

Service Automation and Dynamic Provisioning Techniques in IP/MPLS Environments

Christian Jacquenet

Gilles Bourdon

Mohamed Boucadair

 WILEY

Contents

Preface	xi
Acknowledgements	xiii
PART I ARCHITECTURES AND PROTOCOLS FOR SERVICE AUTOMATION	1
1 Introduction	3
1.1 To Begin With	3
1.1.1 <i>On IP Networks in General, and Routers in Particular</i>	3
1.1.2 <i>On the Usefulness of Dynamic Routing Protocols in IP Networks</i>	5
1.1.3 <i>On the Inability of an IGP to Address Interdomain Communication Needs</i>	7
1.1.4 <i>On the BGP-4 Protocol</i>	9
1.1.5 <i>The Rise of MPLS</i>	10
1.2 Context and Motivation of this Book	13
1.2.1 <i>Classifying Capabilities</i>	14
1.2.2 <i>Services and Policies</i>	14
1.2.3 <i>The Need for Automation</i>	15
1.3 How this Book is Organized	16
1.4 What Is and What Should Never Be	16
References	16
2 Basic Concepts	19
2.1 What is a Policy?	19
2.2 Deriving Policies into Rules and Configuration Tasks	19
2.2.1 <i>Instantiation</i>	20
2.2.2 <i>Device Identification</i>	20
2.2.3 <i>Translation</i>	21
2.3 Storing Policies	21
2.4 Policy and Device Configuration	21
2.5 Policy-based Management Model	22
2.5.1 <i>Reaching a Policy Decision</i>	24
2.5.2 <i>Requirements for a PEP-PDP Communication Protocol</i>	24
References	25

3	The RADIUS Protocol and its Extensions	27
3.1	Protocol Design	27
3.1.1	<i>Protocol Structure and Messages</i>	28
3.1.2	<i>Forces and Weaknesses</i>	36
3.1.3	<i>Authorization and Provisioning with RADIUS</i>	39
3.2	RADIUS Extensions	44
3.2.1	<i>EAP Support with RADIUS</i>	44
3.2.2	<i>Interim Accounting</i>	47
3.2.3	<i>Dynamic Authorization</i>	49
3.2.4	<i>Using RADIUS for Assignment, Prioritization and Filtering with VLANs</i>	51
3.2.5	<i>Filtering IP Traffic</i>	52
3.2.6	<i>Future Extensions</i>	53
3.2.7	<i>RADIUS and its Future</i>	55
	References	59
4	The Diameter Protocol	61
4.1	Learning from RADIUS Deficiencies	61
4.1.1	<i>General Requirements</i>	62
4.1.2	<i>Authentication Requirements</i>	63
4.1.3	<i>Authorization Requirements</i>	64
4.1.4	<i>Accounting Requirements</i>	64
4.1.5	<i>Diameter is Born</i>	64
4.2	Diameter: Main Characteristics	65
4.2.1	<i>Diameter Network Entities</i>	66
4.2.2	<i>Diameter Applications</i>	67
4.2.3	<i>Sessions and Connections</i>	67
4.2.4	<i>Diameter Routing</i>	68
4.2.5	<i>Peer Discovery</i>	70
4.2.6	<i>Peer Connection Maintenance for Reliable Transmissions</i>	71
4.3	Protocol Details	71
4.3.1	<i>Diameter Header</i>	71
4.3.2	<i>AVP Format</i>	73
4.3.3	<i>Command Codes</i>	74
4.3.4	<i>Accounting</i>	76
4.4	Diameter Network Access Application (NASREQ)	76
4.4.1	<i>AVP Usage for NASREQ</i>	77
4.4.2	<i>Enhanced Authorization Parameters</i>	78
4.4.3	<i>Enhanced Authorization Examples</i>	80
4.5	Diameter Credit Control Application	81
4.6	Diameter in NGN/IMS Architecture for QoS Control	82
4.6.1	<i>What is an NGN?</i>	82
4.6.2	<i>QoS Control in ETSI/TISPAN Architecture</i>	85
	References	90

5	The Common Open Policy Service (COPS) Protocol	91
5.1	A New Scheme for Policy-based Admission Control	91
5.2	A Client–Server Architecture	92
5.3	The COPS Protocol	94
5.3.1	<i>The COPS Header</i>	94
5.3.2	<i>The COPS Message Objects</i>	95
5.4	COPS Messages	97
5.4.1	<i>Client-Open (OPN)</i>	97
5.4.2	<i>Client-Accept (CAT)</i>	97
5.4.3	<i>Request (REQ)</i>	97
5.4.4	<i>Decision (DEC)</i>	98
5.4.5	<i>Other COPS Messages</i>	99
5.5	Summary of COPS Operations	100
5.6	Use of COPS in Outsourcing Mode	101
5.7	Use of COPS in Provisioning Mode	101
5.7.1	<i>On the Impact of Provisioning Mode on COPS Operations</i>	102
5.7.2	<i>On the Impact of Provisioning Mode on PEP–PDP Exchanges</i>	103
5.8	Security of COPS Messages	104
	References	104
6	The NETCONF Protocol	105
6.1	NETCONF at a Glance	105
6.1.1	<i>Introduction</i>	105
6.1.2	<i>Motivations for Introducing NETCONF</i>	106
6.1.3	<i>NETCONF, an IETF Initiative</i>	107
6.1.4	<i>Missions of the IETF NETCONF Working Group</i>	107
6.1.5	<i>NETCONF-related Literature</i>	108
6.1.6	<i>What is In? What is Out?</i>	109
6.2	NETCONF Protocol Overview	109
6.2.1	<i>Some Words about XML</i>	110
6.2.2	<i>NETCONF Terminology</i>	114
6.2.3	<i>NETCONF Layer Model</i>	114
6.2.4	<i>NETCONF Communication Phases</i>	116
6.2.5	<i>NETCONF Data</i>	117
6.2.6	<i>NETCONF Capability Exchange</i>	118
6.2.7	<i>RPC Layer</i>	120
6.2.8	<i>NETCONF Filtering</i>	129
6.3	NETCONF Protocol Operations	131
6.3.1	<i>Retrieve Configuration Data</i>	135
6.3.2	<i>Get</i>	137
6.3.3	<i>Delete Configuration Data</i>	137
6.3.4	<i>Copy Configuration</i>	138
6.3.5	<i>Edit Configuration Data</i>	139
6.3.6	<i>Close a NETCONF Session</i>	142
6.3.7	<i>Kill a Session</i>	143

6.3.8	<i>Lock NETCONF Sessions</i>	144
6.3.9	<i>Unlock NETCONF Sessions</i>	145
6.3.10	<i>Validate Configuration Data</i>	146
6.3.11	<i>Commit Configuration Changes</i>	148
6.3.12	<i>Discard Changes of Configuration Data</i>	149
6.3.13	<i>NETCONF Notification Procedure</i>	149
6.4	NETCONF Transport Protocol	153
6.4.1	<i>NETCONF as Transport-independent Protocol</i>	153
6.4.2	<i>Transport Protocol Alternatives</i>	153
6.5	NETCONF Capabilities	162
6.5.1	<i>URL Capability</i>	163
6.5.2	<i>XPath Capability</i>	165
6.5.3	<i>Writable-Running Capability</i>	166
6.5.4	<i>Candidate Configuration Capability</i>	167
6.5.5	<i>Confirmed Commit Capability</i>	167
6.5.6	<i>Validate Capability</i>	168
6.5.7	<i>Distinct Startup Capability</i>	169
6.5.8	<i>Rollback on Error Capability</i>	170
6.5.9	<i>Notification Capability</i>	171
6.6	Configuring a Network Device	171
6.7	NETCONF Content Layer	173
	References	173

7	Control and Provisioning of Wireless Access Points (CAPWAP)	175
7.1	CAPWAP to Address Access Point Provisioning Challenges	176
7.2	CAPWAP Concepts and Terminology	176
7.3	Objectives: What do we Expect from CAPWAP?	180
7.4	CAPWAP Candidate Protocols	182
7.5	The CAPWAP Protocol	183
7.6	CAPWAP Future	186
	References	186

PART II APPLICATION EXAMPLES OF SERVICE AUTOMATION AND DYNAMIC RESOURCE PROVISIONING TECHNIQUES 187

8	Dynamic Enforcement of QoS Policies	189
8.1	Introduction	189
8.1.1	<i>What is Quality of Service, Anyway?</i>	189
8.1.2	<i>The Need for Service Level Specifications</i>	192
8.2	An Example	193
8.3	Enforcing QoS Policies in Heterogeneous Environments	193
8.3.1	<i>SLS-inferred QoS Policy Enforcement Schemes</i>	193
8.3.2	<i>Policy Rules for Configuring DiffServ Elements</i>	197
	References	198

9	Dynamic Enforcement of IP Traffic Engineering Policies	199
9.1	<i>Introduction</i>	199
9.2	<i>Terminology Considerations</i>	200
9.3	<i>Reference Model</i>	201
9.4	<i>COPS Message Content</i>	202
9.4.1	<i>Request Messages (REQ)</i>	202
9.4.2	<i>Decision Messages (DEC)</i>	203
9.4.3	<i>Report Messages (RPT)</i>	203
9.5	<i>COPS-PR Usage of the IP TE Client-Type</i>	204
9.6	<i>Scalability Considerations</i>	205
9.6.1	<i>A Tentative Metric Taxonomy</i>	205
9.6.2	<i>Reporting the Enforcement of an IP Traffic Engineering Policy</i>	206
9.7	<i>IP TE PIB Overview</i>	206
9.8	<i>COPS Usage for IP TE Accounting Purposes</i>	207
	<i>References</i>	208
10	Automated Production of BGP/MPLS-based VPN Networks	211
10.1	<i>Introduction</i>	211
10.2	<i>Approach</i>	212
10.3	<i>Use of Policies to Define Rules</i>	214
10.4	<i>Instantiation of IP VPN Information Model Classes</i>	214
10.5	<i>Policy Components of an IP VPN Information Model</i>	215
10.5.1	<i>Physical Components of an IP VPN Information Model</i>	216
10.5.2	<i>Virtual Components of an IP VPN Information Model</i>	217
10.5.3	<i>Inheritance Hierarchy</i>	218
10.6	<i>Dynamic Production of IP VPN Services</i>	221
10.7	<i>Context of a Multidomain Environment</i>	222
10.7.1	<i>A Bit of Terminology</i>	222
10.7.2	<i>Reference Model</i>	223
10.8	<i>Possible Extensions of the VPN Model</i>	224
	<i>References</i>	224
11	Dynamic Enforcement of Security Policies in IP/MPLS Environments	227
11.1	<i>Enforcing Security Policies for Web-based Access Control</i>	227
11.2	<i>Enforcing Security Policies in Companies with 802.1X</i>	235
	<i>References</i>	238
12	Future Challenges	239
12.1	<i>Introduction</i>	239
12.1.1	<i>Current Issues with Configuration Procedures</i>	239
12.1.2	<i>Towards Service-driven Configuration Policies</i>	240
12.2	<i>Towards the Standardization of Dynamic Service Subscription and Negotiation Techniques</i>	241
12.2.1	<i>Basic Motivation</i>	241
12.2.2	<i>Commercial Framework</i>	241
12.2.3	<i>A Service-oriented Architecture</i>	242

12.2.4	<i>Publishing and Accessing Services</i>	243
12.2.5	<i>Example of Automated IP VPN Service Composition</i>	244
12.3	Introducing Self-organizing Networks	246
12.3.1	<i>What is a Self-organizing Network?</i>	246
12.3.2	<i>Characteristics of SON Networks and Devices</i>	247
12.3.3	<i>On Self-management</i>	248
12.3.4	<i>SON Algorithms and How to Use Them for Enhancing Dynamic Policy Enforcement Schemes</i>	248
12.3.5	<i>SON-inferred Business Opportunities</i>	249
	References	249
APPENDICES		251
Appendix 1 XML Schema for NETCONF RPCs and Operations		253
Appendix 2 XML Schema for NETCONF Notifications		269
Appendix 3 Example of an IP Traffic Engineering Policy Information Base (IP TE PIB)		273
Appendix 4 Example of an IP TE Accounting PIB		297
Appendix 5 Description of Classes of an IP VPN Information Model		311
A5.1	Introduction	311
A5.2	Policy Class Definitions	311
Index		329