Setting up a Netflow Collector

Background

This page shows a step by step account on installing a netflow collector using `flow-capture` on a RHEL4 system. All files will be installed onto `/opt/netflow/`.

Prerequisites

flow-tools 0.68 (here)

Flow-tools compilation

```
[x@nettest13 ~]$ sudo mkdir /opt/netflow
Password:
[x@nettest13 ~]$ mkdir /opt/netflow/src
[x@nettest13 ~]$ cd /opt/netflow/src
[x@nettest13 src]$ mkdir flow-tools
[x@nettest13 src]$ cd flow-tools
[x@nettest13 flow-tools]$ wget ftp://ftp.eng.oar.net/pub/flow-tools/flow-tools-0.68.tar.gz
[x@nettest13 flow-tools]$ tar xfz flow-tools-0.68.tar.gz
[x@nettest13 flow-tools]$ cd flow-tools-0.68
```

```
[x@nettest13 flow-tools-0.68]$ ./configure --prefix=/opt/netflow/
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking for gcc... gcc
checking for C compiler default output... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ANSI C... none needed
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking for a BSD-compatible install... /usr/bin/install -c
checking whether make sets $(MAKE)... (cached) yes
checking for bison... bison -y
checking for ranlib... ranlib
checking for flex... flex
checking for yywrap in -lfl... yes
checking lex output file root... lex.yy
checking whether yytext is a pointer... yes
checking for main in -ly... yes
checking for zlibVersion in -lz... yes
checking for allow_severity in -lwrap... yes
checking for dirent.h that defines DIR... yes
checking for library containing opendir... none required
checking how to run the C preprocessor... gcc -E
checking for egrep... grep -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
checking for memory.h... yes
checking for strings.h... yes
checking for inttypes.h... yes
checking for stdint.h... yes
```

```
checking for unistd.h... yes
checking fcntl.h usability... yes
checking fcntl.h presence... yes
checking for fcntl.h... yes
checking features.h usability... yes
checking features.h presence... yes
checking for features.h... yes
checking limits.h usability... yes
checking limits.h presence... yes
checking for limits.h... yes
checking malloc.h usability... yes
checking malloc.h presence... yes
checking for malloc.h... yes
checking for string.h... (cached) yes
checking for strings.h... (cached) yes
checking sys/time.h usability... yes
checking sys/time.h presence... yes
checking for sys/time.h... yes
checking syslog.h usability... yes
checking syslog.h presence... yes
checking for syslog.h... yes
checking for unistd.h... (cached) yes
checking for sin_len in sockaddr_in ...
no
checking for an ANSI C-conforming const... yes
checking for off_t... yes
checking for pid_t... yes
checking for size_t... yes
checking for struct stat.st_rdev... yes
checking whether time.h and sys/time.h may both be included... yes
checking whether struct tm is in sys/time.h or time.h... time.h
checking for stdlib.h... (cached) yes
checking for unistd.h... (cached) yes
checking for getpagesize... yes
checking for working mmap... yes
checking for working alloca.h... yes
checking for alloca... yes
checking return type of signal handlers... void
checking for gethostbyname in -lnsl... yes
checking for socket in -lsocket... no
checking for gethostname... yes
checking for gettimeofday... yes
checking for select... yes
checking for socket... yes
checking for strdup... yes
checking for strtoul... yes
checking for timelocal... yes
checking for sigaction... yes
checking for strsep... yes
checking for strerror... yes
checking for strtoull... yes
checking strtoul returns 64 bits... yes
configure: creating ./config.status
config.status: creating lib/Makefile
config.status: creating src/Makefile
config.status: creating bin/Makefile
config.status: creating Makefile
config.status: creating docs/Makefile
config.status: creating lib/ftpaths.h
config.status: creating configs/Makefile
config.status: creating docs/flow-capture.1
config.status: creating docs/flow-capture.html
config.status: creating docs/flow-nfilter.1
config.status: creating docs/flow-nfilter.html
config.status: creating docs/flow-print.1
config.status: creating docs/flow-print.html
config.status: creating docs/flow-report.1
config.status: creating docs/flow-report.html
config.status: creating docs/flow-receive.1
config.status: creating docs/flow-receive.html
config.status: creating docs/flow-tag.1
```

```
config.status: creating docs/flow-tag.html
config.status: creating docs/flow-mask.1
config.status: creating docs/flow-mask.html
config.status: creating docs/flow-fanout.1
config.status: creating docs/flow-fanout.html
config.status: creating docs/flow-xlate.1
config.status: creating docs/flow-xlate.html
config.status: creating docs/flow-rpt2rrd.1
config.status: creating docs/flow-rpt2rrd.html
config.status: creating docs/flow-rptfmt.1
config.status: creating docs/flow-rptfmt.html
config.status: creating docs/flow-log2rrd.1
config.status: creating docs/flow-log2rrd.html
config.status: creating lib/ftconfig.h
config.status: lib/ftconfig.h is unchanged
config.status: executing depfiles commands

Please subscribe to the flow-tools mailing list by sending a message to
flow-tools-request@splintered.net

Now type make to continue the build process
```

```
[x@nettest13 flow-tools-0.68]$ make
Making all in lib
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/lib'
make  all-am
make[2]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/lib'
source='ftio.c' object='ftio.o' libtool=no \
depfile='.deps/ftio.Po' tmpdepfile='.deps/ftio.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftio.c' || echo './'`ftio.c
ftio.c: In function `readn':
ftio.c:2270: warning: use of cast expressions as lvalues is deprecated
ftio.c: In function `writen':
ftio.c:2295: warning: use of cast expressions as lvalues is deprecated
source='ftswap.c' object='ftswap.o' libtool=no \
depfile='.deps/ftswap.Po' tmpdepfile='.deps/ftswap.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftswap.c' || echo './'`ftswap.c
source='ftencode.c' object='ftencode.o' libtool=no \
depfile='.deps/ftencode.Po' tmpdepfile='.deps/ftencode.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftencode.c' || echo './'`ftencode.c
source='ftdecode.c' object='ftdecode.o' libtool=no \
depfile='.deps/ftdecode.Po' tmpdepfile='.deps/ftdecode.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftdecode.c' || echo './'`ftdecode.c
source='ftprof.c' object='ftprof.o' libtool=no \
depfile='.deps/ftprof.Po' tmpdepfile='.deps/ftprof.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftprof.c' || echo './'`ftprof.c
source='bit1024.c' object='bit1024.o' libtool=no \
depfile='.deps/bit1024.Po' tmpdepfile='.deps/bit1024.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'bit1024.c' || echo './'`bit1024.c
source='fmt.c' object='fmt.o' libtool=no \
depfile='.deps/fmt.Po' tmpdepfile='.deps/fmt.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'fmt.c' || echo './'`fmt.c
source='support.c' object='support.o' libtool=no \
depfile='.deps/support.Po' tmpdepfile='.deps/support.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'support.c' || echo './'`support.c
source='ftfile.c' object='ftfile.o' libtool=no \
depfile='.deps/ftfile.Po' tmpdepfile='.deps/ftfile.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftfile.c' || echo './'`ftfile.c
source='fttlv.c' object='fttlv.o' libtool=no \
```

```
depfile='.deps/fttlv.Po' tmpdepfile='.deps/fttlv.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'fttlv.c' || echo './'`fttlv.c
fttlv.c: In function `fttlv_enc_uint32':
fttlv.c:71: warning: use of cast expressions as lvalues is deprecated
fttlv.c:74: warning: use of cast expressions as lvalues is deprecated
fttlv.c: In function `fttlv_enc_uint16':
fttlv.c:110: warning: use of cast expressions as lvalues is deprecated
fttlv.c:113: warning: use of cast expressions as lvalues is deprecated
fttlv.c: In function `fttlv_enc_uint8':
fttlv.c:148: warning: use of cast expressions as lvalues is deprecated
fttlv.c:151: warning: use of cast expressions as lvalues is deprecated
fttlv.c: In function `fttlv_enc_str':
fttlv.c:186: warning: use of cast expressions as lvalues is deprecated
fttlv.c:189: warning: use of cast expressions as lvalues is deprecated
fttlv.c: In function `fttlv_enc_ifname':
fttlv.c:233: warning: use of cast expressions as lvalues is deprecated
fttlv.c:236: warning: use of cast expressions as lvalues is deprecated
fttlv.c:239: warning: use of cast expressions as lvalues is deprecated
fttlv.c:242: warning: use of cast expressions as lvalues is deprecated
fttlv.c: In function `fttlv_enc_ifalias':
fttlv.c:290: warning: use of cast expressions as lvalues is deprecated
fttlv.c:293: warning: use of cast expressions as lvalues is deprecated
fttlv.c:296: warning: use of cast expressions as lvalues is deprecated
fttlv.c:299: warning: use of cast expressions as lvalues is deprecated
fttlv.c:302: warning: use of cast expressions as lvalues is deprecated
source='ftmap.c' object='ftmap.o' libtool=no \
depfile='.deps/ftmap.Po' tmpdepfile='.deps/ftmap.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftmap.c' || echo './'`ftmap.c
source='ftrec.c' object='ftrec.o' libtool=no \
depfile='.deps/ftrec.Po' tmpdepfile='.deps/ftrec.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftrec.c' || echo './'`ftrec.c
source='fterr.c' object='fterr.o' libtool=no \
depfile='.deps/fterr.Po' tmpdepfile='.deps/fterr.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'fterr.c' || echo './'`fterr.c
source='ftchash.c' object='ftchash.o' libtool=no \
depfile='.deps/ftchash.Po' tmpdepfile='.deps/ftchash.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftchash.c' || echo './'`ftchash.c
ftchash.c: In function `ftchash_foreach':
ftchash.c:329: warning: use of cast expressions as lvalues is deprecated
source='ftsym.c' object='ftsym.o' libtool=no \
depfile='.deps/ftsym.Po' tmpdepfile='.deps/ftsym.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftsym.c' || echo './'`ftsym.c
source='radix.c' object='radix.o' libtool=no \
depfile='.deps/radix.Po' tmpdepfile='.deps/radix.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'radix.c' || echo './'`radix.c
source='fttag.c' object='fttag.o' libtool=no \
depfile='.deps/fttag.Po' tmpdepfile='.deps/fttag.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'fttag.c' || echo './'`fttag.c
source='ftfil.c' object='ftfil.o' libtool=no \
depfile='.deps/ftfil.Po' tmpdepfile='.deps/ftfil.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftfil.c' || echo './'`ftfil.c
source='ftstat.c' object='ftstat.o' libtool=no \
depfile='.deps/ftstat.Po' tmpdepfile='.deps/ftstat.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftstat.c' || echo './'`ftstat.c
source='getdate.c' object='getdate.o' libtool=no \
depfile='.deps/getdate.Po' tmpdepfile='.deps/getdate.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'getdate.c' || echo './'`getdate.c
source='ftxfield.c' object='ftxfield.o' libtool=no \
depfile='.deps/ftxfield.Po' tmpdepfile='.deps/ftxfield.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
```

```
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftxfield.c' || echo './'`ftxfield.c
source='ftmask.c' object='ftmask.o' libtool=no \
depfile='.deps/ftmask.Po' tmpdepfile='.deps/ftmask.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftmask.c' || echo './'`ftmask.c
source='ftvar.c' object='ftvar.o' libtool=no \
depfile='.deps/ftvar.Po' tmpdepfile='.deps/ftvar.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftvar.c' || echo './'`ftvar.c
source='ftxlate.c' object='ftxlate.o' libtool=no \
depfile='.deps/ftxlate.Po' tmpdepfile='.deps/ftxlate.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I. -I./lib -I. -I. -I.    -g -Wall -g -Wall -c `test -f 'ftxlate.c' || echo './'`ftxlate.c
rm -f libft.a
ar cru libft.a ftio.o ftswap.o ftencode.o ftdecode.o ftprof.o bit1024.o fmt.o support.o ftfile.o fttlv.o ftmap.
o ftrec.o fterr.o ftchash.o ftsym.o radix.o fttag.o ftfil.o ftstat.o getdate.o ftxfield.o ftmask.o ftvar.o
ftxlate.o
ranlib libft.a
make[2]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/lib'
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/lib'
Making all in src
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/src'
source='flow-capture.c' object='flow-capture.o' libtool=no \
depfile='.deps/flow-capture.Po' tmpdepfile='.deps/flow-capture.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-capture.c' || echo './'`flow-
capture.c
gcc -g -Wall -g -Wall   -o flow-capture -L../lib flow-capture.o -lft  -lnsl -lwrap -lz
source='flow-cat.c' object='flow-cat.o' libtool=no \
depfile='.deps/flow-cat.Po' tmpdepfile='.deps/flow-cat.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-cat.c' || echo './'`flow-cat.
c
gcc -g -Wall -g -Wall   -o flow-cat -L../lib flow-cat.o -lft -lnsl -lwrap -lz
source='flow-stat.c' object='flow-stat.o' libtool=no \
depfile='.deps/flow-stat.Po' tmpdepfile='.deps/flow-stat.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-stat.c' || echo './'`flow-
stat.c
gcc -g -Wall -g -Wall   -o flow-stat -L../lib flow-stat.o -lft -lnsl -lwrap -lz
source='flow-print.c' object='flow-print.o' libtool=no \
depfile='.deps/flow-print.Po' tmpdepfile='.deps/flow-print.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-print.c' || echo './'`flow-
print.c
gcc -g -Wall -g -Wall   -o flow-print -L../lib flow-print.o -lft -lnsl -lwrap -lz
source='flow-dscan.c' object='flow-dscan.o' libtool=no \
depfile='.deps/flow-dscan.Po' tmpdepfile='.deps/flow-dscan.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-dscan.c' || echo './'`flow-
dscan.c
gcc -g -Wall -g -Wall   -o flow-dscan -L../lib flow-dscan.o -lft -lnsl -lwrap -lz
source='flow-send.c' object='flow-send.o' libtool=no \
depfile='.deps/flow-send.Po' tmpdepfile='.deps/flow-send.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-send.c' || echo './'`flow-
send.c
gcc -g -Wall -g -Wall   -o flow-send -L../lib flow-send.o -lft -lnsl -lwrap -lz
source='flow-receive.c' object='flow-receive.o' libtool=no \
depfile='.deps/flow-receive.Po' tmpdepfile='.deps/flow-receive.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-receive.c' || echo './'`flow-
receive.c
gcc -g -Wall -g -Wall   -o flow-receive -L../lib flow-receive.o -lft -lnsl -lwrap -lz
source='flow-gen.c' object='flow-gen.o' libtool=no \
depfile='.deps/flow-gen.Po' tmpdepfile='.deps/flow-gen.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-gen.c' || echo './'`flow-gen.
c
gcc -g -Wall -g -Wall   -o flow-gen -L../lib flow-gen.o -lft -lnsl -lwrap -lz
source='flow-expire.c' object='flow-expire.o' libtool=no \
```

```
depfile='.deps/flow-expire.Po' tmpdepfile='.deps/flow-expire.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-expire.c' || echo './'`flow-
expire.c
gcc -g -Wall -g -Wall   -o flow-expire -L../lib flow-expire.o -lft -lnsl -lwrap -lz
source='flow-filter.c' object='flow-filter.o' libtool=no \
depfile='.deps/flow-filter.Po' tmpdepfile='.deps/flow-filter.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-filter.c' || echo './'`flow-
filter.c
source='aclyacc.c' object='aclyacc.o' libtool=no \
depfile='.deps/aclyacc.Po' tmpdepfile='.deps/aclyacc.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'aclyacc.c' || echo './'`aclyacc.c
y.tab.c: In function `yyparse':
y.tab.c:417: warning: implicit declaration of function `yylex'
y.tab.c:458: warning: implicit declaration of function `yyerror'
source='acllex.c' object='acllex.o' libtool=no \
depfile='.deps/acllex.Po' tmpdepfile='.deps/acllex.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'acllex.c' || echo './'`acllex.c
lex.yy.c:1225: warning: 'yyunput' defined but not used
source='acl2.c' object='acl2.o' libtool=no \
depfile='.deps/acl2.Po' tmpdepfile='.deps/acl2.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'acl2.c' || echo './'`acl2.c
gcc -g -Wall -g -Wall   -o flow-filter -L../lib flow-filter.o aclyacc.o acllex.o acl2.o -lft -lfl  -ly -lnsl -
lwrap -lz
source='flow-export.c' object='flow_export-flow-export.o' libtool=no \
depfile='.deps/flow_export-flow-export.Po' tmpdepfile='.deps/flow_export-flow-export.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib     -g -Wall -c -o flow_export-flow-export.o `test -f 'flow-export.
c' || echo './'`flow-export.c
gcc -g -Wall -g -Wall   -o flow-export -L../lib flow_export-flow-export.o -lft   -lnsl -lwrap -lz
source='flow-header.c' object='flow-header.o' libtool=no \
depfile='.deps/flow-header.Po' tmpdepfile='.deps/flow-header.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-header.c' || echo './'`flow-
header.c
gcc -g -Wall -g -Wall   -o flow-header -L../lib flow-header.o -lft -lnsl -lwrap -lz
source='flow-split.c' object='flow-split.o' libtool=no \
depfile='.deps/flow-split.Po' tmpdepfile='.deps/flow-split.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-split.c' || echo './'`flow-
split.c
gcc -g -Wall -g -Wall   -o flow-split -L../lib flow-split.o -lft -lnsl -lwrap -lz
source='flow-xlate.c' object='flow-xlate.o' libtool=no \
depfile='.deps/flow-xlate.Po' tmpdepfile='.deps/flow-xlate.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-xlate.c' || echo './'`flow-
xlate.c
gcc -g -Wall -g -Wall   -o flow-xlate -L../lib flow-xlate.o -lft  -lnsl -lwrap -lz
source='flow-merge.c' object='flow-merge.o' libtool=no \
depfile='.deps/flow-merge.Po' tmpdepfile='.deps/flow-merge.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-merge.c' || echo './'`flow-
merge.c
gcc -g -Wall -g -Wall   -o flow-merge -L../lib flow-merge.o -lft -lnsl -lwrap -lz
source='flow-import.c' object='flow-import.o' libtool=no \
depfile='.deps/flow-import.Po' tmpdepfile='.deps/flow-import.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-import.c' || echo './'`flow-
import.c
gcc -g -Wall -g -Wall   -o flow-import -L../lib flow-import.o -lft -lnsl -lwrap -lz
source='flow-fanout.c' object='flow-fanout.o' libtool=no \
depfile='.deps/flow-fanout.Po' tmpdepfile='.deps/flow-fanout.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-fanout.c' || echo './'`flow-
fanout.c
gcc -g -Wall -g -Wall   -o flow-fanout -L../lib flow-fanout.o -lft -lnsl -lwrap -lz
source='flow-tag.c' object='flow-tag.o' libtool=no \
```

```
depfile='.deps/flow-tag.Po' tmpdepfile='.deps/flow-tag.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-tag.c' || echo './'`flow-tag.
c
gcc -g -Wall -g -Wall   -o flow-tag -L../lib flow-tag.o -lft -lnsl -lwrap -lz
source='flow-nfilter.c' object='flow-nfilter.o' libtool=no \
depfile='.deps/flow-nfilter.Po' tmpdepfile='.deps/flow-nfilter.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-nfilter.c' || echo './'`flow-
nfilter.c
gcc -g -Wall -g -Wall   -o flow-nfilter -L../lib flow-nfilter.o -lft -lnsl -lwrap -lz
source='flow-report.c' object='flow-report.o' libtool=no \
depfile='.deps/flow-report.Po' tmpdepfile='.deps/flow-report.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-report.c' || echo './'`flow-
report.c
gcc -g -Wall -g -Wall   -o flow-report -L../lib flow-report.o -lft -lnsl -lwrap -lz
source='flow-mask.c' object='flow-mask.o' libtool=no \
depfile='.deps/flow-mask.Po' tmpdepfile='.deps/flow-mask.TPo' \
depmode=gcc3 /bin/sh ../depcomp \
gcc -I./../lib -L./../lib  -I. -I. -I../lib    -g -Wall -g -Wall -c `test -f 'flow-mask.c' || echo './'`flow-
mask.c
gcc -g -Wall -g -Wall   -o flow-mask -L../lib flow-mask.o -lft -lnsl -lwrap -lz
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/src'
Making all in bin
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/bin'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/bin'
Making all in configs
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/configs'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/configs'
Making all in docs
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/docs'
make[1]: Nothing to be done for `all'.
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/docs'
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68'
make[1]: Nothing to be done for `all-am'.
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68'
```

```
[x@nettest13 flow-tools-0.68]$ make install
Making install in lib
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/lib'
make[2]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/lib'
/bin/sh ../mkinstalldirs /opt/netflow//lib
mkdir -p -- /opt/netflow//lib
 /usr/bin/install -c -m 644 libft.a /opt/netflow//lib/libft.a
 ranlib /opt/netflow//lib/libft.a
/bin/sh ../mkinstalldirs /opt/netflow//include
mkdir -p -- /opt/netflow//include
 /usr/bin/install -c -m 644 ftlib.h /opt/netflow//include/ftlib.h
 /usr/bin/install -c -m 644 ftqueue.h /opt/netflow//include/ftqueue.h
 /usr/bin/install -c -m 644 radix.h /opt/netflow//include/radix.h
 /usr/bin/install -c -m 644 ftpaths.h /opt/netflow//include/ftpaths.h
 /usr/bin/install -c -m 644 ftconfig.h /opt/netflow//include/ftconfig.h
make[2]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/lib'
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/lib'
Making install in src
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/src'
make[2]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/src'
/bin/sh ../mkinstalldirs /opt/netflow//bin
mkdir -p -- /opt/netflow//bin
  /usr/bin/install -c flow-capture /opt/netflow//bin/flow-capture
  /usr/bin/install -c flow-cat /opt/netflow//bin/flow-cat
  /usr/bin/install -c flow-stat /opt/netflow//bin/flow-stat
  /usr/bin/install -c flow-print /opt/netflow//bin/flow-print
  /usr/bin/install -c flow-dscan /opt/netflow//bin/flow-dscan
  /usr/bin/install -c flow-send /opt/netflow//bin/flow-send
```

```
  /usr/bin/install -c flow-receive /opt/netflow//bin/flow-receive
  /usr/bin/install -c flow-gen /opt/netflow//bin/flow-gen
  /usr/bin/install -c flow-expire /opt/netflow//bin/flow-expire
  /usr/bin/install -c flow-filter /opt/netflow//bin/flow-filter
  /usr/bin/install -c flow-export /opt/netflow//bin/flow-export
  /usr/bin/install -c flow-header /opt/netflow//bin/flow-header
  /usr/bin/install -c flow-split /opt/netflow//bin/flow-split
  /usr/bin/install -c flow-xlate /opt/netflow//bin/flow-xlate
  /usr/bin/install -c flow-merge /opt/netflow//bin/flow-merge
  /usr/bin/install -c flow-import /opt/netflow//bin/flow-import
  /usr/bin/install -c flow-fanout /opt/netflow//bin/flow-fanout
  /usr/bin/install -c flow-tag /opt/netflow//bin/flow-tag
  /usr/bin/install -c flow-nfilter /opt/netflow//bin/flow-nfilter
  /usr/bin/install -c flow-report /opt/netflow//bin/flow-report
  /usr/bin/install -c flow-mask /opt/netflow//bin/flow-mask
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/src'
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/src'
Making install in bin
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/bin'
make[2]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/bin'
/bin/sh ../mkinstalldirs /opt/netflow//bin
 /usr/bin/install -c flow-log2rrd /opt/netflow//bin/flow-log2rrd
 /usr/bin/install -c flow-rptfmt /opt/netflow//bin/flow-rptfmt
 /usr/bin/install -c flow-rpt2rrd /opt/netflow//bin/flow-rpt2rrd
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/bin'
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/bin'
Making install in configs
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/configs'
make[2]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/configs'
make[2]: Nothing to be done for `install-exec-am'.
/bin/sh ../mkinstalldirs /opt/netflow//var/cfg
mkdir -p -- /opt/netflow//var/cfg
 /usr/bin/install -c -m 644 map.cfg /opt/netflow//var/cfg/map.cfg
 /usr/bin/install -c -m 644 tag.cfg /opt/netflow//var/cfg/tag.cfg
 /usr/bin/install -c -m 644 filter.cfg /opt/netflow//var/cfg/filter.cfg
 /usr/bin/install -c -m 644 stat.cfg /opt/netflow//var/cfg/stat.cfg
 /usr/bin/install -c -m 644 mask.cfg /opt/netflow//var/cfg/mask.cfg
 /usr/bin/install -c -m 644 xlate.cfg /opt/netflow//var/cfg/xlate.cfg
/bin/sh ../mkinstalldirs /opt/netflow//var/sym
mkdir -p -- /opt/netflow//var/sym
 /usr/bin/install -c -m 644 ip-prot.sym /opt/netflow//var/sym/ip-prot.sym
 /usr/bin/install -c -m 644 ip-type.sym /opt/netflow//var/sym/ip-type.sym
 /usr/bin/install -c -m 644 tcp-port.sym /opt/netflow//var/sym/tcp-port.sym
 /usr/bin/install -c -m 644 asn.sym /opt/netflow//var/sym/asn.sym
 /usr/bin/install -c -m 644 tag.sym /opt/netflow//var/sym/tag.sym
make[2]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/configs'
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/configs'
Making install in docs
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/docs'
make[2]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68/docs'
make[2]: Nothing to be done for `install-exec-am'.
/bin/sh ../mkinstalldirs /opt/netflow//man/man1
mkdir -p -- /opt/netflow//man/man1
 /usr/bin/install -c -m 644 ./flow-capture.1 /opt/netflow//man/man1/flow-capture.1
 /usr/bin/install -c -m 644 ./flow-cat.1 /opt/netflow//man/man1/flow-cat.1
 /usr/bin/install -c -m 644 ./flow-dscan.1 /opt/netflow//man/man1/flow-dscan.1
 /usr/bin/install -c -m 644 ./flow-expire.1 /opt/netflow//man/man1/flow-expire.1
 /usr/bin/install -c -m 644 ./flow-export.1 /opt/netflow//man/man1/flow-export.1
 /usr/bin/install -c -m 644 ./flow-fanout.1 /opt/netflow//man/man1/flow-fanout.1
 /usr/bin/install -c -m 644 ./flow-filter.1 /opt/netflow//man/man1/flow-filter.1
 /usr/bin/install -c -m 644 ./flow-gen.1 /opt/netflow//man/man1/flow-gen.1
 /usr/bin/install -c -m 644 ./flow-header.1 /opt/netflow//man/man1/flow-header.1
 /usr/bin/install -c -m 644 ./flow-import.1 /opt/netflow//man/man1/flow-import.1
 /usr/bin/install -c -m 644 ./flow-merge.1 /opt/netflow//man/man1/flow-merge.1
 /usr/bin/install -c -m 644 ./flow-print.1 /opt/netflow//man/man1/flow-print.1
 /usr/bin/install -c -m 644 ./flow-receive.1 /opt/netflow//man/man1/flow-receive.1
 /usr/bin/install -c -m 644 ./flow-send.1 /opt/netflow//man/man1/flow-send.1
 /usr/bin/install -c -m 644 ./flow-split.1 /opt/netflow//man/man1/flow-split.1
 /usr/bin/install -c -m 644 ./flow-stat.1 /opt/netflow//man/man1/flow-stat.1
```

```
 /usr/bin/install -c -m 644 ./flow-tools-examples.1 /opt/netflow//man/man1/flow-tools-examples.1
 /usr/bin/install -c -m 644 ./flow-tools.1 /opt/netflow//man/man1/flow-tools.1
 /usr/bin/install -c -m 644 ./flow-tag.1 /opt/netflow//man/man1/flow-tag.1
 /usr/bin/install -c -m 644 ./flow-nfilter.1 /opt/netflow//man/man1/flow-nfilter.1
 /usr/bin/install -c -m 644 ./flow-report.1 /opt/netflow//man/man1/flow-report.1
 /usr/bin/install -c -m 644 ./flow-mask.1 /opt/netflow//man/man1/flow-mask.1
 /usr/bin/install -c -m 644 ./flow-xlate.1 /opt/netflow//man/man1/flow-xlate.1
 /usr/bin/install -c -m 644 ./flow-rptfmt.1 /opt/netflow//man/man1/flow-rptfmt.1
 /usr/bin/install -c -m 644 ./flow-log2rrd.1 /opt/netflow//man/man1/flow-log2rrd.1
 /usr/bin/install -c -m 644 ./flow-rpt2rrd.1 /opt/netflow//man/man1/flow-rpt2rrd.1
make[2]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/docs'
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68/docs'
make[1]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68'
make[2]: Entering directory `/opt/netflow/src/flow-tools/flow-tools-0.68'
make[2]: Nothing to be done for `install-exec-am'.
make[2]: Nothing to be done for `install-data-am'.
make[2]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68'
make[1]: Leaving directory `/opt/netflow/src/flow-tools/flow-tools-0.68'
```

Post configuration

Paths

To allow easy access to the files, let's create a profile.d pathmunge to it

/etc/profile.d/flow-tools.sh

```
pathmunge /opt/netflow/bin
```

Then log back in to the machine and the binaries and man files etc should be ready to use.

init.d

/etc/init.d/flow-capture

```
#!/bin/sh
#
#   Startup/shutdown script for the flow-capture
#
#   Linux chkconfig stuff:
#
#   chkconfig: 2345 55 10
#   description: Startup/shutdown script for the Netflow Capture System
#

# Source function library.
if [ -f /etc/init.d/functions ] ; then
        . /etc/init.d/functions
elif [ -f /etc/rc.d/init.d/functions ] ; then
        . /etc/rc.d/init.d/functions
else
        exit 0
fi

prog=flow-capture

DAEMON="/opt/netflow/bin/flow-capture"
ARGS=" -w /var/netflow/ft 0/0/2055 -S5 -V5 -E10G -n 287 -N 0"

start () {
        echo -n $"Starting $prog: "

        # start daemon
        $DAEMON $ARGS
```

```
        RETVAL=$?
        if [ "$RETVAL" = "0" ]; then
                echo_success
                touch /var/lock/subsys/flow-capture
        else
                echo_failure
        fi
        echo
        return $RETVAL
}

stop () {
        # stop daemon
        echo -n $"Stopping $prog: "
        killproc $DAEMON
        RETVAL=$?
        echo
        [ $RETVAL = 0 ] && rm -f /var/lock/subsys/flow-capture
}

restart() {
        stop
        start
}

case $1 in
        start)
                start
        ;;
        stop)
                stop
        ;;
        restart)
                restart
        ;;
        condrestart)
                [ -f /var/lock/subsys/flow-capture ] && restart || :
        ;;
        status)
                status $DAEMON
        ;;
        *)

        echo $"Usage: $prog {start|stop|restart|condrestart|status}"
        exit 1
esac

exit $RETVAL
```

Router Configuration

Flow-Capture setup