

**TABLE OF CONTENTS**

|                                                                                       |               |
|---------------------------------------------------------------------------------------|---------------|
| <b>Preface.....</b>                                                                   | <b>5</b>      |
| Organization.....                                                                     | 6             |
| Audience .....                                                                        | 7             |
| Conventions used in this book .....                                                   | 8             |
| Acknowledgments.....                                                                  | 9             |
| <br><b>Chapter 1. Network Policies and Cisco Access Lists .....</b>                   | <br><b>10</b> |
| 1.1 Policy sets .....                                                                 | 11            |
| 1.1.1 Characteristics of policy sets .....                                            | 13            |
| 1.1.2 Policy sets in networks.....                                                    | 13            |
| 1.2 The policy toolkit.....                                                           | 16            |
| 1.2.2 Controlling packets passing through a router .....                              | 18            |
| 1.2.3 Controlling routes accepted and distributed.....                                | 19            |
| 1.2.4 Controlling routes accepted and distributed based on route characteristics..... | 20            |
| 1.2.5 Putting it all together.....                                                    | 21            |
| <br><b>Chapter 2. Access List Basics.....</b>                                         | <br><b>22</b> |
| 2.1 Standard access lists.....                                                        | 22            |
| 2.1.1 The implicit deny .....                                                         | 23            |
| 2.1.2 Standard access lists and route filtering.....                                  | 24            |
| 2.1.3 Access list wildcard masks .....                                                | 25            |
| 2.1.4 Specifying hosts in a subnet versus specifying a subnet .....                   | 25            |
| 2.1.5 Access list wildcard masks versus network masks.....                            | 26            |
| 2.1.6 The implicit wildcard mask .....                                                | 27            |
| 2.1.7 Sequential processing in access lists.....                                      | 28            |
| 2.1.8 Standard access lists and packet filtering .....                                | 28            |
| 2.1.9 Generic format of standard access lists.....                                    | 30            |
| 2.2 Extended access lists.....                                                        | 31            |
| 2.2.1 Some general properties of access lists.....                                    | 34            |
| 2.2.2 Matching IP protocols.....                                                      | 34            |
| 2.2.3 More on matching protocol ports.....                                            | 35            |
| 2.2.4 Text substitutes for commonly used ports and masks .....                        | 37            |
| 2.2.5 Generic format of extended access lists.....                                    | 38            |
| 2.3 More on matching .....                                                            | 40            |
| 2.3.1 Good numbering practices .....                                                  | 44            |
| 2.4 Building and maintaining access lists .....                                       | 46            |
| 2.4.1 Risks of deleting access lists as an update technique .....                     | 48            |
| 2.4.2 Displaying access lists .....                                                   | 49            |
| 2.4.3 Storing and saving configurations .....                                         | 50            |
| 2.4.4 Using the implicit deny for ease of maintenance.....                            | 51            |
| 2.5 Named access lists .....                                                          | 51            |
| <br><b>Chapter 3. Implementing Security Policies .....</b>                            | <br><b>52</b> |
| 3.1 Router resource control.....                                                      | 52            |
| 3.1.1 Controlling login mode.....                                                     | 53            |
| 3.1.2 Restricting SNMP access.....                                                    | 56            |
| 3.1.3 The default access list for router resources.....                               | 57            |

|                                                                               |            |
|-------------------------------------------------------------------------------|------------|
| 3.2 Packet filtering and firewalls .....                                      | 58         |
| 3.2.1 A simple example of securing a web server .....                         | 58         |
| 3.2.2 Adding more access to the web server.....                               | 59         |
| 3.2.3 Allowing FTP access to other hosts.....                                 | 60         |
| 3.2.4 Allowing FTP access to the server .....                                 | 61         |
| 3.2.5 Passive mode FTP.....                                                   | 62         |
| 3.2.6 Allowing DNS access .....                                               | 63         |
| 3.2.7 Preventing abuse from the server.....                                   | 64         |
| 3.2.8 Direction of packet flow and extended access lists .....                | 66         |
| 3.2.9 Using the established keyword to optimize performance.....              | 68         |
| 3.2.10 Exploring the inbound access list .....                                | 68         |
| 3.2.11 Session filtering using reflexive access lists.....                    | 75         |
| 3.2.12 An expanded example of packet filtering.....                           | 79         |
| 3.3 Alternatives to access lists .....                                        | 88         |
| 3.3.1 Routing to the null interface .....                                     | 88         |
| 3.3.2 Stopping directed broadcasts .....                                      | 89         |
| 3.3.3 Removing router resources .....                                         | 89         |
| <b>Chapter 4. Implementing Routing Policies.....</b>                          | <b>90</b>  |
| 4.1 Fundamentals of route filtering.....                                      | 90         |
| 4.1.1 Routing information flow .....                                          | 90         |
| 4.1.2 Elements in a routing update.....                                       | 91         |
| 4.1.3 Network robustness.....                                                 | 93         |
| 4.1.4 Business drivers and route preferences.....                             | 96         |
| 4.2 Implementing routing modularity .....                                     | 98         |
| 4.2.1 Minimizing the impact of local routing errors.....                      | 99         |
| 4.2.2 Managing routing updates to stub networks .....                         | 101        |
| 4.2.3 Redistributing routing information between routing protocols .....      | 102        |
| 4.2.4 Minimizing routing updates to stub networks using default networks..... | 103        |
| 4.2.5 Filtering routes distributed between routing processes .....            | 106        |
| 4.3 Implementing route preferences .....                                      | 106        |
| 4.3.1 Eliminating undesired routes .....                                      | 107        |
| 4.3.2 Route preferences through offset-list.....                              | 110        |
| 4.3.3 Route preferences through administrative distance .....                 | 114        |
| 4.4 Alternatives to access lists .....                                        | 119        |
| 4.4.1 Static routing.....                                                     | 119        |
| 4.4.2 Denying all route updates in or out of an interface.....                | 122        |
| <b>Chapter 5. Debugging Access Lists .....</b>                                | <b>123</b> |
| 5.1 Router resource access control lists .....                                | 123        |
| 5.1.1 Checking for correctness.....                                           | 124        |
| 5.1.2 When access lists don't work .....                                      | 125        |
| 5.1.3 Debugging router resource access lists.....                             | 126        |
| 5.2 Packet-filtering access control lists.....                                | 127        |
| 5.2.1 Checking for correctness.....                                           | 128        |
| 5.2.2 Debugging extended access lists.....                                    | 133        |
| 5.3 Route-filtering access control lists.....                                 | 140        |
| 5.3.1 Checking for correctness.....                                           | 140        |
| 5.3.2 Debugging route-filtering access lists.....                             | 151        |

|                                                                        |            |
|------------------------------------------------------------------------|------------|
| <b>Chapter 6. Route Maps.....</b>                                      | <b>155</b> |
| 6.1 Other access list types .....                                      | 156        |
| 6.1.1 Prefix lists .....                                               | 156        |
| 6.1.2 AS-path access lists.....                                        | 159        |
| 6.1.3 BGP community attribute .....                                    | 164        |
| 6.2 Generic route map format .....                                     | 165        |
| 6.3 Interior routing protocols and policy routing.....                 | 168        |
| 6.4 BGP .....                                                          | 171        |
| 6.4.1 Match clauses in BGP.....                                        | 171        |
| 6.4.2 Route maps as command qualifiers .....                           | 173        |
| 6.4.3 Implementing path preferences.....                               | 174        |
| 6.4.4 Propagating route map changes .....                              | 185        |
| 6.5 Debugging route maps and BGP.....                                  | 186        |
| <b>Chapter 7. Case Studies.....</b>                                    | <b>189</b> |
| 7.1 A WAN case study.....                                              | 189        |
| 7.1.1 Security concerns .....                                          | 191        |
| 7.1.2 Robustness concerns .....                                        | 191        |
| 7.1.3 Business concerns .....                                          | 191        |
| 7.1.4 Site 1 router configurations.....                                | 191        |
| 7.1.5 Site 2 router configurations.....                                | 194        |
| 7.1.6 Site 3 router configurations.....                                | 196        |
| 7.2 A firewall case study.....                                         | 199        |
| 7.2.1 Screening router configuration .....                             | 201        |
| 7.2.2 Choke router configuration.....                                  | 204        |
| 7.3 An Internet routing case study .....                               | 207        |
| 7.3.1 Robustness concerns .....                                        | 209        |
| 7.3.2 Security concerns .....                                          | 209        |
| 7.3.3 Policy concerns .....                                            | 209        |
| 7.3.4 Router configurations.....                                       | 210        |
| <b>Appendix A. Extended Access List Protocols and Qualifiers .....</b> | <b>219</b> |
| <b>Appendix B. Binary and Mask Tables.....</b>                         | <b>222</b> |
| <b>Appendix C. Common Application Ports .....</b>                      | <b>226</b> |
| <b>Colophon .....</b>                                                  | <b>227</b> |