

Introduction

These instructions are for a **Vigor 2830 Series Router** running version **3.6.7_db_232201**. They should work on many variants of modern DrayTek routers as the interface and feature are fairly similar, but as usual “your mileage may vary”.

We are using VLAN’s for segregating the home and guest traffic; please note that VLAN’s are fairly good for this, but are designed for traffic segregation/management and NOT security. That said; IMHO, if you are choosing to let strangers use your network they are probably good enough!

Usual disclaimers about backing up your configuration before you start, not attempting this unless you know what you are doing, and that this is simply a record of how I chose to configure my router; this does not mean it’s right, perfect or secure!

LAN Settings

Here we are using LAN 1 for our normal home usage (192.168.2.x), with LAN 2 enabled for openwireless.org.

Index	Status	DHCP	IP Address	Details Page	IPv6
LAN 1	V	V	192.168.2.1	Details Page	IPv6
LAN 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.4.1	Details Page	
LAN 3	<input type="checkbox"/>	<input type="checkbox"/>	192.168.5.1	Details Page	
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	192.168.7.1	Details Page	
IP Routed Subnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.3.1	Details Page	

Subnet	LAN 1	LAN 2	LAN 3	LAN 4
LAN 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LAN 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LAN 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Now click on the [Details Page] for LAN 2.

The “Guest LAN” is configured as 192.168.4.1 with a subnet mask of 255.255.255.0

Set the **DHCP Server** for this LAN for **128 IP Pool Counts**, and point the **Gateway IP Address** to the LAN1 address of the router (in this case) 192.168.2.1.

The **Lease Time** is set for 8 hours (**28800** seconds) and the “Retrieve IP’s from inactive clients” is **checked**.

Network Configuration

Enable Disable

For NAT Usage For Routing Usage

IP Address: 192.168.4.1

Subnet Mask: 255.255.255.0

Note: Disable LAN & Enable LAN shouldn't be in the same subnet.

DHCP Server Configuration

Enable Server Disable Server

Enable Relay Agent

Start IP Address: 192.168.4.32

IP Pool Counts: 128

Gateway IP Address: 192.168.2.1

Lease Time: 28800 (s)

Retrieve IPs from inactive clients periodically

DNS Server IP Address

Primary IP Address: []

Secondary IP Address: []

Next Set the VLANs

The screenshot shows the 'LAN >> VLAN Configuration' page. The 'Enable' checkbox is checked. The table below shows the configuration for VLANs 0 through 7.

VLAN	LAN				Wireless LAN				Subnet	VLAN Tag		
	P1	P2	P3	P4	SSID1	SSID2	SSID3	SSID4		Enable	VID	Priority
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	1	0
VLAN1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input checked="" type="checkbox"/>	1	0
VLAN2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	LAN 2	<input checked="" type="checkbox"/>	2	0
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0
VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN 1	<input type="checkbox"/>	0	0

Below the table, there are instructions and a checkbox: Permit untagged device in P1 to access router. The instructions state: 1. For each VLAN row, if enable is checked for the VLAN Tag then the corresponding VID will be applied to wired LAN traffic. 2. Wireless LAN traffic is always untagged, but will still be a member of the VLAN group selected. 3. Each VID must be unique.

We are using VLAN0 and VLAN1 for our internal traffic, with VLAN2 (with a VLAN ID [VID] Tag of 2) being used for the openwireless.org traffic.

We will be using VLAN ID 2 later with a couple of external Access Points, but we are also assigning the routers internal wireless SSID4 to VLAN 2 only.

Bandwidth Limit

The screenshot shows the 'Bandwidth Management >> Bandwidth Limit' page. The 'Enable' radio button is selected. The 'Default TX Limit' is set to 200 Kbps and the 'Default RX Limit' is set to 800 Kbps. The 'Allow auto adjustment' checkbox is checked. The 'Limitation List' table is as follows:

Index	Start IP	End IP	TX limit	RX limit	Shared
1	192.168.4.1	192.168.4.255	200K	800K	Y
2	192.168.2.1	192.168.2.255	300M	300M	N

The 'Specific Limitation' section shows 'Start IP' and 'End IP' fields, with 'Each' selected as the limitation type. The 'TX Limit' and 'RX Limit' are both set to 0 Kbps. The 'Smart Bandwidth Limit' checkbox is unchecked. A note states: 'For any LAN IP Not in Limitation List, whose session number exceeds 0'. The 'Time Schedule' section is empty.

For your information; I am on a Fibre to the Cabinet line, resulting in measured speed of 26Mbps Down and 2Mbps Up.

Enable the Bandwidth Limit function, and I have mine set to 300M Up and Down for the internal home traffic (192.168.2.x) and 200k UP and 800k down (shared) for the guest (openwireless.org) traffic (192.168.4.x).

You can of course choose to be more or less generous for your guests!



Internal Wireless configuration

The screenshot shows the 'Wireless LAN >> General Setup' page. The 'General Setting (IEEE 802.11)' section is active. 'Enable Wireless LAN' is checked. The Mode is set to 'Mixed(11a+11n 5 GHz)' and the Channel is 'Channel 40, 5200MHz'. A table lists four SSIDs:

	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN
1	<input type="checkbox"/>	<input type="checkbox"/>	[Redacted]	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	[Redacted]	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	[Redacted]	<input type="checkbox"/>	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	openwireless.org	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Notes: Enabling the Isolate Member configuration will forbid the wireless clients associated to the same SSID from connecting to each other. The isolate VPN configuration will isolate the wireless traffic from VPN connections and thus, wireless clients will not be able to access the VPN network under this setting.

Associated Schedule Profiles: [] , [] , [] , []

Note: Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored. Valid settings are profile indexes 1 to 15.

Buttons: OK, Cancel

I am running two additional AP's on the 2.4GHz (normal) band, and so run my router on the 5GHz band – if this is your only AP offering openwireless.org I would suggest you set the Channel to “Mixed 11g + 11n” (2.4GHz)

Set SSID 4 to **openwireless.org** and check the “Isolate Member” box

On the Security page, set the security for SSID 4 to “disable”

The screenshot shows the 'Wireless LAN >> Bandwidth Management' page. The 'SSID 4' tab is selected. The SSID is 'openwireless.org'. 'Enable' is checked. The Bandwidth Limit Type is 'Per Station Limit'. The Upload Limit (Kbps) is 200 and the Download Limit (Kbps) is 800.

Note: 1.Download: Traffic going to any station.Upload: Traffic being sent from a wireless station.
2.Allow auto adjustment could make the best utilization of available bandwidth.

Buttons: OK, Cancel

On the Bandwidth Management page, set SSID 4 Upload and download limits to match the limits you set in “Bandwidth Management” above – in my case 200k upload and 800k download.

Router Management

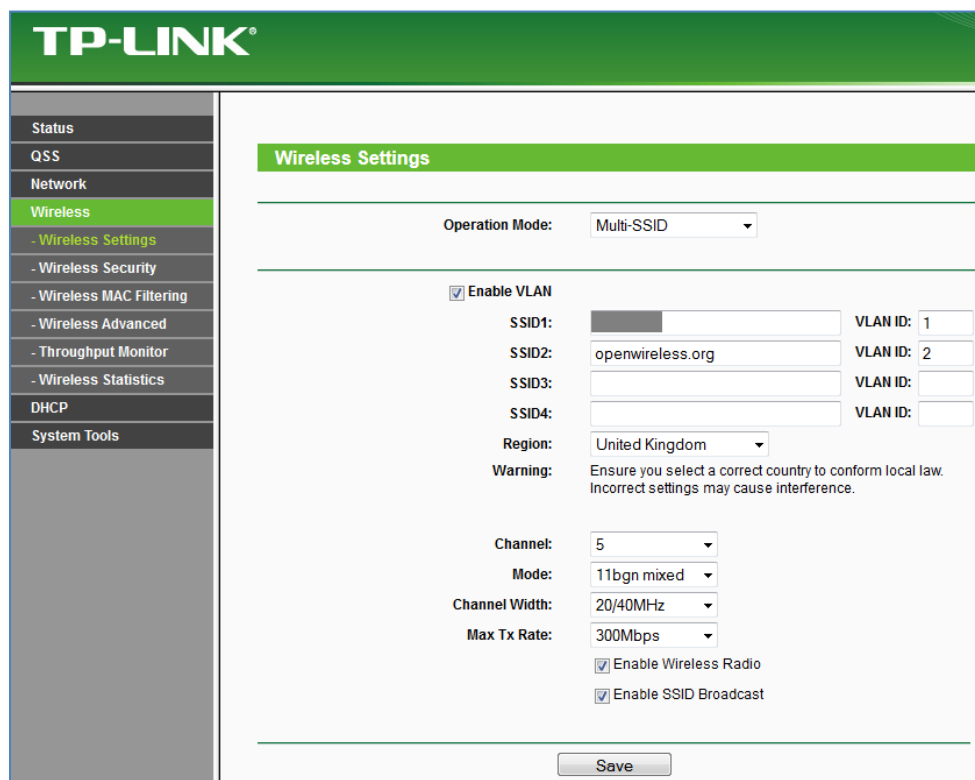
The screenshot displays the management interface for a Vigor2830 Series ADSL2+ Security Firewall. The interface is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with items such as 'Wizards', 'Online Status', 'WAN', 'LAN', 'Load-Balance/Route Policy', 'NAT', 'Firewall', 'User Management', 'Objects Setting', 'CSM', 'Bandwidth Management', 'Applications', 'VPN and Remote Access', 'Certificate Management', 'Wireless LAN', 'SSL VPN', 'USB Application', 'System Maintenance', 'System Status', 'TR-069', 'Admin Setting', 'User Password', 'Login Page Greeting', 'Configuration Backup', 'SysLog / Mail Alert', 'Time and Date', 'SNMP', 'Management', 'Reboot System', 'Firmware Upgrade', 'Activation', 'Diagnostics', 'External Devices', 'Support Area', and 'Product Registration'. The 'Management' item is currently selected and highlighted. The main content area is titled 'System Maintenance >> Management' and contains several configuration sections: 'IPv4 Management Setup' (Router Name: draytek, Default: Disable Auto-Logout), 'Internet Access Control' (Allow management from the Internet: checked, FTP Server, HTTP Server, HTTPS Server, Telnet Server, TR069 Server, SSH Server, Disable PING from the Internet: checked), 'LAN Access Control' (Allow management from LAN: checked, FTP Server, HTTP Server, HTTPS Server, Telnet Server, SSH Server, Apply To Subnet: LAN2, LAN3, LAN4, IP Routed Subnet), 'Management Port Setup' (User Define Ports selected, Telnet Port: 23, HTTP Port: 80, HTTPS Port: 443, FTP Port: 21, TR069 Port: 8069, SSH Port: 22), and 'External Device Control' (No respond to External Device: unchecked). A table for 'Access List from the Internet' has three rows with columns for List, IP, and Subnet Mask. A note at the bottom states: 'Note: Subnet LAN1 is always allowed to access all the router services regardless of "LAN Access Control" settings.' An 'OK' button is located at the bottom center of the main content area.

On the Management Page, I would recommend to disable LAN access control from LAN2, LAN3 and LAN4 so the router can only be configured from a station on your home LAN (LAN1).

Backup

Finally backup your configuration.

Setting remote AP's



The screenshot shows the TP-Link web interface for configuring wireless settings. The left sidebar contains a navigation menu with options: Status, QSS, Network, Wireless (highlighted), Wireless Settings (sub-menu), Wireless Security, Wireless MAC Filtering, Wireless Advanced, Throughput Monitor, Wireless Statistics, DHCP, and System Tools. The main content area is titled "Wireless Settings" and features the following configuration options:

- Operation Mode:** Multi-SSID (dropdown)
- Enable VLAN:** (checkbox)
- SSID1:** [Redacted] **VLAN ID:** 1
- SSID2:** openwireless.org **VLAN ID:** 2
- SSID3:** [Empty] **VLAN ID:** [Empty]
- SSID4:** [Empty] **VLAN ID:** [Empty]
- Region:** United Kingdom (dropdown)
- Warning:** Ensure you select a correct country to conform local law. Incorrect settings may cause interference.
- Channel:** 5 (dropdown)
- Mode:** 11bgn mixed (dropdown)
- Channel Width:** 20/40MHz (dropdown)
- Max Tx Rate:** 300Mbps (dropdown)
- Enable Wireless Radio
- Enable SSID Broadcast

A "Save" button is located at the bottom of the configuration area.

I use two TP-Link AP's to provide extra coverage on the 2.4GHz band; but the concept is the same for most brands out on the market.

Set the **Operation Mode** to "**Multi-SSID**" and then define an SSID (with no security) as **openwireless.org** with a **VLAN ID of 2**.

Set your internal / home SSID(s) with a VLAN ID of 1.

Verification

Connect to each AP in turn, ensuring that;

- Connecting to your home SSID you are allocated an address of 192.168.2.x, and;
Running a speed-test you get full throughput
- Connecting to the SSID openwireless.org you are allocated an address of 192.168.4.x, and;
Running a speed-test you get the throttled throughput you defined

Final thought

I use OpenDNS with my router, pointing the DNS Server IP Address to OpenDNS which then allows me to block the site I consider inappropriate – it's not perfect and can be bypassed by manually setting an alternate DNS server, but affords a little protection – of course your guests on openwireless.org are subject to the same restrictions as your home users and vice-versa.

OpenDNS dashboard showing the 'Web Content Filtering' settings page. The page is for a 'Home' network. The 'Web Content Filtering' section is active, and the 'Custom' filtering level is selected. A grid of categories is shown with checkboxes, many of which are checked, including Academic Fraud, Alcohol, Chat, Drugs, Gambling, Government, Humor, Lingerie/Bikini, News/Media, P2P/File sharing, Podcasts, Portals, Religious, Sexuality, Sports, Tobacco, Video Sharing, Web Spam, Adult Themes, Anime/Manga/Webcomic, Blogs, Classifieds, Ecommerce/Shopping, Financial Institutions, Games, Hate/Discrimination, Instant Messaging, Movies, Non-Profits, Parked Domains, Politics, Proxy/Anonymizer, Research/Reference, Social Networking, Tasteless, Travel, and Webmail. Other categories like Adware, Auctions, Business Services, Dating, Educational Institutions, Forums/Message boards, German Youth Protection, Health and Fitness, Jobs/Employment, Music, Nudity, Photo Sharing, Pornography, Radio, Search Engines, Software/Technology, Television, Typo Squatting, and Weapons are also visible. An 'APPLY' button is at the bottom.

Also set the security categories;

Security settings page showing three sections:

- Malware/Botnet Protection** **Enable basic malware/botnet protection**
When certain Internet-scale botnets are discovered or particularly malicious malware hits, we offer protection to all our users so that as many people as possible can be protected from the threat. At this time, this feature blocks the Conficker virus and the Internet Explorer Zero Day Exploit, and is continually expanded to include other types of malicious sites.
- Phishing Protection** **Enable phishing protection**
By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best data available.
- Suspicious Responses** **Block internal IP addresses**
When enabled, DNS responses containing IP addresses listed in [RFC1918](#) will be filtered out. This helps to prevent [DNS Redirection attacks](#). For example, if `badstuff.attacker.com` points to `192.168.1.1`, this option would filter out that response.

The three blocks of IP addresses filtered in responses are:

10.0.0.0 - 10.255.255.255 (10/8)
172.16.0.0 - 172.31.255.255 (172.16/12)
192.168.0.0 - 192.168.255.255 (192.168/16)

An 'APPLY' button is at the bottom.

Feedback

Thoughts and comments to webmaster (at) beaconsfield-urc (dot) org

