



OPEN 501R ADSL Router Application Note

Traffic Monitoring



Introduction

Monitoring the traffic through your 501R has several uses: verify link performance, verify billing data, and detect possible hacking of your network.

To monitor the traffic, a freeware SNMP tool is used. There are many free SNMP network management/monitoring tools available on the Internet, but here we will use MRTG, an easy to use package for Windows and UNIX/Linux.

This application note will not go into detail on how to install MRTG but will provide links to install documentation on the Internet.

About MRTG

- The official website is <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>
- Some background information can be obtained from <http://faq.mrtg.org/>

Installing MRTG

Windows 95/98/Me

Follow the instructions at <http://www.cruzio.com/~jeffl/mrtg/docs/w95mrtg.htm>.

Note that this guide is aimed at monitoring Windows SNMP objects. You do not need to install SNMP Client Network Services on your PC, as the 501R has SNMP built in.

Windows NT/2000/XP

Follow the instructions at <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/nt-guide.html>

UNIX/Linux

Follow the instructions at <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/unix-guide.html>

Configure MRTG

Use the `cfgmaker` script as described in the install documents above.

The read-only community name for the 501R is `public` by default, but may have been changed. Check by telnetting to the 501R and going to the `MAIN/CONF/SNMP/COMMUNITY` menu.

For example, if your read-only community name is `public` and the IP address of the 501R LAN interface is 192.168.2.254, then the command to create the configuration file would be:

```
perl cfgmaker public@192.168.1.254 --global "WorkDir: c:\www\mrtg" --  
output mrtg.cfg
```

Web servers

You do not need to run a web server to view the MRTG graphs, but it does make things easier if you want to use one PC to monitor the network and access the graphs from other PCs.

The Apache web server is recommended in the previous installation guide, but can be confusing to install and configure for those in a hurry. An more simple alternative web server for Windows and Linux is the Abyss web server from <http://www.aprelum.com/>.

Detecting hacking activity

One use of traffic monitoring to check if there are unexplained high levels of outbound traffic. This may indicate that your computers have been hacked and are being used to launch denial of service attacks.

For more information see the Gibson Research report at <http://grc.com/dos/grcdos.htm>.

If you are concerned about hacking, you may wish to install an intrusion detection package such as Snort from www.snort.org.