN To any host in lan	Refuse forward	<input checked="" type="checkbox"/>

# Addendum :

To have multiple LAN DHCP Servers with your OpenWRT you must also change the MAC Address on the specified interface eg. from x0:xx:xx:xx:xx:xx to x1:xx:xx:xx:xx:xx  
You may find a full-config for the network described in this document at <http://idisk.jumparound.be/public/OpenWrt.tar.gz> login : **root** password : **root** (some differences might exists between my guide and the configuration as I still need to test some stuff).