Installing the Packeteer Linux FDR Tools on RedHat 9.0

created by: Rainer Bemsel – Version 1.0 – Dated: Mar/26/2005

The purpose of this document is to provide you some basic steps to install FDR on Linux RedHat 9.0. The Flow Detail Records (FDR) feature is a method for gathering and processing per-flow statistics. When FDR is enabled, the Packeteer unit will become an ***emitter***, periodically pushing data to a remote system called a ***collector***. The unit will emit records that contain details of all flows that go through PacketShaper/PacketSeeker to a collector, such as Packeteer's ReportCenter 3. Packeteer Linux FDR Tools is open source and distributed under the terms of the license, at the end of this TechNote, which uses the BSD License template.

My System is running Kernel 2.4.20-31.9. Thanks to Richard and Martin, for providing me the necessary information to create this TechNote.

Setting up the collector server machine

These instructions should be sufficient for setting up a minimal RedHat 9 installation with enough capabilities to support the Packeteer flow data recorder tools.

Installing RedHat 9 from CD: (RedHat 9 CDs 1-3)

- boot from CD 1, do a new Red Hat Linux installation
- choose "Workstation" for Installation Type
- accept defaults for all options, including packages, with one exception.
- EXCEPTION: select no firewall (or you won't be able to talk to your web server)

(If you are new to Linux, you may want to consider my 30 Minutes RedHat Core Installation Procedure, which can be found on www.bemsel.com/TechTip/RBE_RH_Easy.PDF)

Once the install is complete, log in as root.

Make sure the apache web server is on:

```
/usr/sbin/apachectl start
```

Log files for apache are typically in /var/log/httpd/

To see what, if anything, might be going wrong:

```
tail /var/log/httpd/error_log
```

To have apache start up automatically at boot time:

```
/sbin/chkconfig --level 35 httpd on
```

If you need to see your ip address:

```
/sbin/ifconfig
```

If you need to see your nic settings:

```
/sbin/mii-tool
```

To change your ip address (especially if you want a static ip address):

```
/usr/sbin/netconfig
```

Rainer's Technical Tips

DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user

The whole package to install FDR Tools is in packeteerfdr-1.0.1.tar.gz. Extract the content. It will create a sub-directory called “packeteerbuilt”.

Make sure, you have internet connection, because GD Installation will connect to **ftp.perl.org**

The remaining instructions, followed top to bottom, should install all necessary Linux pieces.

The following packages are required:

- ❑ postgresql
- ❑ postgresql-libs
- ❑ postgresql-server
- ❑ postgresql-devel
- ❑ gcc
- ❑ binutils
- ❑ cpp
- ❑ glibc
- ❑ glibc-devel
- ❑ glibc-kernheaders
- ❑ zlib
- ❑ zlib-devel
- ❑ libpng
- ❑ libpng-devel
- ❑ libjpeg-devel
- ❑ perl-CPAN
- ❑ perl-DBI
- ❑ perl-DBD-Pg
- ❑ perl-CGI

To get postgresql, compilers, libraries (zlib, PNG, gd), and the CGI and DBI perl modules, execute the following shell script as superuser:

```
[root@Hawkeye packeteerbuilt] sh rh9first.sh
```

Now go get the GD.pm perl library. This is used to create graphics in reports.
If CPAN wants to ask you a bunch of questions, say "no", you don't want to answer manually.

```
[root@Hawkeye packeteerbuilt] perl -MCPAN -e 'shell'

/usr/lib/perl5/5.8.0/CPAN/Config.pm initialized.

Are you ready fro manual configuration? [yes] no

cpan> install GD
```

Answer questions this way:

Where is libgd installed? [/usr/lib] <take the default>
Build JPEG support? [y] y
Build FreeType support? [y] n
Build XPM support? [y] n

To get out of CPAN, "quit".

```
cpan> quit
Lockfile removed.
[root@Hawkeye packeteerbuilt]
```

Troubleshooting tip -- if for some reason CPAN won't run, we found the following to be helpful:

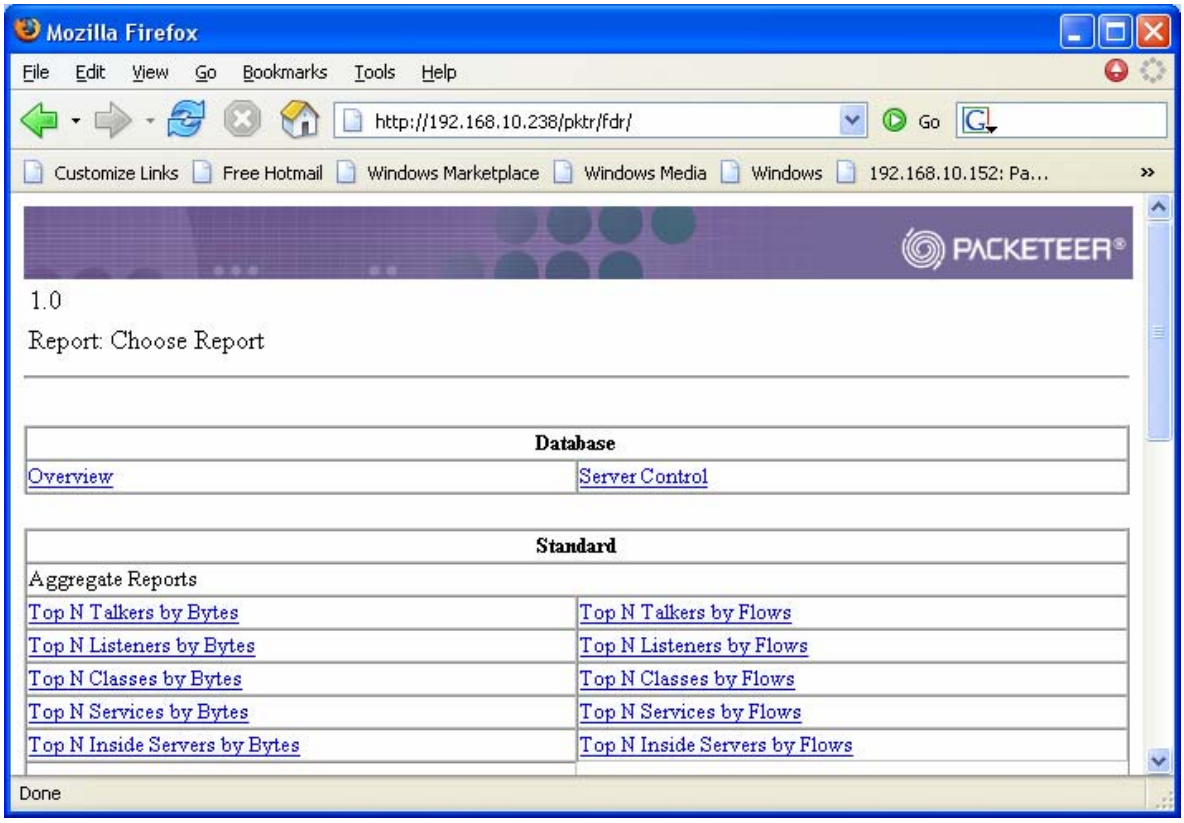
```
locate .pm.links
cd /usr/lib/perl5/5.8.0/CPAN/
mv FirstTime.pm.links FirstTime.pm
cd /usr/lib/perl5/5.8.0
mv CPAN.pm.links CPAN.pm
```

At this point, your machine should be ready for installation of the Packeteer flow tools package.

Execute this script:

```
[root@Hawkeye packeteerbuilt]sh rh9last.sh
Starting postgresql                                        [OK]
Initializing database:                                     [OK]
Starting apache
Adding a postgresql user for the current user
Enter name of user to add:
Adding a postgresql user apache.
Starting fdrcollect…
Creating the database.
Starting PAcketWise FDR Collector:                         [OK]
[root@Hawkeye packeteerbuilt]
```

If all goes well, you should now be ready to go to http://localhost/pktr/fdr to start using the tools.



Only one more step to go

Configuring the PacketShaper

To prepare the PacketShaper to transmit flow records to your collector:

1) Install a PacketWise 7.x image on one or more of your units using the "image load" command or the web interface.

2) After the unit reboots, configure PacketWise to send flow detail records

- Touch access is required to use the setup flowrecords command. Log in using the "touch" password.

- Issue the "setup flow" command to start sending flow records:
  This command changed syntax in PacketWise 7.0.1. Issue the command appropriate to your PacketWise version.

PacketWise 7.0:

```
        setup flow 1 packeteer-1 <linux-ip-addr> 9191 on
or
        setup flow 1 packeteer-2 <linux-ip-addr> 9191 on
```

PacketWise 7.0.1

```
    setup flow id 1 packeteer-1 <linux-ip-addr> 9191 on
or
    setup flow id 1 packeteer-2 <linux-ip-addr> 9191 on
```

packeteer-2 sends flow records that include response time management data, and are larger than packeteer-1 records. If you don't need the **response time management data**, choose packeteer-1.

"setup flow" instructs a PacketShaper to send flow records of the specified type (Packeteer-1 or Packeteer-2) to the ip address of the Linux box where the FDR Collector is installed on port 9191.

3) PacketWise 7.0.1 also requires two additional commands:

```
setup variable flowRecordsSendPktr0 1
setup variable flowRecordsSendPktrP 1
```

To learn more, see the files Queries, and ReadMe in:
/usr/share/doc/packeteerflowtools-1.0.0

Certified Novell Engineer Novell
CERTIFIED CUBE UB EXPERT
SwitchExpert XYLAN CERTIFIED SWITCH EXPERT
Certified Instructor EMEA
CompTIA Security+™ Certified
PACKETEER CERTIFIED EXPERT

Handy to know

To start or stop the Collector:

su root -l -c "/etc/init.d/fdrcollect start"
su root -l -c "/etc/init.d/fdrcollect stop"

To use the FDR command shell, type "fdr" at the shell prompt.

To backup the database:

pg_dump fdr | gzip > fdr.backup.gz

To restore the database (both the schema and the data):

gunzip -c fdr.backup.gz | psql fdr

See the postgres documentation more information about backing up or exporting data from the database.

To delete all the data in your database:

psql fdr
delete from flows;
delete from flowsarchive;
delete from samples;
delete from samplesarchive;
delete from classes;
delete from services;
delete from interfaces;
delete from groups;
delete from groupsofgroups;
vacuum full analyze;

To check and see if you are receiving FDR records you can look at the packets with tcpdump, or check the database

TCPDUMP: (Exit with CTRL+C)

```
[root@Hawkeye root] tcpdump dst port 9191
Tcpdump: listening on eth0
12:38:13.679958 192.168.10.152.9913 > 192.168.10.238.9191: udp 172
```

Detailed documentation about postgres and the queries it accepts can be found at

http://www.postgresql.org/docs/

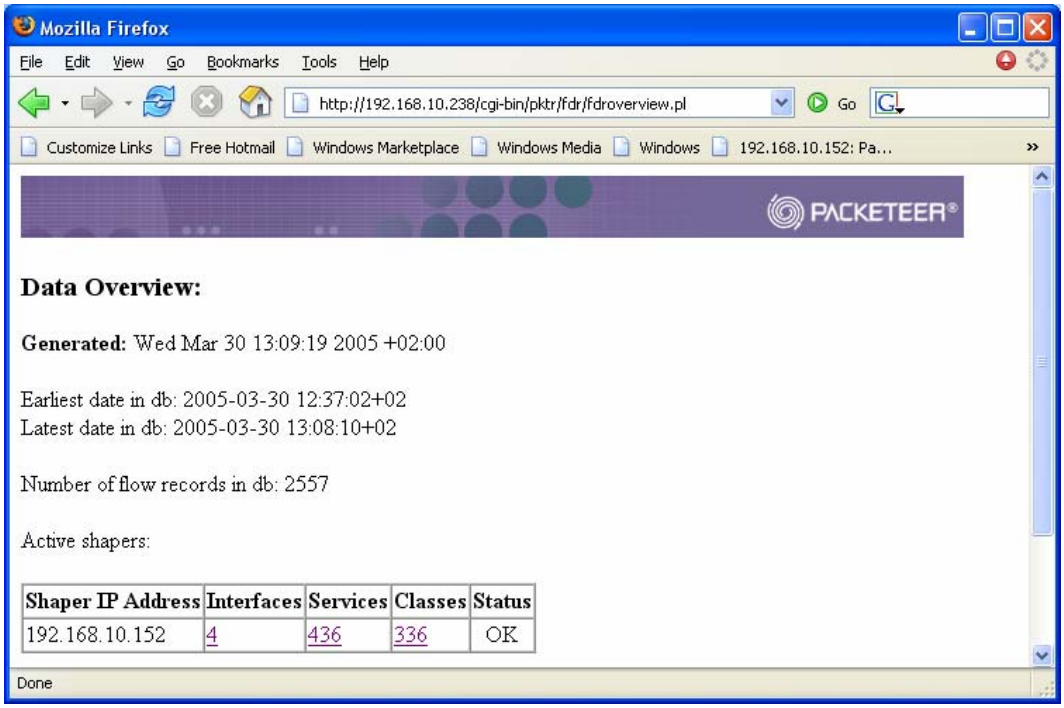
By default it retains two weeks of data

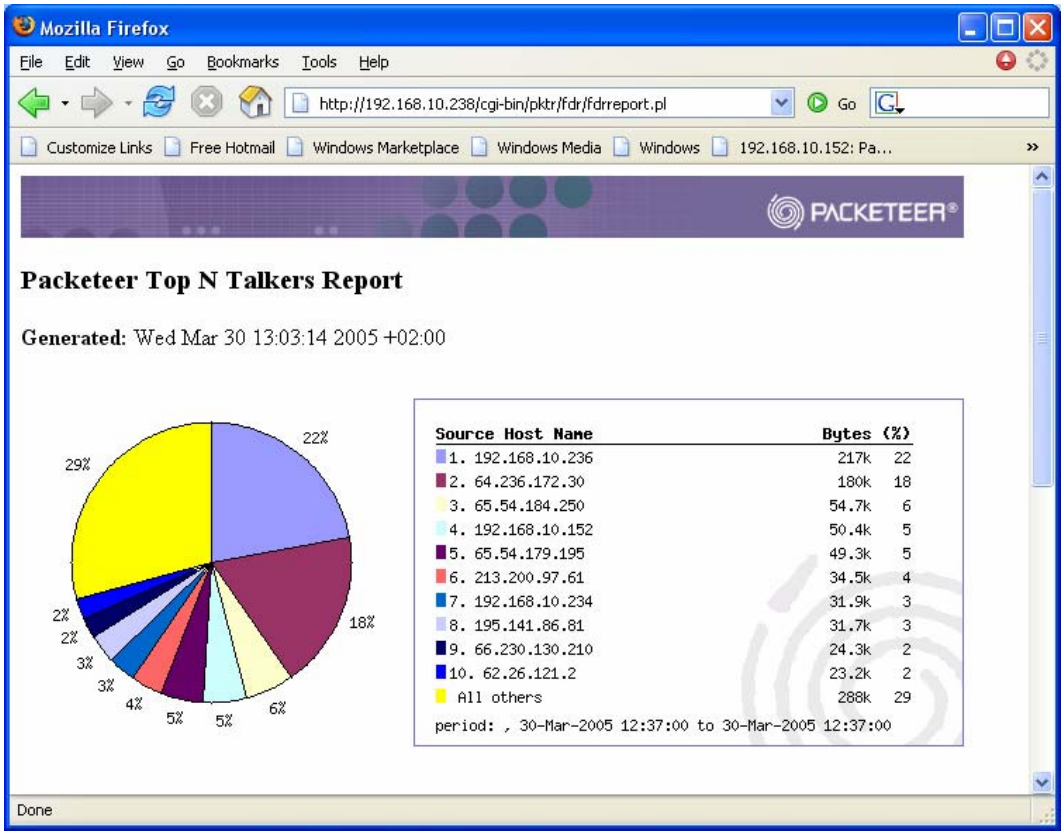
If you wish to modify how much data the database will retain, edit:
/usr/local/share/fdr/etc/cleanup

Checking Postgres:

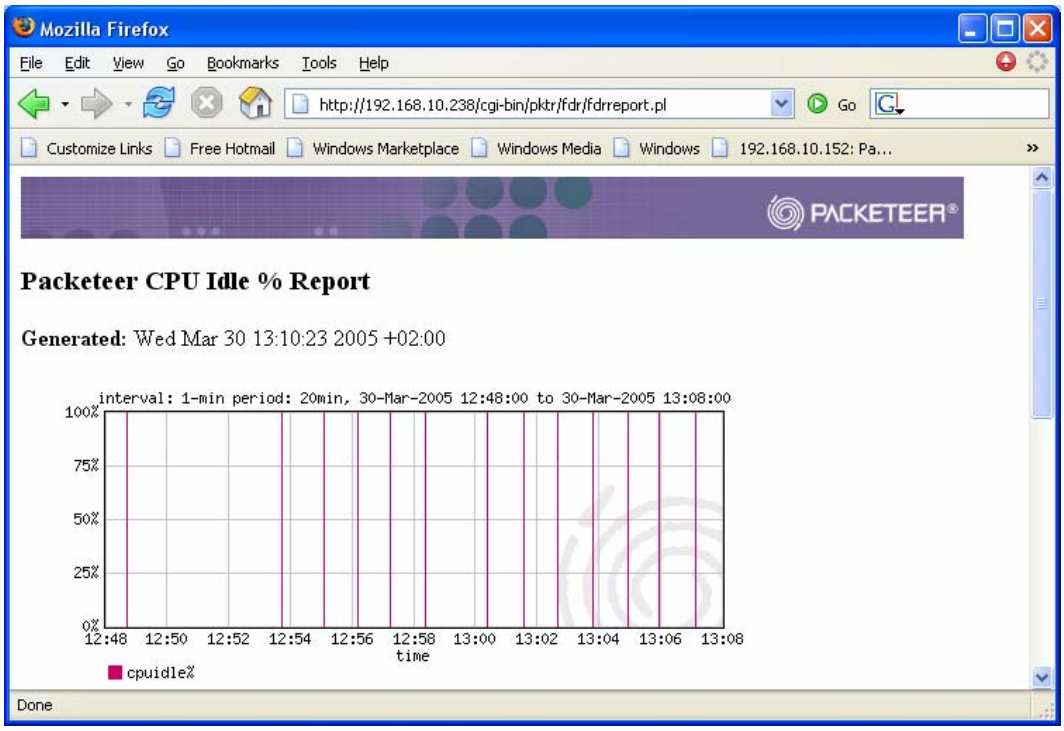
psql fdr
select count(*) from flows;

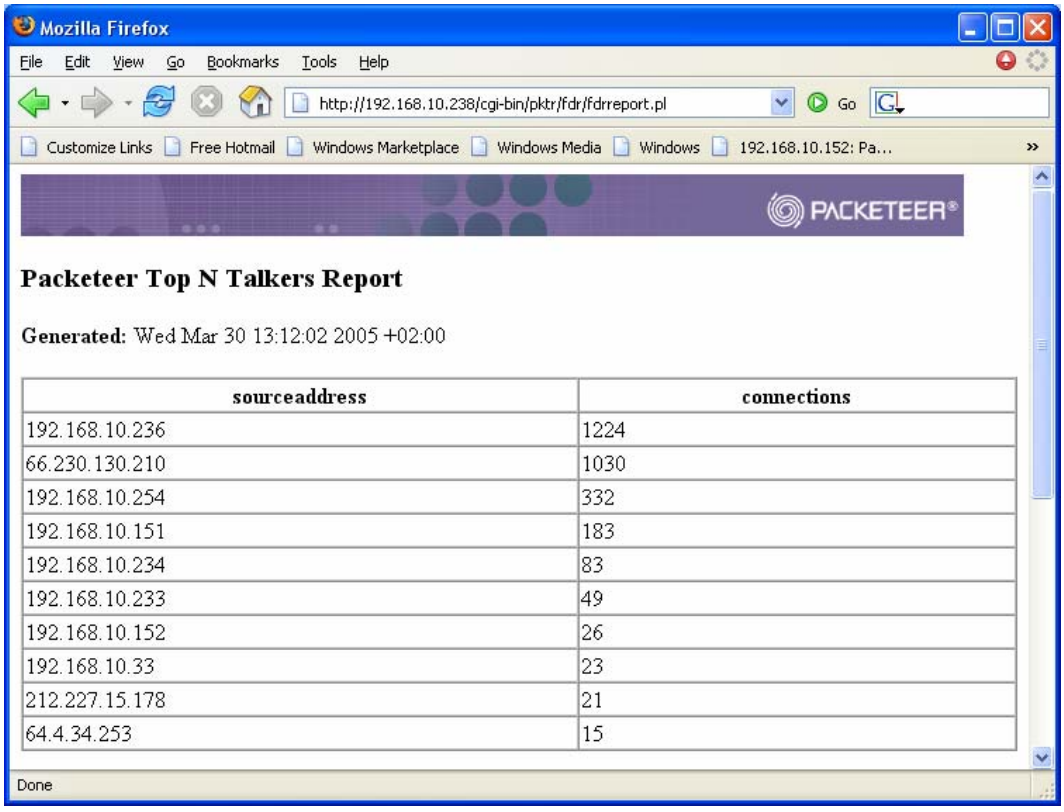
Some Report Examples:





Certified NOVELL ENGINEER Novell
CERTIFIED CUBE EXPERT
SwitchExpert XYLAN CERTIFIED SWITCH EXPERT
Certified Instructor EMEA
CompTIA Security+ Certified
PACKETEER CERTIFIED EXPERT





sourceaddress	connections
192.168.10.236	1224
66.230.130.210	1030
192.168.10.254	332
192.168.10.151	183
192.168.10.234	83
192.168.10.233	49
192.168.10.152	26
192.168.10.33	23
212.227.15.178	21
64.4.34.253	15

Certified Novell Engineer Novell
CERTIFIED CUBE EXPERT
SwitchExpert XYLAN CERTIFIED SWITCH EXPERT
Certified Instructor EMEA
CompTIA Security+™ Certified
PACKETEER CERTIFIED EXPERT


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.10.238/pktr/fdr/index.html
Go
Customize Links Free Hotmail Windows Marketplace Windows Media Windows 192.168.10.152: Pa...
PACKETEER
1.0
Report: Choose Report
Database
Overview
Server Control
Standard
Aggregate Reports
Top N Talkers by Bytes
Top N Talkers by Flows
Top N Listeners by Bytes
Top N Listeners by Flows
Top N Classes by Bytes
Top N Classes by Flows
Top N Services by Bytes
Top N Services by Flows
Top N Inside Servers by Bytes
Top N Inside Servers by Flows
Per-Flow Reports
Most Retransmissions
Longest Completed Flows (bytes)
History Recent
Longest Completed Flows (time)
Policy Summary
Flows with Service Unknown
Time Reports
Shaper CPU Idle Report
Link Utilization
Custom Reports
Ad-Hoc Custom SQL
User Defined Reports
Show
Add
Edit
Delete
User Defined IP Address Groups
Show
Add
Edit
Delete
Documentation
ReadMe
Release Notes
Installation
FDR Shell Queries
OS-specific Installation Notes
Knoppix
Fedora Core 3
Red Hat 9
Installing Red Hat 9
Done

Any inquiries can be addressed to Packeteer via electronic mail at the address: fdr@packeteer.com, or by post: Tools Product Manager, Packeteer, Inc. 10201 N. De Anza Blvd. Cupertino, California USA 95014.

LICENSE:

Copyright (c) 2004-2005, Packeteer, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Packeteer Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER
OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.