

---

# SysLog Setup

---

## Introduction

Syslog is a popular utility in Unix world. For monitoring router activity, you can run a Syslog Daemon which will capture the activity output from the router. This Daemon program can run on a local PC or a remote one elsewhere on the Internet.

## Configuration

Check the **Enable** box to enable syslog service.

**Server IP Address:** The IP address which syslog message can be sent to.

**Destination Port:** The UDP port number which the syslog server is listening. The default value is 514.



The image shows a dialog box titled "SysLog Access Setup". It contains a checkbox labeled "Enable" which is currently unchecked. Below the checkbox are two input fields: "Server IP Address" and "Destination Port". The "Destination Port" field contains the value "514". At the bottom of the dialog box are three buttons: "Cancel", "Clear", and "OK".

Your Vigor router sends many types of syslog messages. Some examples of the syslog messages with their message format are shown next:

Example of User Access log message:

DrayTekSysLog

192.168.1.1

LAN Status

|            |            |
|------------|------------|
| TX Packets | RX Packets |
| 6350       | 1741       |

WAN Status(Static)

|              |            |         |
|--------------|------------|---------|
| GW IP Addr   | TX Packets | RX Rate |
| 172.16.2.6   | 1488       | 6       |
| IP Address   | RX Packets | TX Rate |
| 172.16.2.136 | 3291       | 29      |

Fire Wall Log | VPN Log | **User Access Log** | Call Log | WAN Log | Client | Local TCP Table | Local UDP Table

| Time           | Host      | Message   |
|----------------|-----------|---|
| Jan 1 00:02:28 | vigor2200 | Local User: 192.168.1.10 DNS -> a.r.tv.com                                |
| Jan 1 00:02:28 | vigor2200 | Local User: 192.168.1.10 DNS -> a.r.tv.com                                |
| Jan 1 00:02:28 | vigor2200 | Local User: 192.168.1.10:1543 -> 210.57.49.198:80 (TCP)Web                |
| Jan 1 00:02:28 | vigor2200 | Local User: 192.168.1.10:1544 -> 210.57.49.198:80 (TCP)Web                |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1545 -> 64.124.237.131:80 (TCP)Web               |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1540 -> 64.124.237.131:80 (TCP) close connection |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1545 -> 64.124.237.131:80 (TCP) close connection |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10 DNS -> gserv-cnet.zdnet.com                      |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10 DNS -> gserv-cnet.zdnet.com                      |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1548 -> 64.124.237.131:80 (TCP)Web               |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1549 -> 210.57.49.198:80 (TCP)Web                |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1550 -> 210.57.49.198:80 (TCP)Web                |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1551 -> 64.124.237.131:80 (TCP)Web               |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1552 -> 64.124.237.131:80 (TCP)Web               |
| Jan 1 00:02:29 | vigor2200 | Local User: 192.168.1.10:1553 -> 64.124.237.131:80 (TCP)Web               |

Running... 18:25:41

Example of WAN log message while using ISDN connection:

DrayTekSysLog

Any

LAN Status

|            |            |
|------------|------------|
| TX Packets | RX Packets |
| 0          | 0          |

WAN Status

|            |            |         |
|------------|------------|---------|
| GW IP Addr | TX Packets | RX Rate |
| ....       | 0          | 0       |
| IP Address | RX Packets | TX Rate |
| ....       | 0          | 0       |

Fire Wall Log | VPN Log | User Access Log | Call Log | **WAN Log** | Client | Local TCP Table | Local UDP Table

| Time            | Host      | Message  |
|-----------------|-----------|--|
| May 24 14:22:17 | vigor2200 | ISDN data call at B1 channel - disconnected , no AOC |
| May 24 14:22:13 | vigor2200 | ISDN data call at B1 channel - connected             |
| May 24 11:48:33 | vigor2200 | ISDN data call at B1 channel - disconnected , no AOC |
| May 24 11:48:30 | vigor2200 | ISDN data call at B1 channel - connected             |
| May 24 11:48:29 | vigor2200 | ISDN data call at B1 channel - dialing               |
| May 24 11:48:25 | vigor2200 | ISDN data call at B1 channel - disconnected , no AOC |
| May 24 11:48:22 | vigor2200 | ISDN data call at B1 channel - connected             |
| May 24 11:48:21 | vigor2200 | ISDN data call at B1 channel - dialing               |
| May 24 11:48:17 | vigor2200 | ISDN data call at B1 channel - disconnected , no AOC |
| May 24 11:48:14 | vigor2200 | ISDN data call at B1 channel - connected             |
| May 24 11:48:13 | vigor2200 | ISDN data call at B1 channel - dialing               |
| May 24 11:48:09 | vigor2200 | ISDN data call at B1 channel - disconnected , no AOC |
| May 24 11:48:06 | vigor2200 | ISDN data call at B1 channel - connected             |
| May 24 11:48:05 | vigor2200 | ISDN data call at B1 channel - dialing               |
| May 24 11:48:02 | vigor2200 | ISDN data call at B1 channel - disconnected , no AOC |

Running... 15:51:58

Example of VPN (IPSec) log message while the VPN/IPSec tunnel is being used:

The screenshot shows the DrayTekSysLog application window. At the top, there are status sections for LAN and WAN. The LAN Status shows TX Packets and RX Packets both at 0. The WAN Status shows GW IP Addr, TX Packets, and RX Rate, all at 0. Below these are tabs for different log types: Fire Wall Log, VPN Log, User Access Log, Call Log, WAN Log, Client, Local TCP Table, and Local UDP Table. The VPN Log tab is selected, displaying a table of log messages. The table has three columns: Time, Host, and Message. The messages show a sequence of 'sent MR3, ISAKMP SA established' and 'IPsec SA established' for the host 'Vigor'. The status bar at the bottom shows 'Running...' and the time '18:33:29'.

| Time            | Host  | Message                         |
|-----------------|-------|---------------------------------|
| May 24 17:55:16 | Vigor | sent MR3, ISAKMP SA established |
| May 24 17:55:16 | Vigor | IPsec SA established            |
| May 24 17:57:34 | Vigor | sent MR3, ISAKMP SA established |
| May 24 17:57:34 | Vigor | IPsec SA established            |
| May 24 17:59:30 | Vigor | sent MR3, ISAKMP SA established |
| May 24 17:59:30 | Vigor | IPsec SA established            |
| May 24 18:04:10 | Vigor | sent MR3, ISAKMP SA established |
| May 24 18:04:10 | Vigor | IPsec SA established            |
| May 24 18:05:10 | Vigor | sent MR3, ISAKMP SA established |
| May 24 18:05:10 | Vigor | IPsec SA established            |
| May 24 18:06:51 | Vigor | sent MR3, ISAKMP SA established |
| May 24 18:06:51 | Vigor | IPsec SA established            |
| May 24 18:07:33 | Vigor | sent MR3, ISAKMP SA established |
| May 24 18:07:33 | Vigor | IPsec SA established            |
| Jan 1 00:00:04  | Vigor | sent MR3, ISAKMP SA established |