

# INDEX

## Symbols & Numbers

| (pipe) symbol, 108  
3Com, 13

## A

ACK (acknowledgment) bit, 16, 50  
active flows, number in `softflowd`  
process, 37  
`$actives_webpage` variable, 144  
ADDR (address) variable, 79  
AggregateScore option, for  
CUFlow, 125  
AH (Authentication Header), 44  
alert destination, in  
FlowTracker, 153  
alert frequency, in FlowTracker, 153  
alert threshold, in FlowTracker, 153  
and logical operator, in filter  
definition, 76  
Apache  
configuring to support  
FlowViewer, 141  
*DocumentRoot* directory, 142  
archiving tracker, 154  
ARIN assignments, downloading  
list, 106  
ARP (Address Resolution Protocol),  
disabling, 34  
as primitive, 69–70  
*asn.sym* file, 106  
Authentication Header (AH), 44  
automating graph production, in  
`gnuplot`, 173–174  
Autonomous System (AS) informa-  
tion, reports, 104

Autonomous System (AS) number  
filters, 74  
Autonomous System (AS) primitive,  
69–70  
autonomous system numbers  
(ASNs), 48  
checking ownership, 106  
average flow time, 84  
average-sized flows, 38

## B

bandwidth graph in `gnuplot`,  
160–172  
combined inbound/outbound  
traffic, 170–172  
total bandwidth report, 160–168  
unidirectional bandwidth  
report, 168–170  
BGP (Border Gateway Protocol), 6  
in flow-print output, 48  
primitives, 67–70  
reports, 104–107, 111–112  
and friendly names, 106–107  
routing, 99  
and routing filters, 74–75  
BGP reports, 104–107  
Big Brother, 4  
binary, converting hex to, 52  
bits per second filters, 74  
boot time, flow-capture program  
startup at, 27  
bootable CD, for flow sensor, 33  
browsers, TCP flows, 16  
BSD operating system  
as collector operating system, 22  
`yacc`, 178

- buckets of time, default size, in FlowGrapher, 151
- bytes
  - converting to kilobits, 163
  - number in flow, 42
  - vs. octets, 43
- bytes per flow, report on, 97

**C**

- Cacti, 3–4
- calculator programs, 52
- CampusIO module, in FlowScan, 123
- cflowd, 32, 117
- Cflow.pm* module, 117, 133–138
  - acting on every file, 137
  - exports, 135–137
  - installing, 118–119
  - return value, 137–138
  - sample script, 133–134
  - testing, 118
  - variables, 134–135
  - verbose mode, 138
- CGI execution, web server configuration to permit, 141
- `$cgi_bin_directory` variable, 143
- Cisco, and NetFlow, 14
- Cisco routers
  - configuring monitor port on, 33
  - configuring NetFlow, 30
  - interface numbers, 68, 100
  - support for NetFlow, 29
- Cisco switches, configuring NetFlow, 30–31
- CiscoWorks, 4
- clipping levels, 73–74
  - for graphs, 166–167
- collectors, 11
  - considerations, 21–22
  - implementing, 24–25
  - log files, 28
  - number needed, 28
  - one per sensor or one for all, 145
  - running sensor on, 34
  - troubleshooting, 29
- color, for trackers in graph, 155
- columns, removing from reports, 109
- combined inbound/outbound traffic graph, 170–172
- comma-separated value (CSV) reports, 83, 108
  - dumping to file, 113
- command line
  - combining filters on, 75–76
  - configuring filter on, 88
  - setting variables on, 107
- comments, for primitives, 62
- commercial network management suites, 4
- company logo, on web page, 144
- comparison graphs, in gnuplot, 175–176
- comparison operators, in primitives, 65
- conditions, vs. primitives, 60
- configuration files
  - alternate, 115–116
  - for FlowScan, 122
  - saving in gnuplot, 160
- Conflicker worm, 186
- connectionless protocol, UDP as, 15–16
- connections
  - report on, 95
  - start and end times, 47
- control bits in TCP, 45, 50–52
- Coordinated Universal Time (UTC)
  - converting to local time, 163
  - time zone offset from, 28
- core switch, flow information from, 23
- counter primitives, 65, 66–67, 73
- Cricket, 3–4
- cropping output in flow reports, 115
- CSV (comma-separated value) reports, 83, 108
  - dumping to file, 113
- CUFlow, 120–121
  - configuring, 124–127
    - AggregateScore option, 125
    - Network statement, 124
    - AS number for tracking traffic, 127

- OutputDir directive, 125
  - Protocol statement, 126
  - Router statements, 126
  - Scoreboard option, 125
  - Service statements, 126
  - Subnet statement, 124
- filtered, 132–133
- flow record splitting and, 130–133
- vs. FlowTracker and FlowGrapher, 140
- graph display, 129–130
- installing, 121–130
- limitations, 132
- timing assumption for FlowScan, 124
- CUGrapher.pl* script, 129
- cutoffs, in FlowViewer, 148

## D

- data files, preparing for graph, 170
- data normalization, 175
- date program, 162
- decimal, converting hex to, 52
- default report in `flow-report`, 82–85
  - flow time distribution, 85
  - modifying, 85–88
  - octets in each flow, 84–85
  - packet size distribution, 84
  - packets per flow, 84
  - timing and totals, 83–84
- default web page, for FlowViewer, 144
- deleting processed files by FlowScan, 129
- destination-as match type, 74
- destination-as report, 105
- destination (Dif) interface, in `flow-print` output, 46
- destination IP address
  - of flow, 42
  - most connected, 93
  - report on, 103
- destination port filters, 70–71
- @devices variable, 145
- Dif (destination) interface, in `flow-print` output, 46

- directories, 114
  - for `flow-tools`, 26
  - for FlowScan, 122, 132
  - for FlowViewer, 142–144
- disk space, for collectors, 22
- DMZs, flows from, 24
- DNS requests, 15, 91
- double primitives, 67, 74
- `dump-flows` command
  - (`softflowctl`), 36
- duration of flows, filtering on, 73

## E

- echo reply ICMP type, 55
- email address, for receiving FlowTracker alerts, 153
- emailServers primitive, 78
- Encapsulating Security Payload (ESP), 44
- end-time match type, 73
- end time value, 113
- end times, for FlowViewer filter, 147
- EndTime, in `flow-print` output, 47
- `$ENV{PATH}` variable, in FlowViewer configuration, 142
- epoch time, 6
- error log, for FlowViewer, 145
- error messages, from *Cflow.pm*, 138
- ESP (Encapsulating Security Payload), 44
- Ethernet
  - monitoring flows on, 30
  - and sensor location, 23–24
- exit command (`softflowctl`), 36
- expired flow statistics, 38
- exporter, filtering by, 72
- `$exporter_directory`, 145
- @exporters, 145
- Extreme, 13

## F

- fields header, for removing columns, 109
- fields setting, in `flow-report`, 83
- FIELDS variable, 89–90
  - in `flow-report`, 86

- file names, for flow-capture files, 28
- files
  - printing graphs to, 168
  - redirecting output to, 113
- filter-definition keyword, 60
- filter-primitive statement, 58
- filter.cfg* file
  - default, 62
  - filter definitions in, 58
  - primitives defined, 79
  - variables defined, 80
- \$filter\_directory*, 144
- filtering. *See also* flow-nfilter program
  - in FlowViewer, 146–147
- filters
  - applying to reports, 109–110
  - broken connections, 182
  - creating, 60
  - of flows for total traffic, 161–162
  - ICMP type and code, 71
  - interface, 75
  - inversion, 77–78
  - logical operators in definitions, 76–78
  - match statements, 70–75
  - next-hop address, 75
  - not-email, 78
  - sensor or exporter, 72
  - source or destination port, 70–71
  - in stat-report statements, 111
  - TCP control bit, 71
  - time, 73
  - using, 61
  - using multiple, 75–76
  - and variables, 78–80
  - webTraffic, 76
- FIN (finish) bit, 51
- FIN request, 17
- find() function (*Cflow.pm*), 134, 137–138
- firewalls
  - checking configuration, 187–188
  - packet-filtering, 45
  - as sensor, 11
- five-tuple IP flow, 10
- flags (control bits) in TCP, 45, 50–52
- flow analysis, 2–3, 10
  - benefits, 189
- flow-capture program
  - log rotation script, 127–128
  - network configuration, 27
  - running, 26–27
- flow-cat, 41–42, 132
- flow export, 7
  - vs. NetFlow, 14
  - and timeouts, 18
- flow files, Perl module for, 117
- flow hit ratio, 128
- flow-nfilter program, 57, 88
  - filters in, 61
  - interface to, 146
  - man page for primitives list, 61
  - primitives, 58–59
  - for splitting flow data, 132
- flow-print, 41–45, 132, 184
  - formats, 46–50, 149
    - including BGP information, 48
  - interfaces and ports in hex, 46–47
  - IP accounting format, 49–50
  - two-line format, 47–48
  - wide-screen display, 48–49
- flow records, 7, 10
  - Perl modules to read, 133
  - speed information, 98
  - splitting
    - and CUFlow, 130–133
    - scripting, 132
- flow-report program, 81, 149
  - customizing appearance, 112–116
    - alternate configuration files, 115–116
  - cropping output, 115
  - CVS dump to file, 113
  - flow-rptfmt options, 113
  - sort order, 114–115
  - time for directing output, 113–114

- default report, 82–85
  - flow time distribution, 85
  - modifying, 85–88
  - octets in each flow, 84–85
  - packet size distribution, 84
  - packets per flow, 84
  - timing and totals, 83–84
- options, 90–91
- report types, 92–107
  - BGP reports, 104–107
  - IP address, 92–93
  - network protocol and port, 94–96
  - routing, interfaces, and next hops, 99–103
  - sensor output, 104
  - traffic size, 96–97
  - traffic speed, 97–99
  - strftime variables, 114
- flow-rptfmt program, 83, 91, 108
  - options, 113
- flow-stat, 149
- flow system architecture, 11–12
- flow time distribution, in flow-report
  - default report, 85
- flow-tools, 6, 12
  - converting flowd data to, 179–180
  - installing, 25
  - website, 25
- flow-tools-ng* package, 25
- \$flow\_bin\_directory*, 144
- flowcap script, 152
- flowd
  - configuring, 178–179
  - converting data to flow-tools, 179–180
  - installing, 178
- flowd2ft script, 179–180
- \$flow\_data\_directory*, 145
- flowdumper, 118, 119–120
- FlowFileGlob configuration value, in FlowScan, 123
- FlowGrapher, 139, 150–152, 188
  - output, 151–152
  - settings, 150–151
- flows, 6–7, 9–19. *See also* viewing flows
  - analyzing individual from reports, 88–89
  - average-sized, 38
  - basics, 10
  - filtering
    - for total traffic, 161–162
    - for unidirectional traffic, 168–169
  - history, 12–14
  - ICMP, 14–15
    - and ICMP details, 54–55
  - number of seconds active, 47
  - with only TCP resets, graphable data, 107
  - origination, 94
  - packet-sampled, 19
  - problem solving with data, 182–189
  - report information split on 2 lines, 47–48
  - vs. sessions, 11
  - source and destination IP addresses, 42
  - standards, 13–14
  - start and stop times, 88
  - statistical analysis, 82
  - TCP, 16–17
  - termination, 95
  - UDP, 15–16
  - value of information, 10
  - visualization. *See* gnuplot
- flows exported, number in softflowd process, 37
- Flows/Second, in report, 84
- FlowScan, 7, 117, 120–121
  - configuring, 123–124
  - file handling, 128–129
  - installing, 121–130
  - requirements, 121
  - rotation programs and flow-capture, 127–128
  - running, 128
  - startup script, 123
- flowscandata* directory, 132
- flowscanrrd* directory, 132

- FlowTracker, 139, 152–155
  - and FlowGrapher, vs.
    - CUFlow, 140
  - group trackers, 154–155
  - processes, 152
  - settings, 152–153
  - viewing trackers, 153–154
- FlowTracker\_Collector process, 152
- FlowTracker\_Grapher process, 152
- FlowViewer, 139–156
  - configuring, 141–145
    - devices and exporters, 144–145
    - directories and site paths, 142–144
    - website setup, 144
  - default interface, 146
  - filtering flows, 146–147
  - installing, 140–141
  - interface names and, 156
  - manual, 140
  - printed reports, 149
  - reporting parameters, 147–148
  - security, 140
  - statistics reports, 149–150
  - troubleshooting, 145–146
- FlowViewer\_Configuration.pm* configuration file, 141–145
- `$FlowViewer_server` variable,
  - in FlowViewer configuration, 142
- `$FlowViewer_service` variable,
  - in FlowViewer configuration, 142
- formatting report, command for, 83
- FreeBSD, 6
- FreeSBIE, 33
- friendly names, in BGP reports, 106–107
- Fullmer, Mark, 24

**G**

- gasn* script, 106
- gawk, 181
- GD Graphics Library, 141
- GDBM Perl module, 141
- gd::graph Perl module, 141
- ge operator, for time primitives, 66
- Generic Routing Encapsulation (GRE), 44
- GNU awk, 181
- GNU make, 178
- gnuplot, 6
  - automating graph production, 173–174
  - bandwidth graph, 160–172
    - combined inbound/outbound traffic, 170–172
    - total bandwidth report, 160–168
    - unidirectional bandwidth report, 168–170
  - basics, 158
  - comparison graphs, 175–176
  - configuration files, 159–160
  - exiting, 158
  - graph styles, 165–166
  - graphing sine wave, 158–159
  - starting, 158–159
- Grace, 158
- graphs
  - display in CUFlow, 129–130
  - from FlowScan, 121
  - FlowViewer storage of, 143
  - width, 151
- graphs in gnuplot
  - automating production, 173–174
  - bandwidth, 160–172
    - combined inbound/outbound traffic, 170–172
    - total bandwidth report, 160–168
    - unidirectional bandwidth report, 168–170
  - comparison, 175–176
  - printing to files, 168
- `$graphs_directory`, 143
- `$graphs_short` variable, 143
- GRE (Generic Routing Encapsulation), 44
- grid for graph, 165
- group trackers, 154–155

## H

- hard drive, for recycled machine for
  - flow sensor hardware, 33
- hardware sensors, 23
  - configuring, 29–32
  - setup, 32–34
- header information
  - displaying in reports, 90–91
  - in flow file, 41
  - for flow record, 45
- hex
  - converting to decimal and binary, 52
  - showing interfaces and ports in, 46–47
- high-bandwidth connections, identifying, 95
- hostname
  - displaying in reports, 90–91
  - of FlowViewer website, 142
- hosts
  - report on all flows by, 92
  - traffic to nonexistent, 188–189
- HP, 13
- HSRP cluster, 30
- HTML
  - from flow-rptfmt, 113
  - presenting reports in, 91
- HTTP requests, 17, 89
- HTTPS, for FlowViewer website, 140

## I

- IANA (Internet Assigned Numbers Authority), 53
- ICMP (Internet Control Message Protocol), 44
  - flows, 14–15, 54–55
  - primitive to filter redirects, 64
  - type and code filters, 71
  - types and codes, 53–54
- ICMP type and code primitives, 63–64
- icmpcodes, exporting, 136
- icmptypes, exporting, 136
- ifindex primitive, 69

- impulse on graph, 166
- inbound/outbound traffic graph, combined, 170–172
- inbound traffic, determining for flow, 124
- Include Flow If setting, in FlowViewer, 148
- InMon, 180
- input-interface match type, 75
- input-interface report, 100
- input/output-interface reports, 101
- installing
  - flowd, 178
  - FlowViewer, 140–141
- interconnectedness reports, 93
- interface filters, 75
- interface numbers
  - in FlowViewer, 147
  - primitive for, 69
  - SNMP for identifying, 68–69
- interfaces
  - and flow data, 99–100
  - showing in hex, 46–47
- internal network, flow analysis
  - on, 89
- Internet Assigned Numbers Authority (IANA), 53
- Internet border, and sensor location, 23
- Internet Control Message Protocol.  
*See* ICMP (Internet Control Message Protocol)
- Internet Engineering Task Force, 13
- Internet Software Consortium (ISC), 19*n*
- invert keyword, 77–78
- invisibility of network, 2
- IP accounting format, for flow-print output, 49–50
- ip-address-mask primitive, 64–65, 72
- ip-address-prefix-len primitive, 70
- ip-address-prefix primitive, 64–65, 72
- ip-address primitive, 72
- ip-address report, 92
- IP address reports, 92–93

- IP addresses
    - for collectors, 27
    - in FlowViewer, 147, 148
    - match types for, 72
    - primitives for, 64
    - private, flows from, 100
    - reports combining ports with, 96
    - traffic to illegal, 187–188
  - ip-destination-address match
    - type, 72
  - ip-destination-address/
    - input-interface
      - report, 103
  - ip-destination-address/
    - output-interface
      - report, 103
  - ip-destination-address report, 92
  - ip-destination-address-source-count
    - report, 93
  - ip-destination-port match type,
    - 70–71
  - ip-destination-port report, 95
  - ip-exporter-address match type, 72
  - ip-exporter-address report, 104
  - ip flow-export version 7, 31
  - IP Flow Information eXport
    - (IPFIX), 13–14
  - ip flow ingress, 31
  - ip-next-hop-address match type, 75
  - ip-next-hop-address report, 101–102
  - ip-port primitive, 59, 62, 64
  - ip-port report, 94
  - ip-protocol match type, 70
  - IP protocol, primitives, 61–62
  - ip-protocol report, 95–96
  - ip route-cache flow, 31
  - ip-source-address-destination-count
    - report, 93, 186–187
  - ip-source-address/input-interface
    - report, 103
  - ip-source-address match type, 72
  - ip-source-address/output-interface
    - report, 102–103
  - ip-source-address report, 86, 87
    - fields included, 90
  - ip-source/destination port report, 95
  - ip-source-port match type, 70–71
  - ip-source-port report, 94
  - ip-tcp-flags keyword, 71
  - ip-tcp-flags primitive, 63
  - IP version 6 (IPv6), 13
  - IPFIX (IP Flow Information
    - eXport), 13–14
  - IPSec, primitive matching, 62
  - ISC (Internet Software
    - Consortium), 19*n*
- J**
- Juniper, 12, 13
  - Juniper routers
    - configuring NetFlow, 31–32
    - support for NetFlow, 29
- K**
- key for report, 87
  - keywords, vs. primitives, 60
  - kilobits, converting bytes to, 163
  - Kozierok, Charles M., *The TCP/IP Guide*, 9
- L**
- layer 2 flows, capturing, 31
  - libpcap, 37
  - linear-interpolated-flows-octets-
    - packets report, 98–99, 160
  - liner-interpolated-flow-octets-
    - packets report, 107
  - Linux, 6
    - as collector operating system, 22
    - FlowScan startup script for, 123
  - location, of sensor, 23
  - log files
    - for collectors, 28
    - for flow-capture, 26
      - rotation script for, 127–128
  - logical operators
    - in gnuplot, 166–167
    - in primitives, 65
  - lt operator, for time primitives, 66



## M

- Makefile.PL* file, 119
- MANPATH environment
  - variable, 25
- match statement, 60
  - in filters, 70–75
- memory (RAM), 22
- Microsoft DHCP Server,
  - certification, 2
- mid time value, 113
- MRTG, 3–4
- multiple filters, 75–76

## N

- Nagios, 4
- names
  - in BGP reports, 106–107
  - conventions for filters and primitives, 60
  - for primitives, 59
  - of reports, 82
- names option, in flow-report, 91
- \$names\_directory*, 143
- NAT (Network Address Translation), 188
- NetFlow
  - competition, 13
  - configuring
    - on Cisco routers, 30
    - on Cisco switches, 30–31
    - on Juniper routers, 31–32
  - converting sFlow to, 181–182
  - vs. flow export, 14
  - version 9, 177–180
  - versions, 12–13
- netmask, 112
- network
  - generating graphs for, 130
  - of origin for AS, report on,
    - 104–105
  - speed, 98
  - traffic at given time, 98–99
- Network Address Translation (NAT), 188
- network administration, vs. network management, 3

- network administrators
  - role, 2
  - training, 2
- network communication, proof of success, 5
- network flow. *See* flows
- network hardware, checking health of, 4
- network interfaces, for sensor server hardware, 33
- network management
  - vs. network administration, 3
  - tools, 3–5
- network protocol and port reports, 94–96
- network protocol filters, 70
- network protocols. *See* protocols
- Network statement, for CUFlow, 124
- Network Time Protocol (NTP), 6
- “network unreachable” ICMP
  - type, 55
- newasn.sym* file, 106
- next-hop address
  - filters, 75
  - in FlowViewer, 146
  - reporting, 101–102
- \$no\_devices\_or\_exporters*, 145
- Nokia, 12
- normalization of data, 175
- not-email filter, 78
- now time value, 113
- NTP (Network Time Protocol), 6

## O

- octets
  - vs. bytes, 43
  - in flow-report default report,
    - 84–85
- octets per flow, filtering on, 73
- octets report, 97
- OpenSolaris, 22
- OpenView, 4
- operating system, for collectors, 22
- options keyword, 115
- OPTIONS variable, 90–91
  - in flow-report, 86

- or logical operator, in filter definition, 76–77
- organization name, on web page, 144
- `$organization` variable, 129
- origination of flows, 94
- OSPF, filter to match, 61
- outbound traffic, determining for flow, 124
- outliers, eliminating from graph, 166–167
- `OutputDir` directive, for CUFlow, 125
- output-interface match type, 75
- output-interface report, 100

## P

- packages, installing flow-tools from, 25
- packet-capture software, 37
- packet-filtering firewalls, 45
- packet-sampled flows, 19
- packet size distribution, in
  - flow-report default report, 84
- packet-size report, 96
- packet sniffer, 10
- packets
  - dropped
    - by interface counter, 38
    - number in `softflowd` process, 37
    - number in flow, 42
  - packets per flow
    - filtering on, 73
    - in flow-report default report, 84
    - report, 97
  - packets per second (pps), 98
  - packets per second filters, 74
  - packets report, 97
  - password protection, for FlowViewer website, 140
- `PATH` environment variable, 25
- path variable
  - for flow-report, 108
  - setting to pipe, 113
- percent-total option, in flow-report, 91
- percentages, displaying in reports, 90–91
- `perfile()` function, 137
- Perl scripts, 6, 117
- permit statement, 80
- pie charts, in FlowViewer, 148
- ping requests, 14, 54
- pipe symbol (`|`), 108
- plot command (`gnuplot`), 159, 162–163
- plotting program, 6
- port mirroring, switch for, 33
- port monitoring, switch for, 33
- port number primitives, 62
- port scanner, 185
- “port unreachable” ICMP type, 55
- `PORT` variable, 79
- ports
  - common number assignments, 44–45
  - common protocol assignments, 44
  - printing names, 43–44
  - report on used, 94
  - reports combining IP addresses with, 96
  - vs. services, 45
  - showing in hex, 46–47
  - source or destination filters, 70–71
- pps report, 98
- `prefix-mask`, for address format, 112
- primitives, 58–59, 61–70
  - Autonomous System (AS), 69–70
  - for BGP, 67–70
  - comments for, 62
  - comparison operators, 65
  - vs. conditions, 60
  - counter, 66–67, 73
  - double, 67, 74
  - emailServers, 78
  - ICMP type and code, 63–64
  - for interface numbers, 69
  - IP address, 72
  - `ip-address-mask`, 64–65
  - `ip-address-prefix`, 64–65
  - for IP addresses, 64

- IP protocol, 61–62
  - names for, 59
  - port number, 62
  - subnet, 64–65
  - TCP control bit, 63
  - time, 66
- printed reports, in FlowViewer, 149
- printing
  - graphs to files, 168
  - protocol and port names, 43–44
  - setting cutoff for, 148
  - to wide terminal, 45
- private IP addresses, flows from, 100
- private network segments, flows
  - from, 24
- probe, 11. *See also* sensors
- problem solving with flow data, 182–189
- process ID, of `softflowd` process, 37
- promiscuous mode, preventing, 29
- PROT (protocol) variable, 79
- Protocol statement, for CUFlow, 126
- protocols
  - common number assignments, 44–45
  - filtering by, 61
  - in FlowViewer, 147
  - generating graphs for, 130
  - printing names, 43–44
  - report on, 95–96
- PSH (push) bit, 50

## R

- RAM, 22
- ranges of ports, primitives for, 62
- Real Time header, 83
- rebooting, and Cisco router interface numbering, 68, 100
- recipient, report on flows by, 92
- records field, in `flow-report`, 83
- redirecting output to files, 113
- remote facilities, flows from, 24
- report options, in detail report, 82
- report types, 82
- ReportClasses configuration value,
  - in FlowScan, 123
- reporting system, 11

- reports. *See also* flow-report program
  - analyzing individual flows from, 88–89
  - applying filters, 109–110
  - customizing, 107–110
  - definitions, 107
  - displaying headers, hostnames and percentages, 90–91
  - format and output, 108
  - in HTML, 91
  - parameters in FlowViewer, 146, 147–148
  - removing columns, 109
  - reversing sampling, 110–111
- `$reports_directory`, 144
- `$reports_directory` variable, 142
- `$reports_short` variable, 142
- reset-only flows, 107–110
- resets, checking for, 183–184
- response packet, 16
- reversing, sampling, 110–111
- Round Robin Database (RRD), 121
  - converting data to graphs, 129
  - files from FlowTracker, 152
- router interface, filtering by, 75
- Router statements, for CUFlow, 126
- routers, as sensors, 11
- routing, interfaces, and next hops
  - reports, 99–103
- RPTOPT variable, in `flow-report`, 86, 91
- RRD. *See* Round Robin Database (RRD)
- `$rrddir` variable, 129
- RRDtool, 141
- `rrdtool_bin_directory`, 144
- RST (reset) bit, 51
- rst-only filter, 109–110, 183
- RST-only flow, 63, 182
- RTG, 4

## S

- sample time, in FlowGrapher, 151
- sampled packets, 19
- sampling multiplier, in
  - FlowTracker, 153
- sampling rate, 31–32
- sampling, reversing, 110–111

- saving configuration files in
  - gnuplot, 160
- scale keyword, 111
- Scoreboard option, for CUFlow, 125
- scripts
  - for automating graph
    - production, 173–174
  - for flow record splitting, 132
  - flowd2ft, 179–180
- security
  - for FlowViewer, 140
  - for operating system, 22
- sed command, 162
- sensor output reports, 104
- sensor server, setup, 34
- sensors, 11. *See also* softflowd
  - considerations, 22–24
  - filtering by, 72
  - hardware, 23
    - configuring, 29–32
    - setup, 32–34
  - one collector per, 145
  - reporting output, 104
  - running on collector, 34
  - separate collector for each, 28
  - software, 23
    - configuring, 32
- Service statements, for CUFlow, 126
- services
  - generating graphs for, 130
  - vs. ports, 45
- sessions
  - breaking into multiple
    - records, 18
  - vs. flows, 11
- set command (gnuplot), 159, 163
- set output statement (gnuplot), 168
- set terminal statement (gnuplot), 168
- sFlow, 180–182
  - configuring export with
    - sflowerable, 181
- sflowerable, 181
- sflowtool program, 181
- show ip cache flow, 30, 31
- shutdown command (softflowctl), 36
- Sif (source) interface, in flow-print
  - output, 46
- site paths, for FlowViewer, 142–144
- sniffer interface, activating, 34
- sniffer port, 33
- SNMP (Simple Network Management Protocol)
  - identifying interface numbers
    - using, 68–69
  - for network traffic graphs, 3–4
- snmp ifIndex persist option, 100
- snmpwalk, 68
- Soekris, 32
- softflowctl program, 35–39
- softflowd, 34–39
  - running, 35
  - watching, 35–39
    - flow statistics, 36–39
    - tracked flows, 36
- software, finding busted, 182–186
- software sensors, 23. *See also*
  - softflowd
    - configuring, 32
- Solaris, FlowScan startup script
  - for, 123
- SORT variable, in flow-report, 86–88
- sorting
  - in FlowViewer, 148
  - reports, 114
    - by column, 87
    - limitations for, 93
- source-as match type, 74
- source-as report, 104–105
- source code
  - installing *Cflow.pm* from, 119
  - installing flow-tools from, 25–26
- source IP address
  - of flow, 42
  - report on, 102–103
- source-ip-address report, 91
- source port, 16
- source port filters, 70–71
- source (Sif) interface, in flow-print
  - output, 46
- standards, for network flow, 13–14
- start-time match type, 73
- start time value, 113
- start times, for FlowViewer filter, 147
- StartTime, in flow-print output, 47

- startup script
    - for flow-capture, 27
    - for FlowScan, 123, 128
  - stat-definition
    - combining with stat-report, 110
    - for customized flow report, 107–108
  - stat-report
    - combining with stat-definition, 110
    - for customized flow report, 107–108
    - filters in, 111
    - time information use by, 113–114
  - stat.cfg* file, 82, 107, 160–161
  - statistics reports, in FlowViewer, 149–150
  - strftime library, 113
  - subnet primitives, 64–65
  - Subnet statement, for CUFlow, 124
  - SubNetIO module, in FlowScan, 123
  - summary-detail report, 82, 85
  - switches, as sensors, 11
  - SYN-ACK packet, 16
  - SYN-only flow, 182
    - primitive matching flow with only, 63
  - SYN request, 16
  - SYN (synchronize) bit, 50
  - system resources, for collectors, 22
- T**
- tail command, 145
  - tar command, 25
  - TCP (Transmission Control Protocol), 44
    - broken connections, 182
    - common port assignments, 44
    - control bit filters, 71
    - control bits, 50–52
    - defining ports for separate tracking, 126
    - failed connections, 184–186
    - flags, 45
    - primitive for traffic, 59
    - TCP control bit primitives, 63
    - TCP flags
      - in FlowViewer, 147
      - symbolic names, 135
    - TCP flows, 16–17
    - The TCP/IP Guide* (Kozierok), 9
    - TCP three-way handshake, 17
    - tcpdump, 29
    - tcpflags, exporting, 136
    - termination of flows, 95
    - test.plt* file, 160
    - three-way handshake, 17
    - throughput matrix, 101
    - time
      - on graphs, 162
      - need for synchronization, 49
      - use to direct output, 113–114
    - “time exceeded” PCMP type, 54
    - time filters, 73
    - time primitives, 66
    - time scale for graph, 175–176
    - timeouts, flow export and, 18
    - title of graph, in gnuplot, 159
    - total bandwidth report, 160–168
    - totals option, in flow-report, 90–91
    - traceroute, 99
    - tracker, 152
      - viewing, 153–154
    - \$tracker\_directory*, 143
    - Tracking Set Label, in FlowTracker, 153
    - Tracking Type, in FlowTracker, 153
    - \$trackings\_title* variable, 144
    - traffic size reports, 96–97
    - traffic speed reports, 97–99
    - training of network administrators, 2
    - transit provider, 105
    - Transmission Control Protocol. *See* TCP (Transmission Control Protocol)
    - troubleshooting
      - collectors, 29
      - FlowViewer, 145–146
    - Type of Service flag in FlowViewer, 147
    - TYPE variable, in flow-report, 85

## U

- UDP (User Datagram Protocol), 44
  - common port assignments, 44
  - flow-capture listening to port, 27
- UDP flows, 15–16
- unidirectional bandwidth report, 168–170
- Unix epoch time, 6
- URG (urgent) bit, 51
- user complaints, 1–2
- `$user_hyperlink`, 144
- users
  - creating for FlowScan, 122
  - of FlowViewer, 140
  - name for running web server, 141
- UTC (Coordinated Universal Time)
  - converting to local time, 163
  - time zone offset from, 28
- uunet AS primitive, 74

## V

- `VAR_ADDR` primitive, 79–80
- variable-driven filters, 79
  - defining, 79–80
- variables, 86
  - command line for setting, 107
  - creating, 80
- `VAR_PORT` primitive, 79–80
- `VAR_PROT` primitive, 79–80
- viewing flows, 41–55
- VRRP cluster, 30

## W

- `waitSeconds` setting, for FlowScan, 123, 124
- `wanted()` function (*Cflow.pm*), 134
- web farms, 132
- web interface
  - from FlowScan, 121
  - for FlowViewer, 144
- web servers
  - for FlowViewer, 141
  - response from, 88
  - TCP flows, 16
- webTraffic filter, 76
- Webview Netflow Reporter, 155
- Weinhold, Craig, 179
- whois, 106–107
- wide-screen display, for flow-print output, 48–49
- wide terminal, printing to, 45
- Windows, Calculator program, 52
- worms, 93
  - identifying, 186

## X

- X server, 6
  - for gnuplot, 158
- xheader option, in flow-report, 90

## Y

- y-axis label, on graphs, 164–165

## Z

- zero-packet flows, 83