

CONTENTS IN DETAIL

ACKNOWLEDGMENTS

xv

INTRODUCTION

1

Network Administration and Network Management	3
Network Management Tools	3
MRTG, Cricket, and Cacti	3
RTG	4
Nagios and Big Brother	4
CiscoWorks, OpenView, and More	4
Enough Gripping: What's the Solution?	5
Flow-Tools and Its Prerequisites	6
Flows and This Book	6

1

FLOW FUNDAMENTALS

9

What Is a Flow?	10
Flow System Architecture	11
The History of Network Flow	12
NetFlow Versions	12
NetFlow Competition	13
The Latest Standards	13
Flows in the Real World	14
ICMP Flows	14
UDP Flows	15
TCP Flows	16
Other Protocols	17
Flow Export and Timeouts	18
Packet-Sampled Flows	19

2

COLLECTORS AND SENSORS

21

Collector Considerations	21
Operating System	22
System Resources	22
Sensor Considerations	22
Location	23
From Remote Facilities	24
From Private Network Segments/DMZs	24
Implementing the Collector	24

Installing Flow-tools	25
Installing from Packages	25
Installing from Source	25
Running flow-capture	26
Starting flow-capture at Boot	27
How Many Collectors?	28
Collector Log Files	28
Collector Troubleshooting	29
Configuring Hardware Flow Sensors	29
Cisco Routers	30
Cisco Switches	30
Juniper Routers	31
Configuring Software Flow Sensors	32
Setting Up Sensor Server Hardware	32
Network Setup	33
Sensor Server Setup	34
Running the Sensor on the Collector	34
The Sensor: softflowd	34
Running softflowd	35
Watching softflowd	35

3 VIEWING FLOWS 41

Using flow-print	41
Printing Protocol and Port Names	43
Common Protocol and Port Number Assignments	44
Viewing Flow Record Header Information with -p	45
Printing to a Wide Terminal	45
Setting flow-print Formats with -f	46
Showing Interfaces and Ports in Hex with Format -f 0	46
Two Lines with Times, Flags, and Hex Ports Using -f 1	47
Printing BGP Information	48
Wide-Screen Display	48
IP Accounting Format	49
TCP Control Bits and Flow Records	50
ICMP Types and Codes and Flow Records	52
Types and Codes in ICMP	53
Flows and ICMP Details	54

4 FILTERING FLOWS 57

Filter Fundamentals	58
Common Primitives	58
Creating a Simple Filter with Conditions and Primitives	60
Using Your Filter	61

Useful Primitives	61
Protocol, Port, and Control Bit Primitives	61
IP Address and Subnet Primitives	64
Time, Counter, and Double Primitives	65
Interface and BGP Primitives	67
Filter Match Statements	70
Protocols, Ports, and Control Bits	70
Addresses and Subnets	72
Filtering by Sensor or Exporter	72
Time Filters	73
Clipping Levels	73
BGP and Routing Filters	74
Using Multiple Filters	75
Logical Operators in Filter Definitions	76
Logical “or”	76
Filter Inversion	77
Filters and Variables	78
Using Variable-Driven Filters	79
Defining Your Own Variable-Driven Filters	79
Creating Your Own Variables	80

5 REPORTING AND FOLLOW-UP ANALYSIS 81

Default Report	82
Timing and Totals	83
Packet Size Distribution	84
Packets per Flow	84
Octets in Each Flow	84
Flow Time Distribution	85
Modifying the Default Report	85
Using Variables: Report Type	86
Using Variables: SORT	86
Analyzing Individual Flows from Reports	88
Other Report Customizations	89
Choosing Fields	89
Displaying Headers, Hostnames, and Percentages	90
Presenting Reports in HTML	91
Useful Report Types	92
IP Address Reports	92
Network Protocol and Port Reports	94
Traffic Size Reports	96
Traffic Speed Reports	97
Routing, Interfaces, and Next Hops	99
Reporting Sensor Output	104
BGP Reports	104
Customizing Reports	107
Custom Report: Reset-Only Flows	107
More Report Customizations	110
Customizing Report Appearance	112

6 PERL, FLOWSCAN, AND CFLOW.PM 117

Installing Cflow.pm	118
Testing Cflow.pm	118
Install from Operating System Package	118
Install from Source	119
Installing from Source with a Big Hammer	119
flowdumper and Full Flow Information	119
FlowScan and CUFlow	120
FlowScan Prerequisites	121
Installing FlowScan and CUFlow	121
FlowScan User, Group, and Data Directories	122
FlowScan Startup Script	123
Configuring FlowScan	123
Configuring CUFlow: CUFlow.cf	124
Rotation Programs and flow-capture	127
Running FlowScan	128
FlowScan File Handling	128
Displaying CUFlow Graphs	129
Flow Record Splitting and CUFlow	130
Splitting Flows	131
Scripting Flow Record Splitting	132
Filtered CUFlow and Directory Setup	132
Using Cflow.pm	133
A Sample Cflow.pm Script	133
Cflow.pm Variables	134
Other Cflow.pm Exports	135
Acting on Every File	137
Return Value	137
Verbose Mode	138

7 FLOWVIEWER 139

FlowTracker and FlowGrapher vs. CUFlow	140
FlowViewer Security	140
Installing FlowViewer	140
Prerequisites	141
FlowViewer Installation Process	141
Configuring FlowViewer	141
Directories and Site Paths	142
Website Setup	144
Devices and Exporters	144
Troubleshooting the FlowViewer Suite	145
Using FlowViewer	146
Filtering Flows with FlowViewer	146
Reporting Parameters	147
Printed Reports	149
Statistics Reports	149

FlowGrapher	150
FlowGrapher Settings	150
FlowGrapher Output	151
FlowTracker	152
FlowTracker Processes	152
FlowTracker Settings	152
Viewing Trackers	153
Group Trackers	154
Interface Names and FlowViewer	156

8 AD HOC FLOW VISUALIZATION 157

gnuplot 101	158
Starting gnuplot	158
gnuplot Configuration Files	159
Time-Series Example: Bandwidth	160
Total Bandwidth Report	160
Unidirectional Bandwidth Reports	168
Combined Inbound/Outbound Traffic	170
Automating Graph Production	173
Comparison Graphs	175
Data Normalizing	175
Time Scale	175

9 EDGES AND ANALYSIS 177

NetFlow v9	177
Installing flowd	178
Configuring flowd	178
Converting flowd Data to Flow-tools	179
sFlow	180
Configuring sFlow Export with sflowenable	181
Convert sFlow to NetFlow	181
Problem Solving with Flow Data	182
Finding Busted Software	182
Identifying Worms	186
Traffic to Illegal Addresses	187
Traffic to Nonexistent Hosts	188
Afterword	189

INDEX 191