
INDEX

. character, Oak and, 119, 120
+ modifier, Oak and, 120
* modifier, Oak and, 120
[] operator, Oak and, 120–121
- character, Oak and, 121
\$ character, Oak and, 121
\$_ Perl variable, 221
\$? Bourne shell variable, 207
~ character, Oak and, 121
/ character, Oak and, 122
(), substitution with in Oak, 122
comment character, 202, 214
#! script startup character, 202

A

access-list counters, 86
access privileges, SNMP, 12–13
action command, Oak, 124–125
action-limits statement, Oak, 125
anchors, Oak, 121
Apache Web server, 115
arguments, command line. *See* command line arguments
ARGV hash, 222
ARP cache, querying, 24–25, 66, 77–78

B

bash program, 203
binary files, compiled languages and, 200–201
boards, 62–63, 69–71, 73–74. *See also* ports
Bourne shell scripts, 8, 58, 203–214, 230
arguments as variables in, 209–210
bash program and, 203
comment lines (#) in, 202, 214
conditionals in, 207–209
disadvantages of, 214–215
environment variables and, 205–206
exiting of, 213
exiting status and, 206–207

initial line (!) of, 202
input/output redirection, 211–212
interpreting those in another file, 213
loops and, 210
mail formatting with, 228
multiple commands on one line, 204
names of, 202
output, using in, 210–211
PATH environment variable and, 203–204
process ID of, 213–214
running, 201–202
trapping of, 213–214
user-created functions in, 212
variables in, 204–205
bridge MIB (dot1dBridge), 25
bridging. *See* switching
bugs, notifying developers of, 8
burst variable, Neo, 65, 76–77

C

cfgmaker command, MRTG, 44–46, 51–52
chop function, Perl, 218, 221
Cisco devices
Cisco Catalyst 2948, ports on, 63
configuring syslog on, 118–119
monitoring with tcpdump, 170–172
NetFlow and, 83, 86, 87, 89–90
Cisco Express Forwarding (CEF), 86
Cisco IOS ping, 182
command line arguments, scripting and, 75–76, 209–210, 222
comment character (#), 202, 214
commercial software, open source vs., 3–6
community name, SNMP, 12, 13
compiled languages, interpreted languages vs., 200–201
compilers, 200
conditionals, scripts and, 207–209, 216–217
contact lists, storing in variables, 150–151
continuous ping tests, 179–180

cron program, 229–230
 crontab, MRTG and, 49–50
 csh program, 58, 203
 custom tools. *See* scripts

D

denial of service attack, debugging, 78–80, 84, 157–158
 devices, 9
 costs of managing, 1–2
 managing with SNMP. *See* SNMP (Simple Network Management Protocol)
 Neo location syntax for, 60–62
 ping testing, 178–179, 182–183
 querying with Neo, 54, 57, 63, 68–72
 setting Sysmon, 141–147
 domain name server (DNS) lookups, Neo, 57, 76
 domain name server (DNS) options, Sysmon, 149
 dot1dBridge SNMP variables, 25–26

E

e-mail messages. *See* messages
 elif command, Bourne shell and, 208
 elsif command, Perl and, 216–217
 environment variables, scripts and, 58, 203, 205–206, 216
 environmental conditions, Neo queries of, 54, 57, 71
 error messages, logging of, 111–112. *See also* syslog messages, Oak and Ethereal
 exec command, Neo, 76
 exec queue action, Oak and, 124, 125
 exit status, script, 206–207, 227–228

F

facilities, syslog message, 115
 files, testing with scripts, 208, 217
 finite state machine, 227
 fire statement, Oak and, 125
 flap detection, Nagios and, 153
 flow-capture program, 90–91, 93–98
 flow-cat program, 91, 105–106
 flow collectors, 86–87
 flow-dscan program, 91, 99, 103, 105
 flow-expire program, 91, 107
 flow-fanout program, 91, 97, 107–108
 flow-filter program, 91, 108
 flow-header program, 91, 107
 flow-merge program, 91, 105–106

flow-print program, 91, 98, 99–100, 101
 flow-receive program, 90–91, 92–93, 97
 flow-report program, 91, 99, 100–102
 flow-send program, 91, 108
 flow-split program, 91, 106
 flow-stat program, 91, 99, 102–103, 104
 Flow-Tools, 7, 83, 90–108
 capturing flows with, 90–96
 compression of flow data, 97
 filtering data, 108
 header meta information, printing, 107
 installation and configuration, 88–89
 merging data files, 105–106
 multiple host/ports, sending data to, 107–108
 programs included with, 90, 91
 references for, 108
 remote clients, enabling, 98
 removal of flow data, 107
 splitting data files, 106
 stopping flow capture, 97–98
 viewing flow data, 98–105
 flow-xlate program, 91
 flows, network traffic, 84–86, 90–96
 for loops, 210, 222
 forwarding tables, 54–55
 Fullmer, Mark, 83
 functions, user-created, 212

G

GD library, MRTG and, 41, 42–43, 52
 get-next-request SNMP PDU type, 13, 19, 20, 33
 get-request SNMP PDU type, 13, 20
 get-response SNMP PDU type, 13
 GNU General Public License, 39
 GNU readline library, 58, 81
 graphs, MRTG. *See* Multi Router Traffic Grapher (MRTG)
 grep command, 119, 120

H

hardware address translation
 with Neo, 53, 55–56, 66
 with SNMP, 24–25
 hashes, 220
 header command, Oak, 125
 help command, Neo, 75
 hostinfo command, Neo, 76
 hosts, 9
 finding and disabling with Neo, 77–80
 locating with forwarding tables, 54–55
 HTML index pages, generation of MRTG, 47–49

I

ICMP protocol, 175, 178–180
 ICMP packet flow and, 84–85, 86
 ping and, 178, 179, 180
 if statement, Bourne shell
 conditionals and, 208
 ifNumber variable, SNMP, 22
 ifSpeed variable, SNMP, 23
 ifTable variable, SNMP, 22, 23
 ifType variable, SNMP, 24
 input redirection, Bourne shell, 211–212
 interface bandwidth, SNMP and, 23–24
 interface index numbers, SNMP and, 25
 interfaces SNMP variables group, 22–24
 Internet Standard MIB, 14
 interpreted languages, 200–201. *See also* scripts
 interpreter, 200
 IOS ping, 182
 IP addresses
 changing ping source, 181
 translation of with ip.ipNetToMediaTable,
 24–25
 translation of with Neo, 53, 55–56, 66
 translation of with SNMP, 24–25
 IP packets
 tracing path of with MTR, 195–197
 tracing path of with traceroute,
 189–191, 192–193
 viewing with tcpdump, 156–157
 IP protocol, 175
 IP time-to-live value, ping, 181
 ip.ipNetToMediaTable, 24–25, 55–56

J

Jacobson, Van, 155
 Juniper routers, 83

K

kern syslog facility, 115
 key, flow-report, 102
 keyfiles, Neo, 61–62, 80

L

lexicographic order, listing SNMP
 variables in, 19
 licenses, open source software, 2
 linkDown trap, 19
 Linux, 8, 41, 58, 158–159, 175, 191, 194, 203
 list context, 219
 lists, manipulating with Perl, 218–220
 local variables, scripts and,
 203, 205–206, 216

locate command, Neo, 66–67
 location print command, Neo, 60, 76
 locking command, Oak, 125–126
 logger program, 117
 logging command, Cisco IOS, 118–119
 logwatch program, 130
 loops, 210, 222–223, 225–226

M

macmode variable, Neo, 65, 68
 mail, formatting sendmail with scripts,
 228–229
 mail queue action, Oak, 124
 mail syslog facility, 115
 management agent, SNMP, 11
 Management Information Base (MIB),
 14–15, 37–38
 bridge MIB, 25–26
 downloading and installing, 36
 net-snmp tools and, 36
 reverse lookups and, 25
 SNMP variable hierarchy and, 15–16
 tables and, 17–19
 mark syslog facility, 115
 Matt’s traceroute. *See* MTR (Matt’s
 traceroute)
 message queues, Oak and. *See* queues,
 Oak and
 messages
 message headers and subject lines,
 228–229
 syslog. *See* syslog messages, Oak and
 Sysmon and, 144, 145–146, 148,
 150–151
 MIB. *See* Management Information Base (MIB)
 MIB-II, 14, 15
 monitoring scripts. *See* network monitoring
 scripts
 MRTG. *See* Multi Router Traffic Grapher
 (MRTG)
 MTR (Matt’s traceroute), 8, 194–197
 Multi Router Traffic Grapher (MRTG),
 5, 7, 39–54
 configuration, 43–46
 data gathering settings, 49–50
 faulty data in, 50–51
 HTML index page generation, 47–49
 initial data generation, 47
 installation, 41–43
 maintenance of, 51–52
 missing data from, 51
 references for, 52
 review of network patterns with, 39–41
 SNMP and, 39, 41, 45

N

Nagios, 8, 135, 152–154
 nc program. *See* Netcat
 ND tool, 81
 Neo, 7, 53–81
 board and port information from, 54, 67–72
 bugs in, reporting, 58, 81
 built-in variables, 64
 command line arguments, 75–76
 command prompt, 59
 degraded network conditions and, 76–77
 device info command, 71–72
 device summary command, 68–71
 domain name server (DNS) lookups, 57, 76
 general device information and, 54, 57, 71–72
 hosts, finding and disabling problem, 77–80
 installation and configuration, 57–58
 IP address translation with, 53, 55–56, 66
 keyfiles, 61–62, 80
 locate command, 66–67
 location syntax used by, 59–64
 maintenance of, 80
 online help system, 75
 ports, administrative status of, 67, 68
 ports, enabling/disabling, 54, 56–57, 67–68
 power and environmental status reports, 54, 57, 71–72, 80
 printer information from, 57
 references for, 81
 scripts and, 75–76, 80
 shell command execution with, 57, 76
 SNMP and, 53
 switch ports, determining host, 53, 54–55, 66–67
 traffic statistics and, 53, 54, 56, 72–75
 variables, 64–65
 Web sites for, 57, 59, 80
 net-snmp package
 installation and configuration, 27–29
 maintenance of, 37
 Management Information Base (MIB) and, 36
 scripting and, 36–37
 SNMP tools in, 29–36
 Netcat, 8, 98, 185–189
 NetFlow, 7, 83–109
 configuration of on router, 89–90
 data filtering and, 108
 export of data by routers, 86–87

 file rotation rate, 96
 flow capture by, 90–96
 flow collectors and, 87
 flow data compression, 97
 Flow-Tools package for, 83, 88–89
 flows, information in, 87–88
 merging data files, 105–106
 monitoring network traffic with, 83, 84
 multiple host/ports, sending data to, 107–108
 printing of meta information, 107
 process ID files, 96
 references for, 109
 remote clients, enabling, 98
 removal of flow data, 107
 routers and switches offering, 83
 splitting data files, 106
 stopping flow capture, 97–98
 switching paths and, 86
 versions of, 88
 viewing flow data, 98–105
 NetFlow Accounting. *See* NetFlow
 NetFlow Switching. *See* NetFlow
 netstat, 8, 197–198
 network management, 1–2
 network management tools. *See specific tools*
 network monitoring scripts
 inactive, preventing exiting of, 227–228
 loop timing in, 225–226
 SNMP tools and, 36–37
 state changes and, 226–227
 See also Bourne shell scripts; Perl
 network traffic, monitoring
 with MRTG, 39–41
 with Neo, 53, 54, 56, 72–75
 with NetFlow. *See* NetFlow
 with tcpdump, 157, 173
 networked devices, growth in numbers of, 1
 newline syntax, Perl and, 215
 node, 9
 numeric values, scripts comparing, 208, 216

O

Oak, 7, 111–131
 condensing redundant messages, 112, 113
 configuration, 122–130
 critical message notification, 112, 114
 global options, 123
 installation, 114
 invoking and running, 128–129
 maintenance of, 130
 queue definitions, 123–126
 regular expressions and, 119–122, 126–128

report generation, 112–113
 syslog configuration and, 115–119
 unimportant messages, ignoring,
 112, 113
 object identifiers (IDs), SNMP variable,
 15–16
 objects, Sysmon, 141–147, 154
 Oetiker, Tobias, 39
 OID. *See* object identifiers (IDs)
 open source software, 2–6. *See also specific
 tools*
 Open System Interconnection (OSI) network
 models, 8–9
 OpenView, HP’s, 81
 optimum switching, 86
 output redirection, Bourne shell, 212

P

packet analyzers, 155–156, 175, 176
 snoop, 159
 Snort, 175
 tcpdump. *See* tcpdump
 packet flood, tcpdump analysis of, 173
 packet loss rate, 179–180
 packet matching primitives, tcpdump,
 165, 166
 parentheses (), substitution with
 in Oak, 122
 passive tests, Nagios, 153
 PATH environment variable, Bourne shell scripts
 and, 203–204
 pause command, Sysmon, 139
 pcap library, 155, 159–160
 PDU type. *See* Protocol Data Unit (PDU)
 type
 period (.), Oak and, 119, 120
 Perl scripts, 8, 52, 214–224, 230
 collecting output from several
 programs, 224
 command line arguments in, 222
 command output, using, 223
 conditionals and, 216–217
 environment variables and, 216
 exiting of, 223–224
 hashes and, 220
 initial script line (#!), 202
 list manipulation with, 218–220
 loops and, 222
 mail, formatting of with, 228–229
 Multi Router Traffic Grapher (MRTG)
 and, 41
 names for, 202
 reading lines from a file, 220–221
 subroutines, 223
 syntax of, 215

text manipulation with, 217–218
 variable names, 215
 writing to files, 221
 ping, 8, 177–183
 behavior of on different platforms,
 177, 178
 continuous tests, 179–180
 ICMP packet size and, 180–181
 options for, 180–181
 pinging from network devices, 182
 round-trip time (RTT) and, 180
 PNG library, 52
 PNG (Portable Network Graphics), MRTG
 and, 39, 41, 42, 52
 polling software. *See* service monitors
 port commands, Neo, 67–68
 port mapping, bridge MIB (dot1dBridge) and,
 25–26
 port numbers, interface index
 numbers and, 22
 ports
 enabling/disabling with Neo,
 54, 56–57, 67–68
 information on from Neo, 54, 55,
 68–69, 70–71
 Neo syntax for, 62–64
 Neo traffic statistics for, 72–75
 SNMP tables of, 17–19
 See also boards
 power status, Neo queries of,
 54, 57, 71–72, 80
 prescan command, Oak and, 125, 126
 primitives, tcpdump, 165, 166
 print command, Neo, 64–65
 privacy, packet analyzers and, 155–156
 process ID file, changing, 96
 process ID, storing script, 213–214
 programming languages, compiled vs.
 interpreted, 200–201
 promiscuous mode, tcpdump and, 161
 proprietary programs. *See* commercial
 software
 Protocol Data Unit (PDU) types, SNMP and,
 13, 19–20, 33–34

Q

quality, open source software, 5–6
 queue time, Sysmon, 148–149
 queues, Oak and, 122, 123–124
 QuickPage, 154

R

-r Bourne shell conditional, 208
 Rand, Dave, 39

readcom variable, Neo, 65
 Red Hat Linux, 2–3
 regular expressions, Oak and,
 119–122, 126–128, 131
 relative sequence number, TCP, 168
 reload command, Sysmon, 139
 remote clients
 sending flow data to, 98
 Sysmon and, 140
 remote hosts, sending messages to,
 117, 118–119, 131
 repeaters, 54
 resume command, Sysmon, 139
 reverse lookups, SNMP and, 25
 root node, Sysmon configuration and, 141
 root privileges, 161, 195
 round-trip time (RTT), 180
 routers, 41
 flow expiration and, 86
 management by SNMP, 11
 message logs of activity on, 111
 monitoring with MRTG, 41, 49–50
 NetFlow and, 83, 86–87, 89–90
 tracing path of packets through,
 189–191, 192–193, 195–197
 routing tables, viewing with netstat, 198

S

scalar context, Perl and, 219
 Scotty/Tkined, 81
 scripts, 199–230
 Bourne shell, 203–214
 comment lines (#), 202, 214
 cron program and, 229–230
 environment variables and, 202–203
 inactive, preventing exiting of, 227–228
 initial line of (#!), 202
 interpreted languages and, 200–201
 local variables and, 203
 loop timing and, 225–226
 mail, formatting of with, 228–229
 naming of, 202
 Neo and, 75–76, 80
 Perl, 214–224
 SNMP tools and, 36–37
 state changes and, 226–227
 Unix and, 201–202
 security, 6, 12, 13, 76
 semicolon (;), Perl syntax and, 215
 sendmail program, 228–229
 service monitors, 8, 133–155
 benefits of running, 135–136
 Nagios, 135, 152–154
 Sysmon, 135, 136–152
 severity levels, syslog, 116

set command, Neo, 65
 set-request, SNMP PDU type, 13, 20
 set writecom command, Neo, 67–68
 severity level, syslog message, 115, 116–119
 shell commands, executing with Neo, 57, 76
 Simple Network Management Protocol (SNMP).
 See SNMP (Simple Network
 Management Protocol)
 simple variables, request for SNMP, 17
 sleep script command, 225–226
 SMI standard. *See* Structure of Manage-
 ment Information (SMI) standard
 snaplen tcpdump option, 162
 snmp-options variable, MRTG and, 45
 SNMP (Simple Network Management
 Protocol), 7, 11–38
 access privileges, 12–13
 community name and, 12, 13
 device information available for retrieval,
 20–26
 get-next-request and, 13, 19–20, 33
 management agents, 11
 Management Information Base (MIB)
 and, 14–15
 packet header information, 12–13
 Protocol Data Unit (PDU) types, 13,
 19–20, 33–34
 references for, 37–38
 tools for. *See* SNMP tools
 trap PDU type and, 13, 19–20, 33–34
 User Datagram Protocol (UDP)
 and, 12
 variables. *See* SNMP variables
 versions of, 11–12
 SNMP tables, 17–19, 22, 24–25
 SNMP tools (net-smnp)
 maintenance of, 37
 Management Information Base (MIB)
 and, 36
 net-smnp installation and configuration,
 26–29
 scripting with, 36–37
 snmpbulkget, 34
 snmpbulkwalk, 30, 31, 34
 snmpcmd, 30
 snmpd, 35
 snmpdelta, 35
 snmpdf, 35
 snmpget, 29–31, 37
 snmpgetnext, 34
 snmpnetstat, 35
 snmpset, 30, 31, 32
 snmpstatus, 35
 snmpstatust, 35
 snmptable, 35, 36
 snmpstest, 35

- snmptranslate, 35
- snmptrap, 35
- snmptrapd, 33–34,
- snmptrapm, 35
- snmpwalk, 19, 30, 31, 33
- Web sites for, 27
- SNMP variables, 14–15
 - bridge MIB (dot1dBridge), 25–26
 - getting value of writable (snmpset), 32
 - hierarchy of, 15–16
 - interfaces group, 22–24
 - ip.ipNetToMediaTable, 24–25
 - lexicographic ordering of, 19
 - Management Information Base (MIB)
 - and, 14–15
 - naming of, 15
 - object identifiers for, 15–16
 - requests for simple, 17
 - retrieving contiguous segment of (snmpwalk), 33
 - retrieving value of (snmpget), 29–31
 - system group, 20–22
- snoop packet capturing program, 159
- Snort, 175, 176
- Solaris, 8, 41, 58, 115, 159, 191, 194–195
- spawn command, Sysmon, 145–146
- state machines, 226–227
- state transition diagram, 227
- station learning, 54
- stats command, Neo, 72–75
- statsdelay, Neo, 65, 75
- status file, Sysmon, 147
- Structure of Management Information (SMI)
 - standard, 14
- subroutines, Perl, 223
- support services, open source software
 - and, 6
- Swatch, 130
- switch ports, determining host, 53
- switches, 54, 55, 66–67
- switching, 25–26, 86
- sysContact SNMP variable, 20, 21
- sysLocation SNMP variable, 20, 21
- syslog messages, Oak and, 111, 112
 - condensing redundant information, 112, 113
 - ignoring unimportant messages, 112, 113
 - message facility types, 115, 117
 - message severity levels, 116–118
 - notification of critical messages, 112, 114
 - report generation, 112–113
 - sending messages to remote hosts, 117, 118–119, 131
 - sorting of messages by priority, 116
- syslog protocol, configuration of, 115–119

- syslogd program, 131
- Sysmon, 8, 135, 136–152
 - command line options, 140–141
 - configuration file organization, 151
 - global options in, 147–152
 - installation, 136–137
 - maintenance of, 152
 - objects and dependencies in, 141–147
 - online documentation for, 154
 - pausing, 139
 - placement of on server, 136
 - reloading the configuration file, 139
 - remote clients, enabling, 140
 - root node configuration and, 141
 - starting/stopping the Sysmon daemon, 137–138, 139
- Sysmon variables, 150–151
- sysName SNMP variable, 20, 21
- sysObjectID SNMP variable, 20, 21
- sysServices SNMP variable, 20, 21, 22
- system facility, syslog message, 115
- system group SNMP variables, 20–22
- system information, querying with Neo, 71
- system logs, monitoring with Oak. *See* Oak
- sysUpTime variable, SNMP, 14, 15, 20

T

- tcpdump, 8, 155–176
 - binary format, storing data in, 164–165
 - Cisco CatOS devices and, 170–172
 - Cisco IOS devices and, 172
 - command line options, 161–165
 - data capture, setting amount of, 162
 - data that can be viewed with, 156–157
 - debugging with, 157–158, 172–174
 - displaying packets on detection, 164
 - DNS queries, 162, 163
 - Ethernet header information, 164
 - example command lines, 166–167
 - example output, 156–157
 - filtering and, 165
 - hexadecimal output, 163, 168
 - installation, 160
 - interfaces, specifying, 164
 - limitations, 158
 - maintenance of, 175
 - packet matching primitives, 165, 166
 - pcap library and, 155, 159–160
 - pre-installed on Linux, 158–159
 - printing bytes as characters, 168–169
 - printing detailed packet information, 163
 - printing less packet information, 163
 - promiscuous mode, enabling, 161
 - switched network configuration, 169–170

tcpdump, *Continued*

- TCP output format, 167–168
- types of problems solved with, 157
- UDP output format, 167
- versions of, 155, 159, 175

TCPslice, 176

tcsh program, 58, 203

telnet, 8, 183–185

test plug-ins, Nagios, 153

time stamp, syslog message, 115

timeout variable, Neo, 65

traceroute, 8, 189–193

- installation, 191–192
- MTR (Matt’s traceroute), 194–197
- root privileges and, 191–192
- special characters used by, 192
- testing with, 192–193

traffic flood, analyzing with tcpdump, 173

Transmission Control Protocol (TCP)

- flows and, 84, 85–86
- tcpdump and, 167–168

trap command, Bourne shell, 213–214

trap, SNMP PDU type, 13, 19–20, 33–34

TTL field, IP packet, 190

U

Unix, 8, 115–118, 177, 183, 191, 197, 199, 200, 201–202

User Datagram Protocol (UDP), 12, 86, 167, 175, 188

V

variables. *See specific types*

W

Web pages

- generating MRTG HTML, 47–49
- retrieval of and telnet, 183–184

while loops, 210, 222–223

workstation, 9

writcom variable, Neo, 65

Z

zephyr queue action, Oak and, 124

zlib library, MRTG and, 41