

Создание гостевой WiFi зоны.

Внимание! Обратите внимание, что большинство изменяемых настроек действует только на новые соединения. Старые, не закрытые соединения, продолжают работать по старым настройкам. Так, например, если Вы дали команду на компьютере «ping -t 192.168.11.100», Вы можете продолжать получать ответы даже после того, как создали правило запрещающее прохождение icmp пакетов.

1. Создание второй WiFi зоны.

А) Создаём новый профиль безопасности для нашей дополнительной ЗОНЫ:

1. Wireless Settings

2. Profiles

3. Add

	SSID	Broadcast	Security	Encryption	Authentication
<input type="checkbox"/>	default1	DSR-1000N_1	✓	OPEN	NONE

1. Save Settings

2. Don't Save Settings

1.

Profile Configuration

Profile Name: Guest_WiFi

SSID: Guest_WiFi *

Broadcast SSID:

Security: OPEN

Encryption: TKIP

Authentication: PSK

WPA Password: *

Enable Pre-Authentication:

WEP Index and Keys

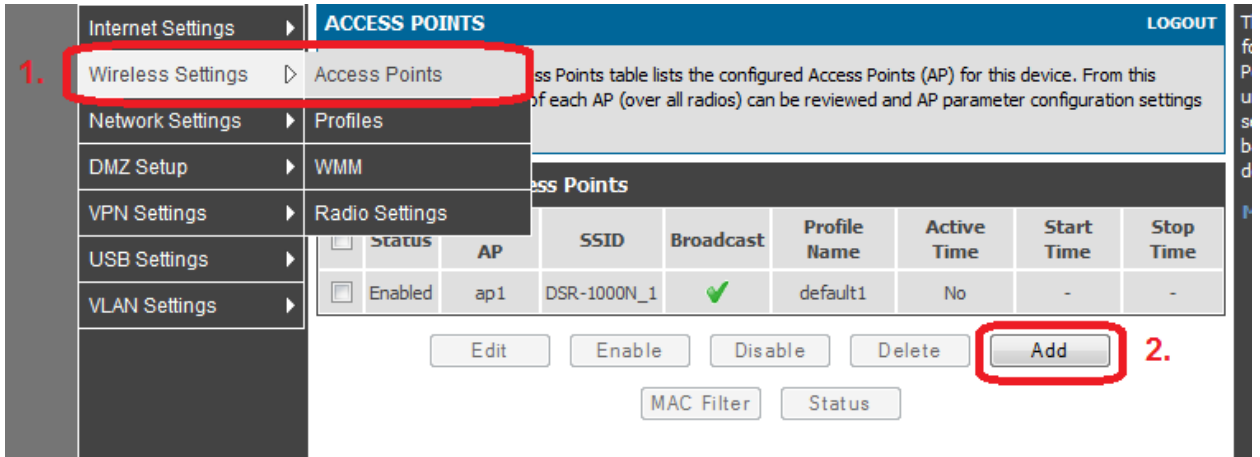
Authentication: Open System

1.

	Profile Name	SSID	Broadcast	Security	Encryption	Authentication
<input type="checkbox"/>	default1	DSR-1000N_1	✓	WPA2	CCMP	PSK
<input type="checkbox"/>	Guest_WiFi	Guest_WiFi	✓	OPEN	NONE	NONE

Edit Delete Add

Б) Создаём дополнительную зону:

1. 

Internet Settings | **ACCESS POINTS** | LOGOUT

Wireless Settings | Access Points

Network Settings | Profiles

DMZ Setup | WMM

VPN Settings | Radio Settings

USB Settings

VLAN Settings

Access Points table lists the configured Access Points (AP) for this device. From this table, the status of each AP (over all radios) can be reviewed and AP parameter configuration settings can be accessed.

Status	AP	SSID	Broadcast	Profile Name	Active Time	Start Time	Stop Time
<input checked="" type="checkbox"/>	ap1	DSR-1000N_1	✓	default1	No	-	-

Edit Enable Disable Delete **Add** 2.

MAC Filter Status

Wireless Settings | This page allows you to create a new AP or edit the configuration of an existing AP. The details will then be displayed in the AP table on the Wireless > Access Points page.

Network Settings | **Save Settings** | Don't Save Settings 2.

DMZ Setup

VPN Settings

USB Settings

VLAN Settings

Access Point Configuration


AP Name: Guest

Profile Name: Guest_WiFi

Active Time:

Start Time: [] hour [] minute [AM]

Stop Time: [] hour [] minute [AM]

WLAN Partition: 

1.

Если необходимо изолировать гостевых клиентов друг от друга, то необходимо включить «WLAN Partition».

Wireless Settings | **ACCESS POINTS** | LOGOUT

Network Settings | The List of Available Access Points table lists the configured Access Points (AP) for this device. From this summary list, the status of each AP (over all radios) can be reviewed and AP parameter configuration settings can be accessed.

DMZ Setup

VPN Settings

USB Settings

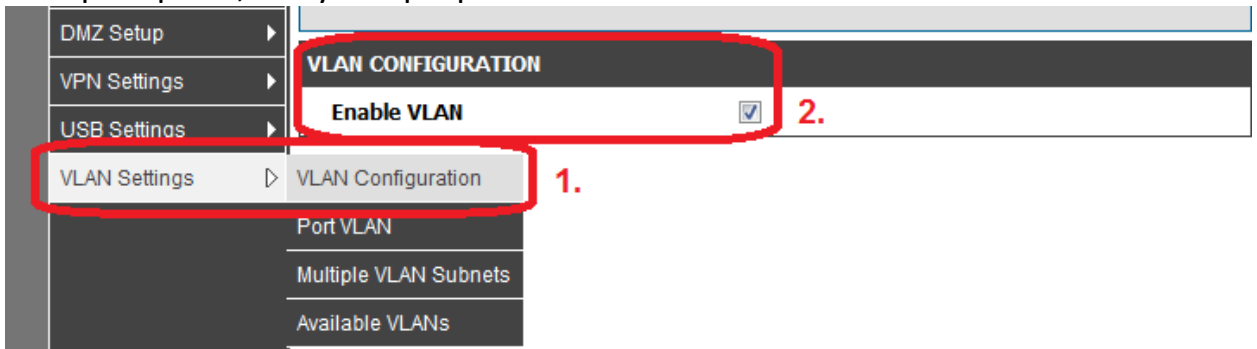
VLAN Settings

List of Available Access Points

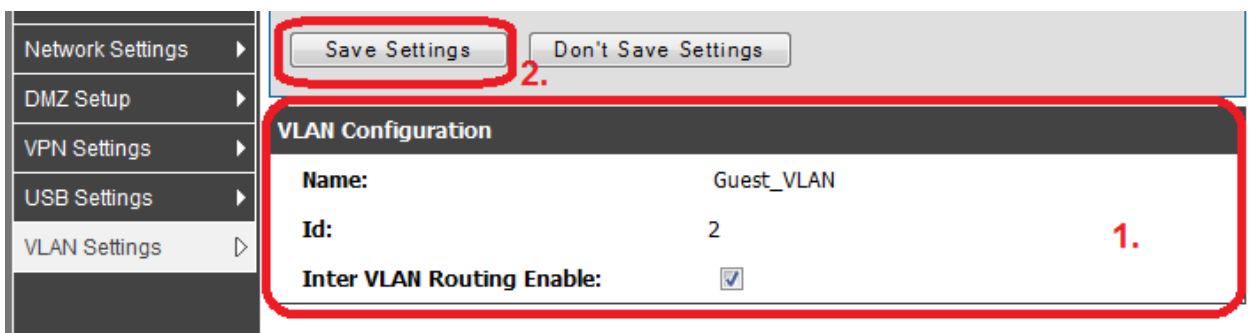
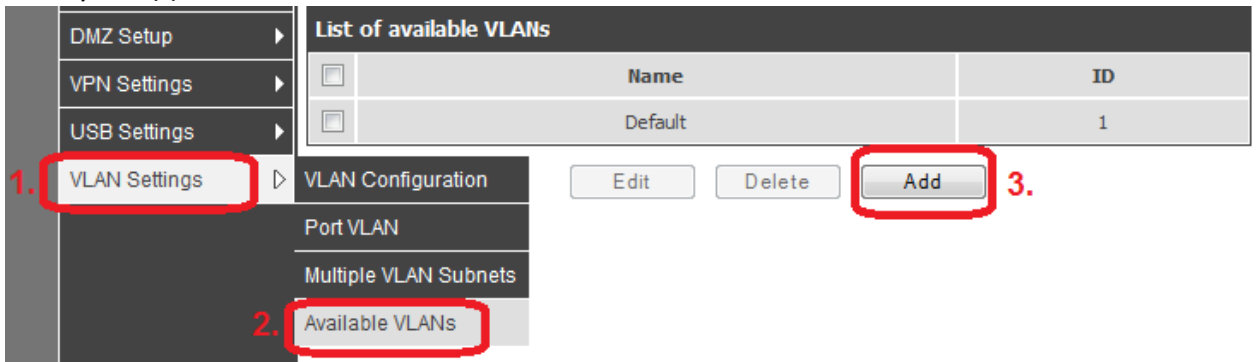
Status	Virtual AP	SSID	Broadcast	Profile Name	Active Time	Start Time	Stop Time
<input checked="" type="checkbox"/>	ap1	DSR-1000N_1	✓	default1	No	-	-
<input checked="" type="checkbox"/>	Guest	Guest_WiFi	✓	Guest_WiFi	No	-	-

2. Создаём новый VLAN и переносим нашу зону в него:

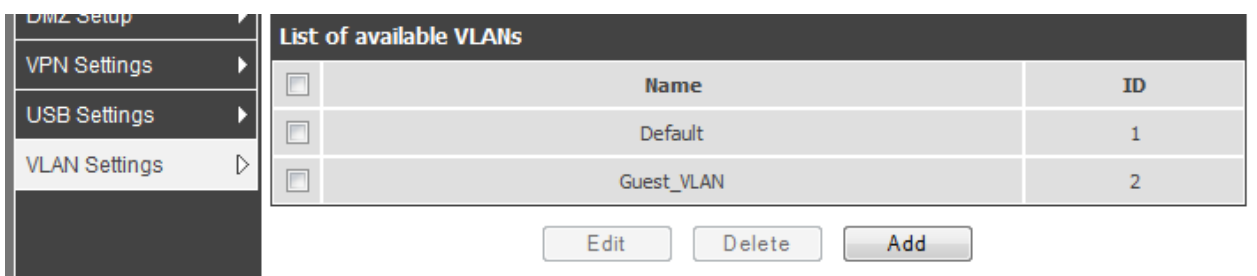
Проверяем, что у нас разрешены VLAN



A) Создаём новый VLAN



Если снять птичку «Inter VLAN Routing Enable», то этот VLAN будет изолирован от остальных VLAN. Однако в этом случае не только из него к Вам, но и от Вас в этот VLAN трафик не пройдёт. Редко, когда необходима такая полная изоляция.



Настраиваем IP-диапазон для нашего нового VLAN:

1. Network Settings

- Network Settings
- DMZ Setup
- VPN Settings
- USB Settings
- 2. VLAN Settings

3. 2

MULTI VLAN SUBNET List			
	Vlan ID	IP Address	Subnet Mask
<input type="checkbox"/>	1	192.168.10.1	255.255.255.0
<input checked="" type="checkbox"/>	2	192.168.2.1	255.255.255.0

4. Edit

Internet Settings

Wireless Settings

Network Settings

DMZ Setup

VPN Settings

USB Settings

VLAN Settings

LOGOUT

MULTI VLAN SUBNET CONFIG

This page shows the list of available multiple VLAN subnets.

Save Settings Don't Save Settings

MULTI VLAN SUBNET

Vlan ID: 2

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

DHCP

DHCP Mode: DHCP Server

Domain Name: DLink

Starting IP Address: 192.168.2.100

Ending IP Address: 192.168.2.254

Primary DNS Server (Optional):

Secondary DNS Server (Optional):

Lease Time: 24 (Hours)

Relay Gateway: 0.0.0.0

LAN Proxy

Enable DNS Proxy:

Б) Привязываем нашу WiFi зону к нашему новому VLAN.

1. VLAN Settings

Port VLAN 2.

3. Edit 4.

Port VLANs				
	Port Name	Mode	PVID	VLAN Membership
<input type="checkbox"/>	Port 1	Access	1	1
<input type="checkbox"/>	Port 2	Access	1	1
<input type="checkbox"/>	Port 3	Access	1	1
<input type="checkbox"/>	Port 4	Access	1	1

Wireless VLANs

	SSID	Mode	PVID	VLAN Membership
<input type="checkbox"/>	DSR-1000N_1	Access	1	1
<input checked="" type="checkbox"/>	Guest_WiFi	Access	1	1

VLAN Configuration

Port Name: Guest_WiFi

Mode: Access

PVID: 2

1. Apply Cancel

2. Apply Cancel

VLAN Membership Configuration

VLAN Membership: 1 2

Apply Cancel

Port 3

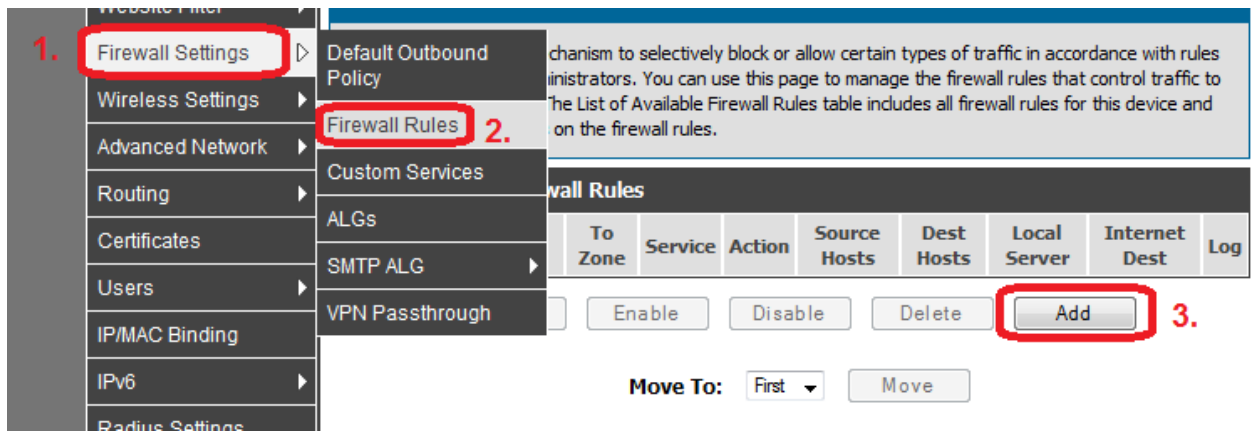
Port 4

Wireless VLANs

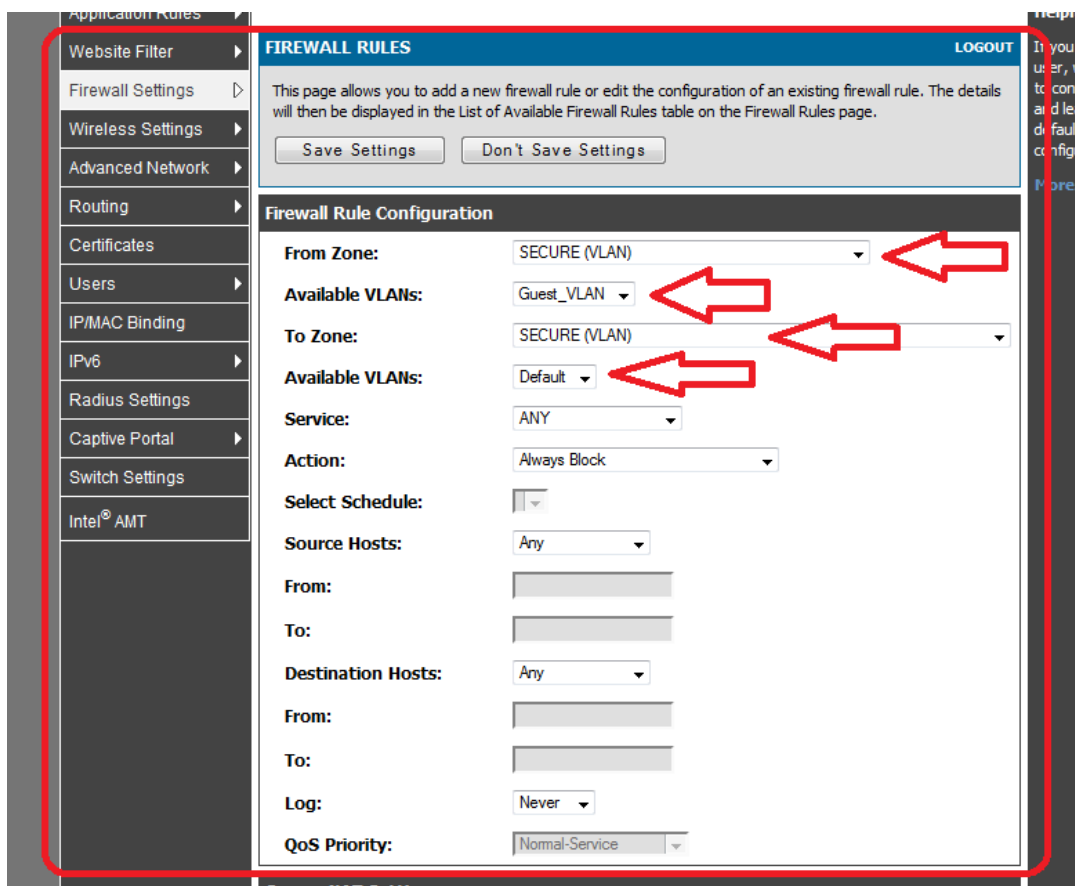
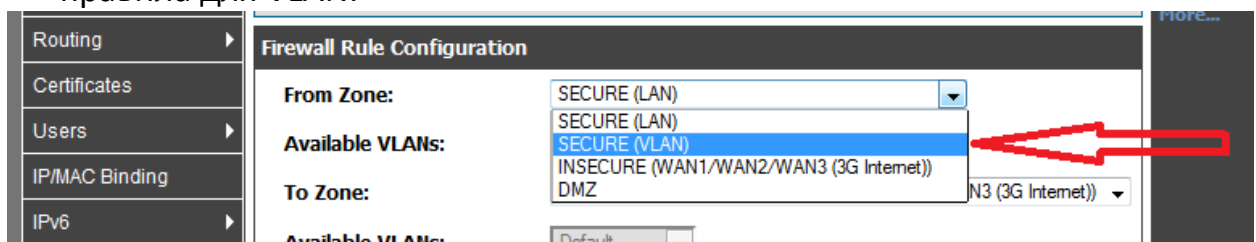
	SSID	Mode	PVID	VLAN Membership
<input type="checkbox"/>	DSR-1000N_1	Access	1	1
<input type="checkbox"/>	Guest_WiFi	Access	2	2

me
be
M

3. Настройка безопасности для гостевой зоны:



Начиная с прошивки 1.04B58, стала доступна возможность создавать правила для VLAN:



Интернет в гостевой зоне есть, Вы получить доступ в гостевую зону можете, а из гостевой зоны в основную – не смогут.