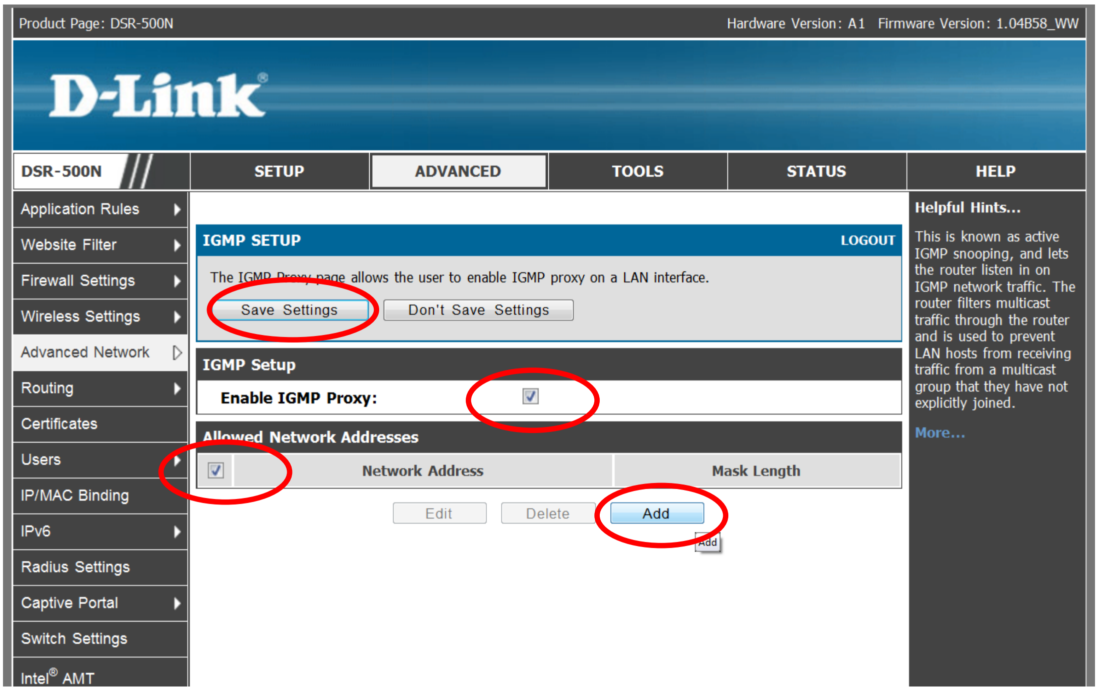
Настройка IGMP на DSR-500/500N/1000/1000N

Примечание: используемая версия firmware 1.04B58_WW или новее.
При необходимости обновить версию до актуальной можно отсюда: http://tsd.dlink.com.tw/

- Включить IGMP Proxy (Advanced -> Advanced Network -> Enable IGMP Proxy) , сохранить.
- Добавить адреса источника мультикаста. Эти записи автоматически создадут необходимые разрешающие правила для Firewall. Для этого нажать «Add» :



IGMP SETUP

The IGMP Proxy page allows the user to enable IGMP proxy on a LAN interface.

IGMP Setup

Enable IGMP Proxy: ☑

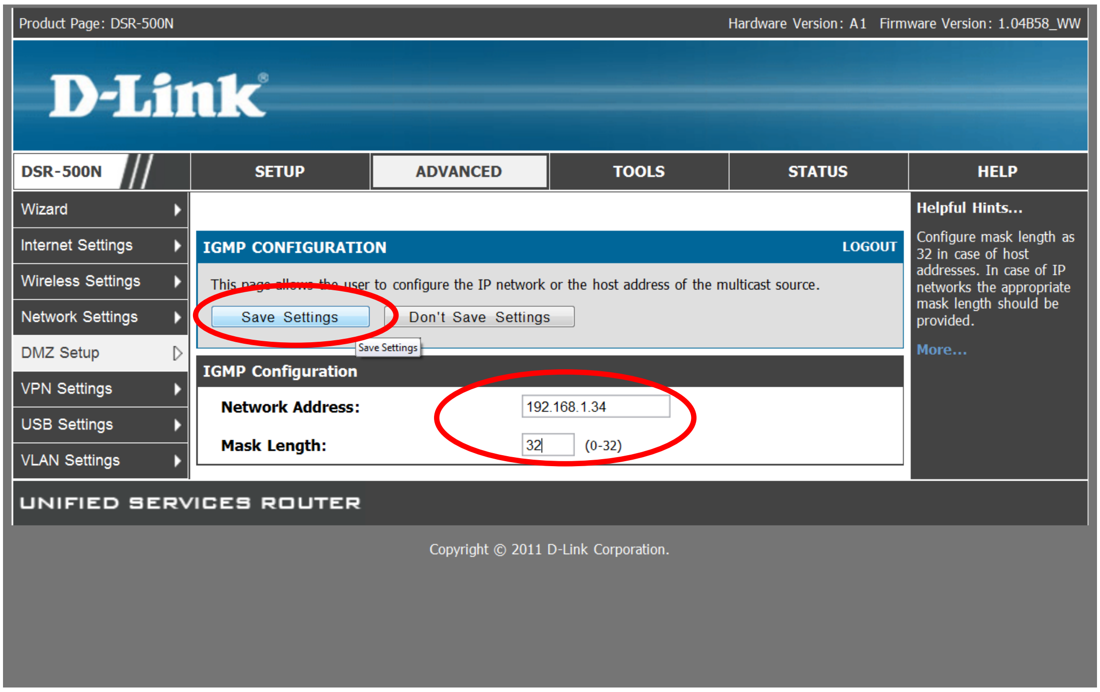
Allowed Network Addresses

☑	Network Address	Mask Length

Helpful Hints...

This is known as active IGMP snooping, and lets the router listen in on IGMP network traffic. The router filters multicast traffic through the router and is used to prevent LAN hosts from receiving traffic from a multicast group that they have not explicitly joined.

- В открывшемся окне в полях «Network Address» и «Mask Length» прописать адрес/маску источников мультикаста, например 192.168.1.34/32, либо сеть (192.168.1.0/24), если источников несколько, и они из одной подсети.



IGMP CONFIGURATION

This page allows the user to configure the IP network or the host address of the multicast source.

IGMP Configuration

Network Address: 192.168.1.34

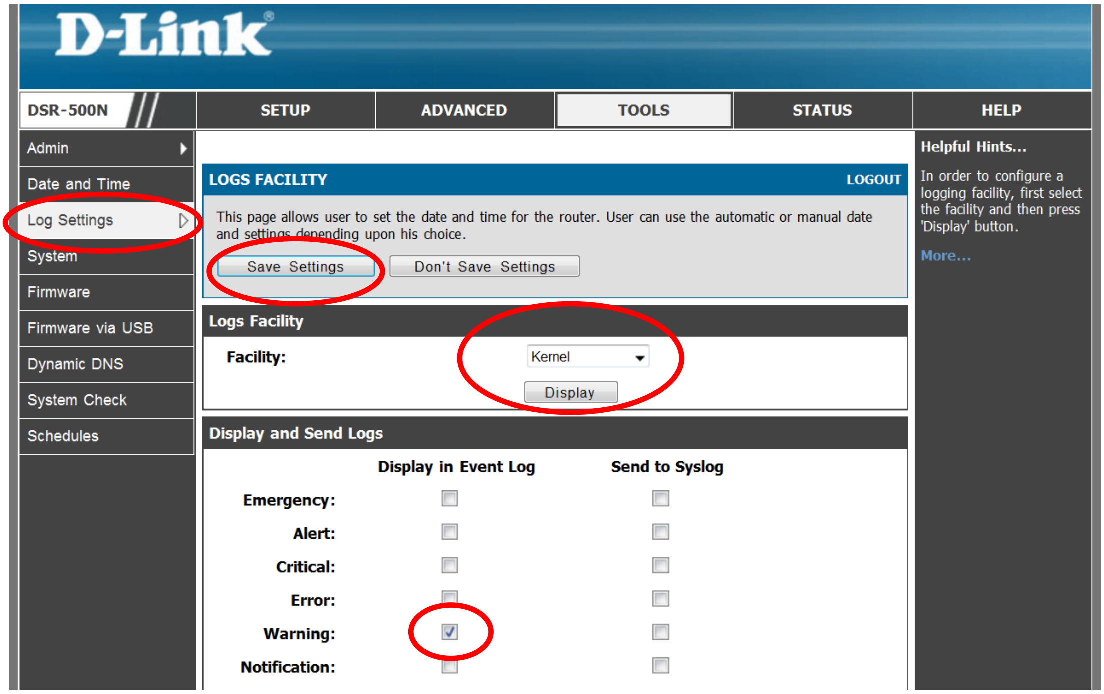
Mask Length: 32 (0-32)

Helpful Hints...

Configure mask length as 32 in case of host addresses. In case of IP networks the appropriate mask length should be provided.

Copyright © 2011 D-Link Corporation.

- Так как адреса, с которых производится вещание IPTV, обычно неизвестны, для их определения необходимо включить Warning - сообщения для Kernel в системном журнале:
TOOLS -> Log Settings -> Logs Facility , выбрать Kernel, нажать Display :



LOGS FACILITY

This page allows user to set the date and time for the router. User can use the automatic or manual date and settings depending upon his choice.

Logs Facility

Facility: Kernel

Display and Send Logs

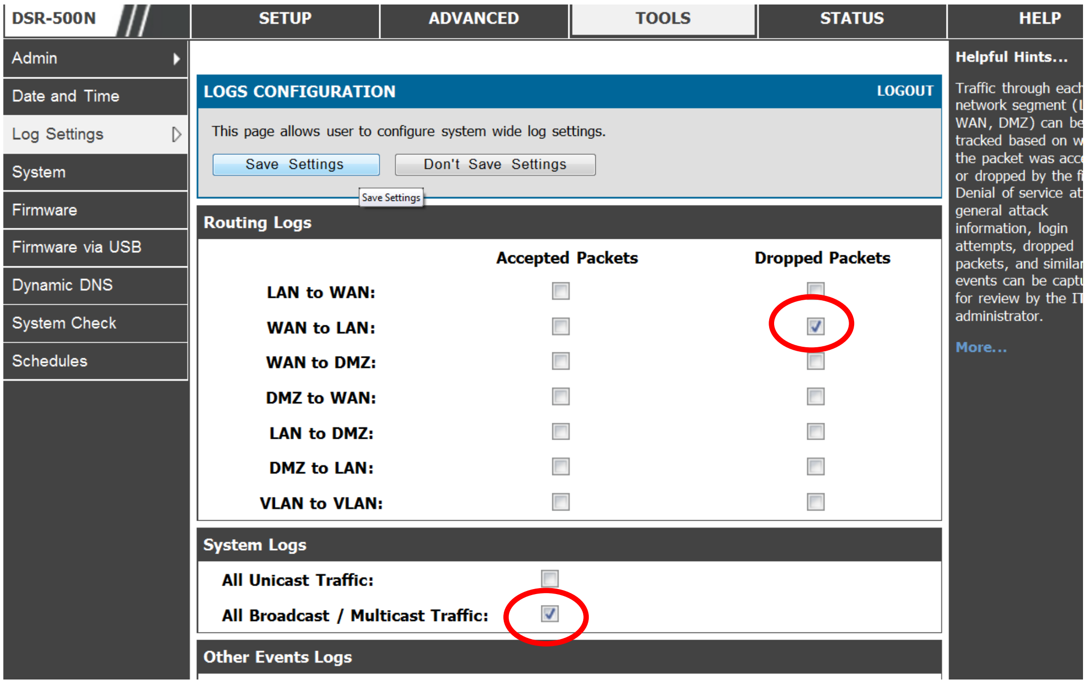
	Display in Event Log	Send to Syslog
Emergency:	☐	☐
Alert:	☐	☐
Critical:	☐	☐
Error:	☐	☐
Warning:	☑	☐
Notification:	☐	☐

Helpful Hints...

In order to configure a logging facility, first select the facility and then press 'Display' button.

More...

И здесь:
Tools -> Log Settings -> Logs Configuration -> Dropped Packets и All Broadcast / Multicast Traffic :



LOGS CONFIGURATION

This page allows user to configure system wide log settings.

Routing Logs

	Accepted Packets	Dropped Packets
LAN to WAN:	☐	☐
WAN to LAN:	☐	☑
WAN to DMZ:	☐	☐
DMZ to WAN:	☐	☐
LAN to DMZ:	☐	☐
DMZ to LAN:	☐	☐
VLAN to VLAN:	☐	☐

System Logs

All Unicast Traffic: ☐
All Broadcast / Multicast Traffic: ☑

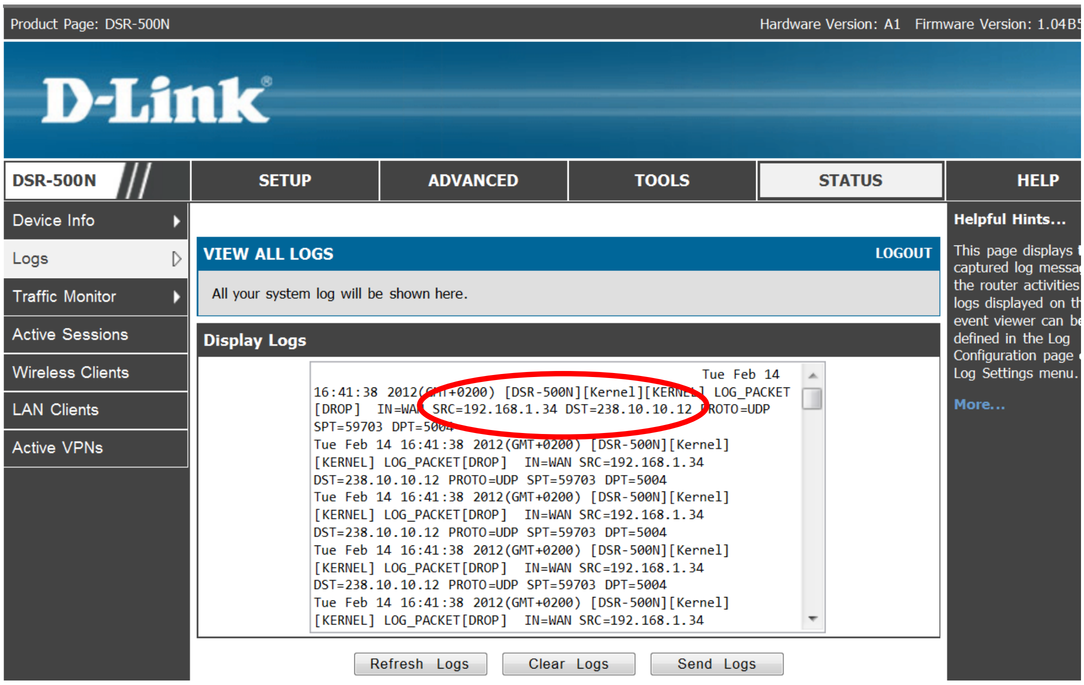
Other Events Logs

Helpful Hints...

Traffic through each network segment (L WAN, DMZ) can be tracked based on w the packet was acc or dropped by the f Denial of service at general attack information, login attempts, dropped packets, and similar events can be capt for review by the IT administrator.

More...

- После ОБЯЗАТЕЛЬНОЙ перегрузки устройства в системном журнале появятся соответствующие сообщения для отброшенных мультикаст-пакетов, в котором присутствует IP-адрес источника (в примере 192.168.1.34) для Multicast-потока 238.10.10.12 :

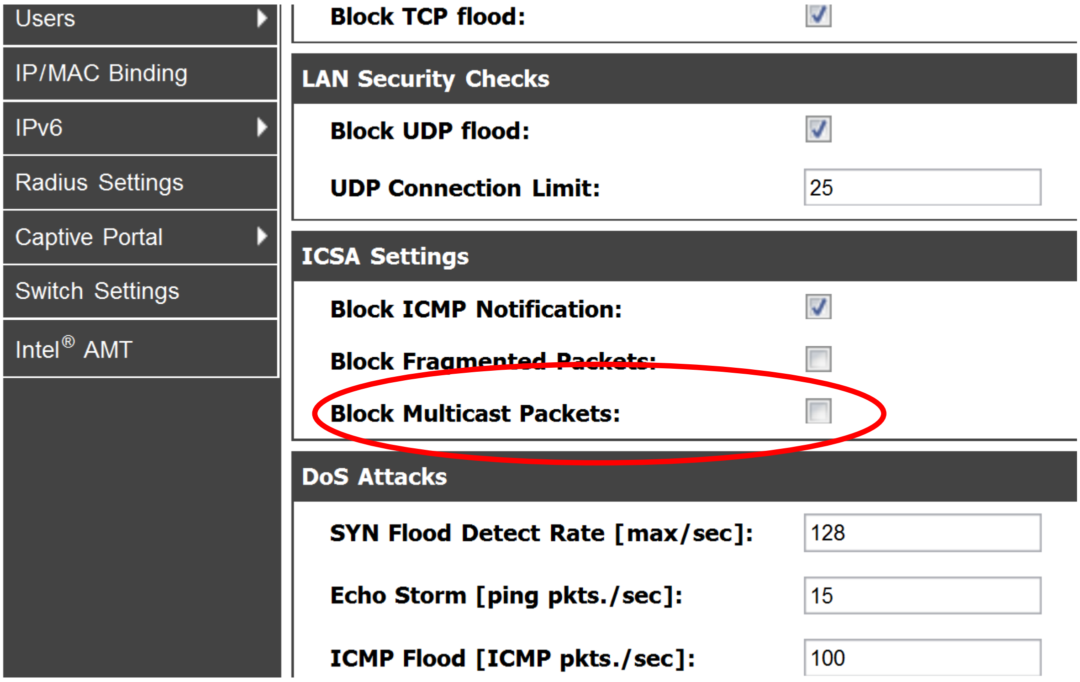


All your system log will be shown here.

```
                                                 Tue Feb 14
16:41:38 2012(GMT+0200) [DSR-500N][Kernel][KERNEL] LOG_PACKET
[DROP]  IN=WAN SRC=192.168.1.34 DST=238.10.10.12 PROTO=UDP
SPT=59703 DPT=5004
Tue Feb 14 16:41:38 2012(GMT+0200) [DSR-500N][Kernel]
[KERNEL] LOG_PACKET[DROP]  IN=WAN SRC=192.168.1.34
DST=238.10.10.12 PROTO=UDP SPT=59703 DPT=5004
Tue Feb 14 16:41:38 2012(GMT+0200) [DSR-500N][Kernel]
[KERNEL] LOG_PACKET[DROP]  IN=WAN SRC=192.168.1.34
DST=238.10.10.12 PROTO=UDP SPT=59703 DPT=5004
Tue Feb 14 16:41:38 2012(GMT+0200) [DSR-500N][Kernel]
[KERNEL] LOG_PACKET[DROP]  IN=WAN SRC=192.168.1.34
DST=238.10.10.12 PROTO=UDP SPT=59703 DPT=5004
Tue Feb 14 16:41:38 2012(GMT+0200) [DSR-500N][Kernel]
[KERNEL] LOG_PACKET[DROP]  IN=WAN SRC=192.168.1.34
```

This page displays t captured log messa the router activities logs displayed on th event viewer can be defined in the Log Configuration page Log Settings menu.

- Так же следует убедиться, что в настройках «Advanced -> Advanced Network -> Attack Checks» не стоит «птичка» на опции «Block Multicast Packets»:



Block TCP flood: ☑

LAN Security Checks

Block UDP flood: ☑

UDP Connection Limit: 25

ICSA Settings

Block ICMP Notification: ☑

Block Fragmented Packets: ☐

Block Multicast Packets: ☐

DoS Attacks

SYN Flood Detect Rate [max/sec]: 128

Echo Storm [ping pkts./sec]: 15

ICMP Flood [ICMP pkts./sec]: 100