



# UAG Series

Unified Access Gateway

Versions: 2.50, 4.00, 4.01, 4.10

Edition 1, 03/2015

## CLI Reference Guide

### Default Login Details

LAN Port	<a href="https://192.168.1.1">https://192.168.1.1</a> (UAG715) <a href="http://172.16.0.1">http://172.16.0.1</a> (UAG2100/ UAG4100/UAG5100 LAN1) <a href="http://172.17.0.1">http://172.17.0.1</a> (UAG2100/ UAG4100/UAG5100 LAN2)
User Name	admin
Password	1234



---

**IMPORTANT!**  
**READ CAREFULLY BEFORE USE.**  
**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

---

This is a Reference Guide for a series of products. Not all products support all firmware features. Screenshots, graphics and commands in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

### **Related Documentation**

- User's Guide  
The User's Guide explains how to use the Web Configurator to configure the UAG.



---

It is recommended you use the Web Configurator to configure the UAG.

---

# About This CLI Reference Guide

## Intended Audience

This manual is intended for people who want to configure ZLD-based UAGs via Command Line Interface (CLI). You should have at least a basic knowledge of TCP/IP networking concepts and topology. Generally, it is organized by feature as outlined in the web configurator.

Note: This guide is intended as a command reference for a series of products. Therefore many commands or command options in this guide may not be available in your product. See your User's Guide for a list of supported features and details about feature implementation.

Note: The version number on the cover page refers to the latest firmware version supported by the UAG. This guide applies to versions 2.50, 4.00, 4.01 and 4.10 at the time of writing.

Please refer to [www.zyxel.com](http://www.zyxel.com) or your product's CD for product specific User Guides and product certifications.

## How To Use This Guide

- 1 Read [Chapter 1 on page 24](#) for how to access and use the CLI (Command Line Interface).
- 2 Read [Chapter 2 on page 37](#) to learn about the CLI user and privilege modes.
- 3 Subsequent chapters are arranged by menu item as defined in the web configurator. Read each chapter carefully for detailed information on that menu item.

Note: Some features cannot be configured in both the web configurator and CLI.

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this guide.

**Warnings tell you about things that could harm you or your device.**

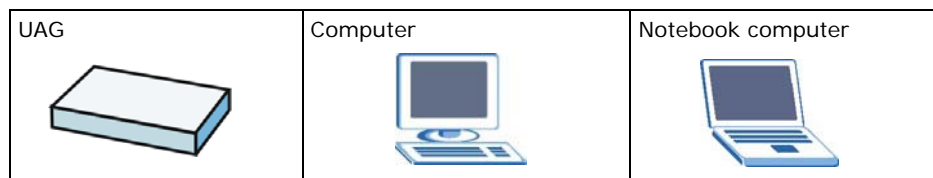
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.






## Syntax Conventions

- The UAG may be referred to as the “UAG”, the “device”, the “system” or the “product” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the “enter” or “return” key on your keyboard.
- “Enter” means for you to type one or more characters and then press the [ENTER] key. “Select” or “choose” means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the “metric” value or the “scientific” value. For example, “k” for kilo may denote “1000” or “1024”, “M” for mega may denote “1000000” or “1048576” and so on.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

## Icons Used in Figures

Figures in this guide may use the following generic icons. The UAG icon is not an exact representation of your device.



Server 	Firewall 	Telephone 
Switch 	Router 	

# Contents Overview

<b>Introduction .....</b>	<b>22</b>
Command Line Interface .....	24
User and Privilege Modes .....	37
<b>Reference .....</b>	<b>41</b>
Object Reference .....	43
Status .....	45
Registration .....	48
AP Management .....	55
Wireless LAN Profiles .....	59
Rogue AP .....	71
Wireless Frame Capture .....	75
Dynamic Channel Selection .....	77
Wireless Load Balancing .....	79
Auto-Healing .....	82
Interfaces .....	84
Trunks .....	106
IP Drop-In .....	111
Route .....	114
Routing Protocol .....	121
Zones .....	125
DDNS .....	128
Virtual Servers .....	131
VPN 1-1 Mapping .....	136
HTTP Redirect .....	140
SMTP Redirect .....	142
ALG .....	145
UPnP .....	148
IP/MAC Binding .....	151
Layer 2 Isolation .....	153
IPnP .....	156
Web Authentication .....	158
Walled Garden .....	166
Advertisement .....	168
RTLS .....	169
Firewall .....	171
Billing .....	177
Payment Service .....	181

Printer Manager .....	184
Free Time .....	186
SMS .....	188
Bandwidth Management .....	190
IPSec VPN .....	195
SSL VPN .....	205
Application Patrol .....	210
Content Filtering .....	213
User/Group .....	224
Application Object .....	232
Addresses .....	235
Services .....	238
Schedules .....	241
AAA Server .....	243
Authentication Objects .....	250
Certificates .....	253
ISP Accounts .....	258
SSL Application .....	260
Endpoint Security .....	262
Dynamic Guest Accounts .....	269
System .....	272
System Remote Management .....	281
File Manager .....	291
Logs .....	304
Reports and Reboot .....	309
Session Timeout .....	315
Diagnostics .....	316
Packet Flow Explore .....	317
Maintenance Tools .....	321
Watchdog Timer .....	326

# Table of Contents

<b>About This CLI Reference Guide</b> .....	<b>3</b>
<b>Document Conventions</b> .....	<b>4</b>
<b>Contents Overview</b> .....	<b>6</b>
<b>Table of Contents</b> .....	<b>8</b>
<b>Part I: Introduction</b> .....	<b>22</b>
<b>Chapter 1</b>	
<b>Command Line Interface</b> .....	<b>24</b>
1.1 Overview .....	24
1.1.1 The Configuration File .....	24
1.2 Accessing the CLI .....	24
1.2.1 Console Port .....	25
1.2.2 Web Configurator Console .....	25
1.2.3 Telnet .....	28
1.2.4 SSH (Secure SHell) .....	28
1.3 How to Find Commands in this Guide .....	28
1.4 How Commands Are Explained .....	29
1.4.1 Background Information (Optional) .....	29
1.4.2 Command Input Values (Optional) .....	29
1.4.3 Command Summary .....	29
1.4.4 Command Examples (Optional) .....	29
1.4.5 Command Syntax .....	29
1.4.6 Changing the Password .....	30
1.5 CLI Modes .....	30
1.6 Shortcuts and Help .....	31
1.6.1 List of Available Commands .....	31
1.6.2 List of Sub-commands or Required User Input .....	31
1.6.3 Entering Partial Commands .....	32
1.6.4 Entering a ? in a Command .....	32
1.6.5 Command History .....	32
1.6.6 Navigation .....	32
1.6.7 Erase Current Command .....	32
1.6.8 The no Commands .....	32
1.7 Input Values .....	33
1.8 Ethernet Interfaces .....	36



1.9 Saving Configuration Changes .....	36
1.10 Logging Out .....	36
<b>Chapter 2</b>	
<b>User and Privilege Modes .....</b>	<b>37</b>
2.1 User And Privilege Modes .....	37
2.1.1 Debug Commands .....	38
<b>Part II: Reference .....</b>	<b>41</b>
<b>Chapter 3</b>	
<b>Object Reference .....</b>	<b>43</b>
3.1 Object Reference Commands .....	43
3.1.1 Object Reference Command Example .....	44
<b>Chapter 4</b>	
<b>Status .....</b>	<b>45</b>
<b>Chapter 5</b>	
<b>Registration .....</b>	<b>48</b>
5.1 myZyXEL.com Overview .....	48
5.2 Subscription Services Available on the UAG .....	48
5.2.1 Content Filtering Subscription Service .....	48
5.2.2 Maximum Number of Managed APs .....	49
5.3 Registration Commands (V2.50 Only) .....	49
5.3.1 Command Examples .....	50
5.4 Registration Status Commands (V4.00 and Later Only) .....	50
5.4.1 Command Examples .....	51
5.5 Country Code .....	51
<b>Chapter 6</b>	
<b>AP Management .....</b>	<b>55</b>
6.1 AP Management Overview .....	55
6.2 AP Management Commands .....	55
6.2.1 AP Management Commands Example .....	58
<b>Chapter 7</b>	
<b>Wireless LAN Profiles .....</b>	<b>59</b>
7.1 Wireless LAN Profiles Overview .....	59
7.2 AP Radio Profile Commands .....	59
7.2.1 AP Profile Commands Example .....	63
7.3 AP Monitor Profile Commands .....	64

7.4 SSID Profile Commands .....	65
7.4.1 SSID Profile Example .....	67
7.5 Security Profile Commands .....	68
7.5.1 Security Profile Example .....	69
7.6 MAC Filter Profile Commands .....	70
7.6.1 MAC Filter Profile Example .....	70
<b>Chapter 8</b>	
<b>Rogue AP.....</b>	<b>71</b>
8.1 Rogue AP Detection Overview .....	71
8.2 Rogue AP Detection Commands .....	71
8.2.1 Rogue AP Detection Examples .....	72
8.3 Rogue AP Containment Overview .....	73
8.4 Rogue AP Containment Commands .....	74
8.4.1 Rogue AP Containment Example .....	74
<b>Chapter 9</b>	
<b>Wireless Frame Capture.....</b>	<b>75</b>
9.1 Wireless Frame Capture Overview .....	75
9.2 Wireless Frame Capture Commands .....	75
9.2.1 Wireless Frame Capture Examples .....	76
<b>Chapter 10</b>	
<b>Dynamic Channel Selection.....</b>	<b>77</b>
10.1 DCS Overview .....	77
10.2 DCS Commands .....	77
10.2.1 DCS Examples .....	78
<b>Chapter 11</b>	
<b>Wireless Load Balancing .....</b>	<b>79</b>
11.1 Wireless Load Balancing Overview .....	79
11.2 Wireless Load Balancing Commands .....	79
11.2.1 Wireless Load Balancing Examples .....	80
<b>Chapter 12</b>	
<b>Auto-Healing .....</b>	<b>82</b>
12.1 Auto-Healing Overview .....	82
12.2 Auto-Healing Commands .....	82
12.2.1 Auto-Healing Examples .....	83
<b>Chapter 13</b>	
<b>Interfaces.....</b>	<b>84</b>
13.1 Interface Overview .....	84

13.1.1 Types of Interfaces .....	84
13.1.2 Relationships Between Interfaces .....	85
13.2 Interface General Commands Summary .....	86
13.2.1 Basic Interface Properties and IP Address Commands .....	87
13.2.2 DHCP Setting Commands .....	90
13.2.3 Interface Parameter Command Examples .....	94
13.2.4 RIP Commands .....	94
13.2.5 OSPF Commands .....	95
13.2.6 Connectivity Check (Ping-check) Commands .....	97
13.3 Ethernet Interface Specific Commands .....	98
13.3.1 MAC Address Setting Commands .....	98
13.3.2 Port Grouping Commands .....	99
13.4 Virtual Interface Specific Commands .....	100
13.4.1 Virtual Interface Command Examples .....	100
13.5 PPPoE/PPTP Specific Commands .....	101
13.5.1 PPPoE/PPTP Interface Command Examples .....	102
13.6 USB Storage Specific Commands .....	102
13.6.1 USB Storage General Commands Example .....	103
13.7 VLAN Interface Specific Commands .....	103
13.7.1 VLAN Interface Command Examples .....	104
13.8 Bridge Specific Commands .....	104
13.8.1 Bridge Interface Command Examples .....	105
<b>Chapter 14</b>	
<b>Trunks.....</b>	<b>106</b>
14.1 Trunks Overview .....	106
14.2 Trunk Scenario Examples .....	106
14.3 Trunk Commands Input Values .....	107
14.4 Trunk Commands Summary .....	107
14.5 Trunk Command Examples .....	108
14.6 Link Sticking .....	109
14.7 Link Sticking Commands Summary .....	109
14.8 Link Sticking Command Example .....	110
<b>Chapter 15</b>	
<b>IP Drop-In.....</b>	<b>111</b>
15.1 Drop-In Mode Overview .....	111
15.1.1 Drop-In Limitations .....	112
15.2 Drop-In Commands .....	112
<b>Chapter 16</b>	
<b>Route.....</b>	<b>114</b>
16.1 Policy Route .....	114

16.2 Policy Route Commands .....	114
16.2.1 Assured Forwarding (AF) PHB for DiffServ .....	117
16.2.2 Policy Route Command Example .....	118
16.3 IP Static Route .....	119
16.4 Static Route Commands .....	119
16.4.1 Static Route Commands Examples .....	120
<b>Chapter 17</b>	
<b>Routing Protocol.....</b>	<b>121</b>
17.1 Routing Protocol Overview .....	121
17.2 Routing Protocol Commands Summary .....	121
17.2.1 RIP Commands .....	122
17.2.2 General OSPF Commands .....	122
17.2.3 OSPF Area Commands .....	123
17.2.4 Virtual Link Commands .....	123
17.2.5 Learned Routing Information Commands .....	124
17.2.6 show ip route Command Example .....	124
<b>Chapter 18</b>	
<b>Zones .....</b>	<b>125</b>
18.1 Zones Overview .....	125
18.2 Zone Commands Summary .....	126
18.2.1 Zone Command Examples .....	127
<b>Chapter 19</b>	
<b>DDNS.....</b>	<b>128</b>
19.1 DDNS Overview .....	128
19.2 DDNS Commands Summary .....	129
19.3 DDNS Commands Example .....	130
<b>Chapter 20</b>	
<b>Virtual Servers .....</b>	<b>131</b>
20.1 Virtual Server Overview .....	131
20.1.1 1:1 NAT and Many 1:1 NAT .....	131
20.2 Virtual Server Commands Summary .....	131
20.2.1 Virtual Server Command Examples .....	133
20.2.2 Tutorial - How to Allow Public Access to a Server .....	134
<b>Chapter 21</b>	
<b>VPN 1-1 Mapping .....</b>	<b>136</b>
21.1 VPN 1-1 Mapping Overview .....	136
21.2 VPN 1-1 Mapping Commands .....	136
21.2.1 vpn-1-1-map pool Sub-commands .....	138

21.2.2 vpn-1-1-map pool Command Examples .....	138
21.2.3 vpn-1-1-map rule Sub-commands .....	138
21.2.4 vpn-1-1-map rule Command Examples .....	139
21.2.5 vpn-1-1-map statistics Command Examples .....	139
<b>Chapter 22</b>	
<b>HTTP Redirect .....</b>	<b>140</b>
22.1 HTTP Redirect Overview .....	140
22.1.1 Web Proxy Server .....	140
22.2 HTTP Redirect Commands .....	140
22.2.1 HTTP Redirect Command Examples .....	141
<b>Chapter 23</b>	
<b>SMTP Redirect .....</b>	<b>142</b>
23.1 SMTP Redirect Overview .....	142
23.1.1 SMTP .....	142
23.2 SMTP Redirect Commands .....	142
23.2.1 smtp-redirect Sub-commands .....	143
23.2.2 SMTP Redirect Command Examples .....	144
<b>Chapter 24</b>	
<b>ALG .....</b>	<b>145</b>
24.1 ALG Introduction .....	145
24.2 ALG Commands .....	146
24.3 ALG Commands Example .....	147
<b>Chapter 25</b>	
<b>UPnP .....</b>	<b>148</b>
25.1 UPnP and NAT-PMP Overview .....	148
25.2 UPnP and NAT-PMP Commands .....	148
25.3 UPnP & NAT-PMP Commands Example .....	149
<b>Chapter 26</b>	
<b>IP/MAC Binding .....</b>	<b>151</b>
26.1 IP/MAC Binding Overview .....	151
26.2 IP/MAC Binding Commands .....	151
26.3 IP/MAC Binding Commands Example .....	152
<b>Chapter 27</b>	
<b>Layer 2 Isolation .....</b>	<b>153</b>
27.1 Layer 2 Isolation Overview .....	153
27.2 Layer 2 Isolation Commands .....	154
27.2.1 Layer 2 Isolation White List Sub-Commands .....	154

27.3 Layer 2 Isolation Commands Example .....	155
<b>Chapter 28</b>	
<b>IPnP .....</b>	<b>156</b>
28.1 IPnP Overview .....	156
28.2 IPnP Commands .....	156
28.3 IPnP Commands Example .....	157
<b>Chapter 29</b>	
<b>Web Authentication .....</b>	<b>158</b>
29.1 Web Authentication Overview .....	158
29.2 Web Authentication Commands .....	158
29.2.1 web-auth login setting Sub-commands .....	160
29.2.2 web-auth policy Sub-commands .....	161
29.2.3 web-auth type default-user-agreement Sub-commands .....	162
29.2.4 web-auth type default-web-portal Sub-commands .....	162
29.2.5 web-auth type profile Sub-commands .....	163
29.2.6 web-auth user-agreement Sub-commands .....	164
29.2.7 Web Authentication Policy Insert Command Example .....	165
<b>Chapter 30</b>	
<b>Walled Garden .....</b>	<b>166</b>
30.1 Walled Garden Overview .....	166
30.2 Walled Garden Commands .....	166
30.2.1 walled-garden rule Sub-commands .....	167
30.2.2 Walled Garden Command Example .....	167
<b>Chapter 31</b>	
<b>Advertisement .....</b>	<b>168</b>
31.1 Advertisement Overview .....	168
31.2 Advertisement Commands .....	168
31.2.1 Advertisement Command Example .....	168
<b>Chapter 32</b>	
<b>RTLS .....</b>	<b>169</b>
32.1 RTLS Overview .....	169
32.1.1 RTLS Configuration Commands .....	170
32.1.2 RTLS Configuration Examples .....	170
<b>Chapter 33</b>	
<b>Firewall .....</b>	<b>171</b>
33.1 Firewall Overview .....	171
33.2 Firewall Commands .....	172

33.2.1 Firewall Sub-Commands .....	174
33.2.2 Firewall Command Examples .....	175
33.3 Session Limit Commands .....	176
<b>Chapter 34</b>	
<b>Billing.....</b>	<b>177</b>
34.1 Billing Overview .....	177
34.2 Billing Commands .....	177
34.2.1 Billing Profile Sub-commands .....	178
34.2.2 Billing Command Example .....	179
<b>Chapter 35</b>	
<b>Payment Service.....</b>	<b>181</b>
35.1 Payment Service Overview .....	181
35.2 Payment-service Commands .....	181
35.2.1 Payment-Service Provider Paypal Sub-commands .....	183
35.2.2 Payment-Service Command Example .....	183
<b>Chapter 36</b>	
<b>Printer Manager .....</b>	<b>184</b>
36.1 Printer Manager Overview .....	184
36.2 Printer-manager Commands .....	184
36.2.1 Printer-manager Printer Sub-commands .....	185
36.2.2 Printer-manager Command Example .....	185
<b>Chapter 37</b>	
<b>Free Time.....</b>	<b>186</b>
37.1 Free Time Overview .....	186
37.2 Free-Time Commands .....	186
37.3 Free-Time Commands Example .....	187
<b>Chapter 38</b>	
<b>SMS .....</b>	<b>188</b>
38.1 SMS Overview .....	188
38.2 SMS Commands .....	188
38.3 SMS Commands Example .....	189
<b>Chapter 39</b>	
<b>Bandwidth Management.....</b>	<b>190</b>
39.1 Bandwidth Management Overview .....	190
39.1.1 BWM Type .....	190
39.2 Bandwidth Management Commands .....	190
39.2.1 Bandwidth Sub-Commands .....	191

39.3 Bandwidth Management Commands Example .....	194
<b>Chapter 40</b>	
<b>IPSec VPN.....</b>	<b>195</b>
40.1 IPSec VPN Overview .....	195
40.2 IPSec VPN Commands Summary .....	196
40.2.1 IKE SA Commands .....	197
40.2.2 IPSec SA Commands (except Manual Keys) .....	199
40.2.3 IPSec SA Commands (for Manual Keys) .....	202
40.2.4 VPN Concentrator Commands .....	202
40.2.5 VPN Configuration Provisioning Commands .....	203
40.2.6 SA Monitor Commands .....	204
<b>Chapter 41</b>	
<b>SSL VPN .....</b>	<b>205</b>
41.1 SSL Access Policy .....	205
41.1.1 SSL Application Objects .....	205
41.1.2 SSL Access Policy Limitations .....	205
41.2 SSL VPN Commands .....	205
41.2.1 SSL VPN Commands .....	206
41.2.2 Setting an SSL VPN Rule Tutorial .....	207
<b>Chapter 42</b>	
<b>Application Patrol.....</b>	<b>210</b>
42.1 Application Patrol Overview .....	210
42.2 Application Patrol Commands Summary .....	210
42.2.1 Application Patrol Commands .....	211
<b>Chapter 43</b>	
<b>Content Filtering.....</b>	<b>213</b>
43.1 Content Filtering Overview .....	213
43.2 Content Filtering Policies .....	213
43.3 External Web Filtering Service .....	213
43.4 Content Filter Command Input Values .....	214
43.5 General Content Filter Commands .....	215
43.6 Content Filter Report Commands .....	217
43.7 Content Filter Profile Commands .....	217
43.8 Content Filter URL Cache Commands .....	220
43.9 Content Filtering Statistics .....	221
43.9.1 Content Filtering Statistics Example .....	221
43.10 Content Filtering Commands Example .....	221
<b>Chapter 44</b>	
<b>User/Group.....</b>	<b>224</b>



44.1 User Account Overview .....	224
44.1.1 User Types .....	224
44.2 User/Group Commands Summary .....	225
44.2.1 User Commands .....	225
44.2.2 User Group Commands .....	226
44.2.3 User Setting Commands .....	227
44.2.4 MAC Auth Commands .....	228
44.2.5 Additional User Commands .....	230
<b>Chapter 45</b>	
<b>Application Object .....</b>	<b>232</b>
45.1 Application Object Commands Summary .....	232
45.1.1 Application Object Commands .....	232
45.1.2 Application Object Group Commands .....	233
<b>Chapter 46</b>	
<b>Addresses .....</b>	<b>235</b>
46.1 Address Overview .....	235
46.2 Address Commands Summary .....	235
46.2.1 Address Object Commands .....	236
46.2.2 Address Group Commands .....	236
<b>Chapter 47</b>	
<b>Services .....</b>	<b>238</b>
47.1 Services Overview .....	238
47.2 Services Commands Summary .....	238
47.2.1 Service Object Commands .....	238
47.2.2 Service Group Commands .....	239
<b>Chapter 48</b>	
<b>Schedules .....</b>	<b>241</b>
48.1 Schedule Overview .....	241
48.2 Schedule Commands Summary .....	241
48.2.1 Schedule Command Examples .....	242
<b>Chapter 49</b>	
<b>AAA Server .....</b>	<b>243</b>
49.1 AAA Server Overview .....	243
49.2 Authentication Server Command Summary .....	243
49.2.1 ad-server Commands .....	243
49.2.2 ldap-server Commands .....	244
49.2.3 radius-server Commands .....	245
49.2.4 radius-server Command Example .....	245

49.2.5 aaa group server ad Commands .....	245
49.2.6 aaa group server ldap Commands .....	246
49.2.7 aaa group server radius Commands .....	247
49.2.8 aaa group server Command Example .....	249
<b>Chapter 50</b>	
<b>Authentication Objects.....</b>	<b>250</b>
50.1 Authentication Objects Overview .....	250
50.2 aaa authentication Commands .....	250
50.2.1 aaa authentication Command Example .....	251
50.3 test aaa Command .....	251
50.3.1 Test a User Account Command Example .....	251
<b>Chapter 51</b>	
<b>Certificates .....</b>	<b>253</b>
51.1 Certificates Overview .....	253
51.2 Certificate Commands .....	253
51.3 Certificates Commands Input Values .....	253
51.4 Certificates Commands Summary .....	254
51.5 Certificates Commands Examples .....	257
<b>Chapter 52</b>	
<b>ISP Accounts.....</b>	<b>258</b>
52.1 ISP Accounts Overview .....	258
52.1.1 PPPoE and PPTP Account Commands .....	258
<b>Chapter 53</b>	
<b>SSL Application .....</b>	<b>260</b>
53.1 SSL Application Overview .....	260
53.1.1 SSL Application Object Commands .....	260
53.1.2 SSL Application Command Examples .....	261
<b>Chapter 54</b>	
<b>Endpoint Security .....</b>	<b>262</b>
54.1 Endpoint Security Overview .....	262
54.1.1 Endpoint Security Commands Summary .....	263
54.1.2 Endpoint Security Object Commands .....	263
54.1.3 Endpoint Security Object Command Example .....	266
<b>Chapter 55</b>	
<b>Dynamic Guest Accounts .....</b>	<b>269</b>
55.1 Dynamic Guest Accounts Overview .....	269
55.2 Dynamic-guest Commands .....	269

55.2.1 dynamic-guest Sub-commands .....	270
55.2.2 Dynamic-guest Command Example .....	271
<b>Chapter 56</b>	
<b>System .....</b>	<b>272</b>
56.1 System Overview .....	272
56.2 Customizing the WWW Login Page .....	272
56.3 Host Name Commands .....	274
56.4 Time and Date .....	274
56.4.1 Date/Time Commands .....	275
56.5 Console Port Speed .....	275
56.6 DNS Overview .....	276
56.6.1 Domain Zone Forwarder .....	276
56.6.2 DNS Commands .....	276
56.6.3 DNS Command Example .....	277
56.7 Authentication Server Overview .....	277
56.7.1 Authentication Server Commands .....	278
56.7.2 Authentication Server Command Examples .....	279
56.8 ZON Overview .....	279
56.8.1 LLDP .....	279
56.8.2 ZON Commands .....	280
56.8.3 ZON Examples .....	280
<b>Chapter 57</b>	
<b>System Remote Management.....</b>	<b>281</b>
57.1 Remote Management Overview .....	281
57.1.1 Remote Management Limitations .....	281
57.1.2 System Timeout .....	281
57.2 Common System Command Input Values .....	282
57.3 HTTP/HTTPS Commands .....	282
57.3.1 HTTP/HTTPS Command Examples .....	284
57.4 SSH .....	284
57.4.1 SSH Implementation on the UAG .....	284
57.4.2 Requirements for Using SSH .....	284
57.4.3 SSH Commands .....	285
57.4.4 SSH Command Examples .....	285
57.5 Telnet .....	286
57.6 Telnet Commands .....	286
57.6.1 Telnet Commands Examples .....	286
57.7 Configuring FTP .....	287
57.7.1 FTP Commands .....	287
57.7.2 FTP Commands Examples .....	287
57.8 SNMP .....	288

57.8.1 Supported MIBs .....	288
57.8.2 SNMP Traps .....	288
57.8.3 SNMP Commands .....	289
57.8.4 SNMP Commands Examples .....	289
57.9 ICMP Filter .....	290
<b>Chapter 58</b>	
<b>File Manager.....</b>	<b>291</b>
58.1 File Directories .....	291
58.2 Configuration Files and Shell Scripts Overview .....	291
58.2.1 Comments in Configuration Files or Shell Scripts .....	292
58.2.2 Errors in Configuration Files or Shell Scripts .....	293
58.2.3 UAG Configuration File Details .....	293
58.2.4 Configuration File Flow at Restart .....	294
58.3 File Manager Commands Input Values .....	294
58.4 File Manager Commands Summary .....	295
58.5 File Manager Command Examples .....	296
58.6 FTP File Transfer .....	296
58.6.1 Command Line FTP File Upload .....	296
58.6.2 Command Line FTP Configuration File Upload Example .....	297
58.6.3 Command Line FTP File Download .....	297
58.6.4 Command Line FTP Configuration File Download Example .....	298
58.7 UAG File Usage at Startup .....	298
58.8 Notification of a Damaged Recovery Image or Firmware .....	299
58.9 Restoring the Recovery Image .....	300
58.10 Restoring the Firmware .....	302
<b>Chapter 59</b>	
<b>Logs .....</b>	<b>304</b>
59.1 Log Commands Summary .....	304
59.1.1 Log Entries Commands .....	304
59.1.2 System Log Commands .....	305
59.1.3 Debug Log Commands .....	306
59.1.4 E-mail Profile Commands .....	307
59.1.5 Console Port Logging Commands .....	308
<b>Chapter 60</b>	
<b>Reports and Reboot.....</b>	<b>309</b>
60.1 Report Commands Summary .....	309
60.1.1 Report Commands .....	309
60.1.2 Report Command Examples .....	310
60.1.3 Session Commands .....	310
60.2 Email Daily Report Commands .....	310

---

60.2.1 Email Daily Report Example .....	312
60.3 Reboot .....	314
<b>Chapter 61</b>	
<b>Session Timeout .....</b>	<b>315</b>
<b>Chapter 62</b>	
<b>Diagnostics .....</b>	<b>316</b>
62.1 Diagnostics .....	316
62.2 Diagnosis Commands .....	316
62.3 Diagnosis Commands Example .....	316
<b>Chapter 63</b>	
<b>Packet Flow Explore .....</b>	<b>317</b>
63.1 Packet Flow Explore .....	317
63.2 Packet Flow Explore Commands .....	317
63.3 Packet Flow Explore Commands Example .....	318
<b>Chapter 64</b>	
<b>Maintenance Tools .....</b>	<b>321</b>
64.1 Maintenance Command Examples .....	323
64.1.1 Packet Capture Command Example .....	324
<b>Chapter 65</b>	
<b>Watchdog Timer .....</b>	<b>326</b>
65.1 Hardware Watchdog Timer .....	326
65.2 Software Watchdog Timer .....	326
65.3 Application Watchdog .....	327
65.3.1 Application Watchdog Commands Example .....	328
<b>List of Commands (Alphabetical) .....</b>	<b>330</b>

---

# **PART I**

## **Introduction**

---



# Command Line Interface

This chapter describes how to access and use the CLI (Command Line Interface).

## 1.1 Overview

If you have problems with your UAG, customer support may request that you issue some of these commands to assist them in troubleshooting.

**Use of undocumented commands or misconfiguration can damage the UAG and possibly render it unusable.**

### 1.1.1 The Configuration File

When you configure the UAG using either the CLI (Command Line Interface) or the web configurator, the settings are saved as a series of commands in a configuration file on the UAG. You can store more than one configuration file on the UAG. However, only one configuration file is used at a time.

You can perform the following with a configuration file:

- Back up UAG configuration once the UAG is set up to work in your network.
- Restore UAG configuration.
- Save and edit a configuration file and upload it to multiple UAGs (of the same model) in your network to have the same settings.

Note: You may also edit a configuration file using a text editor.

## 1.2 Accessing the CLI

You can access the CLI using a terminal emulation program on a computer connected to the console port, from the web configurator or access the UAG using Telnet or SSH (Secure SHell).

Note: The UAG might force you to log out of your session if reauthentication time, lease time, or idle timeout is reached. See [Chapter 44 on page 224](#) for more information about these settings.



## 1.2.1 Console Port

The default settings for the console port are as follows.

**Table 1** Managing the UAG: Console Port

SETTING	VALUE
Speed	115200 bps
Data Bits	8
Parity	None
Stop Bit	1
Flow Control	Off

When you turn on your UAG, it performs several internal tests as well as line initialization. You can view the initialization information using the console port.

- Garbled text displays if your terminal emulation program's speed is set lower than the UAG's.
- No text displays if the speed is set higher than the UAG's.
- If changing your terminal emulation program's speed does not get anything to display, restart the UAG.
- If restarting the UAG does not get anything to display, contact your local customer support.

**Figure 1** Console Port Power-on Display

```
FLASH: AMD 16M

BootModule Version: V1.22 | Mar  8 2012 17:12:28
DRAM: Size = 512 Mbytes

Kernel Version: V2.6.25.4 | 2012-03-15 10:26:57
ZLD Version: V2.50(AACG.0)b2 | 2012-03-15 11:00:44

Press any key to enter debug mode within 1 seconds.
.....
```

After the initialization, the login screen displays.

**Figure 2** Login Screen

```
Welcome to UAG715

Username:
```


Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

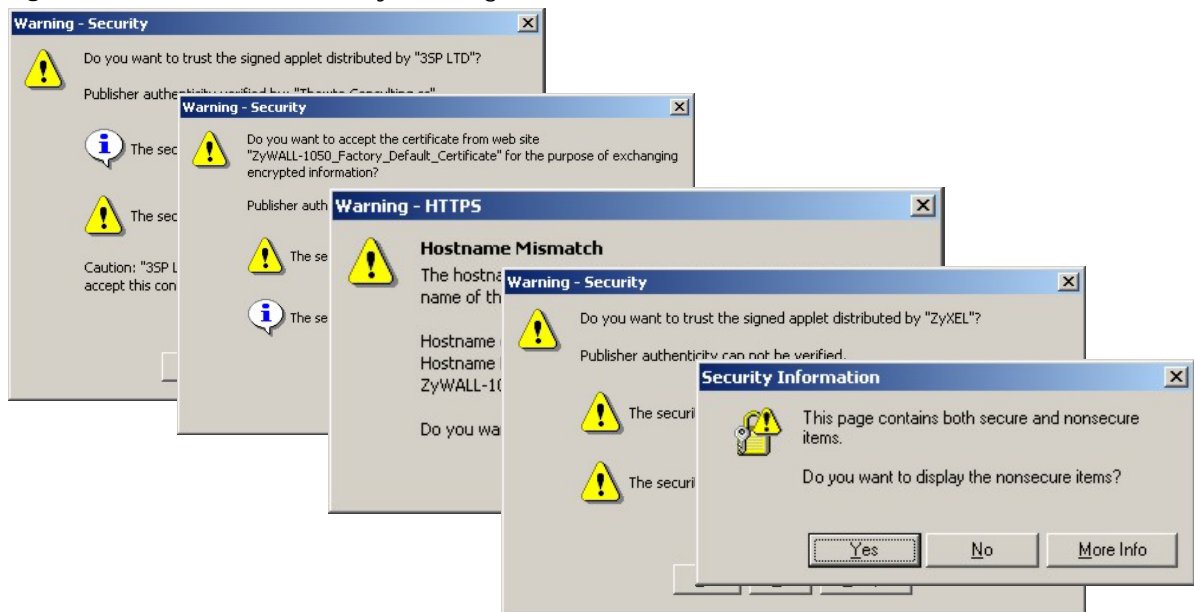
## 1.2.2 Web Configurator Console

Note: Before you can access the CLI through the web configurator, make sure your computer supports the Java Runtime Environment. You will be prompted to download and install the Java plug-in if it is not already installed.

When you access the CLI using the web console, your computer establishes a SSH (Secure SHell) connection to the UAG. Follow the steps below to access the web console.

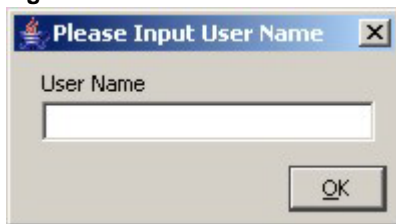
- 1 Log into the web configurator.
- 2 Click the **Console** icon  in the top-right corner of the web configurator screen.
- 3 If the Java plug-in is already installed, skip to step 4. Otherwise, you will be prompted to install the Java plug-in. If the prompt does not display and the screen remains gray, you have to download the setup program.
- 4 The web console starts. This might take a few seconds. One or more security screens may display. Click **Yes** or **Always**.

**Figure 3** Web Console: Security Warnings



Finally, the **User Name** screen appears.

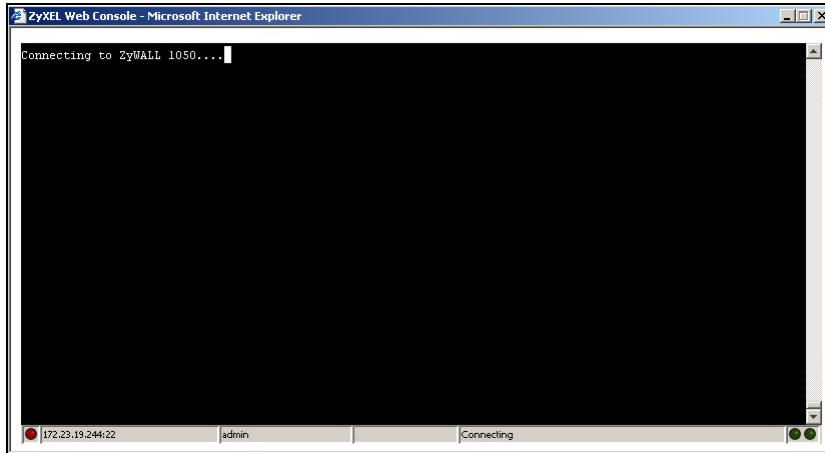
**Figure 4** Web Console: User Name



- 5 Enter the user name you want to use to log in to the console. The console begins to connect to the UAG.

Note: The default login username is **admin**. It is case-sensitive.

**Figure 5** Web Console: Connecting



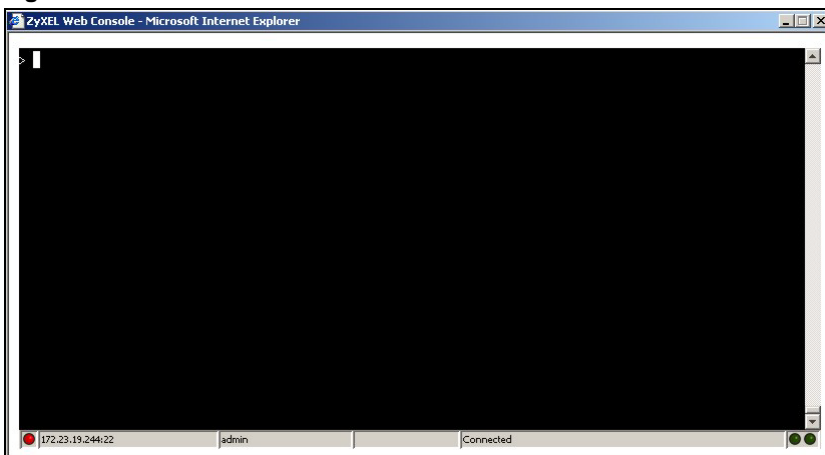
Then, the **Password** screen appears.

**Figure 6** Web Console: Password



- 6 Enter the password for the user name you specified earlier, and click **OK**. If you enter the password incorrectly, you get an error message, and you may have to close the console window and open it again. If you enter the password correctly, the console screen appears.

**Figure 7** Web Console



- 7 To use most commands in this User's Guide, enter `configure terminal`. The prompt should change to Router (config) #.

## 1.2.3 Telnet

Use the following steps to Telnet into your UAG.

- 1 If your computer is connected to the UAG over the Internet, skip to the next step. Make sure your computer IP address and the UAG IP address are on the same subnet.
- 2 In Windows, click **Start** (usually in the bottom left corner) and **Run**. Then type `telnet` and the UAG's IP address. For example, enter `telnet 192.168.1.1` (the default management IP address).
- 3 Click **OK**. A login screen displays. Enter the user name and password at the prompts.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

## 1.2.4 SSH (Secure SHell)

You can use an SSH client program to access the CLI. The following figure shows an example using a text-based SSH client program. Refer to the documentation that comes with your SSH program for information on using it.

Note: The default login username is **admin** and password is **1234**. The username and password are case-sensitive.

**Figure 8** SSH Login Example

```
C:\>ssh2 admin@192.168.1.1
Host key not found from database.
Key fingerprint:
xolor-takel-fipef-zevit-visom-gydog-vetan-bisol-lysob-cuvun-muxex
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes

Host key saved to C:/Documents and Settings/user/Application Data/SSH/hostkeys/
ey_22_192.168.1.1.pub
host key for 192.168.1.1, accepted by user Tue Aug 09 2005 07:38:28
admin's password:
Authentication successful.
```

## 1.3 How to Find Commands in this Guide

You can simply look for the feature chapter to find commands. In addition, you can use the [List of Commands \(Alphabetical\)](#) at the end of the guide. This section lists the commands in alphabetical order that they appear in this guide.

If you are looking at the CLI Reference Guide electronically, you might have additional options (for example, bookmarks or **Find...**) as well.

## 1.4 How Commands Are Explained

Each chapter explains the commands for one keyword. The chapters are divided into the following sections.

### 1.4.1 Background Information (Optional)

Note: See the User's Guide for background information about most features.

This section provides background information about features that you cannot configure in the web configurator. In addition, this section identifies related commands in other chapters.

### 1.4.2 Command Input Values (Optional)

This section lists common input values for the commands for the feature in one or more tables

### 1.4.3 Command Summary

This section lists the commands for the feature in one or more tables.

### 1.4.4 Command Examples (Optional)

This section contains any examples for the commands in this feature.

### 1.4.5 Command Syntax

The following conventions are used in this guide.

- A command or keyword in *courier new* must be entered literally as shown. Do not abbreviate.
- Values that you need to provide are in *italics*.
- Required fields that have multiple choices are enclosed in curly brackets {}.
- A range of numbers is enclosed in angle brackets <>.
- Optional fields are enclosed in square brackets [].
- The | symbol means OR.

For example, look at the following command to create a TCP/UDP service object.

```
service-object object-name {tcp | udp} {eq <1..65535> | range <1..65535> <1..65535>}
```

- 1 Enter `service-object` exactly as it appears.
- 2 Enter the name of the object where you see `object-name`.
- 3 Enter `tcp` or `udp`, depending on the service object you want to create.
- 4 Finally, do one of the following.
  - Enter `eq` exactly as it appears, followed by a number between 1 and 65535.

- Enter range exactly as it appears, followed by two numbers between 1 and 65535.

## 1.4.6 Changing the Password

It is highly recommended that you change the password for accessing the UAG. See [Section 44.2 on page 225](#) for the appropriate commands.

## 1.5 CLI Modes

You run CLI commands in one of several modes.

**Table 2** CLI Modes

	<b>USER</b>	<b>PRIVILEGE</b>	<b>CONFIGURATION</b>	<b>SUB-COMMAND</b>
What <b>Guest</b> users can do	Unable to access	Unable to access	Unable to access	Unable to access
What <b>User</b> users can do	<ul style="list-style-type: none"> <li>• Look at (but not run) available commands</li> </ul>	Unable to access	Unable to access	Unable to access
What <b>Limited-Admin</b> users can do	<ul style="list-style-type: none"> <li>• Look at system information (like <b>Status</b> screen)</li> <li>• Run basic diagnostics</li> </ul>	<ul style="list-style-type: none"> <li>• Look at system information (like <b>Status</b> screen)</li> <li>• Run basic diagnostics</li> </ul>	Unable to access	Unable to access
What <b>Admin</b> users can do	<ul style="list-style-type: none"> <li>• Look at system information (like <b>Status</b> screen)</li> <li>• Run basic diagnostics</li> </ul>	<ul style="list-style-type: none"> <li>• Look at system information (like <b>Status</b> screen)</li> <li>• Run basic diagnostics</li> </ul>	<ul style="list-style-type: none"> <li>• Configure simple features (such as an address object)</li> <li>• Create or remove complex parts (such as an interface)</li> </ul>	<ul style="list-style-type: none"> <li>• Configure complex parts (such as an interface) in the UAG</li> </ul>
How you enter it	Log in to the UAG	Type <b>enable</b> in <b>User</b> mode	Type <b>configure terminal</b> in <b>User</b> or <b>Privilege</b> mode	Type the command used to create the specific part in <b>Configuration</b> mode
What the prompt looks like	Router>	Router#	Router(config)#	(varies by part) Router(zone)# Router(config-if-ge)# ...
How you exit it	Type <b>exit</b>	Type <b>disable</b>	Type <b>exit</b>	Type <b>exit</b>

See [Chapter 44 on page 224](#) for more information about the user types. **User** users can only log in, look at (but not run) the available commands in **User** mode, and log out. **Limited-Admin** users can look at the configuration in the web configurator and CLI, and they can run basic diagnostics in the CLI. **Admin** users can configure the UAG in the web configurator or CLI.

At the time of writing, there is not much difference between **User** and **Privilege** mode for admin users. This is reserved for future use.

## 1.6 Shortcuts and Help

### 1.6.1 List of Available Commands

A list of valid commands can be found by typing ? or [TAB] at the command prompt. To view a list of available commands within a command group, enter <command> ? or <command> [TAB].

**Figure 9** Help: Available Commands Example 1

```
Router> ?
<cr>
apply
atse
clear
configure
----- [Snip] -----
shutdown
telnet
test
traceroute
write
Router>
```

**Figure 10** Help: Available Command Example 2

```
Router> show ?
aaa
access-page
account
ad-server
address-object
----- [Snip] -----
web-auth
workspace
zone
Router> show
```

### 1.6.2 List of Sub-commands or Required User Input

To view detailed help information for a command, enter <command> <sub command> ?.

**Figure 11** Help: Sub-command Information Example

```
Router(config)# ip telnet server ?
;
<cr>
port
rule
|
Router(config)# ip telnet server
```

**Figure 12** Help: Required User Input Example

```
Router(config)# ip telnet server port ?
<1..65535>
Router(config)# ip telnet server port
```

### 1.6.3 Entering Partial Commands

The CLI does not accept partial or incomplete commands. You may enter a unique part of a command and press [TAB] to have the UAG automatically display the full command.

For example, if you enter **config** and press [TAB], the full command of **configure** automatically displays.

If you enter a partial command that is not unique and press [TAB], the UAG displays a list of commands that start with the partial command.

**Figure 13** Non-Unique Partial Command Example

```
Router# c [TAB]
clear      configure copy
Router# co [TAB]
configure copy
```

### 1.6.4 Entering a ? in a Command

Typing a ? (question mark) usually displays help information. However, some commands allow you to input a ?, for example as part of a string. Press [CTRL+V] on your keyboard to enter a ? without the UAG treating it as a help query.

### 1.6.5 Command History

The UAG keeps a list of commands you have entered for the current CLI session. You can use any commands in the history again by pressing the up (↑) or down (↓) arrow key to scroll through the previously used commands and press [ENTER].

### 1.6.6 Navigation

Press [CTRL]+A to move the cursor to the beginning of the line. Press [CTRL]+E to move the cursor to the end of the line.

### 1.6.7 Erase Current Command

Press [CTRL]+U to erase whatever you have currently typed at the prompt (before pressing [ENTER]).

### 1.6.8 The no Commands

When entering the no commands described in this document, you may not need to type the whole command. For example, with the "[no] mss <536..1452>" command, you use "mss 536" to specify the MSS value. But to disable the MSS setting, you only need to type "no mss" instead of "no mss 536".



## 1.7 Input Values

You can use the ? or [TAB] to get more information about the next input value that is required for a command. In some cases, the next input value is a string whose length and allowable characters may not be displayed in the screen. For example, in the following example, the next input value is a string called <description>.

```
Router# configure terminal
Router(config)# interface lan1
Router(config-if)# description
<description>
```

The following table provides more information about input values like <description>.

**Table 3** Input-Value Formats for Strings in CLI Commands

TAG	# VALUES	LEGAL VALUES
*	1	*
<i>all</i>	--	ALL
<i>authentication key</i>	Used in IPsec SA	
	32-40 16-20	"0x" or "0X" + 32-40 hexadecimal values alphanumeric or ; `~!@#\$\$%^&*()_+\\{\}'':,./<>=-
	Used in MD5 authentication keys for RIP/OSPF and text authentication key for RIP	
	0-16	alphanumeric or _-
	Used in text authentication keys for OSPF	
	0-8	alphanumeric or _-
<i>certificate name</i>	1-31	alphanumeric or ;`~!@#\$\$%^&*()_+[\]\{\}'',.-
<i>community string</i>	0-63	alphanumeric or .- first character: alphanumeric or -
<i>connection_id</i>	1+	alphanumeric or -_:
<i>contact</i>	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@\$_%-.
<i>country code</i>	0 or 2	alphanumeric
<i>custom signature file name</i>	0-30	alphanumeric or _-. first character: letter
<i>description</i>	Used in keyword criteria for log entries	
	1-64	alphanumeric, spaces, or '()+,/:=?;!*#@\$_%-.
	Used in other commands	
	1-61	alphanumeric, spaces, or '()+,/:=?;!*#@\$_%-
<i>distinguished name</i>	1-511	alphanumeric, spaces, or .@=, _-
<i>domain name</i>	Used in content filtering	
	0+	lower-case letters, numbers, or .-
	Used in ip dns server	
	0-247	alphanumeric or .- first character: alphanumeric or -
	Used in domainname, ip dhcp pool, and ip domain	
	0-254	alphanumeric or _- first character: alphanumeric or -
<i>email</i>	1-63	alphanumeric or .@_-

**Table 3** Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
<i>e-mail</i>	1-64	alphanumeric or .@_-
<i>encryption key</i>	16-64 8-32	"0x" or "0X" + 16-64 hexadecimal values alphanumeric or ;\ ~!@#\$\$%^&*()_+\\{\}':,./<>==
<i>file name</i>	0-31	alphanumeric or _-
<i>filter extension</i>	1-256	alphanumeric, spaces, or '()+,/:=?;!*#@\$%_-.
<i>fqdn</i>	Used in ip dns server	
	0-252	alphanumeric or .- first character: alphanumeric or -
	Used in ip ddns, time server, device HA, VPN, certificates, and interface ping check	
	0-254	alphanumeric or .- first character: alphanumeric or -
<i>full file name</i>	0-256	alphanumeric or _/.-
<i>hostname</i>	Used in hostname command	
	0-63	alphanumeric or .-_ first character: alphanumeric or -
	Used in other commands	
	0-252	alphanumeric or .- first character: alphanumeric or -
<i>import configuration file</i>	1-26+".conf"	alphanumeric or ;~!@#\$\$%^&*()_+[]{}',.- add ".conf" at the end
<i>import shell script</i>	1-26+".zysh"	alphanumeric or ;~!@#\$\$%^&*()_+[]{}',.- add ".zysh" at the end
<i>initial string</i>	1-64	alphanumeric, spaces, or '()+,/:=!*#@\$%_-.&
<i>isp account password</i>	0-63	alphanumeric or ~!@#\$\$%^&*()_+={} \\;:'<,>./
<i>isp account username</i>	0-30	alphanumeric or -_@\$./
<i>key length</i>	--	512, 768, 1024, 1536, 2048
<i>license key</i>	25	"S-" + 6 upper-case letters or numbers + "-" + 16 upper-case letters or numbers
<i>mac address</i>	--	aa:bb:cc:dd:ee:ff (hexadecimal)
<i>mail server fqdn</i>		lower-case letters, numbers, or -.
<i>name</i>	1-31	alphanumeric or _-
<i>notification message</i>	1-81	alphanumeric, spaces, or '()+,/:=?;!*#@\$%_-.
<i>password: less than 15 chars</i>	1-15	alphanumeric or ~!@#\$\$%^&*()_+={} \\;:'<,>./
<i>password: less than 8 chars</i>	1-8	alphanumeric or ;/?:@&+\$.-!~*')%,\$
<i>password</i>	Used in user and ip ddns	
	1-63	alphanumeric or ~!@#\$\$%^&*()_+={} \\;:'<,>./
	Used in e-mail log profile SMTP authentication	
	1-63	alphanumeric or ~!@#\$\$%^&*()_+={} \\;:'<>./
	Used in device HA synchronization	
	1-63	alphanumeric or ~#%^*_-={}:;.,.
	Used in registration	
	6-20	alphanumeric or .@_-

**Table 3** Input-Value Formats for Strings in CLI Commands (continued)

<b>TAG</b>	<b># VALUES</b>	<b>LEGAL VALUES</b>
<i>phone number</i>	1-20	numbers or , +
<i>preshared key</i>	16-64	"0x" or "0X" + 16-64 hexadecimal values alphanumeric or ; `~!@#\$\$%^&*()_+{\}'./<>=-
<i>profile name</i>	0-30	alphanumeric or _- first character: letters or _-
<i>proto name</i>	1-16	lower-case letters, numbers, or -
<i>protocol name</i>	0-30	alphanumeric or _- first character: letters or _-
<i>quoted string less than 127 chars</i>	1-255	alphanumeric, spaces, or ;/?:@&=+\$\._!~*'()% ,
<i>quoted string less than 63 chars</i>	1-63	alphanumeric, spaces, or ;/?:@&=+\$\._!~*'()% %
<i>quoted string</i>	0+	alphanumeric, spaces, or punctuation marks enclosed in double quotation marks ("") must put a backslash (\) before double quotation marks that are part of input value itself
<i>service name</i>	0-63	alphanumeric or -_@\$/
<i>spi</i>	2-8	hexadecimal
<i>string less than 15 chars</i>	1-15	alphanumeric or -_
<i>string: less than 63 chars</i>	1-63	alphanumeric or `~!@#\$\$%^&*()_+={}  \ ; ' ! < , > . /
<i>string</i>	1+	alphanumeric or -_@
<i>subject</i>	1-61	alphanumeric, spaces, or '()+,./:=?;!*#@\$_%-
<i>system type</i>	0-2	hexadecimal
<i>timezone [-+]hh</i>	--	-12 through +12 (with or without "+")
<i>url</i>	1-511	alphanumeric or '()+,./:=?;!*#@\$_%-
<i>url</i>	Used in content filtering redirect	
	"http://" + "https://" +	alphanumeric or ;/?:@&=+\$\._!~*'()% , starts with "http://" or "https://" may contain one pound sign (#)
	Used in other content filtering commands	
	"http://" +	alphanumeric or ;/?:@&=+\$\._!~*'()% , starts with "http://" may contain one pound sign (#)
<i>user name</i>	Used in VPN extended authentication	
	1-31	alphanumeric or _-
	Used in other commands	
	0-30	alphanumeric or _- first character: letters or _-
<i>username</i>	6-20	alphanumeric or .@_- registration
<i>user name</i>	1+	alphanumeric or -_. logging commands
<i>user@domainname</i>	1-80	alphanumeric or .@_-
<i>vrrp group name: less than 15 chars</i>	1-15	alphanumeric or _-

**Table 3** Input-Value Formats for Strings in CLI Commands (continued)

TAG	# VALUES	LEGAL VALUES
<i>week-day sequence, i.e. 1=first,2=second</i>	1	1-4
<i>xauth method</i>	1-31	alphanumeric or _-
<i>xauth password</i>	1-31	alphanumeric or ; ~!@#\$\$%^&*()_+\\{'':./<>=-
<i>mac address</i>	0-12 (even number)	hexadecimal for example: aa aabbcc aabbccddeeff

## 1.8 Ethernet Interfaces

How you specify an Ethernet interface depends on the UAG model.

- The UAG uses a name such as wan1, wan2, lan1, lan2, or dmz.

## 1.9 Saving Configuration Changes

Use the `write` command to save the current configuration to the UAG.

Note: Always save the changes before you log out after each management session. All unsaved changes will be lost after the system restarts.

## 1.10 Logging Out

Enter the `exit` or `end` command in configure mode to go to privilege mode.

Enter the `exit` command in user mode or privilege mode to log out of the CLI.

# User and Privilege Modes

This chapter describes how to use these two modes.

## 2.1 User And Privilege Modes

This is the mode you are in when you first log into the CLI. (Do not confuse 'user mode' with types of user accounts the UAG uses. See [Chapter 44 on page 224](#) for more information about the user types. 'User' type accounts can only run 'exit' in this mode. However, they may need to log into the device in order to be authenticated for 'user-aware' policies, for example a firewall rule that a particular user is exempt from or a VPN tunnel that only certain people may use.)

Type 'enable' to go to 'privilege mode'. No password is required. All commands can be run from here except those marked with an asterisk. Many of these commands are for trouble-shooting purposes, for example the htm (hardware test module) and debug commands. Customer support may ask you to run some of these commands and send the results if you need assistance troubleshooting your device.

For admin logins, all commands are visible in 'user mode' but not all can be run there. The following table displays which commands can be run in 'user mode'. All commands can be run in 'privilege mode'.

**The htm and psm commands are for ZyXEL's internal manufacturing process.**

**Table 4** User (U) and Privilege (P) Mode Commands

COMMAND	MODE	DESCRIPTION
apply	P	Applies a configuration file.
atse	U/P	Displays the seed code
clear	U/P	Clears system or debug logs or DHCP binding.
configure	U/P	Use 'configure terminal' to enter configuration mode.
copy	P	Copies configuration files.
debug (*)	U/P	For support personnel only! The device needs to have the debug flag enabled.
delete	P	Deletes configuration files.
details	P	Performs diagnostic commands.
diag	P	Provided for support personnel to collect internal system information. It is not recommended that you use these.
diag-info	P	Has the UAG create a new diagnostic file.
dir	P	Lists files in a directory.
disable	U/P	Goes from privilege mode to user mode
enable	U/P	Goes from user mode to privilege mode

**Table 4** User (U) and Privilege (P) Mode Commands (continued)

COMMAND	MODE	DESCRIPTION
exit	U/P	Goes to a previous mode or logs out.
htm	U/P	Goes to htm (hardware test module) mode for testing hardware components. You may need to use the htm commands if your customer support Engineer asks you to during troubleshooting.  Note: These commands are for ZyXEL's internal manufacturing process.
interface	U/P	Dials or disconnects an interface.
no packet-trace	U/P	Turns off packet tracing.
nslookup	U/P	Resolves an IP address to a host name and vice-versa.
packet-trace	U/P	Performs a packet trace.
ping	U/P	Pings an IP address or host name.
psm	U/P	Goes to psm (product support module) mode for setting product parameters. You may need to use the htm commands if your customer support Engineer asks you to during troubleshooting.  Note: These commands are for ZyXEL's internal manufacturing process.
reboot	P	Restarts the device.
release	P	Releases DHCP information from an interface.
rename	P	Renames a configuration file.
renew	P	Renews DHCP information for an interface.
run	P	Runs a script.
setenv	U/P	Turns stop-on-error on (terminates booting if an error is found in a configuration file) or off (ignores configuration file errors and continues booting).
show	U/P	Displays command statistics. See the associated command chapter in this guide.
shutdown	P	Writes all d data to disk and stops the system processes. It does not turn off the power.
telnet	U/P	Establishes a connection to the TCP port number 23 of the specified host name or IP address.
test aaa	U/P	Tests whether the specified user name can be successfully authenticated by an external authentication server.
traceroute	P	Traces the route to the specified host name or IP address.
write	P	Saves the current configuration to the UAG. All unsaved changes are lost after the UAG restarts.

Subsequent chapters in this guide describe the configuration commands. User/privilege mode commands that are also configuration commands (for example, 'show') are described in more detail in the related configuration command chapter.

## 2.1.1 Debug Commands

Debug commands marked with an asterisk (\*) are not available when the debug flag is on and are for ZyXEL service personnel use only. The debug commands follow a Linux-based syntax, so if there is a Linux equivalent, it is displayed in this chapter for your reference. You must know a command listed here well before you use it. Otherwise, it may cause undesired results.

**Table 5** Debug Commands

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
debug alg	FTP/SIP ALG debug commands	
debug billing show shm (*)	Billing debug commands	
debug ca (*)	Certificate debug commands	

**Table 5** Debug Commands (continued)

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
debug capwap (*)	Capwap debug commands	
debug content-filter	Content Filtering debug commands	
debug dns-query (*)	DNS query related debug commands	
debug dynamic-guest (*)	Dynamic guest debug commands	
debug eps	Endpoint security debug commands	
debug force-auth (*)	Authentication policy debug commands	
debug free-time show shm	Free time debug command	
debug gui (*)	Web Configurator related debug commands	
debug hardware (*)	Hardware debug commands	
debug interface	Interface debug commands	
debug interface ifconfig [interface]	Shows system interfaces detail	> ifconfig [interface]
debug interface-group	Port grouping debug commands	
debug ip dns	DNS debug commands	
debug ip virtual-server	Virtual Server (NAT) debug commands	
debug ipsec	IPSec VPN debug commands	
debug l2-isolation (*)	Layer 2 isolation debug commands	
debug logging	System logging debug commands	
debug manufacture	Manufacturing related debug commands	
debug myzyxel server (*)	MyZyXEL.com debug commands	
debug myzyxel2 show (*)	MyZyXEL.com debug commands	
debug myzyxel2 show sms shm	MyZyXEL.com debug command for SMS	
debug network arpignore (*)	Enable/Display the ignoring of ARP responses for interfaces which don't own the IP address	cat /proc/sys/net/ipv4/conf/*/arp_ignore
debug no myzyxel server (*)	Set the myZyXEL.com registration/update server to the official site	
debug payment-service (*)	Payment service debug commands	
debug policy-route (*)	Policy route debug command	
debug printer-manager debug-info (*)	Printer manager debug commands	
debug reset content-filter profiling	Content Filtering debug commands	
debug service-register	Service registration debug command	
debug show content-filter server	Category-based content filtering debug command	
debug show myzyxel server status	Myzyxel.com debug commands	
debug show ipset	Lists the UAG's received cards	
debug show myzyxel server status	Myzyxel.com debug commands	
debug sms-service (*)	SMS service debug commands	
debug smtp-redirect show (*)	SMTP redirect debug commands	
debug sslvpn	SSL VPN debug commands	

**Table 5** Debug Commands (continued)

COMMAND SYNTAX	DESCRIPTION	LINUX COMMAND EQUIVALENT
debug [cmdexec corefile ip  kernel mac-id- rewrite observer switch  system zyinetpkt zysh-ipt-op] (* )	ZLD internal debug commands	
debug update server (* )	Update server debug command	
debug vpn-1-1-map (* )	VPN 1-1 mapping debug commands	
debug web-auth (* )	Web authentication debug commands	
debug [remoteWTP   remoteWTP-cmd] (* )	Controller debug commands	



---

# PART II

## Reference

---



# Object Reference

This chapter describes how to use object reference commands.

## 3.1 Object Reference Commands

The object reference commands are used to see which configuration settings reference a specific object. You can use this table when you want to delete an object because you have to remove references to the object first.

**Table 6** show reference Commands

COMMAND	DESCRIPTION
show reference object username [username]	Displays which configuration settings reference the specified user object.
show reference object address [object_name]	Displays which configuration settings reference the specified address object.
show reference object eps [object_name]	Displays which configuration settings reference the specified endpoint security object.
show reference object service [object_name]	Displays which configuration settings reference the specified service object.
show reference object schedule [object_name]	Displays which configuration settings reference the specified schedule object.
show reference object interface [interface_name   virtual_interface_name]	Displays which configuration settings reference the specified interface or virtual interface object.
show reference object aaa authentication [default   auth_method]	Displays which configuration settings reference the specified AAA authentication object.
show reference object ca category {local remote} [cert_name]	Displays which configuration settings reference the specified authentication method object.
show reference object account pppoe [object_name]	Displays which configuration settings reference the specified PPPoE account object.
show reference object account ptp [object_name]	Displays which configuration settings reference the specified PPTP account object.
show reference object sslvpn application [object_name]	Displays which configuration settings reference the specified SSL VPN application object.
show reference object crypto map [crypto_name]	Displays which configuration settings reference the specified VPN connection object.
show reference object isakmp policy [isakmp_name]	Displays which configuration settings reference the specified VPN gateway object.
show reference object sslvpn policy [object_name]	Displays which configuration settings reference the specified SSL VPN object.
show reference object zone [object_name]	Displays which configuration settings reference the specified zone object.

**Table 6** show reference Commands (continued)

COMMAND	DESCRIPTION
show reference object-group username [username]	Displays which configuration settings reference the specified user group object.
show reference object-group address [object_name]	Displays which configuration settings reference the specified address group object.
show reference object-group service [object_name]	Displays which configuration settings reference the specified service group object.
show reference object-group interface [object_name]	Displays which configuration settings reference the specified trunk object.
show reference object-group aaa ad [group_name]	Displays which configuration settings reference the specified AAA AD group object.
show reference object-group aaa ldap [group_name]	Displays which configuration settings reference the specified AAA LDAP group object.
show reference object-group aaa radius [group_name]	Displays which configuration settings reference the specified AAA RADIUS group object.

### 3.1.1 Object Reference Command Example

This example shows how to check which configuration is using an address object named LAN1\_SUBNET. For the command output, firewall rule 3 named LAN1-to-UAG is using the address object.

```
Router(config)# show reference object address LAN1_SUBNET

LAN1_SUBNET References:
Category
Rule Priority      Rule Name
Description
=====
Firewall
3                 N/A
LAN1-to-UAG
Router(config)#
```

## Status

This chapter explains some commands you can use to display information about the UAG's current operational state.

**Table 7** Status Show Commands

COMMAND	DESCRIPTION
show boot status	Displays details about the UAG's startup state.
show comport status	Displays whether the console and auxiliary ports are on or off.
show cpu status	Displays the CPU utilization.
show disk	Displays the disk utilization.
show extension-slot	Displays the status of the extension card slot and USB ports and the names of devices connected to them.
show fan-speed	Displays the current fan speed.
show led status	Displays the status of each LED on the UAG.
show mac	Displays the UAG's MAC address.
show mem status	Displays what percentage of the UAG's memory is currently being used.
show ram-size	Displays the size of the UAG's on-board RAM.
show redundant-power status	Displays the status of the UAG's power modules. The UAG has two power modules. It can continue operating on a single power module if one fails.
show serial-number	Displays the serial number of this UAG.
show socket listen	Displays the UAG's listening ports
show socket open	Displays the ports that are open on the UAG.
show system uptime	Displays how long the UAG has been running since it last restarted or was turned on.
show version	Displays the UAG's model, firmware and build information.

Here are examples of the commands that display the CPU and disk utilization.

```
Router(config)# show cpu status
CPU utilization: 0 %
CPU utilization for 1 min: 0 %
CPU utilization for 5 min: 0 %
Router(config)# show disk
;      <cr> |
Router(config)# show disk
No. Disk          Size(MB)          Usage
=====
1  image           67                83%
2  onboard flash   163               15%
```

Here are examples of the commands that display the fan speed, MAC address, memory usage, RAM size, and serial number.

```
Router(config)# show fan-speed
FAN1(F00) (rpm): limit(hi)=8000, limit(lo)=1400, max=6115, min=6115, avg=6115
Router(config)# show mac
MAC address: 00:00:AA:80:05:58-00:00:AA:80:05:5C
Router(config)# show mem status
memory usage: 39%
Router(config)# show ram-size
ram size: 512MB
Router(config)# show serial-number
serial number: Z34131340 80-009-011001AA
Router(config)#
```

Here is an example of the command that displays the listening ports.

```
Router(config)# show socket listen
No.   Proto Local_Address      Foreign_Address      State
=====
1     tcp   127.0.0.1:2601      0.0.0.0:0           LISTEN
2     tcp   127.0.0.1:2602      0.0.0.0:0           LISTEN
3     tcp   127.0.0.1:2604      0.0.0.0:0           LISTEN
4     tcp   127.0.0.1:10444     0.0.0.0:0           LISTEN
5     tcp   0.0.0.0:80          0.0.0.0:0           LISTEN
6     tcp   192.168.3.1:53      0.0.0.0:0           LISTEN
7     tcp   10.113.243.21:53    0.0.0.0:0           LISTEN
8     tcp   127.0.0.1:53        0.0.0.0:0           LISTEN
9     tcp   0.0.0.0:21          0.0.0.0:0           LISTEN
10    tcp   0.0.0.0:22          0.0.0.0:0           LISTEN
11    tcp   127.0.0.1:953       0.0.0.0:0           LISTEN
12    tcp   0.0.0.0:443         0.0.0.0:0           LISTEN
Router(config)#
```

Here is an example of the command that displays the open ports.

```
Router(config)# show socket open
No.   Proto Local_Address      Foreign_Address      State
=====
1     udp   0.0.0.0:520         0.0.0.0:0
2     udp   192.168.3.1:4500    0.0.0.0:0
3     udp   10.113.243.21:4500  0.0.0.0:0
4     udp   10.113.243.21:47384 10.113.243.111:514
5     udp   0.0.0.0:161         0.0.0.0:0
6     udp   192.168.3.1:53      0.0.0.0:0
7     udp   10.113.243.21:53    0.0.0.0:0
8     udp   127.0.0.1:53        0.0.0.0:0
9     udp   0.0.0.0:67          0.0.0.0:0
10    udp   0.0.0.0:56915       0.0.0.0:0
11    udp   10.113.243.21:50526 10.113.243.251:514
12    udp   192.168.3.1:500     0.0.0.0:0
13    udp   10.113.243.21:500   0.0.0.0:0
Router(config)#
```

Here are examples of the commands that display the system uptime and model, firmware, and build information.

```
Router> show system uptime
system uptime: 04:18:00
Router> show version
ZyXEL Communications Corp.
model          : UAG715
firmware version: V2.50(AACG.0)
BM version     : 1.22
build date     : 2012-07-20 13:34:43
Router>
```

This example shows the current LED states on the UAG. The **SYS** LED lights on and green.

```
Router> show led status
sys: green
Router>
```

# Registration

This chapter introduces myzyxel.com and shows you how to register the UAG for subscription services using commands.

## 5.1 myZyXEL.com Overview

myZyXEL.com is ZyXEL's online services center where you can register your UAG and manage subscription services available for the UAG. To use a subscription service, you have to register the UAG and activate the corresponding service at myZyXEL.com.

Note: You need to create a myZyXEL.com account before you can register your device and activate the services at myZyXEL.com.

For a UAG that supports firmware version 2.50, you can directly create a myZyXEL.com account, register your UAG and activate a service using the Web Configurator or CLI commands. Alternatively, go to <http://www.myZyXEL.com> with the UAG's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

Note: To activate a service on a UAG that supports firmware version 2.50, you need to access myZyXEL.com via that UAG.

For a UAG that supports firmware version 4.00 or later, go to <http://portal.myZyXEL.com> with the UAG's serial number and LAN MAC address to register it and activate a service. Refer to the web site's on-line help for details.

## 5.2 Subscription Services Available on the UAG

At the time of writing, The UAG715 can use the content filtering subscription service. The UAG4100 and UAG5100 can use the upgrade service to extend the maximum number of the supported managed APs and the LAN/WLAN users that can connect to the UAG at one time.

### 5.2.1 Content Filtering Subscription Service

The content filter allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your UAG accesses an external database that has millions of web sites categorized based on content. You can have the UAG block, block and/or log access to web sites based on these categories.

See the respective chapters for more information about these features.



## 5.2.2 Maximum Number of Managed APs

The UAG is initially configured to support up to one local AP and 8 remote managed APs (such as the NWA5123-NI). You can increase this by subscribing to additional licenses. As of this writing, each license upgrade allows an additional 8 remote managed APs while the maximum number of remote managed APs a single UAG can support is 16.

## 5.3 Registration Commands (V2.50 Only)

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 8** Input Values for General Registration Commands

LABEL	DESCRIPTION
<i>user_name</i>	The user name of your myZyXEL.com account. You must use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
<i>password</i>	The password for the myZyXEL.com account. You must use six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.

The following table describes the commands available for registration. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 9** Command Summary: Registration

COMMAND	DESCRIPTION
<code>device-register checkuser user_name</code>	Checks if the user name exists in the myZyXEL.com database.
<code>device-register username user_name password password [e-mail user@domainname] [country-code country_code] [reseller-name name] [reseller-mail email-address] [reseller-phone phone-number] [vat vat-number]</code>	Registers the device with an existing account or creates a new account and registers the device at one time. <i>country_code</i> : see <a href="#">Table 11 on page 51</a>
<code>service-register checkexpire</code>	Gets information of all service subscriptions from myZyXEL.com and updates the status table.
<code>service-register service-type standard license-key key_value</code>	Activates a standard service subscription with the license key.
<code>service-register service-type trial service content-filter</code>	Activates the content filter trial service subscription.
<code>show device-register status</code>	Displays whether the device is registered and account information.
<code>show service-register reseller-info</code>	Displays your seller's information that you have entered when registration.
<code>show service-register server-type</code>	Displays the type of the register server to which your UAG is connected.
<code>show service-register status all</code>	Displays all service license information.
<code>show service-register status content-filter</code>	Displays content filter service license information.

### 5.3.1 Command Examples

The following commands allow you to register your device with an existing account or create a new account and register the device at one time, and activate a trial service subscription.

```
Router# configure terminal
Router(config)# device-register username alexctsui password 123456
Router(config)# service-register service-type trial service content-filter
```

The following command displays the account information and whether the device is registered.

```
Router# configure terminal
Router(config)# show device-register status
username           : example
password           : 123456
device register status : yes
expiration self check : no
```

The following command displays the service registration status and type and how many days remain before the service expires.

```
Router# configure terminal
Router(config)# show service-register status all
Service           Status      Type      Count      Expiration
=====
Content-Filter    Licensed   Trial      N/A        16
```

## 5.4 Registration Status Commands (V4.00 and Later Only)

The following table describes the commands available for registration status. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 10** Command Summary: Registration

COMMAND	DESCRIPTION
<code>show service-register status all</code>	Displays all service license information.
<code>show service-register status extension-user</code>	Displays extension-user service license information. It also displays the maximum number of wired and wireless users that may connect to the UAG at the same time.
<code>show service-register status external-ap-control</code>	Displays external-ap-control service license information. It also displays how many managed APs the UAG can support with your current license.
<code>show service-register status sms</code>	Displays whether the SMS ticketing service is activated.

## 5.4.1 Command Examples

The following command displays the service registration status and type and how many days remain before the service expires.

```
Router# configure terminal
Router(config)# show service-register status all
Service                Status      Type                Count  Expiration
=====
Extension User        Licensed   standard            299   n/a
External-AP-Control   Licensed   standard             9     n/a
```

## 5.5 Country Code

The following table displays the number for each country.

**Table 11** Country Codes

COUNTRY CODE	COUNTRY NAME	COUNTRY CODE	COUNTRY NAME
001	Afghanistan	002	Albania
003	Algeria	004	American Samoa
005	Andorra	006	Angola
007	Anguilla	008	Antarctica
009	Antigua & Barbuda	010	Argentina
011	Armenia	012	Aruba
013	Ascension Island	014	Australia
015	Austria	016	Azerbaijan
017	Bahamas	018	Bahrain
019	Bangladesh	020	Barbados
021	Belarus	022	Belgium
023	Belize	024	Benin
025	Bermuda	026	Bhutan
027	Bolivia	028	Bosnia and Herzegovina
029	Botswana	030	Bouvet Island
031	Brazil	032	British Indian Ocean Territory
033	Brunei Darussalam	034	Bulgaria
035	Burkina Faso	036	Burundi
037	Cambodia	038	Cameroon
039	Canada	040	Cape Verde
041	Cayman Islands	042	Central African Republic
043	Chad	044	Chile
045	China	046	Christmas Island
047	Cocos (Keeling) Islands	048	Colombia
049	Comoros	050	Congo, Democratic Republic of the

**Table 11** Country Codes (continued)

<b>COUNTRY CODE</b>	<b>COUNTRY NAME</b>	<b>COUNTRY CODE</b>	<b>COUNTRY NAME</b>
051	Congo, Republic of	052	Cook Islands
053	Costa Rica	054	Cote d'Ivoire
055	Croatia/Hrvatska	056	Cyprus
057	Czech Republic	058	Denmark
059	Djibouti	060	Dominica
061	Dominican Republic	062	East Timor
063	Ecuador	064	Egypt
065	El Salvador	066	Equatorial Guinea
067	Eritrea	068	Estonia
069	Ethiopia	070	Falkland Islands (Malvina)
071	Faroe Islands	072	Fiji
073	Finland	074	France
075	France (Metropolitan)	076	French Guiana
077	French Polynesia	078	French Southern Territories
079	Gabon	080	Gambia
081	Georgia	082	Germany
083	Ghana	084	Gibraltar
085	Great Britain	086	Greece
087	Greenland	088	Grenada
089	Guadeloupe	090	Guam
091	Guatemala	092	Guernsey
093	Guinea	094	Guinea-Bissau
095	Guyana	096	Haiti
097	Heard and McDonald Islands	098	Holy See (City Vatican State)
099	Honduras	100	Hong Kong
101	Hungary	102	Iceland
103	India	104	Indonesia
105	Ireland	106	Isle of Man
107	Italy	108	Jamaica
109	Japan	110	Jersey
111	Jordan	112	Kazakhstan
113	Kenya	114	Kiribati
115	Korea, Republic of	116	Kuwait
117	Kyrgyzstan	118	Lao People's Democratic Republic
119	Latvia	120	Lebanon
121	Lesotho	122	Liberia
123	Liechtenstein	124	Lithuania
125	Luxembourg	126	Macau
127	Macedonia, Former Yugoslav Republic	128	Madagascar
129	Malawi	130	Malaysia

**Table 11** Country Codes (continued)

<b>COUNTRY CODE</b>	<b>COUNTRY NAME</b>	<b>COUNTRY CODE</b>	<b>COUNTRY NAME</b>
131	Maldives	132	Mali
133	Malta	134	Marshall Islands
135	Martinique	136	Mauritania
137	Mauritius	138	Mayotte
139	Mexico	140	Micronesia, Federal State of
141	Moldova, Republic of	142	Monaco
143	Mongolia	144	Montserrat
145	Morocco	146	Mozambique
147	Namibia	148	Nauru
149	Nepal	150	Netherlands
151	Netherlands Antilles	152	New Caledonia
153	New Zealand	154	Nicaragua
155	Niger	156	Nigeria
157	Niue	158	Norfolk Island
159	Northern Mariana Islands	160	Norway
161	Not Determined	162	Oman
163	Pakistan	164	Palau
165	Panama	166	Papua New Guinea
167	Paraguay	168	Peru
169	Philippines	170	Pitcairn Island
171	Poland	172	Portugal
173	Puerto Rico	174	Qatar
175	Reunion Island	176	Romania
177	Russian Federation	178	Rwanda
179	Saint Kitts and Nevis	180	Saint Lucia
181	Saint Vincent and the Grenadines	182	San Marino
183	Sao Tome and Principe	184	Saudi Arabia
185	Senegal	186	Seychelles
187	Sierra Leone	188	Singapore
189	Slovak Republic	190	Slovenia
191	Solomon Islands	192	Somalia
193	South Africa	194	South Georgia and the South Sandwich Islands
185	Spain	196	Sri Lanka
197	St Pierre and Miquelon	198	St. Helena
199	Suriname	200	Svalbard and Jan Mayen Islands
201	Swaziland	202	Sweden
203	Switzerland	204	Taiwan
205	Tajikistan	206	Tanzania
207	Thailand	208	Togo
209	Tokelau	210	Tonga

**Table 11** Country Codes (continued)

<b>COUNTRY CODE</b>	<b>COUNTRY NAME</b>	<b>COUNTRY CODE</b>	<b>COUNTRY NAME</b>
211	Trinidad and Tobago	212	Tunisia
213	Turkey	214	Turkmenistan
215	Turks and Caicos Islands	216	Tuvalu
217	US Minor Outlying Islands	218	Uganda
219	Ukraine	220	United Arab Emirates
221	United Kingdom	222	United States
223	Uruguay	224	Uzbekistan
225	Vanuatu	226	Venezuela
227	Vietnam	228	Virgin Islands (British)
229	Virgin Islands (USA)	230	Wallis And Futuna Islands
231	Western Sahara	232	Western Samoa
233	Yemen	234	Yugoslavia
235	Zambia	236	Zimbabwe

# AP Management

This chapter shows you how to configure wireless AP management options on your UAG.

## 6.1 AP Management Overview

The UAG allows you to remotely manage all of the Access Points (APs) on your network. You can manage a number of APs without having to configure them individually as the UAG automatically handles basic configuration for you.

The commands in this chapter allow you to add, delete, and edit the APs managed by the UAG by means of the CAPWAP protocol. An AP must be moved from the wait list to the management list before you can manage it. If you do not want to use this registration mechanism, you can disable it and then any newly connected AP is registered automatically.

## 6.2 AP Management Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 12** Input Values for General AP Management Commands

LABEL	DESCRIPTION
<i>ap_mac</i>	The Ethernet MAC address of the managed AP. Enter 6 hexadecimal pairs separated by colons. You can use 0-9, a-z and A-Z.
<i>ap_model</i>	The model name of the managed AP, such as NWA5160N, NWA5560-N, NWA5550-N, NWA5121-NI or NWA5123-NI.
<i>slot_name</i>	The slot name for the AP's on-board wireless LAN card. Use either <i>slot1</i> or <i>slot2</i> . (The NWA5560-N supports up to 2 radio slots.)
<i>profile_name</i>	The wireless LAN radio profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>ap_description</i>	The AP description. This is strictly used for reference purposes and has no effect on any other settings. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>sta_mac</i>	The MAC address of the wireless client. Enter 6 hexadecimal pairs separated by colons. You can use 0-9, a-z and A-Z.

The following table describes the commands available for AP management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 13** Command Summary: AP Management

COMMAND	DESCRIPTION
<code>capwap ap add ap_mac [ap_model]</code>	Adds the specified AP to the UAG for management. If manual add is disabled, this command can still be used; if you add an AP before it connects to the network, then this command simply preconfigures the management list with that AP's information.
<code>capwap ap fallback disable</code>	Sets the managed AP(s) to not change back to associate with the primary AP controller when the primary AP controller is available.
<code>capwap ap fallback enable</code>	Sets the managed AP(s) to change back to associate with the primary AP controller as soon as the primary AP controller is available.
<code>capwap ap fallback interval &lt;30..86400&gt;</code>	Sets how often (in seconds) the managed AP(s) check whether the primary AP controller is available.
<code>capwap ap kick {all   ap_mac}</code>	Removes the specified AP ( <i>ap_mac</i> ) or all connected APs ( <i>all</i> ) from the management list. Doing this removes the AP(s) from the management list.  If the UAG is set to automatically add new APs to the AP management list, then any kicked APs are added back to the management list as soon as they reconnect.
<code>capwap ap reboot ap_mac</code>	Forces the specified AP ( <i>ap_mac</i> ) to restart. Doing this severs the connections of all associated stations.
<code>capwap ap ap_mac</code>	Enters the sub-command mode for the specified AP.
<code>slot_name ap-profile profile_name</code>	Sets the radio ( <i>slot_name</i> ) to AP mode and assigns a created profile to the radio.
<code>no slot_name ap-profile</code>	Removes the AP mode profile assignment for the specified radio ( <i>slot_name</i> ).
<code>slot_name monitor-profile profile_name</code>	Sets the specified radio ( <i>slot_name</i> ) to monitor mode and assigns a created profile to the radio. Monitor mode APs act as wireless monitors, which can detect rogue APs and help you in building a list of friendly ones. See also <a href="#">Section 7.3 on page 64</a> .
<code>no slot_name monitor-profile</code>	Removes the monitor mode profile assignment for the specified radio ( <i>slot_name</i> ).
<code>description ap_description</code>	Sets the description for the specified AP.
<code>[no] force vlan</code>	Sets whether or not the UAG changes the AP's management VLAN to match the one you configure using the <code>vlan</code> sub-command. The management VLAN on the UAG and AP must match for the UAG to manage the AP.
<code>vlan &lt;1..4094&gt; {tag   untag}</code>	Sets the VLAN ID for the specified AP as well as whether packets sent to and from that ID are tagged or untagged.
<code>exit</code>	Exits the sub-command mode for the specified AP.
<code>capwap manual-add {enable   disable}</code>	Allows the UAG to either automatically add new APs to the network ( <i>disable</i> ) or wait until you manually confirm them ( <i>enable</i> ).
<code>capwap show statistic</code>	Displays statistics about the wireless radio transmitters in each of the APs connected to the UAG.
<code>capwap station kick sta_mac</code>	Forcibly disconnects the specified station from the network.
<code>lan-provision ap ap_mac</code>	Enters the sub-command mode for the specified AP.



**Table 13** Command Summary: AP Management (continued)

COMMAND	DESCRIPTION
<code>lan_port {activate   inactivate} pvid &lt;1..4094&gt;</code>	Enables or disables the specified LAN port on the AP and configures a PVID (Port VLAN ID) for this port.  <i>lan_port</i> : the name of the AP's LAN port (lan1 for example).
<code>vlan_interface {activate   inactivate} vid &lt;1..4094&gt; join lan_port {tag   untag} [lan_port {tag   untag}] [lan_port {tag   untag}]</code>	Creates a new VLAN or configures an existing VLAN. You can disable or enable the VLAN, set the VLAN ID, assign up to three ports to this VLAN as members and set whether the port is to tag outgoing traffic with the VLAN ID.  <i>vlan_interface</i> : the name of the VLAN (vlan1 for example).
<code>[no] vlan_interface</code>	Removes the specified VLAN.
<code>show capwap ap fallback</code>	Displays whether the managed AP(s) will change back to associate with the primary AP controller when the primary AP controller is available.
<code>show capwap ap fallback interval</code>	Displays the interval for how often the managed AP(s) check whether the primary AP controller is available.
<code>show capwap ap wait-list</code>	Displays a list of connected but as-of-yet unmanaged APs. This is known as the 'wait list'.
<code>show capwap ap ap_mac slot_name detail</code>	Displays details for the specified radio ( <i>slot_name</i> ) on the specified AP ( <i>ap_mac</i> ).
<code>show capwap ap {all   ap_mac}</code>	Displays the management list ( <i>all</i> ) or whether the specified AP is on the management list ( <i>ap_mac</i> ).
<code>show capwap ap {all   ap_mac} config status</code>	Displays whether or not any AP's configuration or the specified AP's configuration is in conflict with the UAG's settings for the AP and displays the settings in conflict if there are any.
<code>show capwap ap all statistics</code>	Displays radio statistics for all APs on the management list.
<code>show capwap manual-add</code>	Displays the current manual add option.
<code>show capwap station all</code>	Displays information for all stations connected to the APs on the management list.
<code>show lan-provision ap ap_mac interface {lan_port   vlan_interface   all  ethernet   uplink   vlan}</code>	Displays the port and/or VLAN settings for the specified AP.  You can also set to display settings for a specified port, a specified VLAN, all physical Ethernet ports, the uplink port or all VLANs on the AP.

## 6.2.1 AP Management Commands Example

The following example shows you how to add an AP to the management list, and then edit it.

```
Router# show capwap ap wait-list
index: 1
  IP: 192.168.1.35, MAC: 00:11:11:11:11:FE
  Model: NWA5160N, Description: AP-00:11:11:11:11:FE
index: 2
  IP: 192.168.1.36, MAC: 00:19:CB:00:BB:03
  Model: NWA5160N, Description: AP-00:19:CB:00:BB:03
Router# configure terminal
Router(config)# capwap ap add 00:19:CB:00:BB:03
Router(config)# capwap ap 00:19:CB:00:BB:03
Router(AP 00:19:CB:00:BB:03)# slot1 ap-profile approf01
Router(AP 00:19:CB:00:BB:03)# exit
Router(config)# show capwap ap all
index: 1
  Status: RUN
  IP: 192.168.1.37, MAC: 40:4A:03:05:82:1E
  Description: AP-404A0305821E
  Model: NWA5160N
  R1 mode: AP, R1Prof: default
  R2 mode: AP, R2Prof: n/a
  Station: 0, RadioNum: 2
  Mgnt. VLAN ID: 1, Tag: no
  WTP VLAN ID: 1, WTP Tag: no
  Force VLAN: disable
  Firmware Version: 2.25(AAS.0)b2
  Recent On-line Time: 08:43:04 2013/05/24
  Last Off-line Time: N/A

Router(config)# show capwap ap 40:4A:03:05:82:1E slot1 detail
index: 1
  SSID: ZyXEL, BSSID: 40:4A:03:05:82:1F
  SecMode: NONE, Forward Mode: Local Bridge, Vlan: 1

Router(config)# show capwap ap all statistics
index: 1
  Status: RUN, Loading: -
  AP MAC: 40:4A:03:05:82:1E
  Radio: 1, OP Mode: AP
  Profile: default, MAC: 40:4A:03:05:82:1F
  Description: AP-404A0305821E
  Model: NWA5160N
  Band: 2.4GHz, Channel: 6
  Station: 0
  RxPkt: 4463, TxPkt: 38848
  RxFCS: 1083323, TxRetry: 198478
```

# Wireless LAN Profiles

This chapter shows you how to configure wireless LAN profiles on your UAG.

## 7.1 Wireless LAN Profiles Overview

The managed Access Points designed to work explicitly with your UAG do not have on-board configuration files, you must create “profiles” to manage them. Profiles are preset configurations that are uploaded to the APs and which manage them. They include: Radio and Monitor profiles, SSID profiles, Security profiles, and MAC Filter profiles. Altogether, these profiles give you absolute control over your wireless network.

## 7.2 AP Radio Profile Commands

The radio profile commands allow you to set up configurations for the radios onboard your various APs.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 14** Input Values for General Radio Profile Commands

LABEL	DESCRIPTION
<i>radio_profile_name</i>	The radio profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>wlan_role</i>	Sets the wireless LAN radio operating mode. At the time of writing, you can use <i>ap</i> for Access Point.
<i>wireless_channel_2g</i>	Sets the 2 GHz channel used by this radio profile. The channel range is 1 - 14.  <b>Note:</b> Your choice of channel may be restricted by regional regulations.
<i>wireless_channel_5g</i>	Sets the 5 GHz channel used by this radio profile. The channel range is 36 - 165.  <b>Note:</b> Your choice of channel may be restricted by regional regulations.
<i>wlan_hctw</i>	Sets the HT channel width. Select either <i>auto</i> or <i>20m</i> .
<i>wlan_htgi</i>	Sets the HT guard interval. Select either <i>long</i> or <i>short</i> .
<i>wlan_2g_basic_speed</i>	Sets the basic band rate for 2.4 GHz. The available band rates are 1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0.
<i>wlan_2g_support_speed</i>	Sets the support rate for the 2.4 GHz band. The available band rates are: 1.0, 2.0, 5.5, 11.0, 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0.

**Table 14** Input Values for General Radio Profile Commands (continued)

LABEL	DESCRIPTION
<code>wlan_mcs_speed</code>	Sets the HT MCS rate. The available rates are: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15.
<code>wlan_5g_basic_speed</code>	Sets the basic band rate for 5 GHz. The available band rates are: 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0.
<code>wlan_5g_support_speed</code>	Sets the support rate for the 5 GHz band. The available band rates are: 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0.
<code>chain_mask</code>	Sets the network traffic chain mask. The range is 1 - 7.
<code>wlan_power</code>	Sets the radio output power. Select 100%, 50%, 25%, or 12.5%.
<code>wlan_interface_index</code>	Sets the radio interface index number. The range is 1 - 8.
<code>ssid_profile</code>	Sets the associated SSID profile name. This name must be an existing SSID profile. You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for radio profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 15** Command Summary: Radio Profile

COMMAND	DESCRIPTION
<code>show wlan-radio-profile {all   radio_profile_name}</code>	Displays the radio profile(s).  <i>all</i> : Displays all profiles for the selected operating mode.  <i>radio_profile_name</i> : Displays the specified profile for the selected operating mode.
<code>wlan-radio-profile rename radio_profile_name1 radio_profile_name2</code>	Gives an existing radio profile ( <i>radio_profile_name1</i> ) a new name ( <i>radio_profile_name2</i> ).
<code>[no] wlan-radio-profile radio_profile_name</code>	Enters configuration mode for the specified radio profile. Use the <code>no</code> parameter to remove the specified profile.
<code>[no] activate</code>	Makes this profile active or inactive.
<code>role ap</code>	Sets the operating mode of the radio in this profile.
<code>rsssi-dbm &lt;-20~-76&gt;</code>	When using the RSSI threshold, set a minimum client signal strength for connecting to the AP. -20 dBm is the strongest signal you can require and -76 is the weakest.
<code>[no] rsssi-thres</code>	Sets whether or not to use the Received Signal Strength Indication (RSSI) threshold to ensure wireless clients receive good throughput. This allows only wireless clients with a strong signal to connect to the AP.
<code>band {2.4G   5G} [band-mode {11n   bg   a}]</code>	Sets the radio band (2.4 GHz or 5 GHz) and band mode for this profile. Band mode details:  For 2.4 GHz, <i>11n</i> lets IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n clients associate with the AP.  For 2.4 GHz, <i>bg</i> lets IEEE 802.11b and IEEE 802.11g clients associate with the AP.  For 5 GHz, <i>11n</i> lets IEEE 802.11a and IEEE 802.11n clients associate with the AP.  For 5 GHz, <i>a</i> lets only IEEE 802.11a clients associate with the AP.
<code>[no] disable-dfs-switch</code>	Makes the DFS switch active or inactive. By default this is inactive.

**Table 15** Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
[no] dot11n-disable-coexistence	Fixes the channel bandwidth as 40 MHz. The <code>no</code> command has the AP automatically choose 40 MHz if all the clients support it or 20 MHz if some clients only support 20 MHz.
[no] ctsrts <0..2347>	<p>Sets or removes the RTS/CTS value for this profile.</p> <p>Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).</p> <p>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off.</p> <p>The default is 2347.</p>
[no] frag <256..2346>	<p>Sets or removes the fragmentation value for this profile.</p> <p>The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.</p> <p>The default is 2346.</p>
dtim-period <1..255>	<p>Sets the DTIM period for this profile.</p> <p>Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Active Power Management mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 255.</p> <p>The default is 1.</p>
beacon-interval <40..1000>	<p>Sets the beacon interval for this profile.</p> <p>When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low-power mode before waking up to handle the beacon. This value can be set from 40ms to 1000ms. A high value helps save current consumption of the access point.</p> <p>The default is 100.</p>
[no] ampdu	<p>Activates MPDU frame aggregation for this profile. Use the <code>no</code> parameter to disable it.</p> <p>Message Protocol Data Unit (MPDU) aggregation collects Ethernet frames along with their 802.11n headers and wraps them in a 802.11n MAC header. This method is useful for increasing bandwidth throughput in environments that are prone to high error rates.</p> <p>By default this is enabled.</p>
limit-ampdu <100..65535>	<p>Sets the maximum frame size to be aggregated.</p> <p>By default this is 50000.</p>
subframe-ampdu <2..64>	<p>Sets the maximum number of frames to be aggregated each time.</p> <p>By default this is 32.</p>

**Table 15** Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
[no] amsdu	<p>Activates MPDU frame aggregation for this profile. Use the <i>no</i> parameter to disable it.</p> <p>Mac Service Data Unit (MSDU) aggregation collects Ethernet frames without any of their 802.11n headers and wraps the header-less payload in a single 802.11n MAC header. This method is useful for increasing bandwidth throughput. It is also more efficient than A-MPDU except in environments that are prone to high error rates.</p> <p>By default this is enabled.</p>
limit-amsdu <2290..4096>	<p>Sets the maximum frame size to be aggregated.</p> <p>The default is 4096.</p>
[no] multicast-to-unicast	<p>“Multicast to unicast” broadcasts wireless multicast traffic to all wireless clients as unicast traffic to provide more reliable transmission. The data rate changes dynamically based on the application’s bandwidth requirements. Although unicast provides more reliable transmission of the multicast traffic, it also produces duplicate packets.</p> <p>The <i>no</i> command turns multicast to unicast off to send wireless multicast traffic at the rate you specify with the <i>2g-multicast-speed</i> or <i>5g-multicast-speed</i> command.</p>
[no] block-ack	Makes <i>block-ack</i> active or inactive. Use the <i>no</i> parameter to disable it.
ch-width <i>wlan_htcw</i>	Sets the channel width for this profile.
guard-interval <i>wlan_htgi</i>	<p>Sets the guard interval for this profile.</p> <p>The default for this is <i>short</i>.</p>
2g-basic-speed <i>wlan_2g_basic_speed</i>	<p>Sets the 2.4 GHz basic band rates.</p> <p>The default is 1.0 2.0 5.5 11.0.</p>
2g-channel <i>wireless_channel_2g</i>	Sets the broadcast band for this profile in the 2.4 GHz frequency range. The default is 6.
2g-mcs-speed {disable   <i>wlan_mcs_speed</i> }	<p>Disables or sets the 2.4 GHz HT MCS rate.</p> <p>The default is 0~15.</p>
2g-multicast-speed <i>wlan_2g_support_speed</i>	When you disable multicast to unicast, use this command to set the data rate { 1.0   2.0   ... } in Mbps for 2.4 GHz multicast traffic.
2g-support-speed {disable   <i>wlan_2g_support_speed</i> }	<p>Disables or sets the 2.4 GHz support rate.</p> <p>The default is 1.0~54.0.</p>
5g-basic-speed <i>wlan_5g_basic_speed</i>	<p>Sets the 5 GHz basic band rate.</p> <p>The default is 6.0 12.0 24.0.</p>
5g-channel <i>wireless_channel_5g</i>	Sets the broadcast band for this profile in the 5 GHz frequency range. The default is 36.
5g-mcs-speed {disable   <i>wlan_mcs_speed</i> }	<p>Disables or sets the 5 GHz HT MCS rate.</p> <p>The default is 0~15.</p>
5g-multicast-speed { <i>wlan_5g_basic_speed</i> }	When you disable multicast to unicast, use this command to set the data rate { 6.0   9.0   ... } in Mbps for 5 GHz multicast traffic.

**Table 15** Command Summary: Radio Profile (continued)

COMMAND	DESCRIPTION
<code>5g-support-speed {disable   wlan_5g_support_speed}</code>	Disables or sets the 5 GHz support rate. The default is 6.0~54.0.
<code>[no] htprotection</code>	Activates HT protection for this profile. Use the <code>no</code> parameter to disable it. By default, this is disabled.
<code>output-power wlan_power</code>	Sets the output power for the radio in this profile. The default is 100%.
<code>[no] ssid-profile wlan_interface_index ssid_profile</code>	Assigns an SSID profile to this radio profile. Requires an existing SSID profile. Use the <code>no</code> parameter to disable it.
<code>schedule profile</code>	Specifies a schedule to control when the WLAN of the managed AP (to which this radio profile is applied) is turned on.
<code>no schedule</code>	Disables the WLAN schedule and the managed AP's WLAN is always turned on if the profile is enabled.
<code>tx-mask chain_mask</code>	Sets the outgoing chain mask rate.
<code>rx-mask chain_mask</code>	Sets the incoming chain mask rate.
<code>exit</code>	Exits configuration mode for this profile.

## 7.2.1 AP Profile Commands Example

The following example shows you how to set up the radio profile named 'RADIO01', activate it, and configure it to use the following settings:

- 2.4G band with channel 6
- channel width of 20MHz
- a DTIM period of 2
- a beacon interval of 100ms
- AMPDU frame aggregation enabled
- an AMPDU buffer limit of 65535 bytes
- an AMPDU subframe limit of 64 frames
- AMSDU frame aggregation enabled
- an AMSDU buffer limit of 4096
- block acknowledgement enabled
- a short guard interval
- an output power of 100%

It will also assign the SSID profile labeled 'default' in order to create WLAN VAP (wlan-1-1) functionality within the radio profile.

```
Router(config)# wlan-radio-profile RADIO01
Router(config-profile-radio)# activate
Router(config-profile-radio)# band 2.4G
Router(config-profile-radio)# 2g-channel 6
Router(config-profile-radio)# ch-width 20m
Router(config-profile-radio)# dtim-period 2
Router(config-profile-radio)# beacon-interval 100
Router(config-profile-radio)# ampdu
Router(config-profile-radio)# limit-ampdu 65535
Router(config-profile-radio)# subframe-ampdu 64
Router(config-profile-radio)# amsdu
Router(config-profile-radio)# limit-amsdu 4096
Router(config-profile-radio)# block-ack
Router(config-profile-radio)# guard-interval short
Router(config-profile-radio)# tx-mask 5
Router(config-profile-radio)# rx-mask 7
Router(config-profile-radio)# output-power 100%
Router(config-profile-radio)# ssid-profile 1 default
```

## 7.3 AP Monitor Profile Commands

The monitor profile commands allow you to set up monitor mode configurations that allow your APs to scan for other APs in the vicinity.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 16** Input Values for Monitor Profile Commands

LABEL	DESCRIPTION
<i>monitor_profile_name</i>	The monitor profile name. You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<i>wireless_channel_2g</i>	Sets the 2 GHz channel used by the profile. The channel range is 1 - 14.  Note: Your choice of channel may be restricted by regional regulations.
<i>wireless_channel_5g</i>	Sets the 5 GHz channel used by the profile. The channel range is 36 - 165.  Note: Your choice of channel may be restricted by regional regulations.

The following table describes the commands available for monitor profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 17** Command Summary: Monitor Profile

COMMAND	DESCRIPTION
<code>show wlan-monitor-profile {all   <i>monitor_profile_name</i>}</code>	Displays all monitor profiles or just the specified one.
<code>wlan-monitor-profile rename <i>monitor_profile_name1</i> <i>monitor_profile_name2</i></code>	Gives an existing monitor profile ( <i>monitor_profile_name1</i> ) a new name ( <i>monitor_profile_name2</i> ).



**Table 17** Command Summary: Monitor Profile (continued)

COMMAND	DESCRIPTION
[no] wlan-monitor-profile <i>monitor_profile_name</i>	Enters configuration mode for the specified monitor profile. Use the <i>no</i> parameter to remove the specified profile.
[no] activate	Makes this profile active or inactive. By default, this is enabled.
description <i>description</i>	Sets the description for the profile. You may use up to 60 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive
[no] 2g-scan-channel <i>wireless_channel_2g</i>	Sets the broadcast band for this profile in the 2.4 Ghz frequency range. Use the <i>no</i> parameter to disable it.
[no] 5g-scan-channel <i>wireless_channel_5g</i>	Sets the broadcast band for this profile in the 5 GHz frequency range. Use the <i>no</i> parameter to disable it.
scan-method <i>scan_method</i>	Sets the channel scanning method for this profile.
scan-dwell <100..1000>	Sets the duration in milliseconds that the device using this profile scans each channel.
exit	Exits configuration mode for this profile.

## 7.4 SSID Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 18** Input Values for General SSID Profile Commands

LABEL	DESCRIPTION
<i>ssid_profile_name</i>	The SSID profile name. You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>ssid</i>	The SSID broadcast name. You may use 1-32 alphanumeric characters, underscores (_), or dashes (-). This value is case-sensitive.
<i>wlan_qos</i>	Sets the type of QoS the SSID should use.  <i>disable</i> : Turns off QoS for this SSID.  <i>wmm</i> : Turns on QoS for this SSID. It automatically assigns Access Categories to packets as the device inspects them in transit.  <i>wmm_be</i> : Assigns the "best effort" Access Category to all traffic moving through the SSID regardless of origin.  <i>wmm_bk</i> : Assigns the "background" Access Category to all traffic moving through the SSID regardless of origin.  <i>wmm_vi</i> : Assigns the "video" Access Category to all traffic moving through the SSID regardless of origin.  <i>wmm_vo</i> : Assigns the "voice" Access Category to all traffic moving through the SSID regardless of origin.
<i>vlan_iface</i>	The VLAN interface name of the controller (in this case, it is NXC5200). The maximum VLAN interface number is product-specific; for the UAG, the number is 512.

**Table 18** Input Values for General SSID Profile Commands (continued)

LABEL	DESCRIPTION
<i>securityprofile</i>	Assigns an existing security profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<i>macfilterprofile</i>	Assigns an existing MAC filter profile to the SSID profile. You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<i>description2</i>	Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ). This value is case-sensitive.

The following table describes the commands available for SSID profile management. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 19** Command Summary: SSID Profile

COMMAND	DESCRIPTION
<code>show wlan-ssid-profile {all / ssid_profile_name}</code>	Displays the SSID profile(s).  <i>all</i> : Displays all profiles for the selected operating mode.  <i>ssid_profile_name</i> : Displays the specified profile for the selected operating mode.
<code>wlan-ssid-profile rename ssid_profile_name1 ssid_profile_name2</code>	Gives an existing SSID profile ( <i>ssid_profile_name1</i> ) a new name ( <i>ssid_profile_name2</i> ).
<code>[no] wlan-ssid-profile ssid_profile_name</code>	Enters configuration mode for the specified SSID profile. Use the <i>no</i> parameter to remove the specified profile.
<code>bandselect check-sta-interval &lt;1..60000&gt;</code>	Sets how often (in seconds) the AP checks and deletes old wireless client data.
<code>bandselect drop-authentication &lt;1..16&gt;</code>	Sets how many authentication request from a client to a 2.4GHz Wi-Fi network is ignored during the specified timeout period.
<code>bandselect drop-probe-request &lt;1..32&gt;</code>	Sets how many prob request from a client to a 2.4GHz Wi-Fi network is ignored during the specified timeout period.
<code>bandselect min-sort-interval &lt;1..60000&gt;</code>	Sets the minimum interval (in seconds) at which the AP sorts the wireless client data when the client queue is full.
<code>bandselect mode {disable   force   standard}</code>	To improve network performance and avoid interference in the 2.4 GHz frequency band, you can enable this feature to use the 5 GHz band first. You should set 2.4GHz and 5 GHz radio profiles to use the same SSID and security settings.  <b>Note:</b> The managed APs must be dual-band capable.  <i>disable</i> : to turn off this feature.  <i>force</i> : to have the wireless clients always connect to an SSID using the 5 GHz band. Connections to an SSID using the 2.4GHz band are not allowed. It is recommended you select this option when the AP and wireless clients can function in either frequency band.  <i>standard</i> : to have the AP try to connect the wireless clients to the same SSID using the 5 GHz band. Connections to an SSID using the 2.4GHz band are still allowed.
<code>bandselect time-out-period &lt;1..256&gt;</code>	Sets the timeout period (in seconds) within which the AP drops the specified number of prob or authentication requests to a 2.4GHz Wi-Fi network.

**Table 19** Command Summary: SSID Profile (continued)

COMMAND	DESCRIPTION
[no] block-intra	Enables intra-BSSID traffic blocking. Use the <code>no</code> parameter to disable it in this profile.  By default this is disabled.
downlink-rate-limit <i>data_rate</i>	Sets the maximum incoming transmission data rate (either in mbps or kbps) on a per-station basis.
[no] hide	Prevents the SSID from being publicly broadcast. Use the <code>no</code> parameter to re-enable public broadcast of the SSID in this profile.  By default this is disabled.
[no] macfilter <i>macfilterprofile</i>	Assigns the specified MAC filtering profile to this SSID profile. Use the <code>no</code> parameter to remove it.  By default, no MAC filter is assigned.
qos <i>wlan_qos</i>	Sets the type of QoS used by this SSID.
security <i>securityprofile</i>	Assigns the specified security profile to this SSID profile.
ssid	Sets the SSID. This is the name visible on the network to wireless clients. Enter up to 32 characters, spaces and underscores are allowed.  The default SSID is 'ZyXEL'.
uplink-rate-limit <i>data_rate</i>	Sets the maximum outgoing transmission data rate (either in mbps or kbps) on a per-station basis.
vlan-id <1..4094>	Applies to each SSID profile that uses <code>localbridge</code> . If the VLAN ID is equal to the AP's native VLAN ID then traffic originating from the SSID is not tagged.  The default VLAN ID is 1.
[no] vlan-support	Sets the UAG to tag traffic from the local Virtual AP (VAP) with the VLAN ID specified in this SSID profile.  The <code>no</code> command sets the UAG to not tag traffic from the local Virtual AP (VAP) with the VLAN ID.
exit	Exits configuration mode for this profile.

## 7.4.1 SSID Profile Example

The following example creates an SSID profile with the name 'ZyXEL'. It makes the assumption that both the security profile (SECURITY01) and the MAC filter profile (MACFILTER01) already exist.

```
Router(config)# wlan-ssid-profile SSID01
Router(config-ssid-radio)# ssid ZyXEL
Router(config-ssid-radio)# qos wmm
Router(config-ssid-radio)# data-forward localbridge
Router(config-ssid-radio)# security SECURITY01
Router(config-ssid-radio)# macfilter MACFILTER01
Router(config-ssid-radio)# exit
Router(config)#
```

## 7.5 Security Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 20** Input Values for General Security Profile Commands

LABEL	DESCRIPTION
<i>security_profile_name</i>	The security profile name. You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<i>wep_key</i>	Sets the WEP key encryption strength. Select either <i>64bit</i> or <i>128bit</i> .
<i>wpa_key</i>	Sets the WPA/WPA2 pre-shared key in ASCII. You may use 8~63 alphanumeric characters. This value is case-sensitive.
<i>wpa_key_64</i>	Sets the WPA/WPA2 pre-shared key in HEX. You must use 64 alphanumeric characters.
<i>secret</i>	Sets the shared secret used by your network's RADIUS server.
<i>auth_method</i>	The authentication method used by the security profile.

The following table describes the commands available for security profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 21** Command Summary: Security Profile

COMMAND	DESCRIPTION
<code>show wlan-security-profile {all   security_profile_name}</code>	Displays the security profile(s).  <i>all</i> : Displays all profiles for the selected operating mode.  <i>security_profile_name</i> : Displays the specified profile for the selected operating mode.
<code>wlan-security-profile rename security_profile_name1 security_profile_name2</code>	Gives existing security profile ( <i>security_profile_name1</i> ) a new name, ( <i>security_profile_name2</i> ).
<code>[no] wlan-security-profile security_profile_name</code>	Enters configuration mode for the specified security profile. Use the <i>no</i> parameter to remove the specified profile.
<code>mode {none   wep   wpa   wpa2   wpa2-mix}</code>	Sets the security mode for this profile.
<code>wep &lt;64   128&gt; default-key &lt;1..4&gt;</code>	Sets the WEP encryption strength ( <i>64</i> or <i>128</i> ) and the default key value ( <i>1 ~ 4</i> ).  If you select WEP-64 enter 10 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x11AA22BB33) for each Key used; or enter 5 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey) for each Key used.  If you select WEP-128 enter 26 hexadecimal digits in the range of "A-F", "a-f" and "0-9" (for example, 0x00112233445566778899AABBCC) for each Key used; or enter 13 ASCII characters (case sensitive) ranging from "a-z", "A-Z" and "0-9" (for example, MyKey12345678) for each Key used.  You can save up to four different keys. Enter the <i>default-key</i> ( <i>1 ~ 4</i> ) to save your WEP to one of those four available slots.
<code>wep-auth-type {open   share}</code>	Sets the authentication key type to either <i>open</i> or <i>share</i> .

**Table 21** Command Summary: Security Profile (continued)

COMMAND	DESCRIPTION
wpa-encrypt {tkip   aes   auto}	Sets the WPA/WPA2 encryption cipher type.  auto: This automatically chooses the best available cipher based on the cipher in use by the wireless client that is attempting to make a connection.  tkip: This is the Temporal Key Integrity Protocol encryption method added later to the WEP encryption protocol to further secure. Not all wireless clients may support this.  aes: This is the Advanced Encryption Standard encryption method, a newer more robust algorithm than TKIP Not all wireless clients may support this.
wpa-psk {wpa_key   wpa_key_64}	Sets the WPA/WPA2 pre-shared key.
[no] wpa2-preauth	Enables pre-authentication to allow wireless clients to switch APs without having to re-authenticate their network connection. The RADIUS server puts a temporary PMK Security Authorization cache on the wireless clients. It contains their session ID and a pre-authorized list of viable APs.  Use the no parameter to disable this.
[no] reauth <30..30000>	Sets the interval (in seconds) between authentication requests.  The default is 0.
idle <30..30000>	Sets the idle interval (in seconds) that a client can be idle before authentication is discontinued.  The default is 300.
group-key <30..30000>	Sets the interval (in seconds) at which the AP updates the group WPA/WPA2 encryption key.  The default is 1800.
[no] dot1x-eap	Enables 802.1x secure authentication. Use the no parameter to disable it.
eap {external   internal auth_method}	Sets the 802.1x authentication method.
[no] server-auth <1..2> activate	Activates server authentication. Use the no parameter to deactivate.
server-auth <1..2> ip address ipv4_address port <1..65535> secret secret	Sets the IPv4 address, port number and shared secret of the RADIUS server to be used for authentication.
[no] server-auth <1..2>	Clears the server authentication setting.
exit	Exits configuration mode for this profile.

## 7.5.1 Security Profile Example

The following example creates a security profile with the name 'SECURITY01'.

```
Router(config)# wlan-security-profile SECURITY01
Router(config-security-profile)# mode wpa2
Router(config-security-profile)# wpa-encrypt aes
Router(config-security-profile)# wpa-psk 12345678
Router(config-security-profile)# idle 3600
Router(config-security-profile)# reauth 1800
Router(config-security-profile)# group-key 1800
Router(config-security-profile)# exit
Router(config)#
```

## 7.6 MAC Filter Profile Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 22** Input Values for General MAC Filter Profile Commands

LABEL	DESCRIPTION
<i>macfilter_profile_name</i>	The MAC filter profile name. You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<i>description2</i>	Sets the description of the profile. You may use up to 60 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ). This value is case-sensitive.

The following table describes the commands available for security profile management. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 23** Command Summary: MAC Filter Profile

COMMAND	DESCRIPTION
<code>show wlan-macfilter-profile {all   <i>macfilter_profile_name</i>}</code>	Displays the security profile(s).  <i>all</i> : Displays all profiles for the selected operating mode.  <i>macfilter_profile_name</i> : Displays the specified profile for the selected operating mode.
<code>wlan-macfilter-profile rename <i>macfilter_profile_name1</i> <i>macfilter_profile_name2</i></code>	Gives an existing security profile ( <i>macfilter_profile_name1</i> ) a new name ( <i>macfilter_profile_name2</i> ).
<code>[no] wlan-macfilter-profile <i>macfilter_profile_name</i></code>	Enters configuration mode for the specified MAC filter profile. Use the <i>no</i> parameter to remove the specified profile.
<code>filter-action {allow   deny}</code>	Permits the wireless client with the MAC addresses in this profile to connect to the network through the associated SSID; select <i>deny</i> to block the wireless clients with the specified MAC addresses.  The default is set to <i>deny</i> .
<code>[no] MAC description <i>description2</i></code>	Sets the description of this profile. Enter up to 60 characters. Spaces and underscores allowed.
<code>exit</code>	Exits configuration mode for this profile.

### 7.6.1 MAC Filter Profile Example

The following example creates a MAC filter profile with the name 'MACFILTER01'.

```
Router(config)# wlan-macfilter-profile MACFILTER01
Router(config-macfilter-profile)# filter-action deny
Router(config-macfilter-profile)# MAC 01:02:03:04:05:06 description MAC01
Router(config-macfilter-profile)# MAC 01:02:03:04:05:07 description MAC02
Router(config-macfilter-profile)# MAC 01:02:03:04:05:08 description MAC03
Router(config-macfilter-profile)# exit
Router(config)#
```

# Rogue AP

This chapter shows you how to set up Rogue Access Point (AP) detection and containment.

## 8.1 Rogue AP Detection Overview

Rogue APs are wireless access points operating in a network's coverage area that are not under the control of the network's administrators, and can potentially open holes in the network security. Attackers can take advantage of a rogue AP's weaker (or non-existent) security to gain illicit access to the network, or set up their own rogue APs in order to capture information from wireless clients.

Conversely, a friendly AP is one that the UAG network administrator regards as non-threatening. This does not necessarily mean the friendly AP must belong to the network managed by the UAG; rather, it is any unmanaged AP within range of the UAG's own wireless network that is allowed to operate without being contained. This can include APs from neighboring companies, for example, or even APs maintained by your company's employees that operate outside of the established network.

## 8.2 Rogue AP Detection Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 24** Input Values for Rogue AP Detection Commands

LABEL	DESCRIPTION
<i>ap_mac</i>	Specifies the MAC address (in XX:XX:XX:XX:XX:XX format) of the AP to be added to either the rogue AP or friendly AP list. The <code>no</code> command removes the entry.
<i>description2</i>	Sets the description of the AP. You may use 1-60 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ). This value is case-sensitive.

The following table describes the commands available for rogue AP detection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 25** Command Summary: Rogue AP Detection

COMMAND	DESCRIPTION
<code>rogue-ap detection</code>	Enters sub-command mode for rogue AP detection.
<code>[no] activate</code>	Activates rogue AP detection. Use the <code>no</code> parameter to deactivate rogue AP detection.

**Table 25** Command Summary: Rogue AP Detection (continued)

COMMAND	DESCRIPTION
<code>rogue-ap ap_mac description2</code>	Sets the device that owns the specified MAC address as a rogue AP. You can also assign a description to this entry on the rogue AP list.
<code>no rogue-ap ap_mac</code>	Removes the device that owns the specified MAC address from the rogue AP list.
<code>friendly-ap ap_mac description2</code>	Sets the device that owns the specified MAC address as a friendly AP. You can also assign a description to this entry on the friendly AP list.
<code>no friendly-ap ap_mac</code>	Removes the device that owns the specified MAC address from the friendly AP list.
<code>monitoring flush</code>	Removes all detected APs from the rogue AP list.
<code>exit</code>	Exits configuration mode for rogue AP detection.
<code>show rogue-ap detection monitoring</code>	Displays a table of detected APs and information about them, such as their MAC addresses, when they were last seen, and their SSIDs, to name a few.
<code>show rogue-ap detection list {rogue   friendly   all}</code>	Displays the specified rogue/friendly/all AP list.
<code>show rogue-ap detection status</code>	Displays whether rogue AP detection is on or off.
<code>show rogue-ap detection info</code>	Displays a summary of the number of detected devices from the following categories: rogue, friendly, ad-hoc, unclassified, and total.

## 8.2.1 Rogue AP Detection Examples

This example sets the device associated with MAC address 00:13:49:11:11:11 as a rogue AP, and the device associated with MAC address 00:13:49:11:11:22 as a friendly AP. It then removes MAC address from the rogue AP list with the assumption that it was misidentified.

```
Router(config)# rogue-ap detection
Router(config-detection)# rogue-ap 00:13:49:11:11:11 rogue
Router(config-detection)# friendly-ap 00:13:49:11:11:22 friendly
Router(config-detection)# no rogue-ap 00:13:49:11:11:11
Router(config-detection)# exit
```

This example displays the rogue AP detection list.

```
Router(config)# show rogue-ap detection list rogue
no.    mac                description
contain
=====
1      00:13:49:18:15:5A                0
```



This example shows the friendly AP detection list.

```
Router(config)# show rogue-ap detection list friendly
no.    mac                description
=====
1      11:11:11:11:11:11      third floor
2      00:13:49:11:22:33
3      00:13:49:00:00:05
4      00:13:49:00:00:01
5      00:0D:0B:CB:39:33      dept1
```

This example shows the combined rogue and friendly AP detection list.

```
Router(config)# show rogue-ap detection list all
no.    role                mac                description
=====
1      friendly-ap          11:11:11:11:11:11  third floor
2      friendly-ap          00:13:49:11:22:33
3      friendly-ap          00:13:49:00:00:05
4      friendly-ap          00:13:49:00:00:01
5      friendly-ap          00:0D:0B:CB:39:33  dept1
6      rogue-ap              00:13:49:18:15:5A
```

This example shows both the status of rogue AP detection and the summary of detected APs.

```
Router(config)# show rogue-ap detection status
rogue-ap detection status: on

Router(config)# show rogue-ap detection info
rogue ap: 1
friendly ap: 4
adhoc: 4
unclassified ap: 0
total devices: 0
```

## 8.3 Rogue AP Containment Overview

These commands enable rogue AP containment. You can use them to isolate a device that is flagged as a rogue AP. They are global in that they apply to all managed APs on the network (all APs utilize the same containment list, but only APs set to monitor mode can actively engage in containment of rogue APs). This means if we add a MAC address of a device to the containment list, then every AP on the network will respect it.

**Note:** Containing a rogue AP means broadcasting unviable login data at it, preventing legitimate wireless clients from connecting to it. This is a kind of Denial of Service attack.

## 8.4 Rogue AP Containment Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 26** Input Values for Rogue AP Containment Commands

LABEL	DESCRIPTION
<i>ap_mac</i>	Specifies the MAC address (in XX:XX:XX:XX:XX:XX format) of the AP to be contained. The <code>no</code> command removes the entry.

The following table describes the commands available for rogue AP containment. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 27** Command Summary: Rogue AP Containment

COMMAND	DESCRIPTION
<code>rogue-ap containment</code>	Enters sub-command mode for rogue AP containment.
<code>[no] activate</code>	Activates rogue AP containment. Use the <code>no</code> parameter to deactivate rogue AP containment.
<code>[no] contain ap_mac</code>	Isolates the device associated with the specified MAC address. Use the <code>no</code> parameter to remove this device from the containment list.
<code>exit</code>	Exits configuration mode for rogue AP containment.
<code>show rogue-ap containment config</code>	Displays whether rogue AP containment is enabled or not.
<code>show rogue-ap containment list</code>	Displays the rogue AP containment list.

### 8.4.1 Rogue AP Containment Example

This example contains the device associated with MAC address 00:13:49:11:11:12 then displays the containment list for confirmation.

```
Router(config)# rogue-ap containment
Router(config-containment)# activate
Router(config-containment)# contain 00:13:49:11:11:12
Router(config-containment)# exit
Router(config)# show rogue-ap containment list
no.    mac
=====
1      00:13:49:11:11:12
```

# Wireless Frame Capture

This chapter shows you how to configure and use wireless frame capture on the UAG.

## 9.1 Wireless Frame Capture Overview

Troubleshooting wireless LAN issues has always been a challenge. Wireless sniffer tools like Ethereal can help capture and decode packets of information, which can then be analyzed for debugging. It works well for local data traffic, but if your devices are spaced increasingly farther away then it often becomes correspondingly difficult to attempt remote debugging. Complicated wireless packet collection is arguably an arduous and perplexing process. The wireless frame capture feature in the UAG can help.

This chapter describes the wireless frame capture commands, which allows a network administrator to capture wireless traffic information and download it to an Ethereal/Tcpdump compatible format packet file for analysis.

## 9.2 Wireless Frame Capture Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 28** Input Values for Wireless Frame Capture Commands

LABEL	DESCRIPTION
<i>ip_address</i>	The IP address of the Access Point (AP) that you want to monitor. Enter a standard IPv4 IP address (for example, 192.168.1.2).
<i>mon_dir_size</i>	The total combined size (in kbytes) of all files to be captured. The maximum you can set is 50 megabytes (52428800 bytes.)
<i>file_name</i>	The file name prefix for each captured file. The default prefix is monitor while the default file name is monitor.dump.  You can use 1-31 alphanumeric characters, underscores or dashes but the first character cannot be a number. This string is case sensitive.

The following table describes the commands available for wireless frame capture. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 29** Command Summary: Wireless Frame Capture

COMMAND	DESCRIPTION
<code>frame-capture configure</code>	Enters sub-command mode for wireless frame capture.
<code>src-ip {add del} {ipv4_address / local}</code>	Sets or removes the IPv4 address of an AP controlled by the UAG that you want to capture wireless network traffic going through the AP interfaces. You can use this command multiple times to add additional IPs to the list.
<code>file-prefix file_name</code>	Sets the file name prefix for each captured file. Enter up to 31 alphanumeric characters. Spaces and underscores are not allowed.
<code>files-size mon_dir_size</code>	Sets the total combined size (in kbytes) of all files to be captured.
<code>exit</code>	Exits configuration mode for wireless frame capture.
<code>[no] frame-capture activate</code>	Starts wireless frame capture. Use the <code>no</code> parameter to turn it off.
<code>show frame-capture status</code>	Displays whether frame capture is running or not.
<code>show frame-capture config</code>	Displays the frame capture configuration.

## 9.2.1 Wireless Frame Capture Examples

This example configures the wireless frame capture parameters for an AP located at IP address 192.168.1.2.

```
Router(config)# frame-capture configure
Router(frame-capture)# src-ip add 192.168.1.2
Router(frame-capture)# file-prefix monitor
Router(frame-capture)# files-size 1000
Router(frame-capture)# exit
Router(config)#
```

This example shows frame capture status and configuration.

```
Router(config)# show frame-capture status
capture status: off

Router(config)# show frame-capture config
capture source: 192.168.1.2
file prefix: monitor
file size: 1000
```

# Dynamic Channel Selection

This chapter shows you how to configure and use dynamic channel selection on the UAG.

## 10.1 DCS Overview

Dynamic Channel Selection (DCS) is a feature that allows an AP to automatically select the radio channel upon which it broadcasts by passively listening to the area around it and determining what channels are currently being broadcast on by other devices.

When numerous APs broadcast within a given area, they introduce the possibility of heightened radio interference, especially if some or all of them are broadcasting on the same radio channel. This can make accessing the network potentially rather difficult for the stations connected to them. If the interference becomes too great, then the network administrator must open his AP configuration options and manually change the channel to one that no other AP is using (or at least a channel that has a lower level of interference) in order to give the connected stations a minimum degree of channel interference.

## 10.2 DCS Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 30** Input Values for DCS Commands

LABEL	DESCRIPTION
<i>interval</i>	Enters the dynamic channel selection interval time. The range is 10 ~ 1440 minutes.

The following table describes the commands available for dynamic channel selection. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 31** Command Summary: DCS

COMMAND	DESCRIPTION
<code>[no] dcs activate</code>	Starts dynamic channel selection. Use the <code>no</code> parameter to turn it off.
<code>dcs 2g-selected-channel 2.4g_channels</code>	Sets the channels that are available in the 2.4 GHz band when you manually configure the channels an AP can use.
<code>dcs 5g-selected-channel 5g_channels</code>	Sets the channels that are available in the 5 GHz band when you manually configure the channels an AP can use.

**Table 31** Command Summary: DCS (continued)

COMMAND	DESCRIPTION
<code>dcx client-aware {enable disable}</code>	When enabled, this ensures that an AP will not change channels as long as a client is connected to it. If disabled, the AP may change channels regardless of whether it has clients connected to it or not.
<code>dcx channel-deployment {3-channel 4-channel}</code>	Sets either a 3-channel deployment or a 4-channel deployment.  In a 3-channel deployment, the AP running the scan alternates between the following channels: 1, 6, and 11.  In a 4-channel deployment, the AP running the scan alternates between the following channels: 1, 4, 7, and 11 (FCC) or 1, 5, 9, and 13 (ETSI).  Sets the option that is applicable to your region. (Channel deployment may be regulated differently between countries and locales.)
<code>dcx dcs-2g-method {auto manual}</code>	Sets the AP to automatically search for available channels or manually configures the channels the AP uses in the 2.4 GHz band.
<code>dcx dcs-5g-method {auto manual}</code>	Sets the AP to automatically search for available channels or manually configures the channels the AP uses in the 5 GHz band.
<code>dcx dfs-aware {enable disable}</code>	Enables this to allow an AP to avoid phase DFS channels below the 5 GHz spectrum.
<code>dcx invoke</code>	Sets the managed APs to scan for and select an available channel immediately.
<code>dcx sensitivity-level {high medium low}</code>	Sets how sensitive DCS is to radio channel changes in the vicinity of the AP running the scan.
<code>dcx time-interval interval</code>	Sets the interval that specifies how often DCS should run.
<code>show dcs config</code>	Displays the current DCS configuration.

## 10.2.1 DCS Examples

This example creates a DCS configuration.

```
Router(config)# dcs time-interval 720
Router(config)# dcs sensitivity-level high
Router(config)# dcs client-aware enable
Router(config)# dcs channel-deployment 3-channel
Router(config)# dcs dfs-aware enable
```

This example displays the DCS configuration created in the previous example.

```
Router(config)# show dcs config
dcs activate: no
dcs time interval: 720
dcs sensitivity level: high
dcs client-aware: enable
dcs 2.4-ghz selection method: auto
dcs 2.4-ghz selected channels: none
dcs 2.4-ghz channel deployment: 3-channel
dcs 5-ghz selection method: auto
dcs 5-ghz selected channels: none
dcs 5-ghz DFS-aware: enable
```

# Wireless Load Balancing

This chapter shows you how to configure wireless load balancing.

## 11.1 Wireless Load Balancing Overview

Wireless load balancing is the process whereby you limit the number of connections allowed on an wireless access point (AP) or you limit the amount of wireless traffic transmitted and received on it. Because there is a hard upper limit on the AP's wireless bandwidth, this can be a crucial function in areas crowded with wireless users. Rather than let every user connect and subsequently dilute the available bandwidth to the point where each connecting device receives a meager trickle, the load balanced AP instead limits the incoming connections as a means to maintain bandwidth integrity.

## 11.2 Wireless Load Balancing Commands

The following table describes the commands available for wireless load balancing. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 32** Command Summary: Load Balancing

COMMAND	DESCRIPTION
<code>[no] load-balancing activate</code>	Enables load balancing. Use the <code>no</code> parameter to disable it.
<code>[no] load-balancing kickout</code>	Enables an overloaded AP to disconnect ("kick") idle clients or clients with noticeably weak connections.
<code>load-balancing alpha &lt;1..255&gt;</code>	<p>Sets the load balancing alpha value.</p> <p>When the AP is balanced, then this setting delays a client's association with it by this number of seconds.</p> <p><b>Note:</b> This parameter has been optimized for the UAG and should not be changed unless you have been specifically directed to do so by ZyXEL support.</p>
<code>load-balancing beta &lt;1..255&gt;</code>	<p>Sets the load balancing beta value.</p> <p>When the AP is overloaded, then this setting delays a client's association with it by this number of seconds.</p> <p><b>Note:</b> This parameter has been optimized for the UAG and should not be changed unless you have been specifically directed to do so by ZyXEL support.</p>

**Table 32** Command Summary: Load Balancing (continued)

COMMAND	DESCRIPTION
load-balancing kickInterval <1..255>	Enables the kickout feature for load balancing and also sets the kickout interval in seconds. While load balancing is enabled, the AP periodically disconnects stations at intervals equal to this setting.  This occurs until the load balancing threshold is no longer exceeded.
load-balancing liInterval <1..255>	Sets the interval in seconds that each AP communicates with the other APs in its range for calculating the load balancing algorithm.  Note: This parameter has been optimized for the UAG and should not be changed unless you have been specifically directed to do so by ZyXEL support.
load-balancing mode {station   traffic}	Enables load balancing based on either number of stations (also known as wireless clients) or wireless traffic on an AP.
load-balancing max sta <1..127>	If load balancing by the number of stations/wireless clients, this sets the maximum number of devices allowed to connect to a load-balanced AP.
load-balancing sigma <51..100>	Sets the load balancing sigma value.  This value is algorithm parameter used to calculate whether an AP is considered overloaded, balanced, or underloaded. It only applies to 'by traffic mode'.  Note: This parameter has been optimized for the UAG and should not be changed unless you have been specifically directed to do so by ZyXEL support.
load-balancing timeout <1..255>	Sets the length of time that an AP retains load balancing information it receives from other APs within its range.
load-balancing traffic level {high   low   medium}	If load balancing by traffic threshold, this sets the traffic threshold level.
show load-balancing config	Displays the load balancing configuration.

## 11.2.1 Wireless Load Balancing Examples

The following example shows you how to configure AP load balancing in "by station" mode. The maximum number of stations is set to 1.

```
Router(config)# load-balancing mode station
Router(config)# load-balancing max sta 1
Router(config)# show load-balancing config
load balancing config:
Activate: yes
Kickout: no
Mode: station
Max-sta: 1
Traffic-level: high
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 20
```



The following example shows you how to configure AP load balancing in "by traffic" mode. The traffic level is set to low, and "disassociate station" is enabled.

```
Router(config)# load-balancing mode traffic
Router(config)# load-balancing traffic level low
Router(config)# load-balancing kickout
Router(config)# show load-balancing config
load balancing config:
Activate: yes
Kickout: yes
Mode: traffic
Max-sta: 1
Traffic-level: low
Alpha: 5
Beta: 10
Sigma: 60
Timeout: 20
LIInterval: 10
KickoutInterval: 20
```

# Auto-Healing

This chapter shows you how to configure auto-healing settings.

## 12.1 Auto-Healing Overview

Auto-healing allows you to extend the wireless service coverage area of the managed APs when one of the managed APs fails.

## 12.2 Auto-Healing Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 33** Input Values for Auto-Healing Commands

LABEL	DESCRIPTION
<i>interval</i>	Enters the auto-healing interval time. The range is 5 ~ 30 minutes.

The following table describes the commands available for auto-healing. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 34** Command Summary: Auto-Healing

COMMAND	DESCRIPTION
<code>[no] auto-healing activate</code>	Turns on the auto-healing feature. Use the <code>no</code> parameter to turn it off.
<code>auto-healing healing-interval interval</code>	<p>Sets the interval that specifies how often the managed APs scan their neighborhoods and report the status of neighbor APs to the AP controller (UAG).</p> <p>An AP is considered "failed" if the AP controller obtains the same scan result that the AP is missing from the neighbor list of other APs three times.</p>
<code>auto-healing healing-threshold</code>	Sets a minimum signal strength. A managed AP is added to the neighbor lists only when the signal strength of the AP is stronger than the specified threshold.
<code>auto-healing power-threshold &lt;-50~-80&gt;</code>	<p>Sets a power threshold (in dBm). This value is used to calculate the power level (<code>power-threshold + margin</code>) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas.</p> <p>When the failed AP is working again, its neighbor APs return their output power to the original level.</p>

**Table 34** Command Summary: Auto-Healing (continued)

COMMAND	DESCRIPTION
auto-healing margin	Enters a number from 0 to 9. This value is used to calculate the power level (power-threshold + margin) to which the neighbor APs of the failed AP increase their output power in order to extend their wireless service coverage areas.
auto-healing update	Sets all managed APs to immediately scan their neighborhoods three times in a row and update their neighbor lists to the AP controller (UAG).
show auto-healing config	Displays the current auto-healing configuration.

## 12.2.1 Auto-Healing Examples

This example enables auto-healing and sets the power level (in dBm) to which the neighbor APs of the failed AP increase their output power.

```

Router(config)# auto-healing activate
Router(config)# auto-healing power-threshold -70
Router(config)# show auto-healing config
auto-healing activate: yes
auto-healing interval: 10
auto-healing power threshold: -70 dBm
auto-healing healing threshold: -85 dBm
auto-healing margin: 0
Router(config)#

```

# Interfaces

This chapter shows you how to use interface-related commands.

## 13.1 Interface Overview

In general, an interface has the following characteristics.

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface is bound to at most one zone.
- Many interface can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

Some characteristics do not apply to some types of interfaces.

### 13.1.1 Types of Interfaces

You can create several types of interfaces in the UAG. The types supported vary by UAG model.

- **Port role** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The UAG automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the UAG. You can also assign an IP address and subnet mask to the bridge.
- **PPPoE/PPTP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Virtual interfaces** (IP alias) provide additional routing information in the UAG. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- **Trunks** manage load balancing between interfaces.

Port groups, and trunks have a lot of characteristics that are specific to each type of interface. These characteristics are listed in the following tables and discussed in more detail farther on.

**Table 35** Ethernet, VLAN, Bridge, PPP, and Virtual Interface Characteristics

CHARACTERISTICS	ETHERNET	ETHERNET	VLAN	BRIDGE	PPP	VIRTUAL
Name*	wan1, wan2	lan1, lan2, dmz	vlanx	brx	pppx	**
Configurable Zone	No	No	Yes	Yes	No	No
IP Address Assignment						
Static IP address	Yes	Yes	Yes	Yes	Yes	Yes
DHCP client	Yes	No	Yes	Yes	Yes	No
Routing metric	Yes	Yes	Yes	Yes	Yes	Yes
Interface Parameters						
Bandwidth restrictions	Yes	Yes	Yes	Yes	Yes	Yes
Packet size (MTU)	Yes	Yes	Yes	Yes	Yes	No
Data size (MSS)	Yes	Yes	Yes	Yes	Yes	No
DHCP						
DHCP server	No	Yes	Yes	Yes	No	No
DHCP relay	No	Yes	Yes	Yes	No	No
Connectivity Check	Yes	No	Yes	Yes	Yes	No

\* - Each name consists of 2-4 letters (interface type), followed by a number (x). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, Ethernet interface names are wan1, wan2, lan1, lan2, dmz; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

\*\* - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

## 13.1.2 Relationships Between Interfaces

In the UAG, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports (or port groups). The relationships between interfaces are explained in the following table.

**Table 36** Relationships Between Different Types of Interfaces

INTERFACE	REQUIRED PORT / INTERFACE
<b>port group</b>	physical port
<b>Ethernet interface</b>	physical port port group
<b>VLAN interface</b>	Ethernet interface
<b>bridge interface</b>	Ethernet interface* VLAN interface*
<b>PPPoE/PPTP interface</b>	Ethernet interface* VLAN interface* bridge interface

**Table 36** Relationships Between Different Types of Interfaces (continued)

INTERFACE	REQUIRED PORT / INTERFACE
<b>virtual interface</b>	
(virtual Ethernet interface)	Ethernet interface*
(virtual VLAN interface)	VLAN interface*
(virtual bridge interface)	bridge interface
trunk	Ethernet interface VLAN interface bridge interface PPPoE/PPTP interface

\* - You cannot set up a PPPoE/PPTP interface, virtual Ethernet interface, or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPPoE/PPTP interface on top of it.

## 13.2 Interface General Commands Summary

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 37** Input Values for General Interface Commands

LABEL	DESCRIPTION
<i>interface_name</i>	The name of the interface.  Ethernet interface: The UAG715 and UAG5100 uses a name such as wan1, wan2, lan1, lan2, or dmz.  virtual interface on top of Ethernet interface: add a colon (:) and the number of the virtual interface. For example: lan1:y, y=1 - 4  VLAN interface: vlanx, x = 0 - 4094  virtual interface on top of VLAN interface: vlanx:y, x = 0 - 4094, y = 1 - 4  bridge interface: brx, x = 0 - N, where N depends on the number of bridge interfaces your UAG model supports.  virtual interface on top of bridge interface: brx:y, x = the number of the bridge interface, y = 1 - 4  PPPoE/PPTP interface: pppx, x = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your UAG model supports.
<i>profile_name</i>	The name of the DHCP pool. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>domain_name</i>	Fully-qualified domain name. You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.

The following sections introduce commands that are supported by several types of interfaces.

## 13.2.1 Basic Interface Properties and IP Address Commands

This table lists basic properties and IP address commands.

**Table 38** interface General Commands: Basic Properties and IP Address Assignment

COMMAND	DESCRIPTION
<code>show interface {ethernet   vlan   bridge   ppp   auxiliary} status</code>	Displays the connection status of the specified type of interfaces.
<code>show interface {interface_name   ethernet   vlan   bridge   ppp   virtual ethernet   virtual vlan   virtual bridge   all}</code>	Displays information about the specified interface, specified type of interfaces, or all interfaces.
<code>show interface send statistics interval</code>	Displays the interval for how often the UAG refreshes the sent packet statistics for the interfaces.
<code>show interface summary all</code>	Displays basic information about the interfaces.
<code>show interface summary all status</code>	Displays the connection status of the interfaces.
<code>[no] interface interface_name</code>	Creates the specified interface if necessary and enters sub-command mode. The <code>no</code> command deletes the specified interface.
<code>[no] description description</code>	Specifies the description for the specified interface. The <code>no</code> command clears the description.  <i>description:</i> You can use alphanumeric and () +/ : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
<code>[no] downstream &lt;0..1048576&gt;</code>	This is reserved for future use.  Specifies the downstream bandwidth for the specified interface. The <code>no</code> command sets the downstream bandwidth to 1048576.
<code>exit</code>	Leaves the sub-command mode.
<code>[no] ip address dhcp</code>	Makes the specified interface a DHCP client; the DHCP server gives the specified interface its IP address, subnet mask, and gateway. The <code>no</code> command makes the IP address static IP address for the specified interface. (See the next command to set this IP address.)
<code>[no] ip address ip subnet_mask</code>	Assigns the specified IP address and subnet mask to the specified interface. The <code>no</code> command clears the IP address and the subnet mask.
<code>[no] ip gateway ip</code>	Adds the specified gateway using the specified interface. The <code>no</code> command removes the gateway.
<code>ip gateway ip metric &lt;0..15&gt;</code>	Sets the priority (relative to every gateway on every interface) for the specified gateway. The lower the number, the higher the priority.
<code>[no] metric &lt;0..15&gt;</code>	Sets the PPPoE/PPTP interface's priority relative to other interfaces. The lower the number, the higher the priority.
<code>[no] mss &lt;536..1460&gt;</code>	Specifies the maximum segment size (MSS) the interface is to use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The <code>no</code> command has the interface use its default MSS.
<code>[no] mtu &lt;576..1500&gt;</code>	Specifies the Maximum Transmission Unit, which is the maximum number of bytes in each packet moving through this interface. The UAG divides larger packets into smaller fragments. The <code>no</code> command resets the MTU to 1500.
<code>[no] shutdown</code>	Deactivates the specified interface. The <code>no</code> command activates it.
<code>traffic-prioritize {tcp-ack content-filter dns ipsec-vpn ssl-vpn} bandwidth &lt;0..1048576&gt; priority &lt;1..7&gt; [maximize-bandwidth-usage];</code>	Applies traffic priority when the interface sends TCP-ACK traffic, traffic for querying the content filter, traffic for resolving domain names, or encrypted traffic for an IPsec or SSL VPN tunnel. It also sets how much bandwidth the traffic can use and can turn on maximize bandwidth usage.

**Table 38** interface General Commands: Basic Properties and IP Address Assignment (continued)

COMMAND	DESCRIPTION
traffic-prioritize {tcp-ack content-filter dns ipsec-vpn ssl-vpn} deactivate	Turns off traffic priority settings for when the interface sends the specified type of traffic.
[no] upstream <0..1048576>	Specifies the upstream bandwidth for the specified interface. The no command sets the upstream bandwidth to 1048576.
interface reset {interface_name virtual_interface_name all}	Resets the interface statistics TxPkts (transmitted packets) and RxPkts (received packets) counts to 0. You can use the show interface summary all status command to see the interface statistics.
interface send statistics interval <15..3600>	Sets how often the UAG sends interface statistics to external servers. For example, syslog server and Vantage Report server.
show interface-name	Displays all PPP and Ethernet interface system name and user-defined name mappings.
interface-name {ppp_interface   ethernet_interface} user_defined_name	Specifies a name for a PPP or an Ethernet interface. It can use alphanumeric characters, hyphens, and underscores, and it can be up to 11 characters long.  <i>ppp_interface   ethernet_interface</i> : This must be the system name of a PPP or an Ethernet interface. Use the show interface-name command to see the system name of interfaces.  <i>user_defined_name</i> : <ul style="list-style-type: none"> <li>This name cannot be one of the follows: "ethernet", "ppp", "vlan", "bridge", "virtual", "status", "summary", "all"</li> <li>This name cannot begin with one of the follows either: "ppp", "vlan", "br".</li> </ul>
interface-rename old_user_defined_name new_user_defined_name	Modifies the user-defined name of a PPP or an Ethernet interface.

### 13.2.1.1 Basic Interface Properties Command Examples

The following commands make Ethernet interface wan1 a DHCP client.

```
Router# configure terminal
Router(config)# interface wan1
Router(config-if)# ip address dhcp
Router(config-if)# exit
```



This example shows how to modify the name of interface lan2 to “VIP”. First you have to check the interface system name (ge4 in this example) on the UAG. Then change the name and display the result.

```
Router> show interface-name
No.  System Name      User Defined Name
=====
1    ge1              wan1
2    ge2              wan2
3    ge3              lan1
4    ge4              lan2
5    ge5              dmz
Router> configure terminal
Router(config)# interface-name ge4 VIP
Router(config)# show interface-name
No.  System Name      User Defined Name
=====
1    ge1              wan1
2    ge2              wan2
3    ge3              lan1
4    ge4              VIP
5    ge5              dmz
Router(config)#
```

This example shows how to change the user defined name from VIP to Partner. Note that you have to use the “interface-rename” command if you do not know the system name of the interface. To use the “interface-name” command, you have to find out the corresponding system name first (ge4 in this example). This example also shows how to change the user defined name from Partner to Customer using the “interface-name” command.

```
Router(config)# interface-rename VIP Partner
Router(config)# show interface-name
No.  System Name      User Defined Name
=====
1    ge1              wan1
2    ge2              wan2
3    ge3              lan1
4    ge4              Partner
5    ge5              dmz
Router(config)#
Router(config)# interface-name ge4 Customer
Router(config)# show interface-name
No.  System Name      User Defined Name
=====
1    ge1              wan1
2    ge2              wan2
3    ge3              lan1
4    ge4              Customer
5    ge5              dmz
```

This example shows how to restart an interface. You can check all interface names on the UAG. Then use either the system name or user-defined name of an interface (ge4 or Customer in this example) to restart it.

```
Router> show interface-name
No.  System Name      User Defined Name
=====
1    ge1               wan1
2    ge2               wan2
3    ge3               lan1
4    ge4               Customer
5    ge5               dmz
Router> configure terminal
Router(config)# interface reset ge4
Router(config)# interface reset Customer
Router(config)#
```

## 13.2.2 DHCP Setting Commands

This table lists DHCP setting commands. DHCP is based on DHCP pools. Create a DHCP pool if you want to assign a static IP address to a MAC address or if you want to specify the starting IP address and pool size of a range of IP addresses that can be assigned to DHCP clients. There are different commands for each configuration. Afterwards, in either case, you have to bind the DHCP pool to the interface.

**Table 39** interface Commands: DHCP Settings

COMMAND	DESCRIPTION
<code>show ip dhcp dhcp-options</code>	Shows the DHCP extended option settings.
<code>show ip dhcp pool [profile_name]</code>	Shows information about the specified DHCP pool or about all DHCP pools.
<code>show ip dhcp pool profile_name dhcp-options</code>	Shows the specified DHCP pool's DHCP extended option settings.
<code>ip dhcp pool rename profile_name profile_name</code>	Renames the specified DHCP pool from the first <i>profile_name</i> to the second <i>profile_name</i> .
<code>[no] ip dhcp pool profile_name</code>	Creates a DHCP pool if necessary and enters sub-command mode. You can use the DHCP pool to create a static entry or to set up a range of IP addresses to assign dynamically.  About the sub-command settings: <ul style="list-style-type: none"> <li>• If you use the <code>host</code> command, the UAG treats this DHCP pool as a static DHCP entry.</li> <li>• If you do not use the <code>host</code> command and use the <code>network</code> command, the UAG treats this DHCP pool as a pool of IP addresses.</li> <li>• If you do not use the <code>host</code> command or the <code>network</code> command, the DHCP pool is not properly configured and cannot be bound to any interface.</li> </ul> The <code>no</code> command removes the specified DHCP pool.
<code>show</code>	Shows information about the specified DHCP pool.
	Use the following commands to create a static DHCP entry. If you do not use the <code>host</code> command, the commands that are not in this section have no effect, but you can still set them.

**Table 39** interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
[no] host <i>ip</i>	Specifies the static IP address the UAG should assign. Use this command, along with <i>hardware-address</i> , to create a static DHCP entry.  Note: The IP address must be in the same subnet as the interface to which you plan to bind the DHCP pool.  When this command is used, the UAG treats this DHCP pool like a static entry, regardless of the <i>network</i> setting. The <i>no</i> command clears this field.
[no] hardware-address <i>mac_address</i>	Reserves the DHCP pool for the specified MAC address. Use this command, along with <i>host</i> , to create a static DHCP entry. The <i>no</i> command clears this field.
[no] client-identifier <i>mac_address</i>	Specifies the MAC address that appears in the DHCP client list. The <i>no</i> command clears this field.
[no] client-name <i>host_name</i>	Specifies the host name that appears in the DHCP client list. The <i>no</i> command clears this field.  <i>host_name</i> : You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
	Use the following commands to create a pool of IP addresses. These commands have no effect if you use the <i>host</i> command. You can still set them, however.
dhcp-option <1..254> <i>option_name</i> {boolean <0..1>  uint8 <0..255>   uint16 <0..65535>   uint32 <0..4294967295>   ip <i>ipv4</i> [ <i>ipv4</i> [ <i>ipv4</i> ]]   fqdn <i>fqdn</i> [ <i>fqdn</i> [ <i>fqdn</i> ]]   text <i>text</i>   hex <i>hex</i>   vivc <i>enterprise_id hex_s</i> [ <i>enterprise_id hex_s</i> ]   vivs <i>enterprise_id hex_s</i> [ <i>enterprise_id hex_s</i> ]	Adds or edits a DHCP extended option for the specified DHCP pool.  <i>text</i> : String of up to 250 characters  <i>hex</i> : String of up to 250 hexadecimal pairs.  <i>vivc</i> : Vendor-Identifying Vendor Class option. A DHCP client may use this option to unambiguously identify the vendor that manufactured the hardware on which the client is running, the software in use, or an industry consortium to which the vendor belongs.  <i>enterprise_id</i> : Number <0..4294967295>.  <i>hex_s</i> : String of up to 120 hexadecimal pairs.  <i>vivs</i> : Vendor-Identifying Vendor-Specific option. DHCP clients and servers may use this option to exchange vendor-specific information.
no dhcp-option <1..254>	Removes the DHCP extended option for the specified DHCP pool.
network IP/<1..32> network <i>ip mask</i> no network	Specifies the IP address and subnet mask of the specified DHCP pool. The subnet mask can be written in w.x.y.z format or in /<1..32> format.  Note: The DHCP pool must have the same subnet as the interface to which you plan to bind it.  The <i>no</i> command clears these fields.
[no] default-router <i>ip</i>	Specifies the default gateway DHCP clients should use. The <i>no</i> command clears this field.
[no] description <i>description</i>	Specifies a description for the DHCP pool for identification. The <i>no</i> command removes the description.
[no] domain-name <i>domain_name</i>	Specifies the domain name assigned to DHCP clients. The <i>no</i> command clears this field.

**Table 39** interface Commands: DHCP Settings (continued)

COMMAND	DESCRIPTION
[no] starting-address <i>ip</i> pool-size <1..65535>	Sets the IP start address and maximum pool size of the specified DHCP pool. The final pool size is limited by the subnet mask.  Note: You must specify the <code>network</code> number first, and the start address must be in the same subnet.  The <code>no</code> command clears the IP start address and maximum pool size.
[no] first-dns-server { <i>ip</i>   <i>interface_name</i> {1st-dns   2nd-dns   3rd-dns}   Device}	Sets the first DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the UAG itself. The <code>no</code> command resets the setting to its default value.
[no] second-dns-server { <i>ip</i>   <i>interface_name</i> {1st-dns   2nd-dns   3rd-dns}   Device}	Sets the second DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the UAG itself. The <code>no</code> command resets the setting to its default value.
[no] third-dns-server { <i>ip</i>   <i>interface_name</i> {1st-dns   2nd-dns   3rd-dns}   Device}	Sets the third DNS server to the specified IP address, the specified interface's first, second, or third DNS server, or the UAG itself. The <code>no</code> command resets the setting to its default value.
[no] first-wins-server <i>ip</i>	Specifies the first WINS server IP address to assign to the remote users. The <code>no</code> command removes the setting.
[no] second-wins-server <i>ip</i>	Specifies the second WINS server IP address to assign to the remote users. The <code>no</code> command removes the setting.
[no] lease {<0..365> [<0..23> [<0..59>]]   infinite}	Sets the lease time to the specified number of days, hours, and minutes or makes the lease time infinite. The <code>no</code> command resets the first DNS server setting to its default value.
interface <i>interface_name</i>	Enters sub-command mode.
[no] ip dhcp-pool <i>profile_name</i>	Binds the specified interface to the specified DHCP pool. You have to remove any DHCP relays first. The <code>no</code> command removes the binding.
[no] ip helper-address <i>ip</i>	Creates the specified DHCP relay. You have to remove the DHCP pool first, if the DHCP pool is bound to the specified interface. The <code>no</code> command removes the specified DHCP relay.
release dhcp <i>interface-name</i>	Releases the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode.
renew dhcp <i>interface-name</i>	Renews the TCP/IP configuration of the specified interface. The interface must be a DHCP client. This command is available in privilege mode, not configuration mode.
show ip dhcp binding [ <i>ip</i> ]	Displays information about DHCP bindings for the specified IP address or for all IP addresses.
clear ip dhcp binding { <i>ip</i>   *}	Removes the DHCP bindings for the specified IP address or for all IP addresses.

### 13.2.2.1 DHCP Setting Command Examples

The following example uses these commands to configure DHCP pool DHCP\_TEST.

```
Router# configure terminal
Router(config)# ip dhcp pool DHCP_TEST
Router(config-ip-dhcp-pool)# network 192.168.1.0 /24
Router(config-ip-dhcp-pool)# domain-name zyxel.com
Router(config-ip-dhcp-pool)# first-dns-server 10.1.5.1
Router(config-ip-dhcp-pool)# second-dns-server gel 1st-dns
Router(config-ip-dhcp-pool)# third-dns-server 10.1.5.2
Router(config-ip-dhcp-pool)# default-router 192.168.1.1
Router(config-ip-dhcp-pool)# lease 0 1 30
Router(config-ip-dhcp-pool)# starting-address 192.168.1.10 pool-size 30
Router(config-ip-dhcp-pool)# hardware-address 00:0F:20:74:B8:18
Router(config-ip-dhcp-pool)# client-identifier 00:0F:20:74:B8:18
Router(config-ip-dhcp-pool)# client-name TWtester1
Router(config-ip-dhcp-pool)# exit
Router(config)# interface gel
Router(config-if)# ip dhcp-pool DHCP_TEST
Router(config-if)# exit
Router(config)# show ip dhcp server status
binding interface : gel
  binding pool    : DHCP_TEST
```

### 13.2.2.2 DHCP Extended Option Setting Command Example

The following example configures the DHCP\_TEST pool with a SIP server (code 120) extended DHCP option with one IP address to provide to the SIP clients.

```
Router# configure terminal
Router(config)# ip dhcp pool DHCP_TEST
Router(config-ip-dhcp-pool)# dhcp-option 120 sip ip 192.168.1.20
Router(config-ip-dhcp-pool)# exit
```

## 13.2.3 Interface Parameter Command Examples

This table shows an example of each interface type's sub-commands. The sub-commands vary for different interface types.

**Table 40** Examples for Different Interface Parameters

ETHERNET	VIRTUAL INTERFACE	PPPOE/PPTP
Router(config)# interface wan1 Router(config-if-wan1)# description downstream exit ip mac mss mtu no ping-check shutdown traffic-prioritize type upstream use-defined-mac	Router(config)# interface wan1:1 Router(config-if-vir)# description downstream exit ip no shutdown upstream	Router(config)# interface wan1_ppp Router(config-if-ppp)# account bind connectivity description downstream exit local-address metric mss mtu no ping-check remote-address shutdown traffic-prioritize upstream
VLAN	BRIDGE	
Router(config)# interface vlan1 Router(config-if-vlan)# description downstream exit ip mss mtu no ping-check port shutdown traffic-prioritize type upstream vlan-id	Router(config)# interface br0 Router(config-if-brg)# description downstream exit ip join mss mtu no ping-check shutdown traffic-prioritize type upstream	

## 13.2.4 RIP Commands

This table lists the commands for RIP settings.

**Table 41** interface Commands: RIP Settings

COMMAND	DESCRIPTION
router rip	Enters sub-command mode.
[no] network <i>interface_name</i>	Enables RIP for the specified interface. The no command disables RIP for the specified interface.
[no] passive-interface <i>interface_name</i>	Sets the RIP direction of the specified interface to in-only. The no command makes RIP bi-directional in the specified interface.
[no] outonly-interface <i>interface_name</i>	Sets the RIP direction of the specified interface to out-only. The no command makes RIP bi-directional in the specified interface.
interface <i>interface_name</i>	Enters sub-command mode.

**Table 41** interface Commands: RIP Settings (continued)

COMMAND	DESCRIPTION
[no] ip rip {send   receive} version <1..2>	Sets the send or receive version to the specified version number. The no command sets the send or received version to the current global setting for RIP. See <a href="#">Chapter 17 on page 121</a> for more information about routing protocols.
[no] ip rip v2-broadcast	Enables RIP-2 packets using subnet broadcasting. The no command uses multi-casting.
show rip {global   interface {all   interface_name}}	Displays RIP settings.

## 13.2.5 OSPF Commands

This table lists the commands for OSPF settings.

**Table 42** interface Commands: OSPF Settings

COMMAND	DESCRIPTION
router ospf	Enters sub-command mode.
[no] network interface_name area ip	Makes the specified interface part of the specified area. The no command removes the specified interface from the specified area, disabling OSPF in this interface.
[no] passive-interface interface_name	Sets the OSPF direction of the specified interface to in-only. The no command makes OSPF bi-directional in the specified interface.
interface interface_name	Enters sub-command mode.
[no] ip ospf priority <0..255>	Sets the priority of the specified interface to the specified value. The no command sets the priority to 1.
[no] ip ospf cost <1..65535>	Sets the cost to route packets through the specified interface. The no command sets the cost to 10.
no ip ospf authentication	Disables authentication for OSPF in the specified interface.
ip ospf authentication	Enables text authentication for OSPF in the specified interface.
ip ospf authentication message-digest	Enables MD5 authentication for OSPF in the specified interface.
ip ospf authentication same-as-area	To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. This command makes OSPF authentication in the specified interface follow the settings in the corresponding area.
[no] ip ospf authentication-key password	Sets the simple text password for OSPF text authentication in the specified interface. The no command clears the text password. <i>password</i> : 1-8 alphanumeric characters or underscores
ip ospf message-digest-key <1..255> md5 password	Sets the ID and password for OSPF MD5 authentication in the specified interface. <i>password</i> : 1-16 alphanumeric characters or underscores
no ip ospf message-digest-key	Clears the ID and password for OSPF MD5 authentication in the specified interface.
[no] ip ospf hello-interval <1..65535>	Sets the number of seconds between "hello" messages to peer routers. These messages let peer routers know the UAG is available. The no command sets the number of seconds to 10. See <code>ip ospf dead-interval</code> for more information.

**Table 42** interface Commands: OSPF Settings (continued)

COMMAND	DESCRIPTION
[no] ip ospf dead-interval <1..65535>	Sets the number of seconds the UAG waits for “hello” messages from peer routers before it assumes the peer router is not available and deletes associated routing information. The no command sets the number of seconds to 40. See ip ospf hello-interval for more information.
[no] ip ospf retransmit-interval <1..65535>	Sets the number of seconds the UAG waits for an acknowledgment in response to a link state advertisement before it re-sends the advertisement.  Link state advertisements (LSA) are used to share the link state and routing information between routers.



## 13.2.6 Connectivity Check (Ping-check) Commands

Use these commands to have an interface regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the UAG stops routing to the gateway. The UAG resumes routing to the gateway the first time the gateway passes the connectivity check.

This table lists the ping-check commands

**Table 43** interface Commands: Ping Check

COMMAND	DESCRIPTION
<code>show ping-check [interface_name   status]</code>	Displays information about ping check settings for the specified interface or for all interfaces.  <code>status</code> : displays the current connectivity check status for any interfaces upon which it is activated.
<code>[no] connectivity-check continuous-log activate</code>	Use this command to have the UAG logs connectivity check result continuously. The <code>no</code> command disables the setting.
<code>show connectivity-check continuous-log status</code>	Displays the continuous log setting about connectivity check.
<code>interface interface_name</code>	Enters sub-command mode.
<code>[no] ping-check activate</code>	Enables ping check for the specified interface. The <code>no</code> command disables ping check for the specified interface.
<code>ping-check {domain_name   ip   default-gateway}</code>	Specifies what the UAG pings for the ping check; you can specify a fully-qualified domain name, IP address, or the default gateway for the interface.
<code>ping-check {domain_name   ip   default-gateway} period &lt;5..30&gt;</code>	Specifies what the UAG pings for the ping check and sets the number of seconds between each ping check.
<code>ping-check {domain_name   ip   default-gateway} timeout &lt;1..10&gt;</code>	Specifies what the UAG pings for the ping check and sets the number of seconds the UAG waits for a response.
<code>ping-check {domain_name   ip   default-gateway} fail-tolerance &lt;1..10&gt;</code>	Specifies what the UAG pings for the ping check and sets the number of times the UAG times out before it stops routing through the specified interface.
<code>ping-check {domain_name   ip   default-gateway} method {icmp   tcp}</code>	Sets how the UAG checks the connection to the gateway.  <code>icmp</code> : ping the gateway you specify to make sure it is still available.  <code>tcp</code> : perform a TCP handshake with the gateway you specify to make sure it is still available.
<code>ping-check {domain_name   ip   default-gateway} port &lt;1..65535&gt;</code>	Specifies the port number to use for a TCP connectivity check.

### 13.2.6.1 Connectivity Check Command Example

The following commands show you how to set the WAN1 interface to use a TCP handshake on port 8080 to check the connection to IP address 1.1.1.2

```
Router# configure terminal
Router(config)# interface wan1
Router(config-if-wan1)# ping-check 1.1.1.2 method tcp port 8080
Router(config-if-wan1)# exit
Router(config)# show ping-check
Interface: wan1
Check Method: tcp
IP Address: 1.1.1.2
Period: 30
Timeout: 5
Fail Tolerance: 5
Activate: yes
Port: 8080
Router(config)#
```

## 13.3 Ethernet Interface Specific Commands

This section covers commands that are specific to Ethernet interfaces.

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 44** Input Values for Ethernet Interface Commands

LABEL	DESCRIPTION
<i>interface_name</i>	The name of the Ethernet interface. This depends on the UAG model. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.

### 13.3.1 MAC Address Setting Commands

This table lists the commands you can use to set the MAC address of an interface.

**Table 45** interface Commands: MAC Setting

COMMAND	DESCRIPTION
<code>interface <i>interface_name</i></code>	Enters sub-command mode.
<code>no mac</code>	Has the interface use its default MAC address.
<code>mac <i>mac</i></code>	Specifies the MAC address the interface is to use.

**Table 45** interface Commands: MAC Setting (continued)

COMMAND	DESCRIPTION
<code>type {internal   external   general}</code>	<p>Sets which type of network you will connect this interface. The UAG automatically adds default route and SNAT settings for traffic it routes from internal interfaces to external interfaces; for example LAN to WAN traffic.</p> <p><code>internal</code>: Set this to connect to a local network. Other corresponding configuration options: DHCP server and DHCP relay. The UAG automatically adds default SNAT settings for traffic flowing from this interface to an external interface.</p> <p><code>external</code>: Set this to connect to an external network (like the Internet). The UAG automatically adds this interface to the default WAN trunk.</p> <p><code>general</code>: Set this if you want to manually configure a policy route to add routing and SNAT settings for the interface.</p>
<code>no use-defined-mac</code>	Has the interface use its default MAC address.
<code>use-defined-mac</code>	Has the interface use a MAC address that you specify.

### 13.3.2 Port Grouping Commands

This section covers commands that are specific to port grouping.

Note: In CLI, representative interfaces are also called representative ports.

**Table 46** Basic Interface Setting Commands

COMMAND	DESCRIPTION
<code>show port-grouping</code>	Displays which physical ports are assigned to each representative interface.
<code>port-grouping interface_name port &lt;1..x&gt;</code>	<p>Adds the specified physical port to the specified representative interface.</p> <p>&lt;1..x&gt; where x equals the highest numbered port for your UAG model.</p>
<code>no port &lt;1..x&gt;</code>	Removes the specified physical port from its current representative interface and adds it to its default representative interface (for example, port x --> gex).
<code>port status Port&lt;1..x&gt;</code>	Enters a sub-command mode to configure the specified port's settings.
<code>[no] duplex &lt;full   half&gt;</code>	Sets the port's duplex mode. The no command returns the default setting.
<code>exit</code>	Leaves the sub-command mode.
<code>[no] negotiation auto</code>	Sets the port to use auto-negotiation to determine the port speed and duplex. The no command turns off auto-negotiation.
<code>[no] speed &lt;100,10&gt;</code>	Sets the Ethernet port's connection speed in Mbps. The no command returns the default setting.
<code>show port setting</code>	Displays the Ethernet port negotiation, duplex, and speed settings.
<code>show port status</code>	Displays statistics for the Ethernet ports.

### 13.3.2.1 Port Grouping Command Examples

The following commands add physical port 5 to interface lan1.

```
Router# configure terminal
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5
=====
1  wan1                  yes  no  no  no  no
2  wan2                  no   yes no  no  no
3  lan1                  no   no  yes no  no
4  lan2                  no   no  no  yes no
5  dmz                   no   no  no  no  yes
Router(config)# port-grouping lan1
Router(config-port-grouping)# port 5
Router(config-port-grouping)# exit
Router(config)# show port-grouping
No. Representative Name  Port1 Port2 Port3 Port4 Port5
=====
1  wan1                  yes  no  no  no  no
2  wan2                  no   yes no  no  no
3  lan1                  no   no  yes no  yes
4  lan2                  no   no  no  yes no
5  dmz                   no   no  no  no  no
```

The following commands set port 1 to use auto-negotiation auto and port 2 to use a 10 Mbps connection speed and half duplex.

```
Router(config)# port status Port1
Router(config-port-status)# negotiation auto
Router(config-port-status)# exit
Router(config)# port status Port2
Router(config-port-status)# duplex half
Router(config-port-status)# speed 10
Router(config-port-status)# exit
Router(config)# exit
```

## 13.4 Virtual Interface Specific Commands

Virtual interfaces use many of the general interface commands discussed at the beginning of [Section 13.2 on page 86](#). There are no additional commands for virtual interfaces.

### 13.4.1 Virtual Interface Command Examples

The following commands set up a virtual interface on top of Ethernet interface lan1. The virtual interface is named lan1:1 with the following parameters: IP 1.2.3.4, subnet 255.255.255.0,

gateway 4.6.7.8, upstream bandwidth 345, downstream bandwidth 123, and description "I am vir interface".

```
Router# configure terminal
Router(config)# interface lan1:1
Router(config-if-vir)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vir)# ip gateway 4.6.7.8
Router(config-if-vir)# upstream 345
Router(config-if-vir)# downstream 123
Router(config-if-vir)# description I am vir interface
Router(config-if-vir)# exit
```

## 13.5 PPPoE/PPTP Specific Commands

This section covers commands that are specific to PPPoE/PPTP interfaces. PPPoE/PPTP interfaces also use many of the general interface commands discussed at the beginning of [Section 13.2 on page 86](#).

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 47** Input Values for PPPoE/PPTP Interface Commands

LABEL	DESCRIPTION
<i>interface_name</i>	PPPoE/PPTP interface: pppx, x = 0 - N, where N depends on the number of PPPoE/PPTP interfaces your UAG model supports.
<i>profile_name</i>	The name of the ISP account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

This table lists the PPPoE/PPTP interface commands.

**Table 48** interface Commands: PPPoE/PPTP Interfaces

COMMAND	DESCRIPTION
interface dial <i>interface_name</i>	Connects the specified PPPoE/PPTP interface.
interface disconnect <i>interface_name</i>	Disconnects the specified PPPoE/PPTP interface.
interface <i>interface_name</i>	Creates the specified interface if necessary and enters sub-command mode.
[no] account <i>profile_name</i>	Specifies the ISP account for the specified PPPoE/PPTP interface. The no command clears the ISP account field.
[no] bind <i>interface_name</i>	Specifies the base interface for the PPPoE/PPTP interface. The no command removes the base interface.
[no] connectivity {nail-up   dial-on-demand}	Specifies whether the specified PPPoE/PPTP interface is always connected (nail-up) or connected only when used (dial-on-demand). The no command sets it to dial-on-demand.
[no] local-address <i>ip</i>	Specifies a static IP address for the specified PPPoE/PPTP interface. The no command makes the PPPoE/PPTP interface a DHCP client; the other computer assigns the IP address.
[no] remote-address <i>ip</i>	Specifies the IP address of the PPPoE/PPTP server. If the PPPoE/PPTP server is not available at this IP address, no connection is made. The no command lets the UAG get the IP address of the PPPoE/PPTP server automatically when it establishes the connection.

**Table 48** interface Commands: PPPoE/PPTP Interfaces (continued)

COMMAND	DESCRIPTION
[no] mss <536..1452>	Specifies the maximum segment size (MSS) the interface can use. MSS is the largest amount of data, specified in bytes, that the interface can handle in a single, unfragmented piece. The no command has the UAG use its default MSS setting.
mtu <576..1492>	Sets the Maximum Transmission Unit in bytes.
show interface ppp system-default	Displays system default PPP interfaces (non-deletable) that come with the UAG.
show interface ppp user-define	Displays all PPP interfaces that were manually configured on the UAG.

### 13.5.1 PPPoE/PPTP Interface Command Examples

The following commands show you how to configure PPPoE/PPTP interface ppp0 with the following characteristics: base interface wan1, ISP account **Hinet**, local address 1.1.1.1, remote address 2.2.2.2, MTU 1200, upstream bandwidth 345, downstream bandwidth 123, description "I am ppp0", and dialed only when used.

```
Router# configure terminal
Router(config)# interface ppp0
Router(config-if-ppp)# account Hinet
Router(config-if-ppp)# bind wan1
Router(config-if-ppp)# local-address 1.1.1.1
Router(config-if-ppp)# remote-address 2.2.2.2
Router(config-if-ppp)# mtu 1200
Router(config-if-ppp)# upstream 345
Router(config-if-ppp)# downstream 123
Router(config-if-ppp)# connectivity dial-on-demand
Router(config-if-ppp)# description I am ppp0
Router(config-if-ppp)# exit
```

The following commands show you how to connect and disconnect ppp0.

```
Router# interface dial ppp0
Router# interface disconnect ppp0
```

## 13.6 USB Storage Specific Commands

Use these commands to configure settings that apply to the USB storage device connected to the UAG.

Note: For the UAG which supports more than one USB ports, these commands only apply to the USB storage device that is first attached to the UAG.

**Table 49** USB Storage General Commands

COMMAND	DESCRIPTION
show usb-storage	Displays the status of the connected USB storage device.
[no] usb-storage activate	Enables or disables the connected USB storage service.
usb-storage warn <i>number</i> <percentage megabyte>	Sets a number and the unit (percentage or megabyte) to have the UAG send a warning message when the remaining USB storage space is less than the set value.

**Table 49** USB Storage General Commands (continued)

COMMAND	DESCRIPTION
usb-storage mount	Mounts the connected USB storage device.
usb-storage unmount	Unmounts the connected USB storage device.
[no] logging usb-storage	Sets to have the UAG log or not log any information about the connected USB storage device(s) for the system log.
show logging status usb-storage	Displays the logging settings for the connected USB storage device.
logging usb-storage category category level <all normal>	Configures the logging settings for the specified category for the connected USB storage device.
logging usb-storage category category disable	Stops logging for the specified category to the connected USB storage device.
logging usb-storage flushThreshold <1..100>	Configures the maximum storage space (in percentage) for storing system logs on the connected USB storage device.
[no] diag-info copy usb-storage	Sets to have the UAG save or stop saving the current system diagnostics information to the connected USB storage device. You may need to send this file to customer support for troubleshooting.
show diag-info copy usb-storage	Displays whether (enable or disable) the UAG saves the current system diagnostics information to the connected USB storage device.
[no] corefile copy usb-storage	Sets to have the UAG save or not save a process's core dump to the connected USB storage device if the process terminates abnormally (crashes). You may need to send this file to customer support for troubleshooting.
show corefile copy usb-storage	Displays whether (enable or disable) the UAG saves core dump files to the connected USB storage device.

### 13.6.1 USB Storage General Commands Example

This example shows how to display the status of the connected USB storage device.

```
Router> show usb-storage
USBStorage Configuration:
Activation: enable
Criterion Number: 100
Criterion Unit: megabyte
USB Storage Status:
Device description: N/A
Usage: N/A
Filesystem: N/A
Speed: N/A
Status: none
Detail: none
```

## 13.7 VLAN Interface Specific Commands

This section covers commands that are specific to VLAN interfaces. VLAN interfaces also use many of the general interface commands discussed at the beginning of [Section 13.2 on page 86](#).

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 50** Input Values for VLAN Interface Commands

LABEL	DESCRIPTION
<i>interface_name</i>	VLAN interface: <i>vlanx</i> , <i>x</i> = 0 - 4094 See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.

This table lists the VLAN interface commands.

**Table 51** interface Commands: VLAN Interfaces

COMMAND	DESCRIPTION
<code>interface interface_name</code>	Creates the specified interface if necessary and enters sub-command mode.
<code>[no] port interface_name</code>	Specifies the Ethernet interface on which the VLAN interface runs. The <code>no</code> command clears the port.
<code>[no] vlan-id &lt;1..4094&gt;</code>	Specifies the VLAN ID used to identify the VLAN. The <code>no</code> command clears the VLAN ID.
<code>show port vlan-id</code>	Displays the Ethernet interface VLAN settings.

## 13.7.1 VLAN Interface Command Examples

The following commands show you how to set up VLAN `vlan100` with the following parameters: VLAN ID 100, interface `lan1`, IP 1.2.3.4, subnet 255.255.255.0, MTU 598, gateway 2.2.2.2, description "I am vlan100", upstream bandwidth 345, and downstream bandwidth 123.

```
Router# configure terminal
Router(config)# interface vlan100
Router(config-if-vlan)# vlan-id 100
Router(config-if-vlan)# port lan1
Router(config-if-vlan)# ip address 1.2.3.4 255.255.255.0
Router(config-if-vlan)# ip gateway 2.2.2.2
Router(config-if-vlan)# mtu 598
Router(config-if-vlan)# upstream 345
Router(config-if-vlan)# downstream 123
Router(config-if-vlan)# description I am vlan100
Router(config-if-vlan)# exit
```

## 13.8 Bridge Specific Commands

This section covers commands that are specific to bridge interfaces. Bridge interfaces also use many of the general interface commands discussed at the beginning of [Section 13.2 on page 86](#).



The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 52** Input Values for Bridge Interface Commands

LABEL	DESCRIPTION
<i>interface_name</i>	The name of the interface.  VLAN interface: <i>vlanx</i> , <i>x</i> = 0 - 4094  bridge interface: <i>brx</i> , <i>x</i> = 0 - N, where N depends on the number of bridge interfaces your UAG model supports.  See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.

This table lists the bridge interface commands.

**Table 53** interface Commands: Bridge Interfaces

COMMAND	DESCRIPTION
<code>interface <i>interface_name</i></code>	Creates the specified interface if necessary and enters sub-command mode.
<code>[no] join <i>interface_name</i></code>	Adds the specified Ethernet interface or VLAN interface to the specified bridge. The <code>no</code> command removes the specified interface from the specified bridge.
<code>show bridge available member</code>	Displays the available interfaces that could be added to a bridge.

### 13.8.1 Bridge Interface Command Examples

The following commands show you how to set up a bridge interface named `br0` with the following parameters: member `lan1`, IP `1.2.3.4`, subnet `255.255.255.0`, MTU `598`, gateway `2.2.2.2`, upstream bandwidth `345`, downstream bandwidth `123`, and description "I am `br0`".

```

Router# configure terminal
Router(config)# interface br0
Router(config-if-brg)# join lan1
Router(config-if-brg)# ip address 1.2.3.4 255.255.255.0
Router(config-if-brg)# ip gateway 2.2.2.2
Router(config-if-brg)# mtu 598
Router(config-if-brg)# upstream 345
Router(config-if-brg)# downstream 123
Router(config-if-brg)# description I am br0
Router(config-if-brg)# exit

```

This chapter shows you how to configure trunks on your UAG.

## 14.1 Trunks Overview

You can group multiple interfaces together into trunks to have multiple connections share the traffic load to increase overall network throughput and enhance network reliability. If one interface's connection goes down, the UAG sends traffic through another member of the trunk. For example, you can use two interfaces for WAN connections. You can connect one interface to one ISP (or network) and connect the another to a second ISP (or network). The UAG can balance the load between multiple connections. If one interface's connection goes down, the UAG can automatically send its traffic through another interface.

You can use policy routing to specify through which interface to send specific traffic types. You can use trunks in combination with policy routing. You can also define multiple trunks for the same physical interfaces. This allows you to send specific traffic types through the interface that works best for that type of traffic, and if that interface's connection goes down, the UAG can still send its traffic through another interface.

## 14.2 Trunk Scenario Examples

Suppose one of the UAG's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You may want to set that interface as active and set another interface (connected to another ISP) to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

Another example would be if you use multiple ISPs that provide different levels of service to different places. Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routing and trunks to send traffic for your European branch offices primarily through ISP A and traffic for your Australian branch offices primarily through ISP B.

## 14.3 Trunk Commands Input Values

The following table explains the values you can input with the `interface-group` commands.

**Table 54** interface-group Command Input Values

LABEL	DESCRIPTION
<i>group-name</i>	A descriptive name for the trunk. The name cannot start with a number. This value is case-sensitive.
<i>interface-name</i>	The name of an interface, it could be an Ethernet, PPP, VLAN or bridge interface. The possible number of each interface type and the abbreviation to use depends on the UAG model. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.
<i>num</i>	The interface's position in the trunk's list of members <1..8>.
<CR>	Carriage Return (the "enter" key).

## 14.4 Trunk Commands Summary

The following table lists the `interface-group` commands. You must use the `configure` terminal command to enter the configuration mode before you can use these commands. See [Table 54 on page 107](#) for details about the values you can input with these commands.

**Table 55** interface-group Commands Summary

COMMAND	DESCRIPTION
<code>show interface-group {system-default user-define group-name}</code>	Displays pre-configured system default trunks, your own user configuration trunks or a specified trunk's settings.
<code>[no] interface-group group-name</code>	Creates a trunk name and enters the trunk sub-command mode where you can configure the trunk. The <code>no</code> command removes the trunk.
<code>algorithm {wrr llf spill-over}</code>	Sets the trunk's load balancing algorithm.
<code>exit</code>	Leaves the trunk sub-command mode.
<code>flush</code>	Deletes a trunk's interface settings.
<code>interface {num append insert num} interface-name [weight &lt;1..10&gt; limit &lt;1..2097152&gt; passive]</code>	This subcommand adds an interface to a trunk. Sets the interface's number. It also sets the interface's weight and spillover limit or sets it to be passive.
<code>loadbalancing-index &lt;inbound outbound total&gt;</code>	Use this command only if you use least load first or spill-over as the trunk's load balancing algorithm.  Set either <code>inbound</code> , <code>outbound</code> , or <code>total</code> (outbound and inbound) traffic to which the UAG will apply the specified algorithm. Outbound traffic means the traffic travelling from an internal interface (ex. LAN) to an external interface (ex. WAN). Inbound traffic means the opposite.
<code>mode {normal trunk}</code>	Sets the mode for a trunk. Do this first in the trunk's sub-command mode.
<code>move &lt;1..8&gt; to &lt;1..8&gt;</code>	Changes a the interface order in a trunk.
<code>[no] interface {num interface-name}</code>	Removes an interface from the trunk.
<code>system default-interface-group group-name</code>	Sets the UAG to first attempt to use the the specified WAN trunk.
<code>[no] system default-snat</code>	Enables or disables Source NAT (SNAT). When SNAT is enabled, the UAG uses the IP address of the outgoing interface as the source IP address of the packets it sends out through the WAN interfaces.

**Table 55** interface-group Commands Summary (continued)

COMMAND	DESCRIPTION
show system default-snat	Displays whether the UAG enable SNAT or not. The UAG performs SNAT by default for traffic going to or from the WAN interfaces.
show system default-interface-group	Displays the WAN trunk the UAG first attempts to use.

## 14.5 Trunk Command Examples

The following example creates a weighted round robin trunk for Ethernet interfaces wan1 and wan2. The UAG sends twice as much traffic through ge1.

```
Router# configure terminal
Router(config)# interface-group wrd-example
Router(if-group)# mode trunk
Router(if-group)# algorithm wrd
Router(if-group)# interface 1 wan1 weight 2
Router(if-group)# interface 2 wan2 weight 1
Router(if-group)# exit
Router(config)#
```

The following example creates a least load first trunk for Ethernet interface lan1 and VLAN 5, which will only apply to outgoing traffic through the trunk. The UAG sends new session traffic through the least utilized of these interfaces.

```
Router# configure terminal
Router(config)# interface-group llf-example
Router(if-group)# mode trunk
Router(if-group)# algorithm llf
Router(if-group)# interface 1 lan1
Router(if-group)# interface 2 vlan5
Router(if-group)# loadbalancing-index outbound
Router(if-group)# exit
Router(config)#
```

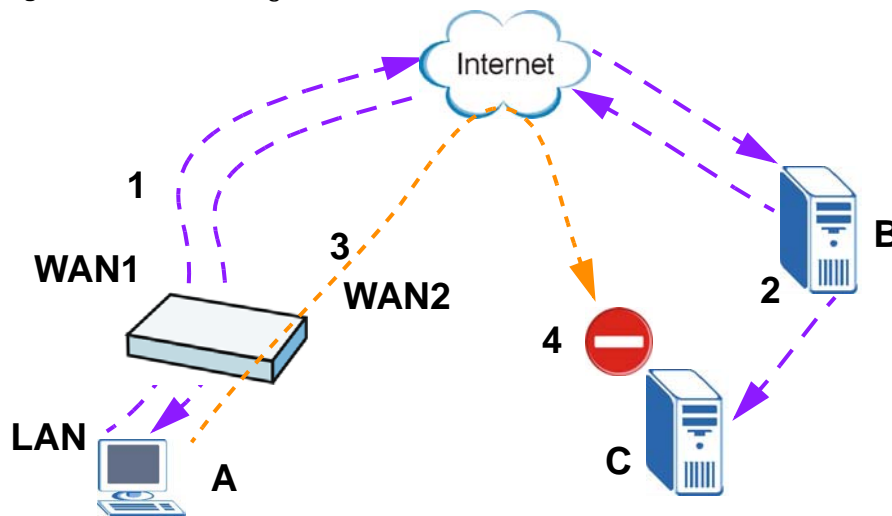
The following example creates a spill-over trunk for Ethernet interfaces wan1 and wan2, which will apply to both incoming and outgoing traffic through the trunk. The UAG sends traffic through wan1 until it hits the limit of 1000 kbps. The UAG sends anything over 1000 kbps through wan2.

```
Router# configure terminal
Router(config)# interface-group spill-example
Router(if-group)# mode trunk
Router(if-group)# algorithm spill-over
Router(if-group)# interface 1 wan1 limit 1000
Router(if-group)# interface 2 wan2 limit 1000
Router(if-group)# loadbalancing-index total
Router(if-group)# exit
Router(config)#
```

## 14.6 Link Sticking

You can have the UAG send each local computer's traffic through a single WAN interface for a specified period of time. This is useful when a redirect server forwards a user request for a file and informs the file server that a particular WAN IP address is requesting the file. If the user's subsequent sessions came from a different WAN IP address, the file server would deny the request. Here is an example.

**Figure 14** Link Sticking



- 1 LAN user **A** tries to download a file from server **B** on the Internet. The UAG uses WAN1 to send the request to server **B**.
- 2 However remote server **B** is actually a redirect server. So server **B** sends a file list to LAN user **A**. The file list lets LAN user **A**'s computer know that the desired file is actually on file server (**C**). At the same time, register server **B** informs file server **C** that a computer located at the WAN1's IP address will download a file.
- 3 The UAG is using active/active load balancing. So when LAN user **A** tries to retrieve the file from file server **C**, the request goes out through WAN2.
- 4 File server **C** finds that the request comes from WAN2's IP address instead of WAN1's IP address and rejects the request.
- 5 If link sticking had been configured, the UAG would have still used WAN1 to send LAN user **A**'s request to file server **C** and the file server would have given the file to **A**.

## 14.7 Link Sticking Commands Summary

The following table lists the `ip load-balancing link-sticking` commands for link sticking. (The link sticking commands have the prefix `ip load-balancing` because they affect the UAG's load balancing behavior.) You must use the `configure terminal` command to enter the configuration

mode before you can use these commands. See [Table 54 on page 107](#) for details about the values you can input with these commands.

**Table 56** ip load-balancing link-sticking Commands Summary

COMMAND	DESCRIPTION
[no] ip load-balancing link-sticking activate	Turns link sticking on or off.
[no] ip load-balancing link-sticking timeout <i>timeout</i>	Sets for how many seconds (30-3600) the UAG sends all of each local computer's traffic through one WAN interface.
show ip load-balancing link-sticking status	Displays the current link sticking settings.

## 14.8 Link Sticking Command Example

This example shows how to activate link sticking and set the timeout to 600 seconds (ten minutes).

```
Router(config)# ip load-balancing link-sticking activate
Router(config)# ip load-balancing link-sticking timeout 600
Router(config)# show ip load-balancing link-sticking status
active      : yes
timeout     : 300
```

## IP Drop-In

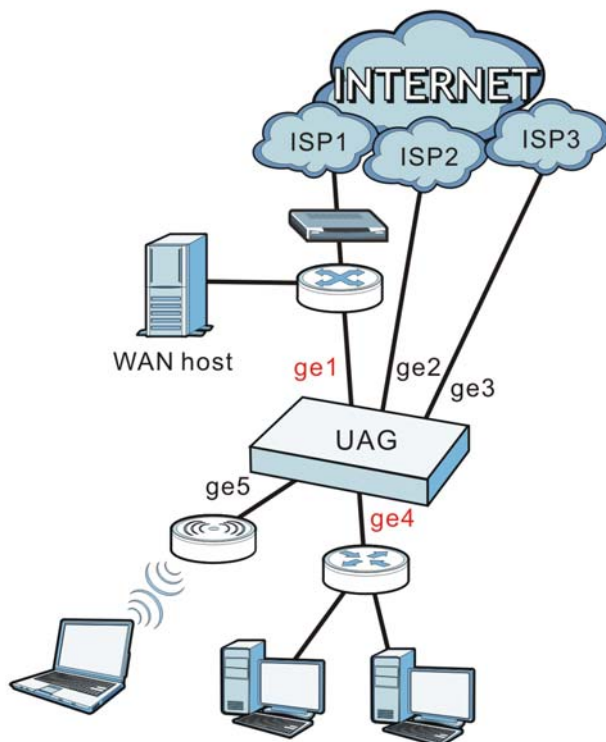
This chapter explains some commands you can use to set the UAG interfaces to work in drop-in mode.

### 15.1 Drop-In Mode Overview

When the UAG is in drop-in mode, you can deploy it in your existing network without changing the network architecture and use its multiple WAN feature to connect to more than one ISP. Before deployment, you need to set one WAN interface and one LAN interface on the UAG to work in drop-in mode. The drop-in WAN interface can connect to the original ISP. The drop-in LAN interface is connected to the existing NAT router or firewall (if any) in your network. A second WAN interface which is not in drop-in mode is connected to another ISP. You can use trunks for WAN traffic load-balancing to increase overall network throughput and reliability.

Note: The WAN interface (ge1, for example) in drop-in mode must use a static IP address. You must disable the DHCP service on the LAN interface (ge4, for example) in drop-in mode via the web configurator or using the `interface interface_name no ip dhcp pool profile_name` command.

In the following example, the drop-in WAN interface is **ge1** and the drop-in LAN interface is **ge4**.



## 15.1.1 Drop-In Limitations

- The interfaces in drop-in mode cannot join the port group of the interfaces that are not in drop-in mode. But other interfaces can join a drop-in interface's port group.
- The interfaces in drop-in mode cannot be part of a bridge interface.
- You must configure a drop-in WAN interface's IP address before setting it to work in drop-in mode.
- You cannot create a policy route, static route, NAT rule or VPN 1-1 mapping rule for an interface in drop-in mode.
- You cannot enable IPnP, UPnP or Layer-2 isolation on a LAN interface in drop-in mode. The interface cannot be used for printer management and web authentication nor provide SMS, free time and billing services.

## 15.2 Drop-In Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 57** Input Values for General Drop-In Commands

LABEL	DESCRIPTION
<i>interface_name</i>	The name of the Ethernet interface. This depends on the UAG model. See <a href="#">Table 57 on page 112</a> for detailed information about the interface name.

This table lists the `ip drop-in` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 58** IP Drop-In Commands

COMMAND	DESCRIPTION
<code>no ip drop-in activate</code>	Disables the drop-in mode on the UAG.
<code>ip drop-in activate</code>	Enables the drop-in mode on the UAG.
<code>exit</code>	Leaves the sub-command mode.
<code>[no] wan-host ipv4_address</code>	Sets the IPv4 address of the host that is connected to the UAG's drop-in WAN interface and can be accessed by the devices connected to the UAG's drop-in LAN interface. The <code>no</code> command removes the host IP address.
<code>wan-interface interface_name lan-interface interface_name</code>	Sets the WAN interface and LAN interface of the UAG, which are to be in drop-in mode.
<code>show ip drop-in status</code>	Displays whether drop-in mode is enabled on the UAG and the WAN and LAN interfaces that are set to work in drop-in mode.
<code>show ip drop-in wan-host</code>	Displays the IP address of the WAN host in drop-in mode.



The following example shows you how to set the drop-in WAN interface and LAN interface, set a WAN host, turn on the drop-in mode and show the settings.

```
Router> configure terminal
Router(config)# ip drop-in
Router(drop-in)# wan-host 10.1.2.3
Router(drop-in)# wan-interface wan1 lan-interface lan1
Router(drop-in)# activate
Router(drop-in)# exit
Router(config)# show ip drop-in status
active      : yes
wan_interface: wan1
lan_interface: lan1
Router(config)# show ip drop-in wan-host
Index      WanHost
=====
1          10.1.2.3
Router(config)#
```

This chapter shows you how to configure policies for IP routing and static routes on your UAG.

## 16.1 Policy Route

Traditionally, routing is based on the destination address only and the UAG takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

## 16.2 Policy Route Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 59** Input Values for General Policy Route Commands

LABEL	DESCRIPTION
<i>address_object</i>	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>interface_name</i>	The name of the interface. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.
<i>policy_number</i>	The number of a policy route. 1 - <i>X</i> where <i>X</i> is the highest number of policy routes the UAG model supports. See the UAG's User's Guide for details.
<i>schedule_object</i>	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>service_name</i>	The name of the service (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>user_name</i>	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for policy route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 60** Command Summary: Policy Route

COMMAND	DESCRIPTION
[no] bwm activate	Globally enables bandwidth management. You must globally activate bandwidth management to have individual policy routes policies apply bandwidth management. The <code>no</code> command globally disables bandwidth management.
policy { <i>policy_number</i>   append   insert <i>policy_number</i> }	Enters the policy-route sub-command mode to configure, add or insert a policy.
[no] auto-destination	When you set <code>tunnel</code> as the next-hop type (using the <code>next-hop tunnel</code> command) for this route, you can use this command to have the UAG use the local network of the peer router that initiated an incoming dynamic IPsec tunnel as the destination address of the policy instead of what you configure by using the <code>destination</code> command. The <code>no</code> command disables the setting.
[no] auto-disable	When you set <code>interface</code> or <code>trunk</code> as the next-hop type (using the <code>next-hop interface</code> or <code>next-hop trunk</code> command) for this route, you can use this command to have the UAG automatically disable this policy route when the next-hop's connection is down. The <code>no</code> command disables the setting.
[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage]	Sets the maximum bandwidth and priority for the policy. The <code>no</code> command removes bandwidth settings from the rule. You can also turn maximize bandwidth usage on or off.
conn-check {IPv4   FQDN } method {icmp   tcp} period <5..600> timeout <1..10> fail-tolerance <1..10> [port <1..65535>]	<p>Sets the domain name or IP address of the gateway to which the matched packets are routed. The UAG can regularly check the connection to the gateway you specified to make sure it is still available.</p> <p>icmp   tcp: Select how the UAG checks the connection. The gateway must be configured to respond to the method you select.</p> <p>period &lt;5..600&gt;: Enter the number of seconds between connection check attempts.</p> <p>timeout &lt;1..10&gt;: Enter the number of seconds to wait for a response before the attempt is a failure.</p> <p>fail-tolerance &lt;1..10&gt;: Enter the number of consecutive failures allowed before the UAG stops routing through the gateway.</p> <p>port &lt;1..65535&gt;: Specify the port number to use for a TCP connectivity check.</p>
[no] conn-check activate	Turns on the connection check. The <code>no</code> command disables it.
[no] deactivate	Disables the specified policy. The <code>no</code> command enables the specified policy.
[no] description <i>description</i>	Sets a descriptive name for the policy. The <code>no</code> command removes the name for the policy.
[no] destination { <i>address_object</i>  any}	Sets the destination IP address the matched packets must have. The <code>no</code> command resets the destination IP address to the default ( <code>any</code> ). <code>any</code> means all IP addresses.
[no] dscp {any   <0..63>}	Sets a custom DSCP code point (0~63). This is the DSCP value of incoming packets to which this policy route applies. <code>any</code> means all DSCP value or no DSCP marker.

**Table 60** Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[no] dscp class {default   <i>dscp_class</i> }	Sets a DSCP class. Use <code>default</code> to apply this policy route to incoming packets that are marked with DSCP value 0. Use one of the pre-defined AF classes (including af11~af13, af21~af23, af31~af33, and af41~af43) to apply this policy route to incoming packets that are marked with the DSCP AF class.  The “af” entries stand for Assured Forwarding. The number following the “af” identifies one of four classes and one of three drop preferences. See <a href="#">Assured Forwarding (AF) PHB for DiffServ on page 117</a> for more details.
dscp-marking <0..63>	Sets a DSCP value to have the UAG apply that DSCP value to the route's outgoing packets.
dscp-marking class {default   <i>dscp_class</i> }	Sets how the UAG handles the DSCP value of the outgoing packets that match this route. Set this to <code>default</code> to have the UAG set the DSCP value of the packets to 0. Set this to an “af” class (including af11~af13, af21~af23, af31~af33, and af41~af43) which stands for Assured Forwarding. The number following the “af” identifies one of four classes and one of three drop preferences. See <a href="#">Assured Forwarding (AF) PHB for DiffServ on page 117</a> for more details.
no dscp-marking	Use this command to have the UAG not modify the DSCP value of the route's outgoing packets.
exit	Leaves the sub-command mode.
[no] interface <i>interface_name</i>	Sets the interface on which the incoming packets are received. The <code>no</code> command resets the incoming interface to the default ( <code>any</code> ). <code>any</code> means all interfaces.
[no] next-hop {auto gateway <i>address_object</i>  interface <i>interface_name</i>  trunk <i>trunk_name</i>  tunnel <i>tunnel_name</i> }	Sets the next-hop to which the matched packets are routed. The <code>no</code> command resets next-hop settings to the default ( <code>auto</code> ).
[no] schedule <i>schedule_object</i>	Sets the schedule. The <code>no</code> command removes the schedule setting to the default ( <code>none</code> ). <code>none</code> means any time.
[no] service { <i>service_name</i>  any}	Sets the IP protocol. The <code>no</code> command resets service settings to the default ( <code>any</code> ). <code>any</code> means all services.
[no] snat {outgoing-interface pool { <i>address_object</i> }}	Sets the source IP address of the matched packets that use SNAT. The <code>no</code> command removes source NAT settings from the rule.
[no] source { <i>address_object</i>  any}	Sets the source IP address that the matched packets must have. The <code>no</code> command resets the source IP address to the default ( <code>any</code> ). <code>any</code> means all IP addresses.
[no] sslvpn <i>tunnel_name</i>	Sets the incoming interface to an SSL VPN tunnel. The <code>no</code> command removes the SSL VPN tunnel through which the incoming packets are received.
[no] trigger <1..8> incoming <i>service_name</i> trigger <i>service_name</i>	Sets a port triggering rule. The <code>no</code> command removes port trigger settings from the rule.
trigger append incoming <i>service_name</i> trigger <i>service_name</i>	Adds a new port triggering rule to the end of the list.
trigger delete <1..8>	Removes a port triggering rule.
trigger insert <1..8> incoming <i>service_name</i> trigger <i>service_name</i>	Adds a new port triggering rule before the specified number.
trigger move <1..8> to <1..8>	Moves a port triggering rule to the number that you specified.
[no] tunnel <i>tunnel_name</i>	Sets the incoming interface to an IPSec VPN tunnel. The <code>no</code> command removes the IPSec VPN tunnel through which the incoming packets are received.

**Table 60** Command Summary: Policy Route (continued)

COMMAND	DESCRIPTION
[no] user <i>user_name</i>	Sets the user name. The <code>no</code> command resets the user name to the default ( <code>any</code> ). <code>any</code> means all users.
[no] policy controll-ipsec-dynamic-rules activate	Enables the UAG to use policy routes to manually specify the destination addresses of dynamic IPsec rules. You must manually create these policy routes. The UAG automatically obtains source and destination addresses for dynamic IPsec rules that do not match any of the policy routes.  The <code>no</code> command has the UAG automatically obtain source and destination addresses for all dynamic IPsec rules.
policy default-route	Enters the policy-route sub-command mode to set a route with the name "default-route".
policy delete <i>policy_number</i>	Removes a routing policy.
policy flush	Clears the policy routing table.
policy list table	Displays all policy route settings.
policy move <i>policy_number</i> to <i>policy_number</i>	Moves a routing policy to the number that you specified.
[no] policy override-direct-route activate	Has the UAG forward packets that match a policy route according to the policy route instead of sending the packets to a directly connected network. Use the <code>no</code> command to disable it.
[no] policy controll-virtual-server-rules activate	Gives policy routes priority over NAT virtual server rules (1-1 SNAT). Use the <code>no</code> command to give NAT virtual server rules priority over policy routes.
show bwm activation	Displays whether or not the global setting for bandwidth management on the UAG is enabled.
show bwm-usage < [policy-route <i>policy_number</i> ]   [interface <i>interface_name</i> ]	Displays the specified policy route or interface's bandwidth allotment, current bandwidth usage, and bandwidth usage statistics.
show policy-route [ <i>policy_number</i> ]	Displays all or specified policy route settings.
show policy-route begin <1..200> end <1..200>	Displays the specified range of policy route settings.
show policy-route conn-check [<1..5000>]	Displays the connection check settings for the specified policy route.
show policy-route conn-check status [<1..5000>]	Displays the connection check status for the specified policy route.
show policy-route controll-ipsec-dynamic-rules	Displays whether the UAG checks policy routes first before IPsec dynamic rules.
show policy-route override-direct-route	Displays whether or not the UAG forwards packets that match a policy route according to the policy route instead of sending the packets to a directly connected network.
show policy-route controll-virtual-server-rules	Displays whether or not policy routes have priority over NAT virtual server rules (1-1 SNAT).
show policy-route rule_count	Displays the number of policy routes that have been configured on the UAG.
show policy-route underlayer-rules	Displays all policy route rule details for advanced debugging.

## 16.2.1 Assured Forwarding (AF) PHB for DiffServ

Assured Forwarding (AF) behavior is defined in RFC 2597. The AF behavior group defines four AF classes. Inside each class, packets are given a high, medium or low drop precedence. The drop precedence determines the probability that routers in the network will drop packets when congestion occurs. If congestion occurs between classes, the traffic in the higher class (smaller

numbered class) is generally given priority. Combining the classes and drop precedence produces the following twelve DSCP encodings from AF11 through AF43. The decimal equivalent is listed in brackets.

**Table 61** Assured Forwarding (AF) Behavior Group

	CLASS 1	CLASS 2	CLASS 3	CLASS 4
Low Drop Precedence	AF11 (10)	AF21 (18)	AF31 (26)	AF41 (34)
Medium Drop Precedence	AF12 (12)	AF22 (20)	AF32 (28)	AF42 (36)
High Drop Precedence	AF13 (14)	AF23 (22)	AF33 (30)	AF43 (38)

## 16.2.2 Policy Route Command Example

The following commands create two address objects (TW\_SUBNET and GW\_1) and insert a policy that routes the packets (with the source IP address TW\_SUBNET and any destination IP address) through the interface wan1 to the next-hop router GW\_1. This route uses the IP address of the outgoing interface as the matched packets' source IP address.

```

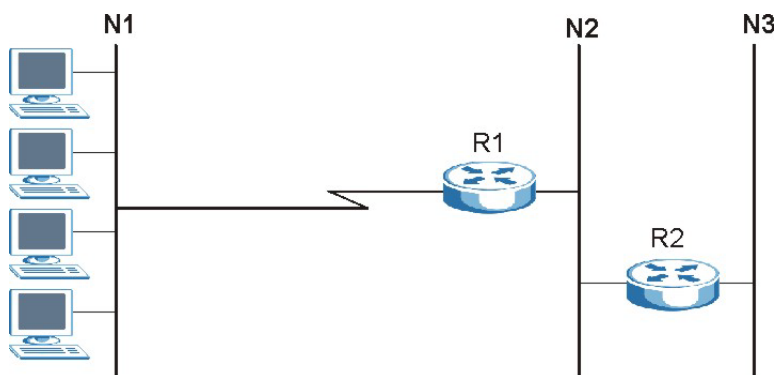
Router(config)# address-object TW_SUBNET 192.168.2.0 255.255.255.0
Router(config)# address-object GW_1 192.168.2.250
Router(config)# policy insert 1
Router(policy-route)# description example
Router(policy-route)# destination any
Router(policy-route)# interface gel
Router(policy-route)# next-hop gateway GW_1
Router(policy-route)# snat outgoing-interface
Router(policy-route)# source TW_SUBNET
Router(policy-route)# exit
Router(config)# show policy-route 1
index: 1
  active: yes
  description: example
  user: any
  schedule: none
  interface: wan1
  tunnel: none
  sslvpn: none
  source: TW_SUBNET
  destination: any
  DSCP code: any
  service: any
  nexthop type: Gateway
  nexthop: GW_1
  nexthop state: Not support
  auto destination: no
  bandwidth: 0
  bandwidth priority: 0
  maximize bandwidth usage: no
  SNAT: outgoing-interface
  DSCP marking: preserve
  amount of port trigger: 0
Router(config)#

```

## 16.3 IP Static Route

The UAG has no knowledge of the networks beyond the network that is directly connected to the UAG. For instance, the UAG knows about network **N2** in the following figure through gateway **R1**. However, the UAG is unable to route a packet to network **N3** because it doesn't know that there is a route through the same gateway **R1** (via gateway **R2**). The static routes are for you to tell the UAG about the networks beyond the network connected to the UAG directly.

**Figure 15** Example of Static Routing Topology



## 16.4 Static Route Commands

The following table describes the commands available for static route. You must use the `configure terminal` command to enter the configuration mode before you can use these commands. See [Section Table 59 on page 114](#) for information on input values.

**Table 62** Command Summary: Static Route

COMMAND	DESCRIPTION
<code>[no] ip route {w.x.y.z} {w.x.y.z} {interface w.x.y.z} &lt;0..127&gt;</code>	Sets a static route. The <code>no</code> command deletes a static route.
<code>ip route replace {w.x.y.z} {w.x.y.z} {interface w.x.y.z} &lt;0..127&gt; with {w.x.y.z} {w.x.y.z} {interface w.x.y.z} &lt;0..127&gt;</code>	Changes an existing route's settings.
<code>show ip route-settings</code>	Displays static route information. Use <code>show ip route</code> to see learned route information. See <a href="#">Section 17.2.5 on page 124</a> .
<code>[no] ip route control-virtual-server-rules activate</code>	Gives static routes priority over NAT virtual server rules (1-1 SNAT). It also automatically gives policy routes priority over NAT virtual server rules. Use the <code>no</code> command to give NAT virtual server rules priority over static routes.
<code>show ip route control-virtual-server-rules</code>	Displays whether or not static routes have priority over NAT virtual server rules (1-1 SNAT).

## 16.4.1 Static Route Commands Examples

The following command sets a static route with IP address 10.10.10.0 and subnet mask 255.255.255.0 and with the next-hop interface wan1. Then use the `show` command to display the setting.

```
Router(config)# ip route 10.10.10.0 255.255.255.0 wan1
Router(config)#
Router(config)# show ip route-settings
Route           Netmask           Nexthop           Metric
=====
10.10.10.0      255.255.255.0    ge1                0
```



## Routing Protocol

This chapter describes how to set up RIP and OSPF routing protocols for the UAG.

### 17.1 Routing Protocol Overview

Routing protocols give the UAG routing information about the network from other routers. The UAG then stores this routing information in the routing table, which it uses when it makes routing decisions. In turn, the UAG can also provide routing information via routing protocols to other routers.

The UAG supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared in [Table 63 on page 121](#), and they are discussed further in the next two sections.

**Table 63** OSPF vs. RIP

	OSPF	RIP
Network Size	Large	Small (with up to 15 routers)
Metric	Bandwidth, hop count, throughput, round trip time and reliability.	Hop count
Convergence	Fast	Slow

### 17.2 Routing Protocol Commands Summary

The following table describes the values required for many routing protocol commands. Other values are discussed with the corresponding commands.

**Table 64** Input Values for Routing Protocol Commands

LABEL	DESCRIPTION
<i>ip</i>	The 32-bit name of the area or virtual link in IP address format.
<i>authkey</i>	The password for text or MD5 authentication. You may use alphanumeric characters or underscores(_).  text password: 1-8 characters long MD5 password: 1-16 characters long

The following sections list the routing protocol commands.

## 17.2.1 RIP Commands

This table lists the commands for RIP.

**Table 65** router Commands: RIP

COMMAND	DESCRIPTION
router rip	Enters sub-command mode.
[no] network <i>interface_name</i>	Enables RIP on the specified Ethernet interface. The no command disables RIP on the specified interface.
[no] redistribute {static   ospf}	Enables redistribution of routing information learned from the specified source. The no command disables redistribution from the specified source.
redistribute {static   ospf} metric <0..16>	Sets the metric when redistributing routing information learned from the specified source.
[no] version <1..2>	Sets the default RIP version for all interfaces with RIP enabled. If the interface RIP version is blank, the interface uses the default version. This is not available in the GUI. The no command sets the default RIP version to 2.
[no] passive-interface <i>interface_name</i>	Sets the direction to "In-Only" for the specified interface. The no command sets the direction to bi-directional.
[no] authentication mode {md5   text}	Sets the authentication mode for RIP. The no command sets the authentication mode to "none".
[no] authentication string <i>authkey</i>	Sets the password for text authentication. The no command clears the password.
authentication key <1..255> key-string <i>authkey</i>	Sets the MD5 ID and password for MD5 authentication.
no authentication key	Clears the MD5 ID and password.
[no] outonly-interface <i>interface_name</i>	Sets the direction to "Out-Only" for the specified interface. The no command sets the direction to "BiDir".

## 17.2.2 General OSPF Commands

This table lists the commands for general OSPF configuration.

**Table 66** router Commands: General OSPF Configuration

COMMAND	DESCRIPTION
router ospf	Enters sub-command mode.
[no] redistribute {static   rip}	Enables redistribution of routing information learned from the specified non-OSPF source. The no command disables redistribution from the specified non-OSPF source.
[no] redistribute {static   rip} metric-type <1..2> metric <0..16777214>	Sets the metric for routing information learned from the specified non-OSPF source. The no command clears the metric.
[no] passive-interface <i>interface_name</i>	Sets the direction to "In-Only" for the specified interface. The no command sets the direction to "BiDir".
[no] router-id IP	Sets the 32-bit ID (in IP address format) of the UAG. The no command resets it to "default", or the highest available IP address.

## 17.2.3 OSPF Area Commands

This table lists the commands for OSPF areas.

**Table 67** router Commands: OSPF Areas

COMMAND	DESCRIPTION
router ospf	Enters sub-command mode.
[no] network <i>interface</i> area IP	Adds the specified interface to the specified area. The no command removes the specified interface from the specified area.
[no] area IP [{stub   nssa}]	Creates the specified area and sets it to the indicated type. The no command removes the area.
[no] area IP authentication	Enables text authentication in the specified area. The no command disables authentication in the specified area.
[no] area IP authentication message-digest	Enables MD5 authentication in the specified area. The no command disables authentication in the specified area.
[no] area IP authentication authentication-key <i>authkey</i>	Sets the password for text authentication in the specified area. The no command clears the password.
[no] area IP authentication message-digest-key <1..255> md5 <i>authkey</i>	Sets the MD5 ID and password for MD5 authentication in the specified area. The no command clears the MD5 ID and password.

## 17.2.4 Virtual Link Commands

This table lists the commands for virtual links in OSPF areas.

**Table 68** router Commands: Virtual Links in OSPF Areas

COMMAND	DESCRIPTION
show ospf area IP virtual-link	Displays information about virtual links for the specified area.
router ospf	
[no] area IP virtual-link IP	Creates the specified virtual link in the specified area. The no command removes the specified virtual link.
[no] area IP virtual-link IP authentication	Enables text authentication in the specified virtual link. The no command disables authentication in the specified virtual link.
[no] area IP virtual-link IP authentication message-digest	Enables MD5 authentication in the specified virtual link. The no command disables authentication in the specified virtual link.
[no] area IP virtual-link IP authentication authentication-key <i>authkey</i>	Sets the password for text authentication in the specified virtual link. The no command clears the password in the specified virtual link.
[no] area IP virtual-link IP authentication message-digest-key <1..255> md5 <i>authkey</i>	Sets the MD5 ID and password for MD5 authentication in the specified virtual link. The no command clears the MD5 ID and password in the specified virtual link.
[no] area IP virtual-link IP authentication same-as-area	Sets the virtual link's authentication method to the area's default authentication.
[no] area IP virtual-link IP authentication authentication-key <i>authkey</i>	Sets the password for text authentication in the specified virtual link. The no command clears the password.
area IP virtual-link IP message-digest-key <1..255> md5 <i>authkey</i>	Sets the MD5 ID and password for MD5 authentication in the specified virtual link.
no area IP virtual-link IP message-digest-key <1..255>	Clears the MD5 ID in the specified virtual link.

## 17.2.5 Learned Routing Information Commands

This table lists the commands to look at learned routing information.

**Table 69** ip route Commands: Learned Routing Information

COMMAND	DESCRIPTION
show ip route [kernel   connected   static   ospf   rip   bgp]	Displays learned routing and other routing information.

## 17.2.6 show ip route Command Example

The following example shows learned routing information on the UAG.

```
Router> show ip route
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask    Gateway          IFace           Metric    Flags    Persist
=====
0.0.0.0/0             172.16.1.254    wan1            0         ASG      -
127.0.0.0/8          0.0.0.0         lo              0         ACG      -
172.16.1.0/24        0.0.0.0         wan1            0         ACG      -
192.168.1.0/24       0.0.0.0         lan1            0         ACG      -
192.168.2.0/24       0.0.0.0         lan2            0         ACG      -
192.168.3.0/24       0.0.0.0         dmz             0         ACG      -
```

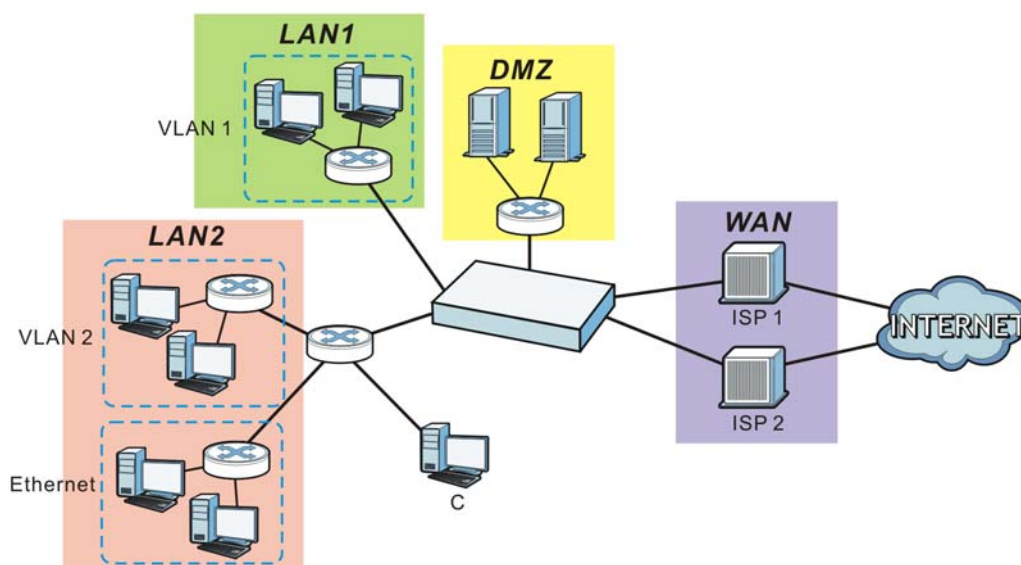
Set up zones to configure network security and network policies in the UAG.

## 18.1 Zones Overview

A zone is a group of interfaces and VPN tunnels. The UAG uses zones, not interfaces, in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface, and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

**Figure 16** Example: Zones



## 18.2 Zone Commands Summary

The following table describes the values required for many zone commands. Other values are discussed with the corresponding commands.

**Table 70** Input Values for Zone Commands

LABEL	DESCRIPTION
<i>profile_name</i>	<p>The name of a zone, or the name of a VPN tunnel.</p> <p>Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.</p> <p>About the pre-defined zones in the UAG:</p> <ul style="list-style-type: none"> <li>• The lan1 interface always belongs to the LAN1 zone.</li> <li>• The lan2 interface always belongs to the LAN2 zone.</li> <li>• The dmz interface always belongs to the DMZ zone.</li> <li>• The wan1, wan2, wan1_ppp, or wan2_ppp interfaces always belong to the WAN zone.</li> </ul>

This table lists the zone commands.

**Table 71** zone Commands

COMMAND	DESCRIPTION
<code>show zone [profile_name]</code>	Displays information about the specified zone or about all zones.
<code>show zone binding-iface</code>	Displays each interface and zone mappings.
<code>show zone default-binding</code>	Displays the pre-configured interface and zone mappings that come with the UAG.
<code>show zone none-binding</code>	Displays the interfaces, tunnels and SSL VPNs that are not associated with a zone yet.
<code>show zone system-default</code>	Displays the pre-configured default zones that you cannot delete from the UAG.
<code>show zone user-define</code>	Displays all customized zones.
<code>[no] zone profile_name</code>	Creates the zone if necessary and enters sub-command mode. The <code>no</code> command deletes the zone.
<code>zone profile_name</code>	Enter the sub-command mode.
<code>[no] block</code>	Blocks intra-zone traffic. The <code>no</code> command allows intra-zone traffic.
<code>[no] interface interface_name</code>	Adds the specified interface to the specified zone. The <code>no</code> command removes the specified interface from the specified zone. See <a href="#">Section 13.2 on page 86</a> for information about interface names.
<code>[no] crypto profile_name</code>	Adds the specified IPSec VPN tunnel to the specified zone. The <code>no</code> command removes the specified IPSec VPN tunnel from the specified zone.
<code>[no] sslvpn profile_name</code>	Adds the specified SSL VPN tunnel to the specified zone. The <code>no</code> command removes the specified SSL VPN tunnel from the specified zone.

## 18.2.1 Zone Command Examples

The following commands add interfaces vlan123 and vlan234 to zone A and block intra-zone traffic.

```

Router# configure terminal
Router(config)# zone A
Router(zone)# interface vlan123
Router(zone)# interface vlan234
Router(zone)# block
Router(zone)# exit
Router(config)# show zone
No. Name                               Block Member
=====
1  LAN1                                 no   lan1
2  LAN2                                 no   lan2
3  WAN                                  yes  wan1,wan2,wan1_ppp,wan2_ppp
4  DMZ                                  yes  dmz
5  SSL_VPN                              no
6  IPSec_VPN                            no
7  A                                     yes  vlan123,vlan234
Router(config)# show zone A
blocking intra-zone traffic: yes
No. Type                               Member
=====
1  interface                             vlan123
2  interface                             vlan234

```

This chapter describes how to configure dynamic DNS (DDNS) services for the UAG.

## 19.1 DDNS Overview

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

Set up a dynamic DNS account with a supported DNS service provider to be able to use Dynamic DNS services with the UAG. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the UAG supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

**Table 72** Network > DDNS

DDNS SERVICE PROVIDER	SERVICE TYPES SUPPORTED	WEBSITE	NOTES
DynDNS	Dynamic DNS, Static DNS, and Custom DNS	www.dyndns.com)	
Dynu	Basic, Premium	www.dynu.com	
No-IP	No-IP	www.no-ip.com	
Peanut Hull	Peanut Hull	www.oray.cn	Chinese website

Note: Record your DDNS account's user name, password, and domain name to use to configure the UAG.

After, you configure the UAG, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.



## 19.2 DDNS Commands Summary

The following table describes the values required for many DDNS commands. Other values are discussed with the corresponding commands.

**Table 73** Input Values for DDNS Commands

LABEL	DESCRIPTION
<i>profile_name</i>	The name of the DDNS profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table lists the DDNS commands.

**Table 74** ip ddns Commands

COMMAND	DESCRIPTION
<code>show ddns [<i>profile_name</i>]</code>	Displays information about the specified DDNS profile or about all DDNS profiles.
<code>[no] ip ddns profile <i>profile_name</i></code>	Creates the specified DDNS profile if necessary and enters sub-command mode. The <code>no</code> command deletes it.
<code>[no] service-type {dyndns   dyndns_static   dyndns_custom   dynu-basic   dynu-premium   no-ip   peanut-hull   3322-dyn   3322-static}</code>	Sets the service type in the specified DDNS profile. The <code>no</code> command clears it.
<code>[no] username <i>username</i> password <i>password</i></code>	Sets the username and password in the specified DDNS profile. The <code>no</code> command clears these fields.  <i>username</i> : You can use up to 31 alphanumeric characters and the underscore (_).  <i>password</i> : You can use up to 64 alphanumeric characters and the underscore (_).
<code>[no] host <i>hostname</i></code>	Sets the domain name in the specified DDNS profile. The <code>no</code> command clears the domain name.  <i>hostname</i> : You may up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
<code>[no] ip-select {iface   auto   custom}</code>	Sets the IP address update policy in the specified DDNS profile. The <code>no</code> command clears the policy.
<code>[no] ip-select-backup {iface   auto   custom}</code>	Sets the alternate IP address update policy in the specified DDNS profile. The <code>no</code> command clears the policy.
<code>[no] custom <i>ip</i></code>	Sets the static IP address in the specified DDNS profile. The <code>no</code> command clears it.
<code>[no] backup-custom <i>ip</i></code>	Sets the static IP address for the backup interface in the specified DDNS profile. The <code>no</code> command clears it.
<code>[no] mx {<i>ip</i>   <i>domain_name</i>}</code>	Enables the mail exchanger and sets the fully-qualified domain name of the mail server to which mail from this domain name is forwarded. The <code>no</code> command disables the mail exchanger.  <i>domain_name</i> : You may use up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
<code>[no] wan-iface <i>interface_name</i></code>	Sets the WAN interface in the specified DDNS profile. The <code>no</code> command clears it.

**Table 74** ip ddns Commands (continued)

COMMAND	DESCRIPTION
[no] backup-iface <i>interface_name</i>	Sets the backup WAN interface in the specified DDNS profile. The no command clears it.
[no] ha-iface <i>interface_name</i>	Sets the HA interface in the specified DDNS profile. The no command clears it.
[no] backmx	Enables the backup mail exchanger. The no command disables it.
[no] wildcard	Enables the wildcard feature. The no command disables it.
[no] https activate	Encrypts traffic using SSL (port 443), including traffic with username and password, to the DDNS server. Not all DDNS providers support this option.  The no command disables it.
[no] url <i>url</i>	Sets the URL that can be used to access the server that will host the DDNS service. For example, # url /api/dynamic/update.php?hostname=home.example.com& ip=10.1.1.1  The no command disables it.
[no] ddns-server <i>fqdn</i>	Sets the IP address of the server that will host the DDNS service. For example, # ddns-server www.dnspark.net  The no command disables it.
[no] additional-ddns-options {--dyndns_system   --ip_server_name}	Available for User custom. Enter one of the following. <ul style="list-style-type: none"> <li>--ip_server_name which should be the URL to get the server's public IP address - for example, http://myip.easylife.tw/</li> <li>--dyndns_system to specify the DYNDNS Server type - for example, dyndns@dyndns.org</li> </ul>

## 19.3 DDNS Commands Example

The following example sets up a DDNS profile where the interface is wan1 and uses HTTP.

```
Router# configure terminal
Router(config)# ip ddns profile bbb
# activate
# service-type user-custom
# username yjyeh001 password xxxxxx
# host yjye007.dyndns.org
# wan-iface wan1
# url /nic/update?
# ddns-server members.dyndns.org
# additional-ddns-options --dyndns_system dyndns@dyndns.org
```

## Virtual Servers

This chapter describes how to set up, manage, and remove virtual servers. Virtual server commands configure NAT.

### 20.1 Virtual Server Overview

Virtual server is also known as port forwarding or port translation.

Virtual servers are computers on a private network behind the UAG that you want to make available outside the private network. If the UAG has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

#### 20.1.1 1:1 NAT and Many 1:1 NAT

1:1 NAT - If the private network server will initiate sessions to the outside clients, use 1:1 NAT to have the UAG translate the source IP address of the server's outgoing traffic to the same public IP address that the outside clients use to access the server.

Many 1:1 NAT - If you have a range of private network servers that will initiate sessions to the outside clients and a range of public IP addresses, use many 1:1 NAT to have the UAG translate the source IP address of each server's outgoing traffic to the same one of the public IP addresses that the outside clients use to access the server. The private and public ranges must have the same number of IP addresses.

One many 1:1 NAT rule works like multiple 1:1 NAT rules, but it eases the configuration effort since you only create one rule.

### 20.2 Virtual Server Commands Summary

The following table describes the values required for many virtual server commands. Other values are discussed with the corresponding commands.

**Table 75** Input Values for Virtual Server Commands

LABEL	DESCRIPTION
<i>service_object</i>	The name of a service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>profile_name</i>	The name of the virtual server. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table lists the virtual server commands.

**Table 76** ip virtual-server Commands

COMMAND	DESCRIPTION
<code>show ip virtual-server [profile_name]</code>	Displays information about the specified virtual server or about all the virtual servers.
<code>no ip virtual-server profile_name</code>	Deletes the specified virtual server.
<code>ip virtual-server profile_name interface interface_name original-ip {any   ip   address_object} map-to {address_object   ip} map-type any [nat-loopback [nat-1-1-map] [deactivate]   nat-1-1-map [deactivate]   deactivate]</code>	<p>Creates or modifies the specified virtual server and maps the specified destination IP address (for all destination ports) to <a href="#">the specified destination address object or IP address</a>. The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (<i>address-object</i>). NAT loopback allows local users to use a domain name to access this virtual server.</p> <p>Select what kind of NAT this rule is to perform.</p> <p><code>nat-1-1-map</code>: means the NAT type is either 1:1 NAT or many 1:1 NAT. See <a href="#">Section 20.1.1 on page 131</a> for more information.</p> <p>Using this command without <code>nat-1-1-map</code> means the NAT type is Virtual Server. This makes computers on a private network behind the UAG available to a public network outside the UAG (like the Internet).</p> <p>The <code>deactivate</code> command disables the virtual server rule.</p>
<code>ip virtual-server profile_name interface interface_name original-ip {any   IP   address_object} map-to {address_object   ip} map-type port protocol {any   tcp   udp} original- port &lt;1..65535&gt; mapped-port &lt;1..65535&gt; [nat-loopback [nat-1-1- map] [deactivate]   nat-1-1-map [deactivate]   deactivate]</code>	<p>Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and destination port) to <a href="#">the specified (destination IP address and destination port)</a>. The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (<i>address-object</i>). NAT loopback allows local users to use a domain name to access this virtual server.</p> <p><code>nat-1-1-map</code>: means the NAT type is either 1:1 NAT or many 1:1 NAT. See <a href="#">Section 20.1.1 on page 131</a> for more information.</p> <p>Using this command without <code>nat-1-1-map</code> means the NAT type is Virtual Server. This makes computers on a private network behind the UAG available to a public network outside the UAG (like the Internet).</p> <p>The <code>deactivate</code> command disables the virtual server rule.</p>
<code>ip virtual-server profile_name interface interface_name original-ip {any   IP   address_object} map-to {address_object   ip} map-type ports protocol {any   tcp   udp} original- port-begin &lt;1..65535&gt; original-port- end &lt;1..65535&gt; mapped-port-begin &lt;1..65535&gt; [nat-loopback [nat-1-1- map] [deactivate]   nat-1-1-map [deactivate]   deactivate]</code>	<p>Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and range of destination ports) to <a href="#">the specified (destination IP address and range of destination ports)</a>. The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (<i>address-object</i>). NAT loopback allows local users to use a domain name to access this virtual server.</p> <p><code>nat-1-1-map</code>: means the NAT type is either 1:1 NAT or many 1:1 NAT. See <a href="#">Section 20.1.1 on page 131</a> for more information.</p> <p>Using this command without <code>nat-1-1-map</code> means the NAT type is Virtual Server. This makes computers on a private network behind the UAG available to a public network outside the UAG (like the Internet).</p> <p>The <code>deactivate</code> command disables the virtual server rule.</p>

**Table 76** ip virtual-server Commands (continued)

COMMAND	DESCRIPTION
<pre>ip virtual-server profile_name interface interface_name original-ip {any   IP   address_object} map-to {address_object   ip} map-type original-service service_object mapped-service service_object [nat- loopback [nat-1-1-map] [deactivate]   nat-1-1-map [deactivate]   deactivate]</pre>	<p>Creates or modifies the specified virtual server and maps the specified (destination IP address, protocol, and service object) to <a href="#">the specified (destination IP address and service object)</a>. The original destination IP is defined by the specified interface (any), the specified IP address (IP), or the specified address object (<i>address-object</i>). NAT loopback allows local users to use a domain name to access this virtual server.</p> <p><i>nat-1-1-map</i>: means the NAT type is either 1:1 NAT or many 1:1 NAT. See <a href="#">Section 20.1.1 on page 131</a> for more information.</p> <p>Using this command without <i>nat-1-1-map</i> means the NAT type is Virtual Server. This makes computers on a private network behind the UAG available to a public network outside the UAG (like the Internet).</p> <p>The <i>deactivate</i> command disables the virtual server rule.</p>
<pre>ip virtual-server {activate   deactivate} profile_name</pre>	Activates or deactivates the specified virtual server.
<pre>ip virtual-server delete profile_name</pre>	Deletes the specified virtual server.
<pre>ip virtual-server flush</pre>	Deletes all virtual servers.
<pre>ip virtual-server insert rule_number</pre>	Adds a rule before the specified rule number.
<pre>ip virtual-server move rule_number to rule_number</pre>	Moves a rule to the number you specified.
<pre>ip virtual-server rename profile_name profile_name</pre>	Renames the specified virtual server from the first <i>profile_name</i> to the second <i>profile_name</i> .

## 20.2.1 Virtual Server Command Examples

The following command creates virtual server WAN-LAN\_H323 on the wan1 interface that maps IP addresses 10.0.0.8 to 192.168.1.56. for TCP protocol traffic on port 1720. It also adds a NAT loopback entry.

```
Router# configure terminal
Router(config)# ip virtual-server WAN-LAN_H323 interface wan1 original-ip 10.0.0.8
map-to 192.168.1.56 map-type port protocol tcp original-port 1720 mapped-port 1720
nat-loopback
Router(config)#
```

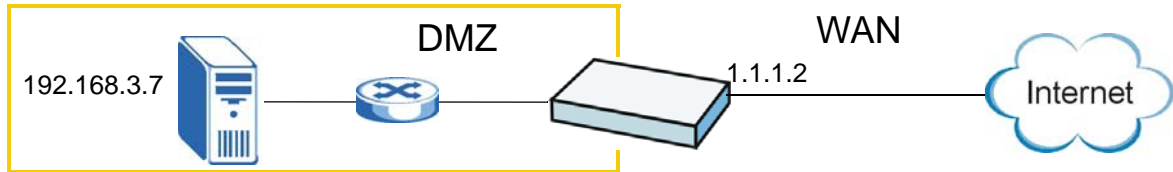
The following command shows information about all the virtual servers in the UAG.

```
Router(config)# show ip virtual-server
virtual server: WAN-LAN_H323
  active: yes
  interface: wan1
  NAT-loopback active: yes
  NAT 1-1: no
  original IP: 10.0.0.8
  mapped IP: 192.168.1.56
  mapping type: port
  protocol type: tcp
  original service:
  mapped service:
  original start port: 1720
  original end port:
  mapped start port: 1720
  mapped end port:
Router(config)#
```

## 20.2.2 Tutorial - How to Allow Public Access to a Server

This is an example of making an HTTP (web) server in the DMZ zone accessible from the Internet (the WAN zone). You will use a public IP address of 1.1.1.2 on the wan1 interface and map it to the HTTP server's private IP address of 192.168.3.7.

**Figure 17** Public Server Example Network Topology



Follow the following steps for the setting.

### 1 Configure Address object

Create two address objects. One is named DMZ\_HTTP for the HTTP server's private IP address of 192.168.3.7. The other one is named wan1\_HTTP for the wan1 public IP address of 1.1.1.2.

```
Router# configure terminal
Router(config)# address-object DMZ_HTTP 192.168.3.7
Router(config)# address-object wan1_HTTP 1.1.1.2
Router(config)#
```

### 2 Configure NAT

You need a NAT rule to send HTTP traffic coming to IP address 1.1.1.2 on wan1 to the HTTP server's private IP address of 192.168.3.7. Use the following settings:

- This NAT rule is for any HTTP traffic coming in on wan1 to IP address 1.1.1.2.
- The NAT rule sends this traffic to the HTTP server's private IP address of 192.168.3.7 (defined in the DMZ\_HTTP object).

- HTTP traffic and the HTTP server in this example both use TCP port 80. So you set the port mapping type to “port”, the protocol type to “TCP”, and the original and mapped ports to “80”.

```
Router(config)# ip virtual-server To-VirtualServer-WWW interface wan1 original-ip
wan1_HTTP map-to DMZ_HTTP map-type port protocol tcp original-port 80 mapped-port 80
Router(config)#
```

### 3 Configure firewall

Create a firewall rule to allow HTTP traffic from the WAN zone to the DMZ web server.

```
Router(config)# firewall insert 1
Router(config)# description To-VirtualServer-WWW
Router(config)# from WAN
Router(config)# to DMZ
Router(config)# destinationip DMZ_HTTP
Router(config)# service HTTP
Router(config)# exit
Router(config)# write
Router(config)#
```

Now the public can go to IP address 1.1.1.2 to access the HTTP server.

## VPN 1-1 Mapping

This chapter shows you how to configure VPN 1-1 mapping on your UAG.

### 21.1 VPN 1-1 Mapping Overview

VPN 1-1 mapping allows an authenticated user in your network to access the Internet or an external server using a public IP address different from the one used by the UAG's WAN interface. With VPN 1-1 mapping, each user that logs into the UAG and matches a pre-configured mapping rule can obtain an individual public IP address. This helps especially when multiple users need to access different remote servers through separate VPN tunnels via the UAG. Each user can use a unique public IP address to transmit traffic through a separate VPN tunnel. The VPN connection will not be disconnected due to response packets with the same source IP address coming from remote servers in different VPN tunnels.

### 21.2 VPN 1-1 Mapping Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 77** Input Values for vpn-1-1-map Commands

LABEL	DESCRIPTION
<i>interface_name</i>	The name of the interface. This depends on the UAG model. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.
<i>profile_name</i>	The name of the pool profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>address_object</i>	The name of an IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>user_name</i>	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.



The following table describes the commands available for VPN 1-1 mapping. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

**Table 78** Command Summary: `vpn-1-1-map`

COMMAND	DESCRIPTION
<code>[no] vpn-1-1-map activate</code>	Enables VPN 1-1 mapping on the UAG. The <code>no</code> command disables VPN 1-1 mapping on the UAG.
<code>[no] vpn-1-1-map pool profile_name</code>	Enters the <code>vpn-1-1-map pool</code> sub-command mode to create the specified VPN 1-1 mapping pool profile. See <a href="#">Table 79 on page 138</a> for the sub-commands. The <code>no</code> command removes the pool profile.  A pool profile defines the public IP address(es) that the UAG assigns to the matched users and the interface through which the user's traffic is forwarded.
<code>[no] vpn-1-1-map rule &lt;1..16&gt;</code>	Enters the <code>vpn-1-1-map rule</code> sub-command mode to create the specified VPN 1-1 mapping rule. See <a href="#">Table 80 on page 138</a> for the sub-commands. The <code>no</code> command removes the rule.
<code>vpn-1-1-map pool rename profile_name profile_name</code>	Renames the specified VPN 1-1 mapping pool profile (first <code>profile_name</code> ) to the specified name (second <code>profile_name</code> ).
<code>vpn-1-1-map rule append</code>	Enters the <code>vpn-1-1-map rule</code> sub-command mode to create a new VPN 1-1 mapping rule at the end of the current list. See <a href="#">Table 80 on page 138</a> for the sub-commands.
<code>vpn-1-1-map rule flush</code>	Clears all VPN 1-1 mapping rules.
<code>vpn-1-1-map rule insert &lt;1..16&gt;</code>	Enters the <code>vpn-1-1-map rule</code> sub-command mode to add a new VPN 1-1 mapping rule before the specified rule number. See <a href="#">Table 80 on page 138</a> for the sub-commands.
<code>vpn-1-1-map rule move &lt;1..16&gt; to &lt;1..16&gt;</code>	Moves the specified rule to the specified location and renumbers the other rules accordingly.
<code>show vpn-1-1-map activation</code>	Shows whether the VPN 1-1 mapping feature is enabled or disabled on the UAG.
<code>show vpn-1-1-map pool [profile_name]</code>	Displays settings of the specified or all pool profiles.
<code>show vpn-1-1-map rule [&lt;1..16&gt;]</code>	Displays settings of the specified or all VPN 1-1 mapping rules.
<code>show vpn-1-1-map rule begin &lt;1..16&gt; end &lt;1..16&gt;</code>	Displays settings for a range of VPN 1-1 mapping rules.
<code>show vpn-1-1-map statistics summary</code>	Displays statistics for each of the VPN 1-1 mapping rules
<code>show vpn-1-1-map user-mapping summary</code>	Displays the status of the active users to which the UAG applied a VPN 1-1 mapping rule

## 21.2.1 vpn-1-1-map pool Sub-commands

The following table describes the sub-commands for the vpn-1-1-map pool command.

**Table 79** vpn-1-1-map pool Sub-commands

COMMAND	DESCRIPTION
<code>address address_object</code>	Configures the name of the IP address object the profile is set to use. An address object presents the IP address(es), which can be assigned to the matched users by the UAG.  Note: You cannot configure an address group object at the time of writing.  Note: It's recommended that the IP addresses of the configured address object and the WAN interface are in the same subnet so that the UAG can receive response packets from the remote node.
<code>exit</code>	Leaves the sub-command mode.
<code>interface interface_name</code>	Sets the interface through which the UAG sends traffic from the matched users.

## 21.2.2 vpn-1-1-map pool Command Examples

The following commands create a pool profile and display the settings.

```
Router# configure terminal
Router(config)# vpn-1-1-map pool pool1
Router(vpn-1-1-map-pool-pool1)# address WAN-1
Router(vpn-1-1-map-pool-pool1)# interface wan1
Router(vpn-1-1-map-pool-pool1)# exit
Router(config)# show vpn-1-1-map pool
Pool: pool1
  address: WAN-1
  interface: wan1
Router(config)#
```

## 21.2.3 vpn-1-1-map rule Sub-commands

The following table describes the sub-commands for several vpn-1-1-map rule commands. Note that not all rule commands use all the sub-commands listed here.

**Table 80** vpn-1-1-map rule Sub-commands

COMMAND	DESCRIPTION
<code>activate</code>	Enables the VPN 1-1 mapping rule.
<code>deactivate</code>	Disables the VPN 1-1 mapping rule.
<code>exit</code>	Leaves the sub-command mode.
<code>flush pool</code>	Removes all pool profile(s) and resets the pool profile setting to the default (any). any means all IP address.

**Table 80** vpn-1-1-map rule Sub-commands (continued)

COMMAND	DESCRIPTION
[no] pool <i>profile_name</i>	Sets the name of the pool profile used by this rule. You can associate up to four pool profiles to a VPN 1-1 mapping rule. The <code>no</code> command removes the specified pool file.
[no] user { <i>user_name</i>  any}	Sets the user or user group for which you want to use this rule. The <code>no</code> command resets the user setting to the default ( <code>any</code> ). <code>any</code> means all users.

## 21.2.4 vpn-1-1-map rule Command Examples

The following commands create a VPN 1-1 mapping rule, enable it and display the settings.

```
Router# configure terminal
Router(config)# vpn-1-1-map rule 1
Router(vpn-1-1-map-rule-1)# activate
Router(vpn-1-1-map-rule-1)# pool pool1
Router(vpn-1-1-map-rule-1)# pool pool2
Router(vpn-1-1-map-rule-1)# user Michael
Router(vpn-1-1-map-rule-1)# exit
Router(config)# show vpn-1-1-map rule
Rule: 1
  active: yes
  user: Michael
  pool: pool1,pool2
Router(config)#
```

## 21.2.5 vpn-1-1-map statistics Command Examples

The following command shows statistics for each of the VPN 1-1 mapping rules. This displays how many times the UAG applied the rule to a user successfully or failed to apply the rule to a user. This also shows the maximum number of times the UAG has applied the rule to a user successfully.

```
Router# show vpn-1-1-map statistics summary
Rule: 1
  active: yes
  user: Michael
  pool: pool1
  assigned: 0
  failed: 0
  peak usage: 0
Router#
```

# HTTP Redirect

This chapter shows you how to configure HTTP redirection on your UAG.

## 22.1 HTTP Redirect Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the UAG) to a web proxy server.

### 22.1.1 Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

## 22.2 HTTP Redirect Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 81** Input Values for HTTP Redirect Commands

LABEL	DESCRIPTION
<i>description</i>	The name to identify the rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>interface_name</i>	The name of the interface. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.

The following table describes the commands available for HTTP redirection. You must use the configure terminal command to enter the configuration mode before you can use these commands.

**Table 82** Command Summary: HTTP Redirect

COMMAND	DESCRIPTION
<code>ip http-redirect <i>description</i> interface <i>interface_name</i> redirect-to <i>w.x.y.z</i> &lt;1..65535&gt;</code>	Sets a HTTP redirect rule.
<code>ip http-redirect <i>description</i> interface <i>interface_name</i> redirect-to <i>w.x.y.z</i> &lt;1..65535&gt; deactivate</code>	Disables a HTTP redirect rule.
<code>ip http-redirect activate <i>description</i></code>	Enables a rule with the specified rule name.

**Table 82** Command Summary: HTTP Redirect (continued)

COMMAND	DESCRIPTION
<code>ip http-redirect deactivate <i>description</i></code>	Disables a rule with the specified rule name.
<code>no ip http-redirect <i>description</i></code>	Removes a rule with the specified rule name.
<code>ip http-redirect flush</code>	Clears all HTTP redirect rules.
<code>show ip http-redirect [<i>description</i>]</code>	Displays HTTP redirect settings.

## 22.2.1 HTTP Redirect Command Examples

The following commands create a HTTP redirect rule, disable it and display the settings.

```
Router# configure terminal
Router(config)# ip http-redirect example1 interface lan1 redirect-to 10.10.2.3 80
Router(config)# ip http-redirect example1 interface lan1 redirect-to 10.10.2.3 80
deactivate
Router(config)# show ip http-redirect
Name                               Interface    Proxy Server    Port    Active
=====
example1                            lan1        10.10.2.3      80     no
```

## SMTP Redirect

This chapter shows you how to configure SMTP redirection on your UAG.

### 23.1 SMTP Redirect Overview

SMTP redirect forwards the authenticated client's SMTP message to a SMTP server, that handles all outgoing e-mail messages. The UAG forwards SMTP traffic using TCP port 25.

#### 23.1.1 SMTP

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of e-mail messages between servers. E-mail clients (also called e-mail applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve e-mail. E-mail clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many e-mail applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

### 23.2 SMTP Redirect Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 83** Input Values for SMTP Redirect Commands

LABEL	DESCRIPTION
<i>interface_name</i>	The name of the interface. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.
<i>domain_name</i>	Fully-qualified domain name. You may use up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character must be alphanumeric.
<i>address_object</i>	The name of an IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>user_name</i>	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for SMTP redirection. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

**Table 84** Command Summary: SMTP Redirect

COMMAND	DESCRIPTION
<code>[no] smtp-redirect &lt;1..16&gt;</code>	Enters the <code>smtp-redirect</code> sub-command mode to set a SMTP redirect rule. The <code>no</code> command removes the rule. See <a href="#">Table 85 on page 143</a> for the sub-commands.
<code>[no] smtp-redirect activate</code>	Enables SMTP redirect on the UAG. The <code>no</code> command disables SMTP redirect on the UAG.
<code>smtp-redirect append</code>	Enters the <code>smtp-redirect</code> sub-command mode to create a new SMTP redirect rule at the end of the current list. See <a href="#">Table 85 on page 143</a> for the sub-commands.
<code>smtp-redirect flush</code>	Clears all SMTP redirect rules.
<code>smtp-redirect insert &lt;1..16&gt;</code>	Enters the <code>smtp-redirect</code> sub-command mode to add a new SMTP redirect rule before the specified rule number. See <a href="#">Table 85 on page 143</a> for the sub-commands.
<code>smtp-redirect move &lt;1..16&gt; to &lt;1..16&gt;</code>	Moves the specified rule to the specified location and renumbers the other rules accordingly.
<code>show smtp-redirect [&lt;1..16&gt;]</code>	Displays settings of the specified or all SMTP redirect rules.
<code>show smtp-redirect activation</code>	Shows whether the SMTP redirect feature is enabled or disabled on the UAG.
<code>show smtp-redirect begin &lt;1..16&gt; end &lt;1..16&gt;</code>	Displays settings for a range of SMTP redirect rules.

## 23.2.1 smtp-redirect Sub-commands

The following table describes the sub-commands for several `smtp-redirect` commands. Note that not all rule commands use all the sub-commands listed here.

**Table 85** smtp-redirect Sub-commands

COMMAND	DESCRIPTION
<code>[no] activate</code>	Enables the SMTP redirect rule. The <code>no</code> command disables the rule.
<code>exit</code>	Leaves the sub-command mode.
<code>[no] interface {interface_name any}</code>	Sets the interface on which the SMTP traffic must be received for the UAG to forward it to the specified SMTP server. The <code>no</code> command resets the interface setting to the default ( <code>any</code> ). <code>any</code> means all interfaces.
<code>[no] server {domain_name ip}</code>	Sets the domain name or the IP address of the SMTP server.
<code>[no] source {address_object any}</code>	Sets the source IP address or address group from which the SMTP traffic should be sent. The <code>no</code> command resets the source setting to the default ( <code>any</code> ). <code>any</code> means all IP address.
<code>[no] user {user_name any}</code>	Sets the user or user group for which you want to use this rule. The <code>no</code> command resets the user setting to the default ( <code>any</code> ). <code>any</code> means all users.

## 23.2.2 SMTP Redirect Command Examples

The following commands create a SMTP redirect rule, enable it and display the settings.

```
Router# configure terminal
Router(config)# smtp-redirect 1
Router(smtp-redirect)# activate
Router(smtp-redirect)# interface lan2
Router(smtp-redirect)# server smtp.zyxel.com.tw
Router(smtp-redirect)# source lan1_1
Router(smtp-redirect)# user admin
Router(smtp-redirect)# exit
Router(config)# show smtp-redirect
smtp redirect rule: 1
  active: yes
  user: admin
  incoming interface: lan2
  source address: any
  smtp server: smtp.zyxel.com.tw
Router(config)#
```



This chapter covers how to use the UAG's ALG feature to allow certain applications to pass through the UAG.

## 24.1 ALG Introduction

The UAG can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the UAG's NAT.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The UAG examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the UAG uses an application for which the UAG has VoIP pass through enabled, the UAG translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

The UAG only needs to use the ALG feature for traffic that goes through the UAG's NAT. The firewall allows related sessions for VoIP applications that register with a server. The firewall allows or blocks peer to peer VoIP traffic based on the firewall rules.

You do not need to use a TURN (Traversal Using Relay NAT) server for VoIP devices behind the UAG when you enable the SIP ALG.

## 24.2 ALG Commands

The following table lists the alg commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 86** alg Commands

COMMAND	DESCRIPTION
<pre>[no] alg sip [inactivity- timeout   signal-port &lt;1025..65535&gt;   signal- extra-port &lt;1025..65535&gt;   media-timeout &lt;1..86400&gt;   signal-timeout &lt;1..86400&gt;   transformation]</pre>	<p>Turns on or configures the ALG.</p> <p>Use <code>inactivity-timeout</code> to have the UAG apply SIP media and signaling inactivity time out limits.</p> <p>Use <code>signal-port</code> with a listening port number (1025 to 65535) if you are using SIP on a port other than UDP 5060.</p> <p>Use <code>signal-extra-port</code> with a listening port number (1025 to 65535) if you are also using SIP on an additional UDP port number, enter it here.</p> <p>Use <code>media-timeout</code> and a number of seconds (1~86400) for how long to allow a voice session to remain idle (without voice traffic) before dropping it.</p> <p>Use <code>signal-timeout</code> and a number of seconds (1~86400) for how long to allow a SIP signaling session to remain idle (without SIP packets) before dropping it.</p> <p>Use <code>transformation</code> to have the UAG modify IP addresses and port numbers embedded in the SIP data payload. You do not need to use this if you have a SIP device or server that will modify IP addresses and port numbers embedded in the SIP data payload.</p> <p>The <code>no</code> command turns off the SIP ALG or removes the settings that you specify.</p>
<pre>[no] alg &lt;h323   ftp&gt; [signal-port &lt;1025..65535&gt;   signal-extra-port &lt;1025..65535&gt;   transformation]</pre>	<p>Turns on or configures the H.323 or FTP ALG.</p> <p>Use <code>signal-port</code> with a listening port number (1025 to 65535) if you are using H.323 on a TCP port other than 1720 or FTP on a TCP port other than 21.</p> <p>Use <code>signal-extra-port</code> with a listening port number (1025 to 65535) if you are also using H.323 or FTP on an additional TCP port number, enter it here.</p> <p>Use <code>transformation</code> to have the UAG modify IP addresses and port numbers embedded in the H.323 or FTP data payload. You do not need to use this if you have an H.323 or FTP device or server that will modify IP addresses and port numbers embedded in the H.323 or FTP data payload.</p> <p>The <code>no</code> command turns off the H.323 or FTP ALG or removes the settings that you specify.</p>
<pre>[no] alg sip defaultport &lt;1..65535&gt;</pre>	<p>Adds (or removes) a custom UDP port number for SIP traffic.</p>
<pre>show alg &lt;sip   h323   ftp&gt;</pre>	<p>Displays the specified ALG's configuration.</p>

## 24.3 ALG Commands Example

The following example turns on pass through for SIP and turns it off for H.323.

```
Router# configure terminal
Router(config)# alg sip
Router(config)# no alg h323
```

## 25.1 UPnP and NAT-PMP Overview

The UAG supports both UPnP and NAT-PMP to permit networking devices to discover each other and connect seamlessly.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. A gateway that supports UPnP is called Internet Gateway Device (IGD). The standardized Device Control Protocol (DCP) is defined by the UPnP Forum for IGDs to configure port mapping automatically.

NAT Port Mapping Protocol (NAT-PMP), introduced by Apple and implemented in current Apple products, is used as an alternative NAT traversal solution to the UPnP IGD protocol. NAT-PMP runs over UDP port 5351. NAT-PMP is much simpler than UPnP IGD and mainly designed for small home networks. It allows a client behind a NAT router to retrieve the router's public IP address and port number and make them known to the peer device with which it wants to communicate. The client can automatically configure the NAT router to create a port mapping to allow the peer to contact it.

## 25.2 UPnP and NAT-PMP Commands

The following table lists the `ip upnp` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 87** ip upnp Commands

COMMAND	DESCRIPTION
<code>ip upnp</code>	Enters the <code>config-upnp</code> sub-command mode to configure the UPnP or NAT-PMP settings.
<code>[no] bypass-firewall activate</code>	Allows traffic from UPnP-enabled or NAT-PMP-enabled applications to bypass the firewall.  The <code>no</code> command has the firewall block all UPnP or NAT-PMP application packets (for example, MSN packets).
<code>link-sticking outgoing interface {interface_name   all}</code>	Specifies through which WAN interface(s) you want to send out traffic from UPnP-enabled or NAT-PMP-enabled applications.  If the WAN interface you specified loses its connection, the UAG attempts to use the other WAN interface. If the other WAN interface also does not work, the UAG drops outgoing packets from UPnP-enabled or NAT-PMP-enabled applications.
<code>[no] listen-interface interface_name</code>	Enables UPnP and/or NAT-PMP on an internal interface.  The <code>no</code> command disables UPnP and/or NAT-PMP on the interface.

**Table 87** ip upnp Commands (continued)

COMMAND	DESCRIPTION
[no] nat-pmp activate	Enables NAT-PMP on the UAG. The no command disables NAT-PMP on the UAG.
[no] upnp-igd activate	Enables UPnP on the UAG. The no command disables UPnP on the UAG.
no ip upnp port-mapping port {<1..65535> type <tcp udp>   all}	Removes all or a specific port mapping rule.
show ip upnp listen-interface	Displays the name(s) of the internal interface(s) on which the UAG supports UPnP and/or NAT-PMP.
show ip upnp port-mapping	Displays the UPnP and/or NAT-PMP port mapping rules on the UAG.
show ip upnp status	Displays the UPnP and/or NAT-PMP configuration.

## 25.3 UPnP & NAT-PMP Commands Example

The following example turns on UPnP and NAT-PMP on the UAG and its two LAN interfaces. It also shows the UPnP and NAT-PMP settings.

```

Router# configure terminal
Router(config)# ip upnp
Router(config-upnp)# nat-pmp activate
Router(config-upnp)# upnp-igd activate
Router(config-upnp)# listen-interface lan1
Router(config-upnp)# listen-interface lan2
Router(config-upnp)# exit
Router(config)# show ip upnp status
upnp active: yes
nat-pmp active: yes
bypass-firewall active: no
link-sticking outgoing: all
Router(config)# show ip upnp listen-interface
interface
=====
lan1
lan2
Router(config)#

```

The following example displays the UAG's port mapping entries and removes the entry with the specified port number and protocol type.

```
Router# configure terminal
Router(config) # show ip upnp port-mapping
No: 0
  Remote Host: (null)
  Client Type: upnp
  External Port: 1122
  Protocol: tcp
  Internal Port: 1122
  Internal Client: 172.16.1.2
  Description: test1
No: 1
  Remote Host: (null)
  Client Type: upnp
  External Port: 5566
  Protocol: tcp
  Internal Port: 5566
  Internal Client: 172.16.1.2
  Description: test2
Router(config)# no ip upnp port-mapping port 5566 type tcp
Router(config)# show ip upnp port-mapping
No: 0
  Remote Host: (null)
  Client Type: upnp
  External Port: 1122
  Protocol: tcp
  Internal Port: 1122
  Internal Client: 172.16.1.2
  Description: test1
Router(config)#
```

## IP/MAC Binding

### 26.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The UAG uses DHCP to assign IP addresses and records to MAC address it assigned each IP address. The UAG then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the UAG.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer with another MAC address that tries to use IP address 192.168.1.27.

### 26.2 IP/MAC Binding Commands

The following table lists the `ip-mac-binding` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 88** ip-mac-binding Commands

COMMAND	DESCRIPTION
<code>[no] ip ip-mac-binding <i>interface_name</i> activate</code>	Turns on IP/MAC binding for the specified interface. The <code>no</code> command turns IP/MAC binding off for the specified interface.
<code>[no] ip ip-mac-binding <i>interface_name</i> log</code>	Turns on the IP/MAC binding logs for the specified interface. The <code>no</code> command turns IP/MAC binding logs off for the specified interface.
<code>ip ip-mac-binding exempt <i>name start-ip end-ip</i></code>	Adds a named IP range as being exempt from IP/MAC binding.
<code>no ip ip-mac-binding exempt <i>name</i></code>	Deletes the named IP range from the list of addresses that are exempt from IP/MAC binding.
<code>show ip ip-mac-binding <i>interface_name</i></code>	Shows whether IP/MAC binding is enabled or disabled for the specified interface.
<code>show ip ip-mac-binding all</code>	Shows whether IP/MAC binding is enabled or disabled for all interfaces.
<code>show ip ip-mac-binding status <i>interface_name</i></code>	Displays the current IP/MAC bindings for the specified interface.
<code>show ip ip-mac-binding status all</code>	Displays the current IP/MAC bindings for all interfaces.
<code>show ip ip-mac-binding exempt</code>	Shows the current IP/MAC binding exempt list.
<code>ip ip-mac-binding clear-drop-count <i>interface_name</i></code>	Resets the packet drop counter for the specified interface.
<code>debug ip ip-mac-binding activate</code>	Turns on the IP/MAC binding debug logs.
<code>no debug ip ip-mac-binding activate</code>	Turns off the IP/MAC binding debug logs.

## 26.3 IP/MAC Binding Commands Example

The following example enables IP/MAC binding on the lan1 interface and displays the interface's IP/MAC binding status.

```
Router# configure terminal
Router(config)# ip ip-mac-binding lan1 activate
Router(config)# show ip ip-mac-binding lan1
Name: lan1
Status: Enable
Log: No
Binding Count: 0
Drop Count: 0
Router(config)#
```



## Layer 2 Isolation

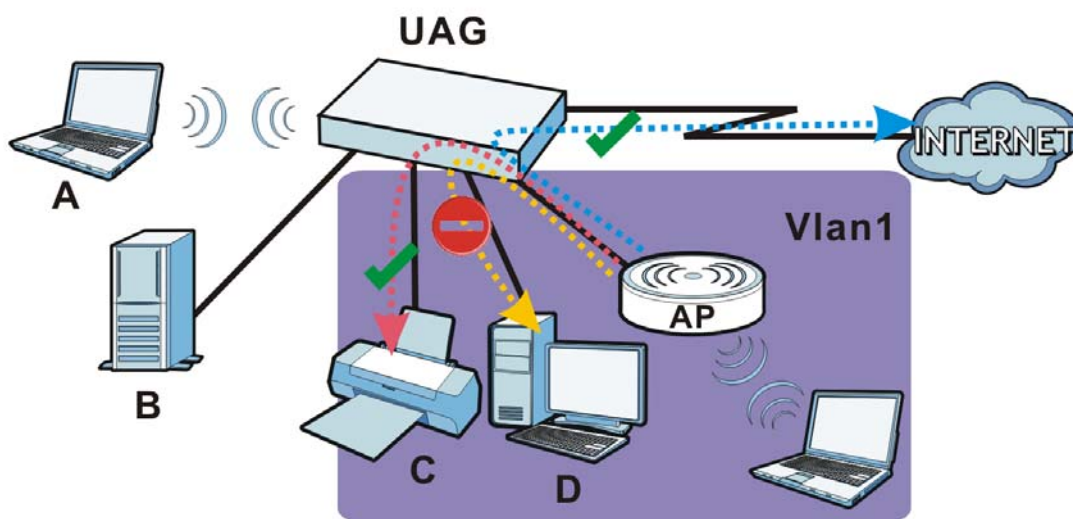
### 27.1 Layer 2 Isolation Overview

Layer-2 isolation is used to prevent connected devices from communicating with each other in the UAG's local network(s), on which layer-2 isolation is enabled, except the devices in the white list.

Note: Layer-2 isolation does not check the wireless traffic.

In the following example, layer-2 isolation is enabled on the UAG's interface Vlan1. A printer, PC and AP are in the Vlan1. The IP address of network printer (C) is added to the white list. The connected AP then cannot communicate with the PC (D), but can access the network printer (C), server (B), wireless client (A) and the Internet.

**Figure 18** Layer-2 Isolation Application



## 27.2 Layer 2 Isolation Commands

The following table lists the `l2-isolation` commands. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 89** l2-isolation Commands

COMMAND	DESCRIPTION
<code>l2-isolation</code>	Enters the layer 2 isolation sub-command mode to enable Layer-2 isolation on the UAG and specific internal interface(s).
<code>[no] activate</code>	Turns on Layer-2 isolation on the UAG. The <code>no</code> command disables Layer-2 isolation on the UAG.
<code>[no] interface interface_name</code>	Turns on Layer-2 isolation on a specific internal interface. The <code>no</code> command disables Layer-2 isolation for the specified interface.
<code>white-list rule_number</code>	Enters the layer 2 isolation white list sub-command mode to set a new rule in the white list. See <a href="#">Table 90 on page 154</a> for the sub-commands.  <i>rule_number</i> : 1 - N, where N depends on the UAG model.
<code>white-list activate</code>	Turns on the white list on the UAG.  IP addresses that are not listed in the white list are blocked from communicating with other devices in the layer-2-isolation-enabled internal interface(s) except for broadcast packets.
<code>white-list append</code>	Enters the layer 2 isolation white list sub-command mode to add a rule to the end of the white list. See <a href="#">Table 90 on page 154</a> for the sub-commands.
<code>white-list flush</code>	Removes all rules in the white list.
<code>white-list no activate</code>	Turns the white list off.
<code>no l2-isolation activate</code>	Disables Layer-2 isolation on the UAG.
<code>no l2-isolation white-list rule_number</code>	Disables the specified rule in the white list.  <i>rule_number</i> : 1 - N, where N depends on the UAG model.
<code>no l2-isolation white-list activate</code>	Turns on the white list on the UAG.
<code>show l2-isolation</code>	Displays whether Layer-2 isolation is enabled on an interface.
<code>show l2-isolation activation</code>	Displays whether Layer-2 isolation is enabled on the UAG.
<code>show l2-isolation white-list [rule_number]</code>	Displays all or a specified white list rule settings.  <i>rule_number</i> : 1 - N, where N depends on the UAG model.
<code>show l2-isolation white-list activation</code>	Displays whether the white list is enabled.

### 27.2.1 Layer 2 Isolation White List Sub-Commands

The following table describes the sub-commands for `l2-isolation white-list` commands.

**Table 90** l2-isolation white-list Sub-commands

COMMAND	DESCRIPTION
<code>[no] activate</code>	Enables the rule. The <code>no</code> command disables the rule.

**Table 90** l2-isolation white-list Sub-commands (continued)

COMMAND	DESCRIPTION
[no] <i>description description</i>	Sets a descriptive name (up to 60 printable ASCII characters) for a rule. The <code>no</code> command removes the descriptive name from the rule.
[no] <i>ip-address ip</i>	Sets an IPv4 address associated with this rule. The <code>no</code> command removes the IP address.  This is the IP address of device that can be accessed by the devices connected to an internal interface on which layer-2 isolation is enabled.

## 27.3 Layer 2 Isolation Commands Example

The following example enables Layer-2 isolation on the UAG and interface lan2. It also creates a rule in the white list to allow access to the device with IP address 172.17.0.66. It then displays the Layer-2 isolation settings.

```

Router# configure terminal
Router(config)# l2-isolation
Router(l2-isolation)# activate
Router(l2-isolation)# interface lan2
Router(l2-isolation)# white-list 1
Router(white-list)# activate
Router(white-list)# description PC
Router(white-list)# ip-address 172.17.0.66
Router(white-list)# exit
Router(config)# show l2-isolation
interface
=====
lan2
Router(config)# show l2-isolation activation
Layer2 Isolation Status: yes
Router(config)# show l2-isolation white-list
layer2 isolation white list rule: 1
  active: yes
  ip address: 172.17.0.66
  description: PC
Router(config)#

```

## 28.1 IPnP Overview

IP Plug and Play (IPnP) allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the UAG are not in the same subnet.

When you disable the IPnP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the UAG's LAN IP address can connect to the UAG or access the Internet through the UAG.

The IPnP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the UAG's IP address.

Note: You must enable NAT to use the IPnP feature.

## 28.2 IPnP Commands

The following table lists the `ipnp` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 91** ipnp Commands

COMMAND	DESCRIPTION
<code>[no] ip ipnp activate</code>	Enables IPnP on the UAG. The <code>no</code> command disables IPnP.
<code>ip ipnp config</code>	Enters the IPnP sub-command mode to enable IPnP on specific internal interface(s).
<code>[no] interface <i>interface_name</i></code>	Enables IPnP on a specific internal interface. The <code>no</code> command disables IPnP for the specified interface.
<code>show ip ipnp activation</code>	Displays whether IPnP is enabled on the UAG.
<code>show ip ipnp interface</code>	Displays whether IPnP is enabled on an interface.

## 28.3 IPnP Commands Example

The following example enables IPnP on the UAG and interface lan1. It also displays the IPnP settings.

```
Router# configure terminal
Router(config)# ip ipnp activate
Router(config)# ip ipnp config
Router(ipnp)# interface lan1
Router(ipnp)# exit
Router(config)# show ip ipnp activation
IPnP Status: yes
Router(config)# show ip ipnp interface
interface
=====
lan1
Router(config)#
```

# Web Authentication

## 29.1 Web Authentication Overview

Web authentication can intercepts network traffic, according to the authentication policies, until the user authenticates his or her connection, usually through a specifically designated login web page. This means all web page requests can initially be redirected to a special web page that requires users to authenticate their sessions. Once authentication is successful, they can then connect to the rest of the network or Internet.

As soon as a user attempt to open a web page, the UAG reroutes his/her browser to a web portal page that prompts he/she to log in.

## 29.2 Web Authentication Commands

This table lists the commands for forcing user authentication. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 92** web-auth Commands

COMMAND	DESCRIPTION
[no] web-auth activate	Enables force user authentication that force users to log in to the UAG before the UAG routes traffic for them. The no command means the user authentication is not required.
web-auth default-rule authentication {required   unnecessary} {no log   log [alert]}	<p>Sets the default authentication policy that the UAG uses on traffic that does not match any exceptional service or other authentication policy.</p> <p><i>required</i>: Users need to be authenticated. They must manually go to the UAG's login screen. The UAG will not redirect them to the login screen.</p> <p><i>unnecessary</i>: Users do not need to be authenticated.</p> <p><i>no log   log [alert]</i>: Select whether to have the UAG generate a log (log), log and alert (log alert) or not (no log) for packets that match this default policy.</p>
web-auth [no] exceptional-service <i>service_name</i>	Sets a service which you want users to be able to access without user authentication. The no command removes the specified service from the exceptional list.
web-auth login setting	Sets the login web page through which the user authenticates his or her connection before he or she can then connect to the rest of the network or Internet. See <a href="#">Table 93 on page 160</a> for the sub-commands.
web-auth method {portal   user-agreement}	Sets a client to authenticate with the UAG through the specifically designated web portal or user agreement page.
web-auth policy <1..1024>	Creates the specified condition for forcing user authentication, if necessary, and enters sub-command mode. The conditions are checked in sequence, starting at 1. See <a href="#">Table 94 on page 161</a> for the sub-commands.

**Table 92** web-auth Commands (continued)

COMMAND	DESCRIPTION
web-auth policy append	Creates a new condition for forcing user authentication at the end of the current list and enters sub-command mode. See <a href="#">Table 94 on page 161</a> for the sub-commands.
web-auth policy insert <1..1024>	Creates a new condition for forcing user authentication at the specified location, renumbers the other conditions accordingly, and enters sub-command mode. See <a href="#">Table 94 on page 161</a> for the sub-commands.
web-auth policy delete <1..1024>	Deletes the specified condition.  To modify a condition, you can insert a new condition (N) and then delete the one (N+1) that you want to modify.
web-auth policy flush	Deletes every condition.
web-auth policy move <1..1024> to <1..1024>	Moves the specified condition to the specified location and renumbers the other conditions accordingly.
web-auth type default-user-agreement	Enters sub-command mode to configure the default user agreement pages and related settings. See <a href="#">Table 95 on page 162</a> for the sub-commands.
web-auth type default-web-portal	Enters sub-command mode to configure the default login page and related settings. See <a href="#">Table 96 on page 162</a> for the sub-commands.
web-auth type profile <i>profile_name</i>	Enters sub-command mode to create an authentication type profile. See <a href="#">Table 97 on page 163</a> for the sub-commands.
web-auth type rename <i>profile_name_old</i> <i>profile_name_new</i>	Gives an existing authentication type profile a new name.
web-auth user-agreement	Enters sub-command mode to configure user agreement pages and related settings. See <a href="#">Table 98 on page 164</a> for the sub-commands.
show web-auth activation	Displays whether forcing user authentication is enabled or not.
show web-auth default-rule	Displays settings of the default web authentication policy.
show web-auth exceptional-service	Displays services that users can access without user authentication.
show web-auth method	Displays whether a client is to authenticate with the UAG through the specifically designated web portal or user agreement page when web authentication is enabled.
show web-auth policy {<1..1024>   all}	Displays details about the policies for forcing user authentication.
show web-auth portal status	Displays the web portal page settings.
show web-auth status	Displays the web portal page or user agreement page settings.
show web-auth type customize-zip {user-agreement   web-portal}	Displays the custom web portal or user agreement files uploaded to the UAG.
show web-auth type {default-user-agreement   default-web-portal   summary}	Displays the settings for the specified web authentication page type, or the summary of the authentication type profiles on the UAG.
show web-auth type profile <i>profile_name</i>	Displays the settings of the specified authentication type profile.
show web-auth user-agreement status	Displays the user agreement page settings.

## 29.2.1 web-auth login setting Sub-commands

The following table describes the sub-commands for the web-auth login setting command.

**Table 93** web-auth login setting Sub-commands

COMMAND	DESCRIPTION
<code>exit</code>	Leaves the sub-command mode.
<code>type {external   internal}</code>	<p>Sets the login page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network.</p> <p><code>internal</code>: Use the default login page built into the UAG.</p> <p><code>external</code>: Use a custom login page from an external web portal instead of the default one built into the UAG. You can configure the look and feel of the web portal page.</p> <p><b>Note:</b> If you select the external option, you cannot use endpoint security to make sure that users' computers meet specific security requirements before they can access the network.</p>
<code>[no] error-url url</code>	<p>Sets the error page's URL; for example, <code>http://IIS server IP Address/error.html</code>. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*') in quotes.</p> <p>The <code>no</code> command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
<code>[no] internal-welcome-url url</code>	<p>Sets the welcome page's URL when you select to use the default login page built into the UAG; for example, <code>http://IIS server IP Address/welcome.html</code>. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*') in quotes.</p> <p>The <code>no</code> command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
<code>[no] login-url url</code>	<p>Sets the login page's URL; for example, <code>http://IIS server IP Address/login.html</code>. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*') in quotes.</p> <p>The <code>no</code> command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
<code>[no] logout-ip ipv4_address</code>	<p>Sets an IP address that users can use to terminate their sessions manually by entering the IP address in the address bar of the web browser.</p> <p>The <code>no</code> command removes the IP address.</p>
<code>[no] logout-url url</code>	<p>Sets the logout page's URL; for example, <code>http://IIS server IP Address/logout.html</code>. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*') in quotes.</p> <p>The <code>no</code> command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
<code>[no] session-url url</code>	<p>Sets the session page's URL; for example, <code>http://IIS server IP Address/session.html</code>. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*') in quotes.</p> <p>The <code>no</code> command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>



**Table 93** web-auth login setting Sub-commands (continued)

COMMAND	DESCRIPTION
[no] <code>terms-of-service</code>	Forces users to agree to the terms before they can use the service. An agreement checkbox will display in the login page.  The <code>no</code> command allows users to use the service without agreeing to the terms.
[no] <code>welcome-url url</code>	Sets the welcome page's URL; for example, <code>http://IIS server IP Address/welcome.html</code> . You can use up to 255 characters (0-9a-zA-Z;/?:@&=+\$.- _!*'()% in quotes).  The <code>no</code> command removes the URL.  The Internet Information Server (IIS) is the web server on which the web portal files are installed.

## 29.2.2 web-auth policy Sub-commands

The following table describes the sub-commands for several web-auth policy commands. Note that not all rule commands use all the sub-commands listed here.

**Table 94** web-auth policy Sub-commands

COMMAND	DESCRIPTION
[no] <code>activate</code>	Activates the specified condition. The <code>no</code> command deactivates the specified condition.
[no] <code>authentication {force   required}</code>	Selects the authentication requirement for users when their traffic matches this policy. The <code>no</code> command means user authentication is not required.  <i>force</i> : Users need to be authenticated and the UAG automatically display the login screen when users who have not logged in yet try to send HTTP traffic.  <i>required</i> : Users need to be authenticated. They must manually go to the login screen. The UAG will not redirect them to the login screen.
[no] <code>description description</code>	Sets the description for the specified condition. The <code>no</code> command clears the description.  <i>description</i> : You can use alphanumeric and ()+/:=?!*#@\$_%- characters, and it can be up to 60 printable ASCII characters long.
[no] <code>destination {address_object   group_name}</code>	Sets the destination criteria for the specified condition. The <code>no</code> command removes the destination criteria, making the condition effective for all destinations.
[no] <code>eps &lt;1..8&gt; eps_object_name</code>	Associates the specified End Point Security (EPS) object with the specified condition. The UAG checks authenticated users' computers against the condition's endpoint security objects in the order of 1 to 8. You have to configure order 1 and then the others if any. The <code>no</code> command removes the specified EPS object's association with the condition.  To apply EPS for this condition, you have to also make sure you enable EPS and set authentication to either <code>required</code> or <code>force</code> for this condition.
[no] <code>eps activate</code>	Enables EPS for the specified condition. The <code>no</code> command means to disable EPS for the condition.
[no] <code>eps periodical-check &lt;1..1440&gt;</code>	Sets a number of minutes the UAG has to repeat the endpoint security check. The <code>no</code> command means that the UAG only perform the endpoint security check when users log in to the UAG.
[no] <code>force</code>	Forces users to log in to the UAG if the specified condition is satisfied. The <code>no</code> command means that users do not log in to the UAG.
<code>interface interface_name</code>	Sets an interface on which packets for the policy must be received.

**Table 94** web-auth policy Sub-commands (continued)

COMMAND	DESCRIPTION
[no] schedule <i>schedule_name</i>	Sets the time criteria for the specified condition. The no command removes the time criteria, making the condition effective all the time.
[no] source { <i>address_object</i>   <i>group_name</i> }	Sets the source criteria for the specified condition. The no command removes the source criteria, making the condition effective for all sources.
eps insert <1..8> <i>eps_object_name</i>	Inserts the specified EPS object for the condition. The number determines the order that this EPS rule is executed in the condition.
eps move <1..8> to <1..8>	Changes an endpoint object's position in the execution order of the condition.
show	Displays information about the specified condition.

### 29.2.3 web-auth type default-user-agreement Sub-commands

The following table describes the sub-commands for several web-auth type default-user-agreement commands. Note that not all rule commands use all the sub-commands listed here.

**Table 95** web-auth type default-user-agreement Sub-commands

COMMAND	DESCRIPTION
[no] idle-detection [timeout <1..60>]	Sets the UAG to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The UAG automatically logs out the access user once the specified idle timeout has been reached.
logon-re-auth-time <0..1440>	Sets the number of minutes the user can be logged into the UAG in one session before having to log in again.

### 29.2.4 web-auth type default-web-portal Sub-commands

The following table describes the sub-commands for several web-auth type default-web-portal commands. Note that not all rule commands use all the sub-commands listed here.

**Table 96** web-auth type default-web-portal Sub-commands

COMMAND	DESCRIPTION
[no] internal-welcome-url <i>url</i>	<p>Sets the welcome page's URL when you select to use the default login page built into the UAG; for example, http://IIS server IP Address/welcome.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$.- _!~*')%) in quotes.</p> <p>The no command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
[no] terms-of-service	<p>Forces users to agree to the terms before they can use the service. An agreement checkbox will display in the login page.</p> <p>The no command allows users to use the service without agreeing to the terms.</p>

## 29.2.5 web-auth type profile Sub-commands

The following table describes the sub-commands for several web-auth type profile commands. Note that not all rule commands use all the sub-commands listed here.

**Table 97** web-auth type profile Sub-commands

COMMAND	DESCRIPTION
<code>customize</code>	Specifies the custom web portal file you want to use in this profile.  Note: You can upload zipped custom web portal files to the UAG using the web configurator.
<code>type {user-agreement   web-portal}</code>	Specifies the type of the web authentication page through which users authenticate their connections.
<code>user-agreement agreement-url url</code>	Sets the user agreement page's URL; for example, <code>http://IIS server IP Address/logout.html</code> . You can use up to 255 characters (0-9a-zA-Z;/?:@&=+\$\._!~*'())% in quotes.  The Internet Information Server (IIS) is the web server on which the user agreement files are installed.
<code>[no] user-agreement idle-detection [timeout &lt;1..60&gt;]</code>	Sets the UAG to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The UAG automatically logs out the access user once the specified idle timeout has been reached.
<code>user-agreement logon-re-auth-time &lt;0..1440&gt;</code>	Sets the number of minutes the user can be logged into the UAG in one session before having to log in again.
<code>[no] user-agreement welcome-url &lt;url&gt;</code>	Sets the welcome page's URL; for example, <code>http://IIS server IP Address/logout.html</code> . You can use up to 255 characters (0-9a-zA-Z;/?:@&=+\$\._!~*'())% in quotes.  The <code>no</code> command removes the URL and sets the UAG to use the welcome page of internal user agreement file.  The Internet Information Server (IIS) is the web server on which the user agreement files are installed.
<code>[no] web-portal error-url url</code>	Sets the error page's URL; for example, <code>http://IIS server IP Address/error.html</code> . You can use up to 255 characters (0-9a-zA-Z;/?:@&=+\$\._!~*'())% in quotes.  The <code>no</code> command removes the URL.  The Internet Information Server (IIS) is the web server on which the web portal files are installed.
<code>web-portal login-url url</code>	Sets the login page's URL; for example, <code>http://IIS server IP Address/login.html</code> . You can use up to 255 characters (0-9a-zA-Z;/?:@&=+\$\._!~*'())% in quotes.  The Internet Information Server (IIS) is the web server on which the web portal files are installed.
<code>[no] web-portal logout-url url</code>	Sets the logout page's URL; for example, <code>http://IIS server IP Address/logout.html</code> . You can use up to 255 characters (0-9a-zA-Z;/?:@&=+\$\._!~*'())% in quotes.  The <code>no</code> command removes the URL.  The Internet Information Server (IIS) is the web server on which the web portal files are installed.

**Table 97** web-auth type profile Sub-commands (continued)

COMMAND	DESCRIPTION
[no] web-portal session-url <i>url</i>	<p>Sets the session page's URL; for example, http://IIS server IP Address/session.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$.~_!~*')%) in quotes.</p> <p>The <code>no</code> command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>
[no] web-portal welcome-url <i>url</i>	<p>Sets the welcome page's URL; for example, http://IIS server IP Address/welcome.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$.~_!~*')%) in quotes.</p> <p>The <code>no</code> command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the web portal files are installed.</p>

## 29.2.6 web-auth user-agreement Sub-commands

The following table describes the sub-commands for several web-auth user-agreement commands. Note that not all rule commands use all the sub-commands listed here.

**Table 98** web-auth user-agreement Sub-commands

COMMAND	DESCRIPTION
[no] agreement-url <i>url</i>	<p>Sets the user agreement page's URL; for example, http://IIS server IP Address/logout.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$.~_!~*')%) in quotes.</p> <p>The <code>no</code> command removes the URL.</p> <p>The Internet Information Server (IIS) is the web server on which the user agreement files are installed.</p>
[no] idle-detection [timeout <1..60>]	Sets the UAG to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The UAG automatically logs out the access user once the specified idle timeout has been reached.
[no] internal-page-customization	Sets the UAG to use the custom user agreement pages that are uploaded to the UAG through the web configurator.
logon-re-auth-time <0..1440>	Sets the number of minutes the user can be logged into the UAG in one session before having to log in again.
type {external   internal}	<p>Sets the user agreement page appears whenever the web portal intercepts network traffic, preventing unauthorized users from gaining access to the network.</p> <p><code>internal</code>: Use the default user agreement page built into the UAG.</p> <p><code>external</code>: Use a custom user agreement page from an external web portal instead of the default one built into the UAG. You can configure the look and feel of the user agreement page.</p>
[no] welcome-url < <i>url</i> >	<p>Sets the welcome page's URL; for example, http://IIS server IP Address/logout.html. You can use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$.~_!~*')%) in quotes.</p> <p>The <code>no</code> command removes the URL and sets the UAG to use the welcome page of internal user agreement file.</p> <p>The Internet Information Server (IIS) is the web server on which the user agreement files are installed.</p>

## 29.2.7 Web Authentication Policy Insert Command Example

The following commands show how to insert a web authentication policy at position 1 of the checking order. This policy applies endpoint security policies and uses the following settings:

- Activate: yes
- Description: EPS-on-LAN
- Source: use address object "LAN1\_SUBNET"
- Destination: use address object "DMZ\_Servers"
- User Authentication: required
- Schedule: no specified
- Endpoint security: Activate
- endpoint security object: use "EPS-WinXP" and "EPS-WinVista" for the first and second checking EPS objects

```
Router# configure terminal
Router(config)# web-auth policy insert 1
Router(config-web-auth-1)# activate
Router(config-web-auth-1)# description EPS-on-LAN
Router(config-web-auth-1)# source LAN1_SUBNET
Router(config-web-auth-1)# destination DMZ_Servers
Router(config-web-auth-1)# authentication force
Router(config-web-auth-1)# no schedule
Router(config-web-auth-1)# eps activate
Router(config-web-auth-1)# eps 1 EPS-WinXP
Router(config-web-auth-1)# eps 2 EPS-WinVista
Router(config-web-auth-1)# exit
```

## Walled Garden

### 30.1 Walled Garden Overview

A user must log in before the UAG allows the user's access to the Internet. However, with a walled garden, you can define one or more web site addresses that all users can access without logging in. These can be used for advertisements for example.

### 30.2 Walled Garden Commands

This table lists the walled-garden commands. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 99** walled-garden Commands

COMMAND	DESCRIPTION
<code>[no] walled-garden activate</code>	Enables the walled garden feature. The <code>no</code> command disables the walled garden feature.
<code>[no] walled-garden rule &lt;1..20&gt;</code>	Creates a walled garden URL link entry for web site that all users are allowed to access without logging in, and enters sub-command mode. See <a href="#">Section Table 100 on page 167</a> for the sub-commands.
<code>walled-garden rule append</code>	Creates a new walled garden URL entry at the end of the current list and enters sub-command mode. See <a href="#">Table 100 on page 167</a> for the sub-commands.
<code>walled-garden rule flush</code>	Deletes all walled garden URL entries.
<code>walled-garden rule insert &lt;1..20&gt;</code>	Creates a new walled garden URL entry at the specified location, renumbers the other entries accordingly, and enters sub-command mode. See <a href="#">Table 100 on page 167</a> for the sub-commands.
<code>walled-garden rule move &lt;1..20&gt; to &lt;1..20&gt;</code>	Moves the specified walled garden URL entry to the specified location and renumbers the other entries accordingly.
<code>show walled-garden activation</code>	Displays whether the walled garden feature is enabled or not.
<code>show walled-garden rule &lt;1..20&gt;</code>	Displays settings of the specified walled garden URL entry.

## 30.2.1 walled-garden rule Sub-commands

The following table describes the sub-commands for several `walled-garden rule` commands. Note that not all rule commands use all the sub-commands listed here.

**Table 100** walled-garden rule Sub-commands

COMMAND	DESCRIPTION
[no] activate	Enables this entry. The <code>no</code> command disables the entry.
[no] name <i>description</i>	Sets a descriptive name for the walled garden link to be displayed in the login screen. The <code>no</code> command clears the description.  <i>description:</i> You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
[no] hidden	Sets the UAG to not display the web site link in the user login screen.  This is helpful if a user's access to a specific web site is required to stay connected but he or she does not need to visit that web site.  The <code>no</code> command displays the the web site link in the user login screen.
[no] url <i>url</i>	Sets the URL or IP address of the web site. Use "http://" followed by up to 262 characters (0-9a-zA-Z;/?:@&=+\$.~!*~*'()%). For example, <code>http://www.example.com</code> or <code>http://172.16.1.35</code> .  The <code>no</code> command removes the web site address.

## 30.2.2 Walled Garden Command Example

This example shows how to enable the walled garden feature and insert a walled garden link rule at position 1 of the checking order. This example also displays the rule settings. The link rule uses the following settings:

- Activate: yes
- Name: Example1
- URL: `www.example.com`

```
Router# configure terminal
Router(config)# walled-garden activate
Router(config)# walled-garden rule insert 1
Router(walled-garden)# activate
Router(walled-garden)# name Example1
Router(walled-garden)# url http://www.example.com
Router(walled-garden)# exit
Router(config)# show walled-garden
walled garden rule: 1
  active: yes
  url: http://www.example.com
  name: Example1
Router(config)#
```

# Advertisement

## 31.1 Advertisement Overview

You can set the UAG to display an advertisement web page as the first web page whenever the user connects to the Internet.

## 31.2 Advertisement Commands

This table lists the advertisement commands. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 101** advertisement Commands

COMMAND	DESCRIPTION
[no] advertisement activate	Enables the advertisement feature. The no command disables the advertisement feature.
advertisement flush	Deletes all advertisement rules.
[no] advertisement name <i>description</i> url <i>url</i>	Sets a descriptive name for the advertisement web page and enters the web site address to create a new rule. The no command removes the advertisement rule.  <i>description</i> : You can use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.  <i>url</i> : the URL or IP address of the web site. Use "http://" followed by up to 262 characters (0-9a-zA-Z;/?:@&+\$.~!*'()%). For example, http://www.example.com or http://172.16.1.35.
advertisement rename <i>description_old</i> <i>description_new</i>	Gives an existing rule a new name.
show advertisement	Displays settings of advertisement rule(s).
show advertisement activation	Displays whether the advertisement feature is enabled or not.

### 31.2.1 Advertisement Command Example

This example shows how to set an advertisement rule and displays the rule settings.

```
Router# configure terminal
Router(config)# advertisement activate
Router(config)# advertisement name example url http://www.example.com
Router(config)# show advertisement
advertisement rule: 1
  name: example
  url: http://www.example.com
Router(config)#
```



## 32.1 RTLS Overview

Ekahau RTLS (Real Time Location Service) tracks battery-powered Wi-Fi tags attached to APs managed by the UAG to create maps, alerts, and reports.

The Ekahau RTLS Controller is the centerpiece of the RTLS system. This server software runs on a Windows computer to track and locate Ekahau tags from Wi-Fi signal strength measurements. Use the UAG with the Ekahau RTLS system to take signal strength measurements at the APs (Integrated Approach / Blink Mode).

You need:

- At least three APs managed by the UAG (the more APs the better since it increases the amount of information the Ekahau RTLS Controller has for calculating the location of the tags)
- IP addresses for the Ekahau Wi-Fi tags
- A dedicated RTLS SSID is recommended
- Ekahau RTLS Controller in blink mode with TZSP Updater enabled
- Secure policies to allow RTLS traffic if the UAG Secure Policy control is enabled or the Ekahau RTLS Controller is behind a firewall.

For example, if the Ekahau RTLS Controller is behind a firewall, open ports 8550, 8553, and 8569 to allow traffic the APs send to reach the Ekahau RTLS Controller.

The following table lists default port numbers and types of packets RTLS uses.

**Table 102** RTLS Traffic Port Numbers

PORT NUMBER	TYPE	DESCRIPTION
8548	TCP	Ekahau T201 location update.
8549	UDP	Ekahau T201 location update.
8550	TCP	Ekahau T201 tag maintenance protocol and Ekahau RTLS Controller user interface.
8552	UDP	Ekahau Location Protocol
8553	UDP	Ekahau Maintenance Protocol
8554	UDP	Ekahau T301 firmware update.
8560	TCP	Ekahau Vision web interface
8562	UDP	Ekahau T301W firmware update.
8569	UDP	Ekahau TZSP Listener Port

## 32.1.1 RTLS Configuration Commands

Use these commands to configure RTLS on the UAG.

**Table 103** RTLS Commands

COMMAND	DESCRIPTION
[no] rtls ekahau activate	Enables RTLS to use Wi-Fi to track the location of Ekahau Wi-Fi tags. The no command disables tracking.
rtls ekahau ip address <ip>	Specifies the IP address of the Ekahau RTLS Controller.
rtls ekahau ip port <1..65535>	Specifies the server port of the Ekahau RTLS Controller.
show rtls ekahau config	Displays RTLS configuration details.
show rtls ekahau cli	Displays commands run on the AP. The AP runs the flush command before executing other commands.

## 32.1.2 RTLS Configuration Examples

The following commands show how to enable RTLS on the UAG, specify the IP address of the Ekahau RTLS Controller and then show the configuration settings.

```
Router# configure terminal
Router(config)# rtls ekahau activate
Router(config)# rtls ekahau ip address 1.1.1.1
Router(config)# exit
Router# show rtls ekahau config
ekahau activate: yes
ekahau address: 1.1.1.1
ekahau port: 8569
Router#
```

The following command displays the commands run on the AP.

```
Router(config)# show rtls ekahau cli
!
rtls ekahau flush
!
rtls ekahau ip port 11111
rtls ekahau ip address 1.1.1.1
rtls ekahau activate
!
Router(config)#
```

## Firewall

This chapter introduces the UAG's firewall and shows you how to configure your UAG's firewall.

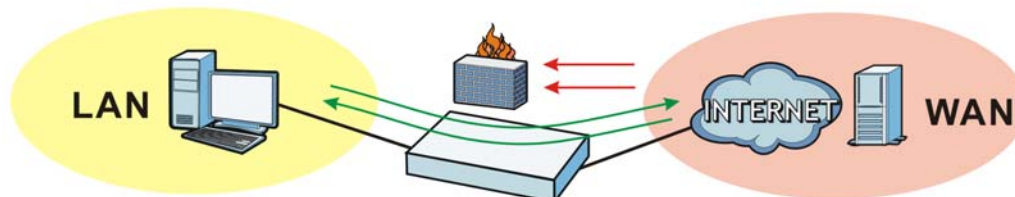
### 33.1 Firewall Overview

The UAG's firewall is a stateful inspection firewall. The UAG restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

A zone is a group of interfaces or VPN tunnels. Group the UAG's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces and/or VPN tunnels in a zone.

This example shows the UAG's default firewall behavior for WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the firewall allows the response. However, the firewall blocks Telnet traffic initiated from the WAN zone and destined for the LAN zone. The firewall allows VPN traffic between any of the networks.

**Figure 19** Default Firewall Action



Your customized rules take precedence and override the UAG's default settings. The UAG checks the schedule, user name (user's login name on the UAG), source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the UAG takes the action specified in the rule.

For example, if you want to allow a specific user from any computer to access one zone by logging in to the UAG, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the UAG and will be disabled after the user logs out of the UAG.

## 33.2 Firewall Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 104** Input Values for General Firewall Commands

LABEL	DESCRIPTION
<i>address_object</i>	The name of the IP address (or address group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>profile_name</i>	The name of the firewall rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>user_name</i>	The name of a user (group). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>zone_object</i>	The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.  The UAG uses pre-defined zone names like DMZ, LAN1, LAN2, SSL VPN, IPSec VPN, and WAN.
<i>rule_number</i>	The priority number of a firewall rule. 1 - X where X is the highest number of rules the UAG model supports. See the UAG's User's Guide for details.
<i>schedule_object</i>	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>service_name</i>	The name of the service (group). You may use 1-31 alphanumeric characters, underscores (_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following table describes the commands available for the firewall. You must use the `configure terminal` command to enter the configuration mode before you can use the configuration commands.

Note: In the UAG running firmware version V4.10 or later, use `secure-policy` to configure the firewall settings.

**Table 105** Command Summary: Firewall

COMMAND	DESCRIPTION
<code>[no] {firewall secure-policy} asymmetrical-route activate</code>	Allows or disallows asymmetrical route topology.
<code>[no] conmlimit max-per-host &lt;1..8192&gt;</code>	Sets the highest number of sessions that the UAG will permit a host to have at one time. The <code>no</code> command removes the settings.
<code>{firewall secure-policy} rule_number</code>	Enters the firewall sub-command mode to set a firewall rule. See <a href="#">Table 106 on page 174</a> for the sub-commands.
<code>{firewall secure-policy} profile_name {zone_object Device} rule_number</code>	Enters the firewall sub-command mode to set a direction specific through-Device rule or to-Device rule. See <a href="#">Table 106 on page 174</a> for the sub-commands.

**Table 105** Command Summary: Firewall (continued)

COMMAND	DESCRIPTION
<code>{firewall secure-policy} profile_name {zone_object Device} append</code>	Enters the firewall sub-command mode to add a direction specific through-Device rule or to-Device rule to the end of the global rule list. See <a href="#">Table 106 on page 174</a> for the sub-commands.
<code>{firewall secure-policy} profile_name {zone_object Device} delete &lt;1..5000&gt;</code>	Removes a direction specific through-Device rule or to-Device rule.  <1..5000>: the index number in a direction specific firewall rule list.
<code>{firewall secure-policy} profile_name {zone_object Device} flush</code>	Removes all direction specific through-Device rule or to-Device rules.
<code>{firewall secure-policy} profile_name {zone_object Device} insert rule_number</code>	Enters the firewall sub-command mode to add a direction specific through-Device rule or to-Device rule before the specified rule number. See <a href="#">Table 106 on page 174</a> for the sub-commands.
<code>{firewall secure-policy} profile_name {zone_object Device} move rule_number to rule_number</code>	Moves a direction specific through-Device rule or to-Device rule to the number that you specified.
<code>[no] {firewall secure-policy} activate</code>	Enables the firewall on the UAG. The no command disables the firewall.
<code>{firewall secure-policy} append</code>	Enters the firewall sub-command mode to add a global firewall rule to the end of the global rule list. See <a href="#">Table 106 on page 174</a> for the sub-commands.
<code>{firewall secure-policy} default-rule action {allow   deny   reject} { no log   log [alert] }</code>	Sets how the firewall handles packets that do not match any other firewall rule.
<code>{firewall secure-policy} delete rule_number</code>	Removes a firewall rule.
<code>{firewall secure-policy} flush</code>	Removes all firewall rules.
<code>{firewall secure-policy} insert rule_number</code>	Enters the firewall sub-command mode to add a firewall rule before the specified rule number. See <a href="#">Table 106 on page 174</a> for the sub-commands.
<code>{firewall secure-policy} move rule_number to rule_number</code>	Moves a firewall rule to the number that you specified.
<code>show conlimit max-per-host</code>	Displays the highest number of sessions that the UAG will permit a host to have at one time.
<code>show {firewall secure-policy}</code>	Displays all firewall settings.
<code>show {firewall secure-policy} rule_number</code>	Displays a firewall rule's settings.
<code>show {firewall secure-policy} profile_name {zone_object Device}</code>	Displays all firewall rules settings for the specified packet direction.
<code>show {firewall secure-policy} profile_name {zone_object Device} rule_number</code>	Displays a specified firewall rule's settings for the specified packet direction.
<code>show {firewall secure-policy} status</code>	Displays whether or not the firewall is active, whether or not asymmetrical route topology is allowed, and the default firewall rule's configuration.
<code>show {firewall secure-policy} block_rules</code>	Displays all the firewall rules that deny access.
<code>show {firewall secure-policy} any Device</code>	Shows all the to-Device firewall rules.

## 33.2.1 Firewall Sub-Commands

The following table describes the sub-commands for several `firewall` commands.

**Table 106** firewall Sub-commands

COMMAND	DESCRIPTION
<code>action {allow deny reject}</code>	Sets the action the UAG takes when packets match this rule.
<code>[no] activate</code>	Enables a firewall rule. The <code>no</code> command disables the firewall rule.
<code>app-profile <i>app_profile_name</i> {[no log]   [log by-profile]}{activate deactivate}</code>	Applies the application patrol profile to traffic that matches the criteria in this rule.  <code>no log</code> : to not generate a log for all traffic that matches criteria in the profile.  <code>log by-profile</code> : to decide whether a log will be generated based on the profile's settings.
<code>cf-profile <i>cf_profile_name</i> {[no log]   [log by-profile]}{activate deactivate}</code>	Applies the content filter profile to traffic that matches the criteria in this rule.  <code>no log</code> : to not generate a log for all traffic that matches criteria in the profile.  <code>log by-profile</code> : to decide whether a log will be generated based on the profile's settings.
<code>[no] ctmatch {dnat   snat}</code>	Use <code>dnat</code> to block packets sent from a computer on the UAG's WAN network from being forwarded to an internal network according to a virtual server rule.  Use <code>snat</code> to block packets sent from a computer on the UAG's internal network from being forwarded to the WAN network according to a 1:1 NAT or Many 1:1 NAT rule.  The <code>no</code> command forwards the matched packets.
<code>[no] description <i>description</i></code>	Sets a descriptive name (up to 60 printable ASCII characters) for a firewall rule. The <code>no</code> command removes the descriptive name from the rule.
<code>[no] destinationip <i>address_object</i></code>	Sets the destination IP address. The <code>no</code> command resets the destination IP address(es) to the default ( <code>any</code> ). <code>any</code> means all IP addresses.
<code>[no] from <i>zone_object</i></code>	Sets the zone on which the packets are received. The <code>no</code> command removes the zone on which the packets are received and resets it to the default ( <code>any</code> ) meaning all interfaces or VPN tunnels.
<code>[no] log [alert]</code>	Sets the UAG to create a log (and optionally an alert) when packets match this rule. The <code>no</code> command sets the UAG not to create a log or alert when packets match this rule.
<code>[no] schedule <i>schedule_object</i></code>	Sets the schedule that the rule uses. The <code>no</code> command removes the schedule settings from the rule.
<code>[no] service <i>service_name</i></code>	Sets the service to which the rule applies. The <code>no</code> command resets the service settings to the default ( <code>any</code> ). <code>any</code> means all services.
<code>[no] sourceip <i>address_object</i></code>	Sets the source IP address(es). The <code>no</code> command resets the source IP address(es) to the default ( <code>any</code> ). <code>any</code> means all IP addresses.
<code>[no] sourceport {tcp udp} {eq &lt;1..65535&gt; range &lt;1..65535&gt; &lt;1..65535&gt;}</code>	Sets the source port for a firewall rule. The <code>no</code> command removes the source port from the rule.

**Table 106** firewall Sub-commands (continued)

COMMAND	DESCRIPTION
[no] to {zone_object Device}	Sets the zone to which the packets are sent. The no command removes the zone to which the packets are sent and resets it to the default (any). any means all interfaces or VPN tunnels.
[no] user user_name	Sets a user-aware firewall rule. The rule is activated only when the specified user logs into the system. The no command resets the user name to the default (any). any means all users.

## 33.2.2 Firewall Command Examples

These are IPv4 firewall configuration examples.

The following example shows you how to add an IPv4 firewall rule to allow a MyService connection from the WAN zone to the IP addresses Dest\_1 in the LAN zone.

- Enter configuration command mode.
- Create an IP address object.
- Create a service object.
- Enter the firewall sub-command mode to add a firewall rule.
- Set the direction of travel of packets to which the rule applies.
- Set the destination IP address(es).
- Set the service to which this rule applies.
- Set the action the UAG is to take on packets which match this rule.

```
Router# configure terminal
Router(config)# service-object MyService tcp eq 1234
Router(config)# address-object Dest_1 10.0.0.10-10.0.0.15
Router(config)# firewall insert 3
Router(firewall)# from WAN
Router(firewall)# to LAN
Router(firewall)# destinationip Dest_1
Router(firewall)# service MyService
Router(firewall)# action allow
```

The following command displays the default IPv4 firewall rule that applies to the WAN to UAG packet direction. The firewall rule number is in the rule's priority number in the global rule list.

```
Router(config)# show firewall WAN Device
firewall rule: 13
description:
user: any, schedule: none
from: WAN, to: Device
source IP: any, source port: any
destination IP: any, service: Default_Allow_WAN_To_Device
log: no, action: allow, status: yes
connection match: no
```

## 33.3 Session Limit Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 107** Input Values for General Session Limit Commands

LABEL	DESCRIPTION
<i>rule_number</i>	The priority number of a session limit rule, 1 - 1000.
<i>address_object</i>	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<i>user_name</i>	The name of a user (group). You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.

The following table describes the session-limit commands. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 108** Command Summary: Session Limit

COMMAND	DESCRIPTION
<code>[no] session-limit activate</code>	Turns the session-limit feature on or off.
<code>session-limit limit &lt;0..8192&gt;</code>	Sets the default number of concurrent NAT/firewall sessions per host.
<code>session-limit rule_number</code>	Enters the session-limit sub-command mode to set a session-limit rule.
<code>[no] activate</code>	Enables the session-limit rule. The <code>no</code> command disables the session limit rule.
<code>[no] address address_object</code>	Sets the source IP address. The <code>no</code> command sets this to <code>any</code> , which means all IP addresses.
<code>[no] description description</code>	Sets a descriptive name (up to 64 printable ASCII characters) for a session-limit rule. The <code>no</code> command removes the descriptive name from the rule.
<code>exit</code>	Quits the sub-command mode.
<code>[no] limit &lt;0..8192&gt;</code>	Sets the limit for the number of concurrent NAT/firewall sessions this rule's users or addresses can have. 0 means any.
<code>[no] user user_name</code>	Sets a session-limit rule for the specified user. The <code>no</code> command resets the user name to the default ( <code>any</code> ). <code>any</code> means all users.
<code>session-limit append</code>	Enters the session-limit sub-command mode to add a session-limit rule to the end of the session-limit rule list.
<code>session-limit delete rule_number</code>	Removes a session-limit rule.
<code>session-limit flush</code>	Removes all session-limit rules.
<code>session-limit insert rule_number</code>	Enters the session-limit sub-command mode to add a session-limit rule before the specified rule number.
<code>session-limit move rule_number to rule_number</code>	Moves a session-limit to the number that you specified.
<code>show session-limit</code>	Shows the session-limit configuration.
<code>show session-limit begin rule_number end rule_number</code>	Shows the settings for a range of session-limit rules.
<code>show session-limit rule_number</code>	Shows the session-limit rule's settings.
<code>show session-limit status</code>	Shows the general session-limit settings.



## 34.1 Billing Overview

You can use the built-in billing function to setup billing profiles. A billing profile describes how to charge users. This chapter also shows you how to select an accounting method or configure a discount price plan.

## 34.2 Billing Commands

This table lists the `billing` commands. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 109** billing Commands

COMMAND	DESCRIPTION
<code>billing accounting-method {accumulation   time-to-finish }</code>	Sets how the UAG accounts the time.  <code>accumulation</code> : to allow each user a one-time login. Once the user logs in, the system starts counting down the pre-defined usage even if the user stops the Internet access before the time period is finished. If a user disconnects and reconnects before the allocated time expires, the user does not have to enter the user name and password to access the Internet again  <code>time-to-finish</code> : to allow each user multiple re-login until the time allocated is used up. The UAG accounts the time that the user is logged in for Internet access
<code>billing accumulation idle-detection timeout &lt;1..60&gt;</code>	Specifies the idle timeout between 1 and 60 minutes. The UAG automatically disconnects a computer from the network after a period of inactivity. The user may need to enter the username and password again before access to the network is allowed.
<code>billing accumulation-expire {day &lt;1..360&gt;   hour &lt;1..24&gt;}</code>	Specifies a time unit and number to set how long to wait before the UAG deletes an idle account.
<code>billing currency {eur   gbp   usd   user-define <i>currency_code</i> }</code>	Sets the appropriate currency unit.  <code>currency_code</code> : enter a three-letter alphabetic code, such as TWD or JPY.
<code>billing decimal-places &lt;2&gt;</code>	Sets the number of decimal places to be used for billing.
<code>billing decimal-symbol {comma   dot}</code>	Sets the UAG to use a dot (.) or a comma (,) for the decimal point.
<code>[no] billing discount activate</code>	Activates the discount price plan.  The <code>no</code> command disables the discount price plan.
<code>billing discount button {a   b   c} [charge-by-level]</code>	Specifies a button to assign the base charge.  <code>charge-by-level</code> : to charge the rate at each successive level from the first level (most expensive per unit) to the highest level (least expensive per unit) that the total purchase reaches.

**Table 109** billing Commands (continued)

COMMAND	DESCRIPTION
[no] billing discount unit <2..10> price <i>price</i>	Creates a new discount level by setting the duration of the billing period that should be reached before the UAG charges users at this level and defining this level's charge per time unit.  The <code>no</code> command removes this discount level.
[no] billing profile <i>profile_name</i>	Creates a billing profile and enters the <code>billing profile</code> sub-command mode to set the price and the duration of the billing period. See <a href="#">Table 110 on page 178</a> for the sub-commands.  The <code>no</code> command removes the specified profile.  <i>profile_name</i> : use up to 31 alphanumeric characters (A-Z, a-z, 0-9) and underscores (_). Spaces are not allowed. The first character must be a letter.
billing profile rename <i>profile_name</i> <i>profile_name</i>	Renames the specified billing profile (first <i>profile_name</i> ) to the specified name (second <i>profile_name</i> ).
billing tax-rate <0..100>	Sets the tax rate. For example, type 6 for a 6% sales tax.
[no] billing tax-rate activate	Sets the UAG to charge sales tax for the account.  The <code>no</code> command sets the UAG to not charge sales tax for the account.
billing unused-expire {day <1..30>   hour <1..24>   minute <30..60>}	Specifies a time unit and number to set how long to wait before the UAG deletes an account that has not been used.
billing username-password-length <4..6>	Sets how many characters the username and password of a newly-created dynamic guest account will have.
[no] billing wlan-ssid-profile <i>profile_name</i>	Sets the name of the SSID profile to which you can apply the general billing settings.  The <code>no</code> command sets the UAG to not apply the billing settings to the SSID profile.
show billing discount default rule	Displays settings of the default discount price plan.
show billing discount rule	Displays settings of the custom discount price plan(s).
show billing discount status	Displays billing discount settings.
show billing profile [ <i>profile_name</i> ]	Displays settings for all or the specified billing profile.
show billing status	Displays the general billing settings, such as the accounting method or tax rate.

### 34.2.1 Billing Profile Sub-commands

The following table describes the sub-commands for the `billing profile` command.

**Table 110** billing profile Sub-commands

COMMAND	DESCRIPTION
[no] activate	Enables the billing profile.  The <code>no</code> command disables the profile.
bandwidth {upload   download} <0..1048576> priority <1..7>	Specifies the maximum bandwidth allowed for the user account in kilobits per second and types a number between 1 and 7 to set the priority for the user's traffic. The smaller the number, the higher the priority.  upload refers to the traffic the UAG sends out from a user. download refers to the traffic the UAG sends to a user.

**Table 110** billing profile Sub-commands (continued)

COMMAND	DESCRIPTION
[no] bandwidth activate	Turns on bandwidth management for the user account. The no command disables bandwidth management for the user account.
price price	Defines each profile's price, up to 999999.99, per time unit.
quota {total   upload   download} megabytes <0..1023>	Sets how much downstream and/or upstream data in Megabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
quota {total   upload   download} gigabytes <0..100>	Sets how much downstream and/or upstream data in Gigabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
quota type {total   upload-download}	Sets a limit for the user account. This only applies to user's traffic that is received or transmitted through the external interface.  <b>Note:</b> When the limit is exceeded, the user is not allowed to access the Internet through the UAG.  total: set a limit on the total traffic in both directions. upload-download: set a limit on the upstream traffic and downstream traffic respectively.
time-period {day <1..365>   hour <1..24>   minute <30..60>}	Sets the duration of the billing period. When this period expires, the user's access will be stopped.

## 34.2.2 Billing Command Example

This example sets the accounting method to `time-to-finish` and configures the idle timeout that elapses before the UAG disconnects a user.

```
Router# configure terminal
Router(config)# billing accounting-method time-to-finish
Router(config)# billing accumulation idle-detection timeout 30
Router(config)#
```

This example enables and creates a custom discount pricing plan. It uses button A to assign the base charge and also shows the discount status and plan settings.

```
Router# configure terminal
Router(config)# billing discount activate
Router(config)# billing discount button a charge-by-level
Router(config)# billing discount unit 3 price 1.9
Router(config)# show billing discount status
Billing discount status:
  activate: yes
  button: a
  charge_by_level: yes
Router(config)#show billing discount rule
No.  Conditions          Unit          Unit price
=====
1    when >=             3             eur 1,90
Router(config)#
```

This example creates a billing profile named `billing_1hour` and displays the profile settings.

```
Router# configure terminal
Router(config)# billing profile billing_1hour
Router(billing profile button-a)# activate
Router(billing profile button-a)# price 2
Router(billing profile button-a)# time-period hour 1
Router(billing profile button-a)# exit
Router(config)# show billing profile
Billing Profile: billing_30mins
  activate: yes
  time period: 30 minute
  price: eur 0,00
Billing Profile: billing_1hour
  activate: yes
  time period: 1 hour
  price: eur 2,00
Router(config)#
```

This example applies the billing profile `billing_1hour` to button A of the web-based account generator and button A on a connected statement printer. It also displays the default discount price plan settings, that is, the billing profile settings for button A when it is selected as the button to assign the base charge.

```
Router# configure terminal
Router(config)# printer-manager button a billing_1hour
Router(config)# show billing discount default rule
No.          Conditions          Unit          Unit price
=====
default    when >=                1            eur 2,00
Router(config)#
```

# Payment Service

## 35.1 Payment Service Overview

The online payment service allows users to purchase access time online with a credit card. You must register with the supported credit card service before you can configure the UAG to handle credit card transactions.

## 35.2 Payment-service Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 111** Input Values for payment-service Commands

LABEL	DESCRIPTION
<i>message</i>	A note that displays in a custom online payment service page. You may use up to 1024 printable ASCII characters. Spaces are allowed.

The following table lists the `payment-service` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 112** payment-service Commands

COMMAND	DESCRIPTION
<code>payment-service account-delivery onscreen {activate   deactivate}</code>	Allows or disallows the UAG to display the user account information in the web screen.
<code>payment-service account-delivery sms {activate   deactivate}</code>	Allows or disallows the UAG to use Short Message Service (SMS) to send account information in a text message to the user's mobile device.
<code>[no] payment-service activate</code>	Enables online payment service. The <code>no</code> command disables online payment service.
<code>payment-service check payment-all-currency</code>	Displays the name of online payment service provider and checks if the currency unit for billing and the currency unit for online payment are the same.
<code>payment-service check payment-currency</code>	Checks if the currency unit for billing and the currency unit for online payment are the same.
<code>payment-service check paypal-currency</code>	Checks if the currency unit for billing and the currency unit for online payment using PayPal are the same.
<code>payment-service fail-page failed-message <i>message</i></code>	Specifies a note to display when the user's online payment failed.

**Table 112** payment-service Commands (continued)

COMMAND	DESCRIPTION
[no] payment-service page-customization	Sets the UAG to use a custom online payment service page.  You can customize the online payment service pages that displays after an unauthorized user click the link in the Web Configurator login screen to purchase access time  The no command sets the UAG to use the default online payment service page built into the device.
payment-service profile-page selection-message <i>message</i>	Configures a note to display in the first welcome page that allows users to choose a billing period they want.
payment-service provider paypal	Enters the payment-service-paypal sub-command mode to configure the PayPal account information. See <a href="#">Table 113 on page 183</a> for the sub-commands.
payment-service provider select paypal	Selects to use PayPal to authorize credit card payments.
payment-service sms-page info-message <i>message</i>	Specifies a note to display if you set the UAG to send account information via SMS text messages.
payment-service success-page account-message <i>message</i>	Configures a note to display above the user account information.
payment-service success-page format-date {dd-mm-yyyy   mm-dd-yyyy   yyyy-mm-dd} format-time {12-hour   24-hour}	Sets the format in which you want to display the date and how long an account is allowed to stay un-used before it expires.
payment-service success-page notification-message <i>message</i>	Specifies the important information you want to display.
payment-service success-page notification-message-color {#00FF00   color_name   rgb(0,0,255)}	Specifies the font color of the important information. You can use the color name, hexadecimal codes, or enter decimal color code of your own.
payment-service success-page successful-message <i>message</i>	Specifies a note to display in the second page after the user's online payment is made successfully.
show payment-service account-delivery	Displays whether the UAG is to display the user account information in the web screen and/or send account information in a text message to the user's mobile device.
show payment-service activation	Displays whether the online payment service is enabled.
show payment-service fail-page settings	Shows the message that displays when the user's online payment failed.
show payment-service page-customization	Displays whether the UAG is to use a custom online payment service page or the default online payment service page built into the device.
show payment-service profile-page settings	Shows the message that displays in the first welcome page to have users choose a billing period they want.
show payment-service provider paypal	Displays your PayPal account information.
show payment-service provider select	Displays the name of online payment service provider used by the UAG to authorize credit card payments.
show payment-service sms-page settings	Shows the note that displays in the text message when you set the UAG to send account information via SMS text messages.
show payment-service success-page settings	Shows all the information or messages that display in the page after the user's online payment is made successfully.

## 35.2.1 Payment-Service Provider Paypal Sub-commands

The following table describes the sub-commands for the `payment-service provider paypal` command.

**Table 113** payment-service provider paypal Sub-commands

COMMAND	DESCRIPTION
<code>[no] account e-mail</code>	Sets your PayPal account name. You should already have a PayPal account to receive credit card payments.  The <code>no</code> command removes the account name.
<code>currency currency_code</code>	Sets the appropriate currency in which payments are made. The available options depend on currencies that PayPal supports.  <i>currency_code</i> : enter a three-letter alphabetic code, such as <code>aud</code> , <code>cad</code> , <code>chf</code> , <code>czk</code> , <code>dkk</code> , <code>eur</code> , <code>gbp</code> , <code>hkd</code> , <code>huf</code> , <code>ils</code> , <code>jpy</code> , <code>mxn</code> , <code>nok</code> , <code>nzd</code> , <code>php</code> , <code>pln</code> , <code>sek</code> , <code>sgd</code> , <code>thb</code> , <code>twd</code> or <code>usd</code> .
<code>gateway url</code>	Sets the address of the PayPal gateway provided to you by PayPal after applying for your PayPal account.
<code>[no] identity-token identity_token</code>	Sets the ID token provided to you by PayPal after successfully applying for your PayPal account.  The <code>no</code> command removes the ID token.

## 35.2.2 Payment-Service Command Example

This example configures the PayPal account information and displays the settings. It also enables online payment service and sets how the UAG provides dynamic guest account information after the user's online payment is done.

```
Router# configure terminal
Router(config)# payment-service provider paypal
Router(payment-service-paypal)# account user@example.com
Router(payment-service-paypal)# currency usd
Router(payment-service-paypal)# gateway https://www.paypal.com/cgi-bin/webscr
Router(payment-service-paypal)# identity-token 125ea8208de14153ac3db60c86eb1f4a
Router(printer-manager)# exit
Router(config)# payment-service activate
Router(config)# payment-service account-delivery onscreen activate
Router(config)# payment-service account-delivery sms activate
Router(config)# show payment-service provider paypal
Payment Service: PayPal
  account: user@example.com
  currency: usd
  identity token: 125ea8208de14153ac3db60c86eb1f4a8
  payment gateway: www.paypal.com/cgi-bin/webscr
Router(config)#
```

## Printer Manager

### 36.1 Printer Manager Overview

You can create dynamic guest accounts and print guest account information by pressing the button on an external statement printer, such as SP350E. Make sure that the printer is connected to the appropriate power and the UAG, and that there is printing paper in the printer. Refer to the printer's documentation for details.

### 36.2 Printer-manager Commands

This table lists the `printer-manager` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 114** printer-manager Commands

COMMAND	DESCRIPTION
[no] <code>printer-manager activate</code>	Allows the UAG to manage and monitor the printer status. The <code>no</code> command disables printer management on the UAG.
<code>printer-manager discover</code>	Detects the printer(s) that is connected to the UAG and display the printer information.
<code>printer-manager button {a   b   c} profile_name</code>	Applies the specified billing profile to a button of the web-based account generator and/or the button on a connected statement printer
[no] <code>printer-manager encrypt activate</code>	Turns on data encryption. Data transmitted between the UAG and the printer will be encrypted with a secret key. The <code>no</code> command disables data encryption.
<code>printer-manager encrypt secret-key secret_key</code>	Sets a key for data encryption. <i>secret_key</i> : four alphanumeric characters (A-Z, a-z, 0-9)
<code>printer-manager multi-printout &lt;1..3&gt;</code>	Sets how many copies of subscriber statements you want to print (1 is the default).
<code>printer-manager port &lt;1..65535&gt;</code>	Sets the number of port on which the UAG sends data to the printer for it to print.
[no] <code>printer-manager printer &lt;1..10&gt;</code>	Enters the <code>printer-manager printer</code> sub-command mode to configure a printer that can be managed by the UAG. See <a href="#">Table 115 on page 185</a> for the sub-commands. The <code>no</code> command removes the specified printer from the printer list.
<code>printer-manager printer append</code>	Enters the <code>printer-manager printer</code> sub-command mode to add a printer to the end of the printer list. See <a href="#">Table 115 on page 185</a> for the sub-commands.
<code>printer-manager printout-type {customized   default}</code>	Sets to use the default account printout format built into the UAG or use a custom account printout format.



**Table 114** printer-manager Commands (continued)

COMMAND	DESCRIPTION
show printer-manager button	Displays the name of billing profile that is applied to each button.
show printer-manager discover-printer-status	Displays information of the printer that is connected to and detected by the UAG.
show printer-manager printer [<1..10>]	Displays settings of all or the specified printer that can be managed by the UAG.
show printer-manager printer-status	Displays information about the printers that are connected and can be managed by the UAG.
show printer-manager printerfw version	Displays the version of the printer firmware currently uploaded to the UAG. The UAG automatically installs it in the connected printers to make sure the printers are upgraded to the same version.
show printer-manager printout-type	Displays the current account printout format.
show printer-manager settings	Displays the printer management settings.
show printer-manager workableIP	Displays the number and IP address(s) of printer(s) that can synchronize with the UAG successfully.

### 36.2.1 Printer-manager Printer Sub-commands

The following table describes the sub-commands for the printer-manager printer command.

**Table 115** printer-manager printer Sub-commands

COMMAND	DESCRIPTION
activate	Enables the entry.
deactivate	Disables the entry.
description <i>description</i>	Sets a descriptive name for the printer.
printer-ip <i>ipv4_address</i>	Sets the IP address of the printer.

### 36.2.2 Printer-manager Command Example

This example adds a printer to the managed printer list and displays the printer settings.

```

Router# configure terminal
Router(config)# printer-manager printer 1
Router(printer-manager)# activate
Router(printer-manager)# description cafe
Router(printer-manager)# printer-ip 172.16.0.123
Router(printer-manager)# exit
Router(config)# show printer-manager printer
printer: 1
  activate: yes
  IPv4 address: 172.16.0.123
  description: cafe
Router(config)#

```

## Free Time

### 37.1 Free Time Overview

With Free Time, the UAG can create dynamic guest accounts that allow users to browse the Internet free of charge for a specified period of time.

### 37.2 Free-Time Commands

The following table lists the `free-time` commands. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 116** free-time Commands

COMMAND	DESCRIPTION
<code>[no] free-time activate</code>	Turns on the free time feature to allow users to get a free account for Internet surfing during the specified time period.  The <code>no</code> command disables the free time feature.
<code>[no] free-time deliver-method onscreen</code>	Sets the UAG to display the user account information in the web screen.  The <code>no</code> command sets the UAG to not display the user account information in the web screen.
<code>[no] free-time deliver-method sms</code>	Sets the UAG to send account information in an SMS text message to the user's mobile device.  The <code>no</code> command sets the UAG to not send account information in an SMS text message to the user's mobile device.
<code>[no] free-time maximum-register-number &lt;1..5&gt;</code>	Specifies the maximum number of the users that are allowed to log in for Internet access with a free guest account before the time specified using the <code>free-time reset-register</code> command.  The <code>no</code> command resets the setting to its default value (1).
<code>[no] free-time reset-register hh:mm</code>	Sets the time in 24-hour format at which the new free time account is allowed to access the Internet.  The <code>no</code> command resets the setting to its default value (00:00).
<code>[no] free-time time-period time_period</code>	Sets the duration of time period (in minutes) for which the free time account is allowed to access the Internet.  <i>time_period</i> : <i>x</i> - <i>y</i> , where <i>x</i> and <i>y</i> depend on the UAG model.  The <code>no</code> command resets the setting to its default value (30).
<code>show free-time status</code>	Displays the free time settings.

## 37.3 Free-Time Commands Example

The following example enables the free time feature and sets the UAG to provide user account information in the web screen and also sent account information via SMS text messages. It then displays the free time settings.

```
Router# configure terminal
Router(config)# free-time activate
Router(config)# free-time deliver-method onscreen
Router(config)# free-time deliver-method sms
Router(config)# show free-time status
Activate: yes
Time Period: 30
Reset Time: 00:00
Maximum registration number before reset time: 1
Delivery Method: onscreen-sms
Router(config)#
```

## 38.1 SMS Overview

The UAG supports Short Message Service (SMS) to send short text messages to mobile devices. At the time of writing, the UAG uses ViaNett as the SMS gateway to help forward SMS messages. You must already have a Vianett account in order to use the SMS service.

## 38.2 SMS Commands

The following table lists the `sms-service` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 117** sms-service Commands

COMMAND	DESCRIPTION
<code>sms-service account-send phone phone_number account user_name password password</code>	Specifies the guest account information and the number of mobile device to which you want to send a text message.
<code>[no] sms-service activate</code>	Enables the SMS service on the UAG. The <code>no</code> command disabled the SMS service.
<code>sms-service default-country-code country_code</code>	Sets the default country code for the mobile phone number to which you want to send SMS messages.  <i>country_code</i> : one to four digits
<code>sms-service provider vianett</code>	Enters the <code>sms-service-vianett</code> sub-command mode to configure your ViaNett account information.
<code>[no] password password</code>	Sets the password for your ViaNett account.
<code>[no] username e-mail</code>	Sets the user name for your ViaNett account.
<code>sms-service provider-select vianett</code>	Selects to use ViaNett as the SMS gateway to help forward SMS messages.
<code>sms-service test-send phone phone_number msg message</code>	Specifies the mobile phone number and message to test whether the UAG can use SMS to send a text message.
<code>show sms-service</code>	Displays the SMS settings.
<code>show sms-service activation</code>	Displays whether the SMS service is enabled.
<code>show sms-service default-country-code</code>	Displays the default country code for the mobile phone number to which you want to send SMS messages.
<code>show sms-service provider vianett</code>	Displays the ViaNett account information.

## 38.3 SMS Commands Example

The following example enables the SMS service on the UAG to provide and configures the ViaNett account information. It then displays the SMS settings.

```
Router# configure terminal
Router(config)# sms-service activate
Router(config)# sms-service provider vianett
Router(sms-service-vianett)# username test@example.com
Router(sms-service-vianett)# password 12345
Router(sms-service-vianett)# exit
Router(config)# show sms-service
enable sms service: yes
SMS Country-Code: 0
SMS Provider-Selected: vianett
SMS Service: Vianett
  username: test@example.com
  password: 12345
Router(config)#
```

# Bandwidth Management

## 39.1 Bandwidth Management Overview

Bandwidth management provides a convenient way to manage the use of various services on the network. It manages general protocols (for example, HTTP and FTP) and applies traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

### 39.1.1 BWM Type

The UAG supports two types of bandwidth management: **shared** and **per-user**.

The **shared** BWM type is selected by default in a bandwidth management rule. All users to which the rule is applied need to share the bandwidth configured in the rule. If the BWM type is set to **per-uer** in a rule, every user that matches the rule can use up to the configured bandwidth by his/her own.

## 39.2 Bandwidth Management Commands

The following table lists the `bwm` commands. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 118** `bwm` Commands

COMMAND	DESCRIPTION
<code>bwm &lt;1..127&gt;</code>	Enters the <code>config-bwm</code> sub-command mode to configure a bandwidth management policy. See <a href="#">Table 119 on page 191</a> for the sub-commands.
<code>[no] bwm activate</code>	Enables bandwidth management on the UAG. The <code>no</code> command disabled bandwidth management.
<code>bwm append</code>	Enters the <code>config-bwm</code> sub-command mode to add a policy to the end of the policy list. See <a href="#">Table 119 on page 191</a> for the sub-commands.
<code>bwm default inbound priority &lt;1..7&gt;</code>	Specifies a number between 1 and 7 to set the priority for incoming traffic that matches the default policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority.
<code>bwm default outbound priority &lt;1..7&gt;</code>	Specifies a number between 1 and 7 to set the priority for outgoing traffic that matches the default policy.
<code>bwm delete &lt;1..127&gt;</code>	Removes a policy.
<code>bwm insert &lt;1..127&gt;</code>	Enters the <code>config-bwm</code> sub-command mode to add a policy before the specified policy number. See <a href="#">Table 119 on page 191</a> for the sub-commands.
<code>bwm modify &lt;1..127&gt;</code>	Enters the <code>config-bwm</code> sub-command mode to configure a bandwidth management policy. See <a href="#">Table 119 on page 191</a> for the sub-commands.

**Table 118** bwm Commands (continued)

COMMAND	DESCRIPTION
bwm move <1..127> to <1..127>	Moves a policy to the number that you specified.
show bwm activation	Displays whether bandwidth management is enabled.
show bwm all	Displays all bandwidth management policies.
show bwm default	Displays the default bandwidth management policy.

## 39.2.1 Bandwidth Sub-Commands

The following table describes the sub-commands for several `bwm` commands.

**Table 119** bwm Sub-commands

COMMAND	DESCRIPTION
[no] activate	Enables a policy. The <code>no</code> command disables the policy.
[no] description <i>description</i>	Sets a descriptive name (up to 60 printable ASCII characters) for a policy.  The <code>no</code> command removes the descriptive name from the policy.
[no] destination <i>address_object</i>	Sets the destination IP address or address group for whom this policy applies.  The <code>no</code> command resets the destination IP address(es) to the default ( <code>any</code> ). <code>any</code> means all IP addresses.
[no] dscp {<0..63>   any   class {af11   af12   af13   af21   af22   af23   af31   af32   af33   af41   af42   af43   cs0   cs1   cs2   cs3   cs4   cs5   cs6   cs7   default   wmm_be0   wmm_be24   wmm_bk16   wmm_bk8   wmm_vi32   wmm_vi40   wmm_vo48   wmm_vo56}}	Specifies a DSCP code point value or sets an AF class or QoS access class of incoming or outgoing packets to which this policy applies.  <code>any</code> means all DSCP value or no DSCP marker.  The <code>no</code> command resets the DSCP code to the default ( <code>any</code> ).
[no] inbound ceiling {<0..1048576>   maximize-bandwidth-usage}	Sets the maximum bandwidth allowed for incoming traffic or enables maximize bandwidth usage to let the traffic matching this policy “borrow” any unused bandwidth on the incoming interface.  The <code>no</code> command resets the inbound maximum bandwidth to the default (0).
[no] inbound guarantee-bandwidth <0..1048576> priority <1..7>	Sets how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use and also sets a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority.  Inbound refers to the traffic the UAG sends to a connection’s initiator.  The <code>no</code> command resets the inbound guarantee bandwidth to the default (0).
[no] inbound-dscp-mark {<0..63>   class {af11   af12   af13   af21   af22   af23   af31   af32   af33   af41   af42   af43   cs0   cs1   cs2   cs3   cs4   cs5   cs6   cs7   default   wmm_be0   wmm_be24   wmm_bk16   wmm_bk8   wmm_vi32   wmm_vi40   wmm_vo48   wmm_vo56}}	Sets the DSCP value to apply to the incoming packets that match this policy.  default: to have the UAG set the DSCP value of the packets to 0.  The <code>no</code> command resets the incoming DSCP code to the default ( <code>preserve</code> ) and have the UAG keep the packets’ original DSCP value.

**Table 119** bwm Sub-commands (continued)

COMMAND	DESCRIPTION
[no] incoming-interface {interface <i>interface_name</i>   trunk <i>group_name</i> }	<p>Sets the source interface of the traffic to which this policy applies.</p> <p><i>interface_name</i>: The name of the interface. This depends on the UAG model. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.</p> <p><i>group_name</i>: A descriptive name for the trunk. The name cannot start with a number. This value is case-sensitive.</p> <p>The <code>no</code> command resets the incoming interface to the default (<i>any</i>).</p>
[no] log [alert]	<p>Sets the UAG to generate a log (and alert) for packets that match the policy.</p> <p>The <code>no</code> command sets the UAG to not generate a log and alert for packets that match the policy.</p>
[no] outbound ceiling {<0..1048576>   maximize-bandwidth-usage}	<p>Sets the maximum bandwidth allowed for outgoing traffic or enables maximize bandwidth usage to let the traffic matching this policy “borrow” any unused bandwidth on the out-going interface.</p> <p>The <code>no</code> command resets the outbound maximum bandwidth to the default (0).</p>
[no] outbound guarantee-bandwidth <0..1048576> priority <1..7>	<p>Sets how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use and also sets a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority.</p> <p>Outbound refers to the traffic the UAG sends out from a connection’s initiator.</p> <p>The <code>no</code> command resets the outbound guarantee bandwidth to the default (0).</p>
[no] outbound-dscp-mark {<0..63>   class {af11   af12   af13   af21   af22   af23   af31   af32   af33   af41   af42   af43   cs0   cs1   cs2   cs3   cs4   cs5   cs6   cs7   default   wmm_be0   wmm_be24   wmm_bk16   wmm_bk8   wmm_vi32   wmm_vi40   wmm_vo48   wmm_vo56}}	<p>Sets the DSCP value to apply to the outgoing packets that match this policy.</p> <p><code>default</code>: to have the UAG set the DSCP value of the packets to 0.</p> <p>The <code>no</code> command resets the outgoing DSCP code to the default (<code>preserve</code>) and have the UAG keep the packets’ original DSCP value.</p>
[no] outgoing-interface {interface <i>interface_name</i>   trunk <i>group_name</i> }	<p>Sets the destination interface of the traffic to which this policy applies.</p> <p><i>interface_name</i>: The name of the interface. This depends on the UAG model. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.</p> <p><i>group_name</i>: A descriptive name for the trunk. The name cannot start with a number. This value is case-sensitive.</p> <p>The <code>no</code> command resets the outgoing interface to the default (<i>any</i>).</p>
[no] schedule <i>schedule_object</i>	<p>Specifies a schedule that defines when the policy applies.</p> <p>The <code>no</code> command resets the schedule to the default (<code>none</code>) to make the policy always effective.</p>



**Table 119** bwm Sub-commands (continued)

COMMAND	DESCRIPTION
[no] service service-object {service_name   any}	<p>Specifies a service or service group to identify the type of traffic to which this policy applies.</p> <p>any: the policy is effective for every service.</p> <p>The no command resets the service to the default (any).</p>
show	Displays the policy settings.
[no] source address_object	<p>Sets the source IP address or address group for whom this policy applies.</p> <p>The no command resets the source IP address(es) to the default (any). any means all IP addresses.</p>
[no] type {per-user   shared}	<p>Sets the type of bandwidth management.</p> <p>per-user: to allow every user that matches this policy to use up to the bandwidth configured in this policy.</p> <p>shared: to have users that match this policy to share the bandwidth configured in this policy.</p> <p>The no command resets the bandwidth management type to the default (shared).</p>
[no] user user_name	<p>Sets a user name or user group to which to apply the policy.</p> <p>The no command resets the user name to the default (any). any means all users.</p>

## 39.3 Bandwidth Management Commands Example

The following example adds a new bandwidth management policy for trial-users to limit incoming and outgoing bandwidth and sets the traffic priority to 3. It then displays the policy settings.

```
Router# configure terminal
Router(config)# bwm append
Router(config-bwm append 6)# activate
Router(config-bwm append 6)# description example
Router(config-bwm append 6)# user trial-users
Router(config-bwm append 6)# inbound guarantee-bandwidth 800 priority 3
Router(config-bwm append 6)# outbound guarantee-bandwidth 700 priority 3
Router(config-bwm append 6)# show
Current Configuration:
index: 6
  Activate: yes
  Description: example
  BWM Type: shared
  Schedule: none
  User: trial-users
  Incoming_Type: any
  Incoming_Interface: any
  Outgoing_Type: any
  Outgoing_Interface: any
  Src: any
  Dst: any
  Service_Type: service-object
  Service_Name: any
  Inbound_Excess: no
  Inbound_Prio: 3
  Inbound: 800
  Inbound_Ceiling: 0
  Outbound_Excess: no
  Outbound_Prio: 3
  Outbound: 700
  Outbound_Ceiling: 0
  DSCP_Code: any
  DSCP_Inbound: preserve
  DSCP_Outbound: preserve
  Log: no
Router(config-bwm append 6)# exit
Router(config)#
```

## IPSec VPN

This chapter explains how to set up and maintain IPSec VPNs in the UAG.

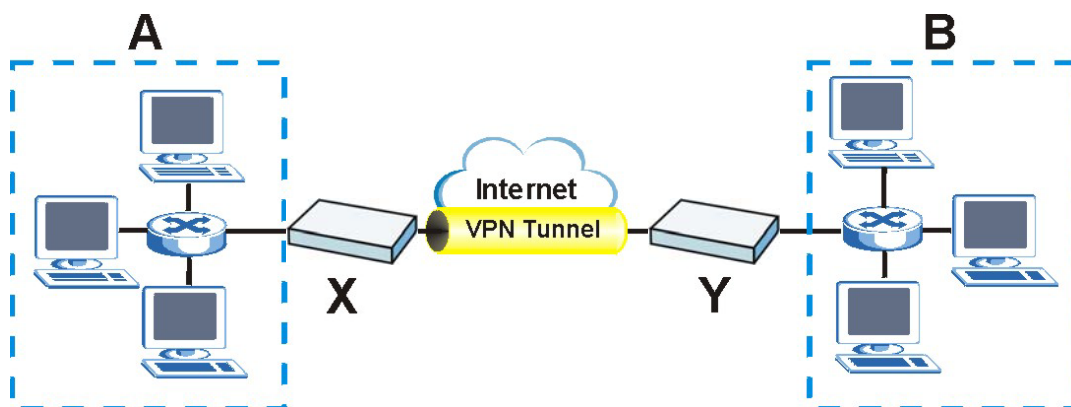
### 40.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure is one example of a VPN tunnel.

**Figure 20** VPN: Example

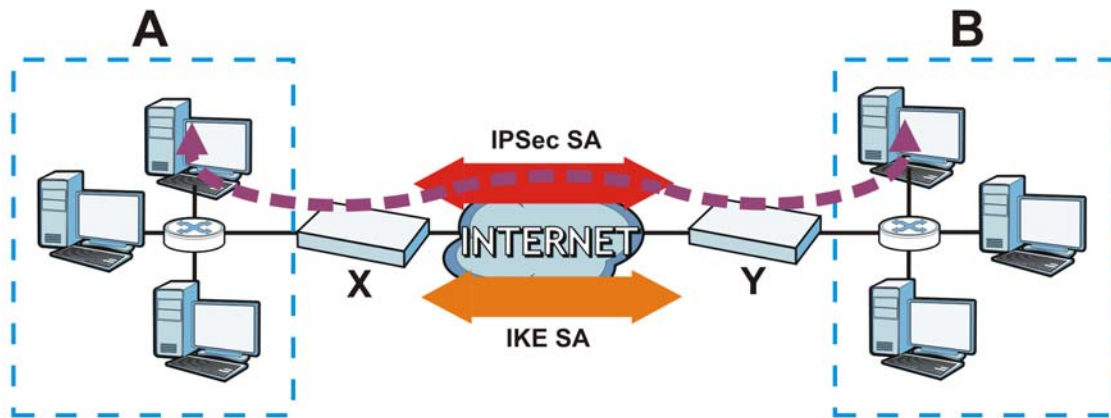


The VPN tunnel connects the UAG (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the UAG and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the UAG and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the UAG

and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

**Figure 21** VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

## 40.2 IPSec VPN Commands Summary

The following table describes the values required for many IPSec VPN commands. Other values are discussed with the corresponding commands.

**Table 120** Input Values for IPSec VPN Commands

LABEL	DESCRIPTION
<i>profile_name</i>	The name of a VPN concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>policy_name</i>	The name of an IKE SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>map_name</i>	The name of an IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>domain_name</i>	Fully-qualified domain name. You may use up to 254 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
<i>e_mail</i>	An e-mail address. You can use up to 63 alphanumeric characters, underscores (_), dashes (-), or @ characters.

**Table 120** Input Values for IPsec VPN Commands (continued)

LABEL	DESCRIPTION
<i>distinguished_name</i>	A domain name. You can use up to 511 alphanumeric, characters, spaces, or .@=, _- characters.
<i>sort_order</i>	Sort the list of currently connected SAs by one of the following classifications.  algorithm encapsulation inbound name outbound policy timeout uptime

The following sections list the IPsec VPN commands.

## 40.2.1 IKE SA Commands

This table lists the commands for IKE SAs (VPN gateways).

**Table 121** isakmp Commands: IKE SAs

COMMAND	DESCRIPTION
show isakmp keepalive	Displays the Dead Peer Detection period.
show isakmp policy [ <i>policy_name</i> ]	Shows the specified IKE SA or all IKE SAs.
isakmp keepalive <2..60>	Sets the Dead Peer Detection period.
[no] isakmp policy <i>policy_name</i>	Creates the specified IKE SA if necessary and enters sub-command mode. The no command deletes the specified IKE SA.
activate deactivate	Activates or deactivates the specified IKE SA.
authentication {pre-share   rsa-sig}	Specifies whether to use a pre-shared key or a certificate for authentication.
certificate <i>certificate-name</i>	Sets the certificate that can be used for authentication.
[no] dpd	Enables Dead Peer Detection (DPD). The no command disables DPD.  DPD allows the UAG to make sure the remote IPsec device is there before transmitting data through the IKE SA.
dpd-interval <15..60>	Sets how often (in seconds) the UAG checks if the remote IPsec device is available. If there has been no traffic from the remote IPsec device during the specified time interval, the UAG sends a message to the remote IPsec device. If it responds, the UAG transmits the data. If it does not respond, the UAG shuts down the IKE SA.
[no] fall-back	Set this to have the UAG reconnect to the primary address when it becomes available again and stop using the secondary connection, if the connection to the primary address goes down and the UAG changes to using the secondary connection.  Users will lose their VPN connection briefly while the UAG changes back to the primary connection. To use this, the peer device at the secondary address cannot be set to use a nailed-up VPN connection.
fall-back-check-interval <60..86400>	Sets how often (in seconds) the UAG checks if the primary address is available.
mode {main   aggressive}	Sets the negotiating mode.

**Table 121** isakmp Commands: IKE SAs (continued)

COMMAND	DESCRIPTION
<code>transform-set isakmp-algo [isakmp_algo [isakmp_algo]]</code>	Sets the encryption and authentication algorithms for each IKE SA proposal.  <i>isakmp_algo</i> : {des-md5   des-sha   3des-md5   3des-sha   aes128-md5   aes128-sha   aes192-md5   aes192-sha   aes256-md5   aes256-sha   aes256-sha256   aes256-sha512}
<code>lifetime &lt;180..3000000&gt;</code>	Sets the IKE SA life time to the specified value.
<code>group1</code> <code>group2</code> <code>group5</code>	Sets the DHx group to the specified group.
<code>[no] natt</code>	Enables NAT traversal. The <code>no</code> command disables NAT traversal.
<code>local-ip {ip {ip   domain_name}   interface interface_name}</code>	Sets the local gateway address to the specified IP address, domain name, or interface.
<code>peer-ip {ip   domain_name} [ip   domain_name]</code>	Sets the remote gateway address(es) to the specified IP address(es) or domain name(s).
<code>keystring pre_shared_key</code>	Sets the pre-shared key that can be used for authentication. The <i>pre_shared_key</i> can be: <ul style="list-style-type: none"> <li>• 8 - 32 alphanumeric characters or <code>;, `~!@#%&amp;^&amp;*_()+\{}!':./&lt;&gt;=-"</code>.</li> <li>• 16 - 64 hexadecimal (0-9, A-F) characters, preceded by "0x".</li> </ul> The pre-shared key is case-sensitive.
<code>local-id type {ip ip   fqdn domain_name   mail e_mail   dn distinguished_name}</code>	Sets the local ID type and content to the specified IP address, domain name, or e-mail address.
<code>peer-id type {any   ip ip   fqdn domain_name   mail e_mail   dn distinguished_name}</code>	Sets the peer ID type and content to any value, the specified IP address, domain name, or e-mail address.
<code>[no] xauth type {server xauth_method   client name username password password}</code>	Enables extended authentication and specifies whether the UAG is the server or client. If the UAG is the server, it also specifies the extended authentication method ( <i>aaa authentication profile_name</i> ); if the UAG is the client, it also specifies the username and password to provide to the remote IPsec router. The <code>no</code> command disables extended authentication.  <i>username</i> : You can use alphanumeric characters, underscores ( <code>_</code> ), and dashes ( <code>-</code> ), and it can be up to 31 characters long.  <i>password</i> : You can use most printable ASCII characters. You cannot use square brackets [ <code>]</code> ], double quotation marks ( <code>"</code> ), question marks ( <code>?</code> ), tabs or spaces. It can be up to 31 characters long.
<code>isakmp policy rename policy_name policy_name</code>	Renames the specified IKE SA (first <i>policy_name</i> ) to the specified name (second <i>policy_name</i> ).

## 40.2.2 IPsec SA Commands (except Manual Keys)

This table lists the commands for IPsec SAs, excluding manual keys (VPN connections using VPN gateways).

**Table 122** crypto Commands: IPsec SAs

COMMAND	DESCRIPTION
[no] crypto ignore-df-bit	Fragment packets larger than the MTU (Maximum Transmission Unit) that have the "don't fragment" bit in the header turned on. The no command has the UAG drop packets larger than the MTU that have the "don't fragment" bit in the header turned on.
show crypto map [map_name]	Shows the specified IPsec SA or all IPsec SAs.
crypto map dial map_name	Dials the specified IPsec SA manually. This command does not work for IPsec SAs using manual keys or for IPsec SAs where the remote gateway address is 0.0.0.0.
[no] crypto map map_name	Creates the specified IPsec SA if necessary and enters sub-command mode. The no command deletes the specified IPsec SA.
activate deactivate	Activates or deactivates the specified IPsec SA.
adjust-mss {auto   <200..1500>}	Set a specific number of bytes for the Maximum Segment Size (MSS) meaning the largest amount of data in a single TCP segment or IP datagram for this VPN connection or use auto to have the UAG automatically set it.
ipsec-isakmp policy_name	Specifies the IKE SA for this IPsec SA and disables manual key.
encapsulation {tunnel   transport}	Sets the encapsulation mode.
transform-set crypto_algo_esp [crypto_algo_esp [crypto_algo_esp]]	Sets the active protocol to ESP and sets the encryption and authentication algorithms for each proposal.  <i>crypto_algo_esp:</i> esp-null-md5   esp-null-sha   esp-null-sha256   esp-null-sha512   esp-des-md5   esp-des-sha   esp-des-sha256   esp-des-sha512   esp-3des-md5   esp-3des-sha   esp-3des-sha256   esp-3des-sha512   esp-aes128-md5   esp-aes128-sha   esp-aes128-sha256   esp-aes128-sha512   esp-aes192-md5   esp-aes192-sha   esp-aes192-sha256   esp-aes192-sha512   esp-aes256-md5   esp-aes256-sha   esp-aes256-sha256   esp-aes256-sha512
transform-set crypto_algo_ah [crypto_algo_ah [crypto_algo_ah]]	Sets the active protocol to AH and sets the encryption and authentication algorithms for each proposal.  <i>crypto_algo_ah:</i> ah-md5   ah-sha   ah-sha256   ah-sha512
scenario {site-to-site-static site-to-site-dynamic remote-access-server remote-access-client}	Select the scenario that best describes your intended VPN connection.  <i>site-to-site:</i> The remote IPsec router has a static IP address or a domain name. This UAG can initiate the VPN tunnel.  <i>site-to-site-dynamic:</i> The remote IPsec router has a dynamic IP address. Only the remote IPsec router can initiate the VPN tunnel.  <i>remote-access-server:</i> Allow incoming connections from IPsec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.  <i>remote-access-client:</i> Choose this to connect to an IPsec server. This UAG is the client (dial-in user) and can initiate the VPN tunnel.

**Table 122** crypto Commands: IPsec SAs (continued)

COMMAND	DESCRIPTION
set security-association lifetime seconds <180..3000000>	Sets the IPsec SA life time.
set pfs {group1   group2   group5   none}	Enables Perfect Forward Secrecy group.
local-policy address_name	Sets the address object for the local policy (local network).
remote-policy address_name	Sets the address object for the remote policy (remote network).
[no] policy-enforcement	Drops traffic whose source and destination IP addresses do not match the local and remote policy. This makes the IPsec SA more secure. The no command allows traffic whose source and destination IP addresses do not match the local and remote policy.  Note: You must allow traffic whose source and destination IP addresses do not match the local and remote policy, if you want to use the IPsec SA in a VPN concentrator.
[no] nail-up	Automatically re-negotiates the SA as needed. The no command does not.
[no] replay-detection	Enables replay detection. The no command disables it.
[no] netbios-broadcast	Enables NetBIOS broadcasts through the IPsec SA. The no command disables NetBIOS broadcasts through the IPsec SA.
[no] out-snat activate	Enables out-bound traffic SNAT over IPsec. The no command disables out-bound traffic SNAT over IPsec.
out-snat source address_name destination address_name snat address_name	Configures out-bound traffic SNAT in the IPsec SA.
[no] in-snat activate	Enables in-bound traffic SNAT in the IPsec SA. The no command disables in-bound traffic SNAT in the IPsec SA.
in-snat source address_name destination address_name snat address_name	Configures in-bound traffic SNAT in the IPsec SA.
[no] in-dnat activate	Enables in-bound traffic DNAT in the IPsec SA. The no command disables in-bound traffic DNAT in the IPsec SA.
in-dnat delete <1..10>	Deletes the specified rule for in-bound traffic DNAT in the specified IPsec SA.
in-dnat move <1..10> to <1..10>	Moves the specified rule (first rule number) to the specified location (second rule number) for in-bound traffic DNAT.
in-dnat append protocol {all   tcp   udp} original-ip address_name <0..65535> <0..65535> mapped-ip address_name <0..65535> <0..65535>	Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and appends this rule to the end of the rule list for in-bound traffic DNAT.
in-dnat insert <1..10> protocol {all   tcp   udp} original-ip address_name <0..65535> <0..65535> mapped-ip address_name <0..65535> <0..65535>	Maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip) and inserts this rule before the specified rule.
in-dnat <1..10> protocol {all   tcp   udp} original-ip address_name <0..65535> <0..65535> mapped-ip address_name <0..65535> <0..65535>	Creates or revises the specified rule and maps the specified IP address and port range (original-ip) to the specified IP address and port range (mapped-ip).
[no] stop-rekeying	Stops the UAG from generating a new key after tunnel renegotiation.  The no command enables the rekeying function.



**Table 122** crypto Commands: IPsec SAs (continued)

COMMAND	DESCRIPTION
<pre>conn-check {IPv4   FQDN   first-and-last} method {icmp   tcp} period &lt;5..600&gt; timeout &lt;1..10&gt; fail-tolerance &lt;1..10&gt; action {log   no-log} [port &lt;1..65535&gt;]</pre>	<p>Turns on the VPN connection check. The UAG can regularly check the VPN connection to the gateway you specified to make sure it is still available. You need to specify the gateway's domain name or IP address, or the first and last IP addresses in the connection's remote policy. Make sure one of these is the peer gateway's LAN IP address.</p> <p><code>icmp   tcp</code>: Select how the UAG checks the connection. The peer must be configured to respond to the method you select.</p> <p><code>period &lt;5..600&gt;</code>: Enter the number of seconds between connection check attempts.</p> <p><code>timeout &lt;1..10&gt;</code>: Enter the number of seconds to wait for a response before the attempt is a failure.</p> <p><code>fail-tolerance &lt;1..10&gt;</code>: Enter the number of consecutive failures allowed before the UAG disconnects the VPN tunnel.</p> <p><code>log</code>: have the UAG generate a log every time it checks this VPN connection.</p> <p><code>port &lt;1..65535&gt;</code>: Specify the port number to use for a TCP connectivity check.</p>
<pre>crypto map rename map_name map_name</pre>	<p>Renames the specified IPsec SA (first <i>map_name</i>) to the specified name (second <i>map_name</i>).</p>

## 40.2.3 IPsec SA Commands (for Manual Keys)

This table lists the additional commands for IPsec SAs using manual keys (VPN connections using manual keys).

**Table 123** crypto map Commands: IPsec SAs (Manual Keys)

COMMAND	DESCRIPTION
<code>crypto map map_name</code>	Creates the specified IPsec SA if necessary and enters sub-command mode. The <code>no</code> command deletes the specified IPsec SA.
<pre>set session-key {ah &lt;256..4095&gt; auth_key   esp &lt;256..4095&gt; [cipher enc_key] authenticator auth_key}</pre>	<p>Sets the active protocol, SPI (&lt;256..4095&gt;), authentication key and encryption key (if any).</p> <p><i>auth_key</i>: You can use any alphanumeric characters or <code>, ;   ^ ~ ! @ # \$ % ^ &amp; * ( ) _ + \ { } ' : . / &lt; &gt; = -</code>. The length of the key depends on the algorithm.</p> <p>md5 - 16-20 characters</p> <p>sha - 20 characters</p> <p>sha256 - 32 characters</p> <p>sha512 - 64 characters</p> <p><i>enc_key</i>: You can use any alphanumeric characters or <code>, ;   ^ ~ ! @ # \$ % ^ &amp; * ( ) _ + \ { } ' : . / &lt; &gt; = -</code>. The length of the key depends on the algorithm.</p> <p>des - 8-32 characters</p> <p>3des - 24-32 characters</p> <p>aes128 - 16-32 characters</p> <p>aes192 - 24-32 characters</p> <p>aes256 - 32 characters</p> <p>If you want to enter the key in hexadecimal, type "0x" at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in "0123456789ABCDEF" is in ASCII format. If you use hexadecimal, you must enter twice as many characters.</p> <p>The UAG automatically ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 1234567890XYZ for a DES encryption key, the UAG only uses 12345678. The UAG still stores the longer key.</p>
<code>local-ip ip</code>	Sets the local gateway address to the specified IP address.
<code>peer-ip ip</code>	Sets the remote gateway address to the specified IP address.

## 40.2.4 VPN Concentrator Commands

This table lists the commands for the VPN concentrator.

**Table 124** vpn-concentrator Commands: VPN Concentrator

COMMAND	DESCRIPTION
<code>show vpn-concentrator [profile_name]</code>	Shows the specified VPN concentrator or all VPN concentrators.
<code>[no] vpn-concentrator profile_name</code>	Creates the specified VPN concentrator if necessary and enters sub-command mode. The <code>no</code> command deletes the specified VPN concentrator.

**Table 124** vpn-concentrator Commands: VPN Concentrator (continued)

COMMAND	DESCRIPTION
[no] crypto <i>map_name</i>	Adds the specified IPsec SA to the specified VPN concentrator. The no command removes the specified IPsec SA from the specified VPN concentrator.
vpn-concentrator rename <i>profile_name</i> <i>profile_name</i>	Renames the specified VPN concentrator (first <i>profile_name</i> ) to the specified name (second <i>profile_name</i> ).

## 40.2.5 VPN Configuration Provisioning Commands

This table lists the commands for VPN configuration provisioning.

**Table 125** vpn-configuration-provision Commands: VPN Configuration Provisioning

COMMAND	DESCRIPTION
vpn-configuration-provision rule { append   <i>conf_index</i>   insert <i>conf_index</i> }	Enters the VPN configuration provisioning sub-command mode to add or edit a rule.  <i>conf_index</i> : The index number of a VPN configuration provisioning rule, 1 to the UAG's maximum number of VPN connection rules.
[no] activate	Turns the VPN configuration provisioning rule on or off.
crypto <i>map_name</i>	Specifies the name of the IPsec VPN connection ( <i>map_name</i> ) to bind to this VPN configuration provisioning rule's user or group.
user <i>username</i>	Specifies a user or group of users allowed to use the UAG IPsec VPN client to retrieve the associated VPN rule settings. A user may belong to a number of groups. If VPN configuration provisioning rules are configured for different groups, the UAG will allow VPN rule setting retrieval based on the first match found. Admin or limited-admin users are not allowed.
no user	Removes the VPN configuration provisioning rule's user or user group configuration. In other words, any users can match the rule. In the GUI "any" will display in the <b>Allowed User</b> field.
exit	Leaves the sub-command mode.
vpn-configuration-provision rule { delete <i>conf_index</i>   move <i>conf_index</i> to <i>conf_index</i> }	Deletes or moves the specified VPN configuration provisioning rule.
[no] vpn-configuration-provision activate	Turns the VPN configuration provisioning service on or off.
vpn-configuration-provision authentication <i>auth_method</i>	Sets the authentication method the VPN configuration provisioning service uses to authenticate users.
show vpn-configuration-provision activation	Displays whether or not the VPN configuration provisioning service is activated.
show vpn-configuration-provision authentication	Displays the authentication method the VPN configuration provisioning service uses to authenticate users.
show vpn-configuration-provision rules	Displays the settings of the configured VPN configuration provisioning rules.

## 40.2.6 SA Monitor Commands

This table lists the commands for the SA monitor.

**Table 126** sa Commands: SA Monitor

COMMAND	DESCRIPTION
<pre>show sa monitor [{begin &lt;1..1000&gt;}   {end &lt;1..1000&gt;}   {crypto-map <i>regex</i>}   {policy <i>regex</i>}   {rsort <i>sort_order</i>}   {sort <i>sort_order</i>}]</pre>	<p>Displays the current IPsec SAs and the status of each one. You can specify a range of SA entries to display. You can also control the sort order of the display and search by VPN connection or (local or remote) policy.</p> <p><i>regex</i>: A keyword or regular expression. Use up to 30 alphanumeric and _+-.()!\$*^:~ {}[]&lt;&gt;/ characters.</p> <p>A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on.</p> <p>Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use "*abc" (without the quotation marks) to specify any VPN connection or policy name that ends with "abc". A VPN connection named "testabc" would match. There could be any number (of any type) of characters in front of the "abc" at the end and the VPN connection or policy name would still match. A VPN connection or policy name named "testacc" for example would not match.</p> <p>A * in the middle of a VPN connection or policy name has the UAG check the beginning and end and ignore the middle. For example, with "abc*123", any VPN connection or policy name starting with "abc" and ending in "123" matches, no matter how many characters are in between.</p> <p>The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.</p> <p>See <a href="#">Table 120 on page 196</a> for other parameter description.</p>
show isakmp sa	Displays current IKE SA and the status of each one.
no sa spi <i>spi</i>	Deletes the SA specified by the SPI. <i>spi</i> : 2-8 hexadecimal (0-9, A-F) characters
no sa tunnel-name <i>map_name</i>	Deletes the specified IPsec SA.
show vpn-counters	Displays VPN traffic statistics.

This chapter shows you how to set up secure SSL VPN access for remote user login.

## 41.1 SSL Access Policy

An SSL access policy allows the UAG to perform the following tasks:

- limit user access to specific applications or files on the network.
- allow user access to specific networks.
- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

### 41.1.1 SSL Application Objects

SSL application objects specify an application type and server that users are allowed to access through an SSL tunnel. See [Chapter 53 on page 260](#) for how to configure SSL application objects.

### 41.1.2 SSL Access Policy Limitations

You cannot delete an object that is used by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

## 41.2 SSL VPN Commands

The following table describes the values required for some SSL VPN commands. Other values are discussed with the corresponding commands.

**Table 127** Input Values for SSL VPN Commands

LABEL	DESCRIPTION
<i>profile_name</i>	The descriptive name of an SSL VPN access policy. You may use up to 31 characters ("a-z", "A-Z", "0-9") with no spaces allowed.
<i>address_object</i>	The name of an IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>application_object</i>	The name of an SSL application object. You may use up to 31 characters ("0-9", "a-z", "A-Z", "-", and "_"). No spaces are allowed.

**Table 127** Input Values for SSL VPN Commands (continued)

LABEL	DESCRIPTION
<code>user_name</code>	The name of a user (group). You may use 1-31 alphanumeric characters, underscores( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<code>eps_profile_name</code>	The name of an endpoint security object.

The following sections list the SSL VPN commands.

## 41.2.1 SSL VPN Commands

This table lists the commands for SSL VPN. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 128** SSL VPN Commands

COMMAND	DESCRIPTION
<code>show sslvpn policy [profile_name]</code>	Displays the settings of the specified SSL VPN access policy.
<code>show ssl-vpn network-extension local-ip</code>	Displays the IP address that the UAG uses in setting up the SSL VPN.
<code>show sslvpn monitor</code>	Displays a list of the users who are currently logged into the VPN SSL client portal.
<code>sslvpn network-extension local-ip ip</code>	Sets the IP address that the UAG uses in setting up the SSL VPN.
<code>sslvpn policy {profile_name   profile_name append   profile_name insert &lt;1..16&gt;}</code>	Enters the SSL VPN sub-command mode to add or edit an SSL VPN access policy.
<code>[no] activate</code>	Turns the SSL VPN access policy on or off.
<code>[no] application application_object</code>	Adds the SSL application object to the SSL VPN access policy.
<code>[no] cache-clean activate</code>	Cleans the cookie, history, and temporary Internet files in the user's browser's cache when the user logs out. The UAG returns them to the values present before the user logged in. The <code>no</code> command disables this setting.
<code>[no] description description</code>	Adds information about the SSL VPN access policy. Use up to 60 characters ("0-9", "a-z", "A-Z", "-" and "_").
<code>[no] eps &lt;1..8&gt; eps_profile_name</code>	Sets endpoint security objects to be used for the SSL VPN access policy. The UAG checks authenticated users' computers against the policy's selected endpoint security objects in the order from 1 to 8 you specified. When a user's computer meets an endpoint security object's requirements the UAG grants access and stops checking.  To make the endpoint security check as efficient as possible, arrange the endpoint security objects in order with the one that the most users should match first and the one that the least users should match last.
<code>[no] eps activate</code>	Sets to have the UAG check that users' computers meet the Operating System (OS) and security requirements of one of the SSL access policy's selected endpoint security objects before granting access. The <code>no</code> command disables this setting.
<code>eps insert &lt;1..8&gt; eps_profile_name</code>	Inserts the specified endpoint security object to the specified position for the endpoint security objects checking order.
<code>eps move &lt;1..8&gt; to &lt;1..8&gt;</code>	Moves the first specified endpoint security object to the second specified endpoint security object's position.
<code>[no] eps periodical-check activate</code>	Sets whether to have the UAG repeat the endpoint security check at a regular interval configured using the next command. The <code>no</code> command disables this setting.

**Table 128** SSL VPN Commands

COMMAND	DESCRIPTION
[no] eps periodical-check <1..1440>	Sets the number of minutes to have the UAG repeat the endpoint security check at a regular interval. The no command disables this setting.
[no] network-extension {activate   ip-pool <i>address_object</i>   1st-dns { <i>address_object</i>   <i>ip</i> }   2nd-dns { <i>address_object</i>   <i>ip</i> }   1st-wins { <i>address_object</i>   <i>ip</i> }   2nd-wins { <i>address_object</i>   <i>ip</i> }   network <i>address_object</i> }	Use this to configure for a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network.  ip-pool: specify the name of the pool of IP addresses to assign to the user computers for the VPN connection.  Specify the names of the DNS or WINS servers to assign to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses.  network: specify a network users can access.
[no] network-extension traffic-enforcement	Forces all SSL VPN client traffic to be sent through the SSL VPN tunnel. The no command disables this setting.
[no] user <i>user_name</i>	Specifies the user or user group that can use the SSL VPN access policy.
sslvpn policy move <1..16> to <1..16>	Moves the specified SSL VPN access policy to the number that you specified.
sslvpn no connection username <i>user_name</i>	Terminates the user's SSL VPN connection and deletes corresponding session information from the UAG.
no sslvpn policy <i>profile_name</i>	Deletes the specified SSL VPN access policy.
sslvpn policy rename <i>profile_name</i> <i>profile_name</i>	Renames the specified SSL VPN access policy.
show workspace application	Displays the SSLVPN resources available to each user when logged into SSLVPN.
show workspace cifs	Displays the shared folders available to each user when logged into SSLVPN.

## 41.2.2 Setting an SSL VPN Rule Tutorial

Here is an example SSL VPN configuration. The SSL VPN rule defines:

- Only users using the "tester" account can use the SSL VPN.
- The UAG will assign an IP address from 192.168.100.1 to 192.168.100.10 (defined in object "IP-POOL") to the computers which match the rule's criteria.
- The UAG will assign two DNS server settings (172.16.1.1 and 172.16.1.2 defined in objects DNS1 and DNS2) to the computers which match the rule's criteria.
- The SSL VPN users are allowed to access the UAG's local network, 172.16.10.0/24 (defined in object "Network1").
- Users have to access the SSL VPN using a computer that complies with all the following criteria (defined in object "EPS-1"):
  - Windows XP is installed.
  - TrendMicro PC-Cillin Internet Security 2007 is installed and activated.

- 1 First of all, configure 10.1.1.254/24 for the IP address of interface wan1 which is an external interface for public SSL VPN to access. Configure 172.16.10.254/24 for the IP address of interface lan2 which is an internal network.

```
Router(config)# interface wan1
Router(config-if-ge)# ip address 10.1.1.254 255.255.255.0
Router(config-if-ge)# exit
Router(config)# interface lan2
Router(config-if-ge)# ip address 172.16.10.254 255.255.255.0
Router(config-if-ge)# exit
```

- 2 Create four address objects for the SSL VPN DHCP pool, DNS servers and the local network for SSL VPN authenticated users to access.

```
Router(config)# address-object IP-POOL 192.168.100.1-192.168.100.10
Router(config)# address-object DNS1 172.16.5.1
Router(config)# address-object DNS2 172.16.5.2
Router(config)# address-object NETWORK1 172.16.10.0/24
```

- 3 Create an endpoint security profile named EPS-1. SSL VPN users' computers must install Windows XP and TrendMicro PC-Cillin Internet Security 2007. Besides, the PC-Cillin anti-virus must be activated.

```
Router(config)# eps profile EPS-1
Router(eps EPS-1)# matching-criteria all
Router(eps EPS-1)# os-type windows
Router(eps EPS-1)# windows-version windows-xp
Router(eps EPS-1)# anti-virus activate
Router(eps EPS-1)# anti-virus TrendMicro_PC-Cillin_Internet_Security_2007 detect-
auto-protection enable
Router(eps EPS-1)# exit
```

- 4 Create the SSL VPN user account named tester with password 1234.

```
Router(config)# username tester password 1234 user-type user
```

- 5 Create an SSL VPN rule named SSL\_VPN\_TEST. Enable it and apply objects you just created.

```
Router(config)# sslvpn policy SSL_VPN_TEST
Router(policy SSL_VPN_TEST)# activate
Router(policy SSL_VPN_TEST)# user tester
Router(policy SSL_VPN_TEST)# network-extension activate
Router(policy SSL_VPN_TEST)# network-extension ip-pool IP-POOL
Router(policy SSL_VPN_TEST)# network-extension 1st-dns DNS1
Router(policy SSL_VPN_TEST)# network-extension 2nd-dns DNS2
Router(policy SSL_VPN_TEST)# network-extension network NETWORK1
Router(policy SSL_VPN_TEST)# eps activate
Router(policy SSL_VPN_TEST)# eps 1 EPS-1
Router(policy SSL_VPN_TEST)# exit
```



**6** Displays the SSL VPN rule settings.

```
Router(config)# show sslvpn policy SSL_VPN_TEST
index: 1
  active: yes
  name: SSL_VPN_TEST
  description:
  user: tester
  ssl application: none
  network extension: yes
  ip pool: IP-POOL
  dns server 1: DNS1
  dns server 2: DNS2
  wins server 1: none
  wins server 2: none
  network: NETWORK1
  cache clean: no
  eps periodical check activation: no
  eps periodical check: 1
  eps activation: yes
  eps: EPS-1
  reference count: 0
```

# Application Patrol

This chapter describes how to set up application patrol for the UAG.

## 42.1 Application Patrol Overview

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, http and ftp) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). Application patrol also has powerful bandwidth management including traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

Note: The UAG checks firewall rules before application patrol rules for traffic going through the UAG. To use a service, make sure both the firewall and application patrol allow the service's packets to go through the UAG.

Application patrol examines every TCP and UDP connection passing through the UAG and identifies what application is using the connection. Then, you can specify, by application, whether or not the UAG continues to route the connection.

## 42.2 Application Patrol Commands Summary

The following table describes the values required for many application patrol commands. Other values are discussed with the corresponding commands.

**Table 129** Input Values for Application Patrol Commands

LABEL	DESCRIPTION
<i>profile_name</i>	Type the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>description</i>	This is a description of the App Patrol Profile.

The following sections list the application patrol commands.

## 42.2.1 Application Patrol Commands

This table lists the application patrol commands.

**Table 130** app Commands: Application Patrol

COMMAND	DESCRIPTION
<code>app rename <i>profile_name_old</i> <i>profile_name_new</i></code>	Renames an existing profile
<code>[no] app log_sid</code>	Generates a log when traffic matches a signature in this category. The <code>no</code> command disables it.
<code>[no] app <i>profile_name</i></code>	Creates a profile with the specified name. You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive. The <code>no</code> command disables it.
<code>[no] description <i>description</i></code>	Write a description of the App Patrol Profile.
<code>application <i>profile_name</i> action {forward drop reject} {no log log [alert]}</code>	Sets the action and generates a log, log and alert or neither ( <code>no</code> ) when traffic matches a signature in this profile. Actions are: <ul style="list-style-type: none"> <li>• <b>forward</b> - routes packets that matches these signatures.</li> <li>• <b>drop</b> - silently drops packets that matches these signatures without notification.</li> <li>• <b>reject</b> - drops packets that matches these signatures and sends notification.</li> </ul>
<code>no application-object <i>profile_name</i></code>	Removes the application object from the named profile.
<code>[no] app statistics collect</code>	Enables application patrol statistics gathering. The <code>no</code> command disables it.
<code>app statistics flush</code>	Clears all application patrol statistics.
<code>show app statistics summary</code>	Shows a summary of application patrol statistics (if any).
<code>show app statistics collect</code>	Shows if application patrol statistics gathering is enabled and if yes, when.
<code>show app signatures version</code>	Displays the App Patrol signature set version number. This number gets larger as the set is enhanced.
<code>show app signatures date</code>	Displays the date (yyyy-mm-dd) and time the set was released.
<code>show app profiles <i>profile_name</i></code>	Shows the description, application name, and object reference number associated with the named profile.
<code>show app profiles <i>profile_name</i> application</code>	Shows the application name, action and log associated with the named profile.

### 42.2.1.1 Application Patrol Command Examples

This command shows details of an application patrol profile created.

```
Router# show app profiles
APP-patrol: 1
  profile name: appl
  description:
  application: ultrasurf_app
  ref: 1
```

These are some other example application patrol usage commands

```
Router(config)# show app statistics collect
collect statistics: yes
collect statistics time: since 2014-06-03 05:39:59 to 2014-06-10 06:20:17
Router(config)# show app signatures version
version: 3.1.4.049
Router(config)# show app signatures date
date: 2013-12-05 18:09:51
Router(config)# app john
Router(config-app-patrol-profile-john)# description this is a dummy profile
Router(config-app-patrol-profile-john)# exit
Router(config)# show app profiles
APP-patrol: 1
  profile name: testfb
  description:
  application: tests
  ref: 0
APP-patrol: 2
  profile name: test
  description: this is a test
  application:
  ref: 0
APP-patrol: 3
  profile name: john
  description: this is a dummy profile
  application:
  ref: 0
Router(config)#
```

# Content Filtering

This chapter covers how to use the content filtering feature to control web access.

## 43.1 Content Filtering Overview

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filtering policies for different addresses, schedules, users or groups and content filtering profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

## 43.2 Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filtering profile.
- Use address and/or user/group objects to define to whose web access to apply the content filtering profile.
- Apply a content filtering profile that you have custom-tailored.

## 43.3 External Web Filtering Service

When you register for and enable the external web filtering service, your UAG accesses an external database that has millions of web sites categorized based on content. You can have the UAG block, block and/or log access to web sites based on these categories.

## 43.4 Content Filter Command Input Values

The following table explains the values you can input with the `content-filter` commands.

**Table 131** Content Filter Command Input Values

LABEL	DESCRIPTION
<i>policy_number</i>	The number of the policy <0 - X > where X depends on the number of content filtering policies the UAG model supports. See the CLI help for details.
<i>address</i>	The name (up to 63 characters) of an existing address object or group to which the policy should be applied.
<i>schedule</i>	The name (up to 63 characters) of an existing schedule to control when the policy should be applied.
<i>filtering_profile</i>	The filtering profile defines how to filter web URLs or content. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>category_name</i>	The name of a web category.  {adult-mature-content  pornography  sexeducation  intimate-apparel-swimsuit  nudity  alcohol-tobacco  illegal-questionable  gambling  violence-hate-racism  weapons  abortion  hacking  phishing  arts-entertainment  business-economy  alternative-spirituality-occult  illegal-drugs  education  cultural-charitable-organization  financial-services  brokerage-trading  online-games  government-legal  military  political-activist-groups  health  computers-internet  search-engines-portals  spyware-malware-sources  spyware-effects-privacy-concerns  job-search-careers  news-media  personals-dating  reference  open-image-media-search  chat-instant-messaging  email  blogs-newsgroups  religion  social-networking  online-storage  remote-access-tools  shopping  auctions  real-estate  society-lifestyle  sexuality-alternative-lifestyles  restaurants-dining-food  sports-recreation-hobbies  travel  vehicles  humor-jokes  software-downloads  pay-to-surf  peer-to-peer  streaming-media-mp3s  proxy-avoidance  for-kids  web-advertisements  web-hosting  extreme  alcohol  tobacco  blogs-personal-pages  web-applications  suspicious  alternative-sexuality-lifestyles  lgbt  non-viewable  content-servers  placeholders}
<i>trust_hosts</i>	The IP address or domain name of a trusted web site. Use a host name such as <code>www.good-site.com</code> . Do not use the complete URL of the site – that is, do not include <code>http://</code> . All subdomains are allowed. For example, entering <code>zyxel.com</code> also allows <code>www.zyxel.com</code> , <code>partner.zyxel.com</code> , <code>press.zyxel.com</code> , etc. Use up to 63 case-insensitive characters (0-9a-z-).  You can enter a single IP address in dotted decimal notation like <code>192.168.2.5</code> .  You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32.  To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take <code>"255.255.255.0"</code> for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).  An example is <code>192.168.2.1/24</code>  You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example <code>192.168.2.5-192.168.2.23</code> .

**Table 131** Content Filter Command Input Values (continued)

LABEL	DESCRIPTION
<i>forbid_hosts</i>	<p>The IP address or domain name of a forbidden web site.</p> <p>Use a host name such as www.bad-site.com into this text field. Do not use the complete URL of the site – that is, do not include “http://”. All subdomains are also blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, etc. Use up to 63 case-insensitive characters (0-9a-z-).</p> <p>You can enter a single IP address in dotted decimal notation like 192.168.2.5.</p> <p>You can enter a subnet by entering an IP address in dotted decimal notation followed by a slash and the bit number of the subnet mask of an IP address. The range is 0 to 32.</p> <p>To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24).</p> <p>An example is 192.168.2.1/24</p> <p>You can enter an IP address range by entering the start and end IP addresses separated by a hyphen, for example 192.168.2.5-192.168.2.23.</p>
<i>keyword</i>	<p>A keyword or a numerical IP address to search URLs for and block access to if they contain it. Use up to 63 case-insensitive characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*’()%,) in double quotes. For example enter “Bad_Site” to block access to any web page that includes the exact phrase “Bad_Site”. This does not block access to web pages that only include part of the phrase (such as “Bad” in this example).</p>
<i>message</i>	<p>The message to display when a web site is blocked. Use up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*’()%,) in quotes. For example, “Access to this web page is not allowed. Please contact the network administrator.”</p>
<i>redirect_url</i>	<p>The URL of the web page to which you want to send users when their web access is blocked by content filtering. The web page you specify here opens in a new frame below the denied access message.</p> <p>Use “http://” followed by up to 255 characters (0-9a-zA-Z;/?:@&amp;=+\$\._!~*’()%,) in quotes. For example, “http://192.168.1.17/blocked access”.</p>
<i>license</i>	<p>The license key (up to 15 characters) for the external web filtering service.</p>
<i>service_timeout</i>	<p>The value specifies the maximum querying time in seconds &lt;1..60&gt;</p>
<i>_timeout</i>	<p>The value specifies the maximum life time in hours &lt;1..720&gt;.</p>
<i>url</i>	<p>The URL of a web site in http://xxx.xxx.xxx format.</p>
<i>rating_server</i>	<p>The hostname or IP address of the rating server.</p>
<i>query_timeout</i>	<p>The value specifies the maximum querying time when testing the connection to an external content filtering server or checking its rating for a URL. &lt;1..60&gt; seconds.</p>

## 43.5 General Content Filter Commands

The following table lists the commands that you can use for general content filter configuration such as enabling content filtering, viewing and ordering your list of content filtering policies, creating a denial of access message or specifying a redirect URL and checking your external web filtering service registration status. Use the `configure terminal` command to enter the configuration

mode to be able to use these commands. See [Table 131 on page 214](#) for details about the values you can input with these commands.

**Table 132** content-filter General Commands

COMMAND	DESCRIPTION
<code>[no] content-filter active</code>	Turns on content filtering. The <code>no</code> command turns it off.
<code>[no] content-filter block message <i>message</i></code>	Sets the message to display when content filtering blocks access to a web page. The <code>no</code> command clears the setting.
<code>[no] content-filter block redirect <i>redirect_url</i></code>	Sets the URL of the web page to which to send users when their web access is blocked by content filtering. The <code>no</code> command clears the setting.
<code>[no] content-filter bypass-vpn</code>	Sets the UAG to not check the packets transmitted through a VPN tunnel against content filtering policies.  The <code>no</code> command allows the UAG to check the VPN packets against content filtering policies.
<code>[no] content-filter cache-timeout <i>_timeout</i></code>	Sets how long the UAG is to keep an entry in the content filtering URL before discarding it. The <code>no</code> command clears the setting.
<code>[no] content-filter default block</code>	Has the UAG block sessions that do not match a content filtering policy. The <code>no</code> command allows sessions that do not match a content filtering policy.
<code>[no] content-filter license <i>license</i></code>	Sets the license key for the external web filtering service. The <code>no</code> command clears the setting.
<code>content-filter passed warning flush</code>	Clears the UAG's record of sessions for which it has given the user a warning before allowing access.
<code>content-filter passed warning timeout &lt;1..1440&gt;</code>	Sets how long to keep records of sessions for which the UAG has given the user a warning before allowing access.
<code>[no] content-filter policy <i>policy_number address schedule filtering_profile</i></code>	Sets a content filtering policy. The <code>no</code> command removes it.
<code>content-filter policy <i>policy_number</i> shutdown</code>	Disables a content filtering policy.
<code>content-filter url-server test bluecoat</code>	Enters the sub-command mode for testing whether or not a web site is saved in the BlueCoat external content filter server's database of restricted web pages.
<code>url [ <i>server rating_server</i> ] [ <i>timeout query_timeout</i> ]</code>	Tests whether or not a web site is saved in the external content filter server's database of restricted web pages.
<code>exit</code>	Leaves the sub-command mode.
<code>content-filter url-server test commtouch</code>	Enters the sub-command mode for testing the Commtouch external content filter server's reachability.
<code>url timeout <i>query_timeout</i></code>	Specify the Commtouch server's URL and how long to wait for a response.
<code>exit</code>	Leaves the sub-command mode.
<code>content-filter zsb port &lt;1..65535&gt;</code>	Sets the port the UAG uses to check if requested web pages pose a threat to users or their computers.
<code>content-filter common-list {<i>trust forbid</i>}</code>	Enters the sub-command for configuring a common list of trusted or forbidden web sites.  The content filtering profile commands let you configure trusted or forbidden URLs for individual profiles. URL checking is applied in the following order: profile trusted web sites, common trusted web sites, profile forbidden web sites, common forbidden web sites, and then profile keywords.



**Table 132** content-filter General Commands (continued)

COMMAND	DESCRIPTION
[no] { <i>ipv4</i>   <i>ipv4_cidr</i>   <i>ipv4_range</i>   <i>wildcard_domainname</i>   <i>tld</i> }	Adds or removes a common trusted or forbidden web site entry. <i>ipv4</i> : IPv4 address <W.X.Y.Z> <i>ipv4_cidr</i> : IPv4 subnet in CIDR format, i.e. 192.168.1.0/32 <W.X.Y.Z>/<1..32> <i>ipv4_range</i> : Range of IPv4 addresses. <W.X.Y.Z>-<W.X.Y.Z> <i>wildcard_domainname</i> : wildcard domain name, i.e. zyxel*.co* (([*a-z0-9\-]){1,63}\.)([*a-z0-9\-]){1,63} <i>tld</i> : top level domain.
exit	Leaves the sub-command mode.
show content-filter passed warning	Displays the UAG's record of sessions for which it has given the user a warning before allowing access.
show content-filter policy	Displays the content filtering policies.
show content-filter settings	Displays the general content filtering settings.
show content-filter common-list {trust forbid}	Displays the common list of trusted or forbidden web sites.

## 43.6 Content Filter Report Commands

See the web configurator User's Guide for more information about how to view content filtering reports after you have activated the category-based content filtering subscription service.

Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

**Table 133** content-filter report Commands Summary

COMMAND	DESCRIPTION
[no] content-filter report server { <i>ipv4</i>   <i>domain_name</i> }	Sets the IP address or the domain name of the server to which the UAG sends content filtering reports.  The <code>no</code> command removes the specified server.
[no] content-filter report deactivate	Sets the UAG to not collect category-based content filtering statistics.  The <code>no</code> command allows the UAG to collect category-based content filtering statistics.

## 43.7 Content Filter Profile Commands

The following table lists the commands that you can use to configure a content filtering policy. A content filtering policy defines which content filter profile should be applied, when it should be applied, and to whose web access it should be applied. Use the `configure terminal` command

to enter the configuration mode to be able to use these commands. See [Table 131 on page 214](#) for details about the values you can input with these commands.

**Table 134** content-filter profile Commands Summary

COMMAND	DESCRIPTION
[no] content-filter profile <i>filtering_profile</i>	Creates a content filtering profile. The <code>no</code> command removes the profile.
[no] content-filter profile <i>filtering_profile</i> custom	Sets a content filtering profile to use a profile's custom settings (lists of trusted web sites and forbidden web sites and blocking of certain web features). The <code>no</code> command has the profile not use the custom settings.
[no] content-filter profile <i>filtering_profile</i> custom activeX	Sets a content filtering profile to block ActiveX controls. The <code>no</code> command sets the profile to allow ActiveX.
[no] content-filter profile <i>filtering_profile</i> custom cookie	Sets a content filtering profile to block Cookies. The <code>no</code> command sets the profile to allow Cookies.
content-filter profile <i>filtering_profile</i> custom-list forbid	Enters the sub-command for configuring the content filtering profile's list of forbidden hosts.
[no] <i>forbid_hosts</i>	Adds a forbidden host to the content filtering profile's list. The <code>no</code> command removes it.
exit	Leaves the sub-command mode.
[no] content-filter profile <i>filtering_profile</i> custom java	Sets a content filtering profile to block Java. The <code>no</code> command sets the profile to allow Java.
content-filter profile <i>filtering_profile</i> custom-list keyword	Enters the sub-command for configuring the content filtering profile's list of forbidden keywords. This has the content filtering profile block access to Web sites with URLs that contain the specified keyword or IP address in the URL.
[no] <i>keyword</i>	Adds a forbidden keyword or IP address to the content filtering profile's list. The <code>no</code> command removes it.
exit	Leaves the sub-command mode.
[no] content-filter profile <i>filtering_profile</i> custom proxy	Sets a content filtering profile to block access to web proxy servers. The <code>no</code> command sets the profile to allow access to proxy servers.
content-filter profile <i>filtering_profile</i> custom-list trust	Enters the sub-command for configuring the content filtering profile's list of trusted hosts.
[no] <i>trust_hosts</i>	Adds a trusted host to the content filtering profile's list. The <code>no</code> command removes it.
exit	Leaves the sub-command mode.
[no] content-filter profile <i>filtering_profile</i> custom trust-allow-features	Sets a content filtering profile to permit Java, ActiveX and Cookies from sites on the trusted list. The <code>no</code> command has the content filtering profile not permit Java, ActiveX and Cookies from sites on the trusted list
[no] content-filter profile <i>filtering_profile</i> custom trust-only	Sets a content filtering profile to only allow access to web sites that are on the trusted list. The <code>no</code> command has the profile allow access to web sites that are not on the trusted list.
[no] content-filter profile <i>filtering_profile</i> url category {category_name}	Sets a content filtering profile to check for specific web site categories. The <code>no</code> command has the profile not check for the specified categories.
content-filter profile <i>filtering_profile</i> url match-unsafe {block   log   pass}	Sets the action for attempted access to web pages that match the profile's selected unsafe categories.  Block access, log access, or allow access.

**Table 134** content-filter profile Commands Summary (continued)

COMMAND	DESCRIPTION
content-filter profile <i>filtering_profile</i> url match {block   log   warn   pass}	Sets the action for attempted access to web pages that match the profile's selected managed categories.  Block access, allow and log access, display a warning message before allowing access, or allow access.
content-filter profile <i>filtering_profile</i> url offline {block   log   warn   pass}	Sets the action for attempted access to web pages if the external content filtering database is unavailable.  Block access, allow and log access, display a warning message before allowing access, or allow access.
content-filter profile <i>filtering_profile</i> url unrate {block   log   warn   pass}	Sets the action for attempted access to web pages that the external web filtering service has not categorized.  Block access, allow and log access, display a warning message before allowing access, or allow access.
no content-filter profile <i>filtering_profile</i> url match-unsafe {log}	Has the UAG not log attempted access to web pages that match the profile's selected unsafe categories.
no content-filter profile <i>filtering_profile</i> url match {log}	Has the UAG not log attempted access to web pages that match the profile's selected managed categories.
no content-filter profile <i>filtering_profile</i> url offline {log}	Has the UAG not log access to web pages if the external content filtering database is unavailable.
no content-filter profile <i>filtering_profile</i> url unrate {log}	Has the UAG not log access to web pages that the external web filtering service has not categorized.
[no] content-filter profile <i>filtering_profile</i> url url-server	Sets a content filtering profile to use the external web filtering service. The no command has the profile not use the external web filtering service.
[no] content-filter service-timeout <i>service_timeout</i>	Sets how many seconds the UAG is to wait for a response from the external content filtering server. The no command clears the setting.
[no] content-filter profile <i>filtering_profile</i> commtouch-url category {category_name}	Sets a CommTouch content filtering profile to check for specific web site categories. The no command has the profile not check for the specified categories.
content-filter profile <i>filtering_profile</i> commtouch-url match-unsafe {block   log   warn   pass}	Sets the action for attempted access to web pages that match the CommTouch profile's selected unsafe categories.  Block access, log access, display a warning message before allowing access, or allow access.
content-filter profile <i>filtering_profile</i> commtouch-url match {block   log   pass}	Sets the action for attempted access to web pages that match the CommTouch profile's selected managed categories.  Block access, allow and log access, or allow access.
content-filter profile <i>filtering_profile</i> commtouch-url offline {block   log   warn   pass}	Sets the action for attempted access to web pages if the CommTouch external content filtering database is unavailable.  Block access, allow and log access, display a warning message before allowing access, or allow access.
content-filter profile <i>filtering_profile</i> commtouch-url unrate {block   log   warn   pass}	Sets the action for attempted access to web pages that the CommTouch external web filtering service has not categorized.  Block access, allow and log access, display a warning message before allowing access, or allow access.
no content-filter profile <i>filtering_profile</i> commtouch-url match-unsafe {log}	Has the UAG not log attempted access to web pages that match the CommTouch profile's selected unsafe categories.

**Table 134** content-filter profile Commands Summary (continued)

COMMAND	DESCRIPTION
<code>no content-filter profile <i>filtering_profile</i> commtouch-url match {log}</code>	Has the UAG not log attempted access to web pages that match the CommTouch profile's selected managed categories.
<code>no content-filter profile <i>filtering_profile</i> commtouch-url offline {log}</code>	Has the UAG not log access to web pages if the CommTouch external content filtering database is unavailable.
<code>no content-filter profile <i>filtering_profile</i> commtouch-url unrate {log}</code>	Has the UAG not log access to web pages that the CommTouch external web filtering service has not categorized.
<code>show content-filter profile [<i>filtering_profile</i>]</code>	Displays the specified content filtering profile's settings or the settings of all them if you don't specify one.

## 43.8 Content Filter URL Cache Commands

The following table lists the commands that you can use to view and configure your UAG's URL caching. You can configure how long a categorized web site address remains in the cache as well as view those web site addresses to which access has been allowed or blocked based on the responses from the external content filtering server. The UAG only queries the external content filtering database for sites not found in the cache.

Use the `configure` terminal command to enter the configuration mode to be able to use these commands. See [Table 131 on page 214](#) for details about the values you can input with these commands.

**Table 135** content-filter url-cache Commands

COMMAND	DESCRIPTION
<code>[no] content-filter cache-timeout <i>_timeout</i></code>	Sets how long to keep a content filtering URL cache entry before discarding it. The <code>no</code> command clears the setting.
<code>show content-filter url-cache [<i>all-category</i>] [<i>begin url_cache_range</i> end <i>url_cache_range</i>] [<i>_count</i>]</code>	Displays the contents of the content filtering URL cache. You can specify a range and number of entries to display.
<code>show content-filter url-cache</code>	Displays the contents of the content filtering URL cache.
<code>content-filter url-cache test</code>	Enters the sub-command mode for testing whether or not a web site is saved in the UAG's database of restricted web pages.
<code>url</code>	Tests whether or not a web site is saved in the UAG's database of restricted web pages.
<code>exit</code>	Leaves the sub-command mode.

## 43.9 Content Filtering Statistics

The following table describes the commands for collecting and displaying content filtering statistics. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 136** Commands for Content Filtering Statistics

COMMAND	DESCRIPTION
<code>[no] content-filter statistics collect</code>	Turn the collection of content filtering statistics on or off.
<code>content-filter statistics flush</code>	Clears the collected statistics.
<code>show content-filter statistics summary</code>	Displays the collected statistics.
<code>show content-filter statistics collect</code>	Displays whether the collection of content filtering statistics is turned on or off.
<code>show content-filter statistics summary</code>	Displays the current content filtering statistics.

### 43.9.1 Content Filtering Statistics Example

This example shows how to collect and display content filtering statistics.

```
Router(config)# content-filter statistics collect
Router(config)# show content-filter statistics summary
total web pages inspected           : 0
  web pages warned by category service : 0
  web pages blocked by category service: 0
  web pages blocked by custom service : 0
    restricted web features           : 0
    forbidden web sites                : 0
    url keywords                       : 0
  web pages blocked without policy    : 0
  web pages passed                    : 0

unsafe web pages                    : 0
other web pages                     : 0
```

## 43.10 Content Filtering Commands Example

The following example shows how to limit the web access for a sales group.

- 1 First, create a sales address object. This example uses a subnet that covers IP addresses 172.16.3.1 to 172.16.3.254.
- 2 Then create a schedule for all day.
- 3 Create a filtering profile for the group.
- 4 You can use the following commands to block sales from accessing adult and pornography websites.
- 5 Enable the external web filtering service.

Note: You must register for the external web filtering service before you can use it (see [Chapter 5 on page 48](#)).

- 6 You can also customize the filtering profile. The following commands block active-X, java and proxy access.
- 7 Append a content filter policy.
- 8 Activate the customization.

```
Router# configure terminal
Router(config)# address-object sales 172.16.3.0/24
Router(config)# schedule-object all_day 00:00 23:59
Router(config)# content-filter profile sales_CF_PROFILE
Router(config)# content-filter profile sales_CF_PROFILE url category adult-mature-content
Router(config)# content-filter profile sales_CF_PROFILE url category pornography
Router(config)# content-filter profile sales_CF_PROFILE url url-server
Router(config)# content-filter profile sales_CF_PROFILE custom java
Router(config)# content-filter profile sales_CF_PROFILE custom activex
Router(config)# content-filter profile sales_CF_PROFILE custom proxy
Router(config)# content-filter profile sales_CF_PROFILE custom
Router(config)# content-filter policy append all_day any RD RD_CF_PROFILE
Router(config)# content-filter activate
```

Use this command to display the settings of the profile.

```

Router(config)# show content-filter profile sales_CF_PROFILE commtouch
service active : yes
url match unsafe: block: no, warn: yes, log: no
url match other : block: yes, warn: no, log: no
url unrate      : block: no, warn: yes, log: no
service offline : block: no, warn: yes, log: no

category settings:
Adult/Mature Content      : yes, Pornography           : yes
Sex Education             : no, Intimate Apparel/Swimsuit : no
Nudity                   : no, Alcohol/Tobacco       : no
Illegal/Questionable     : no, Gambling              : no
Violence/Hate/Racism     : no, Weapons               : no
Abortion                  : no, Hacking                : no
Phishing                  : no, Arts/Entertainment    : no
Business/Economy         : no, Alternative Spirituality/Occult : no
Illegal Drugs             : no, Education              : no
Cultural/Charitable Organization: no, Financial Services      : no
Brokerage/Trading        : no, Online Games           : no
Government/Legal         : no, Military                : no
Political/Activist Groups : no, Health                  : no
Computers/Internet       : no, Search Engines/Portals  : no
Spyware/Malware Sources  : no, Spyware Effects/Privacy Concerns: no
Job Search/Careers       : no, News/Media             : no
Personals/Dating         : no, Reference               : no
Open Image/Media Search  : no, Chat/Instant Messaging  : no
Email                    : no, Blogs/Newsgroups       : no
Religion                  : no, Social Networking      : no
Online Storage           : no, Remote Access Tools    : no
Shopping                 : no, Auctions               : no
Real Estate              : no, Society/Lifestyle      : no
Sexuality/Alternative Lifestyles: no, Restaurants/Dining/Food : no
Sports/Recreation/Hobbies : no, Travel                  : no
Vehicles                 : no, Humor/Jokes            : no
Software Downloads       : no, Pay to Surf            : no
Peer-to-Peer             : no, Streaming Media/MP3s    : no
Proxy Avoidance          : no, For Kids                : no
Web Advertisements       : no, Web Hosting             : no
Extreme                  : no, Alcohol                 : no
Tobacco                  : no, Blogs/Personal Pages    : no
Web Applications         : no, Suspicious              : no
Alternative Sexuality/Lifestyles: no, LGBT                     : no
Non-viewable             : no, Content Servers         : no
Placeholders             : no, Open/Mixed Content      : no
Potentially Unwanted Software : no, Greeting Cards          : no
Audio/Video Clips        : no, Media Sharing            : no
Radio/Audio Streams      : no, TV/Video Streams        : no
Internet Telephony       : no, Online Meetings         : no
Newsgroups/Forums        : no, Art/Culture              : no
Entertainment            : no, Games                    : no
Sports/Recreation        : no, Translation              : no
Alternative Spirituality/Belief : no, Society/Daily Living     : no
-----SNIP!-----

```

## User/Group

This chapter describes how to set up user accounts, user groups, and user settings for the UAG. You can also set up rules that control when users have to log in to the UAG before the UAG routes traffic for them (see [Chapter 29 on page 158](#)).

### 44.1 User Account Overview

A user account defines the privileges of a user logged into the UAG. User accounts are used in firewall rules, in addition to controlling access to configuration and services in the UAG.

#### 44.1.1 User Types

There are the types of user accounts the UAG uses.

**Table 137** Types of User Accounts

TYPE	ABILITIES	LOGIN METHOD(S)
<b>Admin Users</b>		
Admin	Change UAG configuration (web, CLI)	WWW, TELNET, SSH, FTP
Limited-Admin	Look at UAG configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH
<b>Access Users</b>		
User	Access network services Browse user-mode commands (CLI)	WWW, TELNET, SSH
Guest	Access network services	WWW
Ext-User	External user account	WWW
ext-group-user	External group user account	WWW
guest-manager	Create dynamic guest accounts	WWW
pre-subscriber	Access network services	Web Authentication Portal
dynamic-guest	Access network services See <a href="#">Chapter 55 on page 269</a> for more information about the dynamic guest accounts.	Web Authentication Portal

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See [Chapter 50 on page 250](#) for more information about authentication methods.)



## 44.2 User/Group Commands Summary

The following table identifies the values required for many `username/groupname` commands. Other input values are discussed with the corresponding commands.

**Table 138** username/groupname Command Input Values

LABEL	DESCRIPTION
<code>username</code>	The name of the user (account). You may use 1-31 alphanumeric characters, underscores( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<code>groupname</code>	The name of the user group. You may use 1-31 alphanumeric characters, underscores( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive. It cannot be the same as the user name.

The following sections list the `username/groupname` commands.

### 44.2.1 User Commands

The first table lists the commands for users.

**Table 139** username/groupname Commands Summary: Users

COMMAND	DESCRIPTION
<code>show username [username]</code>	Displays information about the specified user or about all users set up in the UAG.
<code>username username nopassword user-type {admin   pre-subscriber   guest-manager   user   guest   limited-admin}</code>	Creates the specified user (if necessary), disables the password, and sets the user type for the specified user.
<code>username username password password user-type {admin   pre-subscriber   guest-manager   user   guest   limited-admin}</code>	Creates the specified user (if necessary); enables and sets the password; and sets the user type for the specified user. <i>password</i> : You can use 1-63 printable ASCII characters, except double quotation marks (") and question marks (?).
<code>username username user-type ext-user</code>	Creates the specified user (if necessary) and sets the user type to <b>Ext-User</b> .
<code>username username user-type mac-address</code>	Creates the specified user (if necessary) and sets the user type to <b>mac-address</b> .
<code>username username user-type ext-group-user associated-aaa-server server_profile group-id id</code>	Specify the value of the AD or LDAP server's Group Membership Attribute that identifies the group to which the specified ext-group-user type user account belongs.
<code>no username username</code>	Deletes the specified user.
<code>username username [no] description description</code>	Sets the description for the specified user. The <code>no</code> command clears the description. <i>description</i> : You can use alphanumeric and <code>()+/:=?!*#@\$_%-</code> characters, and it can be up to 60 characters long.
<code>username username [no] logon-due-time time</code>	Sets the time (in 24-hour format) at which the user will be automatically logged out of the UAG and has to log in again. The <code>no</code> command resets the due time to its default value (12:00).
<code>username username [no] logon-lease-time &lt;0..1440&gt;</code>	Sets the lease time for the specified user. Set it to zero to set unlimited lease time. The <code>no</code> command sets the lease time to five minutes (regardless of the current default setting for new users).

**Table 139** username/groupname Commands Summary: Users (continued)

COMMAND	DESCRIPTION
username <i>username</i> logon-time-setting {default   manual}	Sets the account to use the factory default lease and reauthentication times or custom ones.
username <i>username</i> [no] logon-re-auth-time <0..1440>	Sets the reauthentication time for the specified user. Set it to zero to set unlimited reauthentication time. The no command sets the reauthentication time to thirty minutes (regardless of the current default setting for new users).
username <i>username</i> logon-re-auth-type {due-time   re-auth-time}	Sets whether the specified user will be logged out and have to log into the UAG again according to the due time or reauthentication time settings.
username rename <i>username username</i>	Renames the specified user (first <i>username</i> ) to the specified username (second <i>username</i> ).

### 44.2.1.1 Username Setting Command Examples

The following commands create a new user account and show the user information.

```
Router# configure terminal
Router(config)# username test password 1234 user-type guest
Router(config)# username test logon-due-time 07:30
Router(config)# username test logon-re-auth-type due-time
Router(config)# show username test
username           : test
password           : $1$gRsJDU29$rh1PqNQyspuqhoqgC3n1M1
description        : Local User
user type          : guest
time setting       : manual
lease time         : 1440
re-auth type       : due-time
re-auth time       : 1440
due time           : 07:30
reference count    : 0
Router(config)#
```

### 44.2.2 User Group Commands

This table lists the commands for groups.

**Table 140** username/groupname Commands Summary: Groups

COMMAND	DESCRIPTION
show groupname [ <i>groupname</i> ]	Displays information about the specified user group or about all user groups set up in the UAG.
[no] groupname <i>groupname</i>	Creates the specified user group if necessary and enters sub-command mode. The no command deletes the specified user group.
[no] description <i>description</i>	Sets the description for the specified user group. The no command clears the description for the specified user group.
[no] groupname <i>groupname</i>	Adds the specified user group (second <i>groupname</i> ) to the specified user group (first <i>groupname</i> ).
[no] user <i>username</i>	Adds the specified user to the specified user group.
show	Displays information about the specified user group.
groupname rename <i>groupname groupname</i>	Renames the specified user group (first <i>groupname</i> ) to the specified group-name (second <i>groupname</i> ).

## 44.2.3 User Setting Commands

This table lists the commands for user settings, except for forcing user authentication.

**Table 141** username/groupname Commands Summary: Settings

COMMAND	DESCRIPTION
<code>show users default-setting {all   user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user}}</code>	Displays the default lease and reauthentication times for the specified type of user accounts.
<code>users default-setting [no] logon-lease-time &lt;0..1440&gt;</code>	Sets the default lease time (in minutes) for each new user. Set it to zero to set unlimited lease time. The <code>no</code> command sets the default lease time to five.
<code>users default-setting [no] logon-re-auth-time &lt;0..1440&gt;</code>	Sets the default reauthorization time (in minutes) for each new user. Set it to zero to set unlimited reauthorization time. The <code>no</code> command sets the default reauthorization time to thirty.
<code>users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user}</code>	Sets the default user type for each new user. The <code>no</code> command sets the default user type to user.
<code>users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user} logon-due-time time</code>	Sets the time (in 24-hour format) at which the the specified type of new user will be automatically logged out of the UAG and has to log in again. The <code>no</code> command resets the due time to its default value (12:00).
<code>users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user} logon-lease-time &lt;0..1440&gt;</code>	Sets the default lease time (in minutes) for each type of new user. Set it to zero for unlimited lease time. The <code>no</code> command sets the default lease time to five.
<code>users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user} logon-re-auth-type {due-time   re-auth-time}</code>	Sets whether the specified type of new user will be logged out and have to log into the UAG again according to the due time or reauthentication time settings.
<code>users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user} logon-re-auth-time &lt;0..1440&gt;</code>	Sets the default reauthorization time (in minutes) for each type of new user. Set it to zero for unlimited reauthorization time. The <code>no</code> command sets the default reauthorization time to thirty.
<code>show users kick-previous-settings</code>	Displays whether the UAG is set to disassociate the first user that logged in and allow new user to log in when the maximum number of simultaneous logins by each account is reached.
<code>[no] users kick-previous [billing]</code>	Sets the UAG to disassociate the first user that logged in and allow new user to log in when the maximum number of simultaneous logins by each account is reached.  billing: billing account  The <code>no</code> command sets the UAG to stop new users from logging in when the maximum number of simultaneous logins by each account is reached.
<code>show users retry-settings</code>	Displays the current retry limit settings for users.
<code>[no] users retry-limit</code>	Enables the retry limit for users. The <code>no</code> command disables the retry limit.
<code>[no] users retry-count &lt;1..99&gt;</code>	Sets the number of failed login attempts a user can have before the account or IP address is locked out for lockout-period minutes. The <code>no</code> command sets the retry-count to five.
<code>[no] users lockout-period &lt;1..65535&gt;</code>	Sets the amount of time, in minutes, a user or IP address is locked out after retry-count number of failed login attempts. The <code>no</code> command sets the lockout period to thirty minutes.
<code>show users simultaneous-logon-settings</code>	Displays the current settings for simultaneous logins by users.

**Table 141** username/groupname Commands Summary: Settings (continued)

COMMAND	DESCRIPTION
[no] users simultaneous-logon {administration   access   billing-account} enforce	Enables the limit on the number of simultaneous logins by users of the specified account-type. The no command disables the limit, or allows an unlimited number of simultaneous logins.
[no] users simultaneous-logon {administration   access   billing-account} limit <i>login_number</i>	Sets the limit for the number of simultaneous logins by users of the specified account-type. The no command sets the limit to one.  <i>login_number</i> : The maximum number of simultaneous logins by each user. 1 - X where X is the highest number of simultaneous logins the UAG model supports.
show users update-lease-settings	Displays whether or not access users can automatically renew their lease time.
[no] users update-lease automation	Lets users automatically renew their lease time. The no command prevents them from automatically renewing it.
show users idle-detection-settings	Displays whether or not users are automatically logged out, and, if so, how many minutes of idle time must pass before they are logged out.
[no] users idle-detection	Enables logging users out after a specified number of minutes of idle time. The no command disables logging them out.
[no] users idle-detection timeout <1..60>	Sets the number of minutes of idle time before users are automatically logged out. The no command sets the idle-detection timeout to three minutes.

### 44.2.3.1 User Setting Command Examples

The following commands show the current settings for the number of simultaneous logins.

```
Router# configure terminal
Router(config)# show users simultaneous-logon-settings
enable simultaneous logon limitation for administration account: yes
maximum simultaneous logon per administration account      : 1
enable simultaneous logon limitation for access account    : yes
maximum simultaneous logon per access account              : 3
```

### 44.2.4 MAC Auth Commands

This table lists the commands for mappings MAC addresses to MAC address user accounts.

**Table 142** mac-auth Commands Summary

COMMAND	DESCRIPTION
[no] mac-auth database mac <i>mac_address</i> type ext-mac-address mac-role <i>username</i> description <i>description</i>	Maps the specified MAC address authenticated by an external server to the specified MAC role (MAC address user account).  The no command deletes the mapping between the MAC address and the MAC role.
[no] mac-auth database mac <i>mac_address</i> type int-mac-address mac-role <i>username</i> description <i>description</i>	Maps the specified MAC address authenticated by the UAG's local user database to the specified MAC role (MAC address user account).  The no command deletes the mapping between the MAC address and the MAC role.

**Table 142** mac-auth Commands Summary

COMMAND	DESCRIPTION
[no] mac-auth database mac oui type ext-oui mac-role username description description	Maps the specified OUI (Organizationally Unique Identifier) authenticated by an external server to the specified MAC role (MAC address user account). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.  The no command deletes the mapping between the OUI and the MAC role.
[no] mac-auth database mac oui type int-oui mac-role username description description	Maps the specified OUI (Organizationally Unique Identifier) authenticated by the UAG's local user database to the specified MAC role (MAC address user account). The OUI is the first three octets in a MAC address and uniquely identifies the manufacturer of a network device.  The no command deletes the mapping between the OUI and the MAC role.

#### 44.2.4.1 MAC Auth Example

This example uses an external server to authenticate wireless clients by MAC address. After authentication the UAG maps the wireless client to a mac-address user account (MAC role). Configure user-aware features to control MAC address user access to network services.

The following commands:

- Create a MAC role (mac-address user type user account) named ZyXEL-mac
- Map a wireless client's MAC address of 00:13:49:11:a0:c4 to the ZyXEL-mac MAC role (MAC address user account)
- Modify the WLAN security profile named secureWLAN1 as follows:
  - Turn on MAC authentication
  - Use the authentication method named Auth1
  - Use colons to separate the two-character pairs within account MAC addresses
  - Use upper case letters in the account MAC addresses

```
Router(config)# username ZyXEL-mac user-type mac-address
Router(config)# mac-auth database mac 00:13:49:11:a0:c4 type ext-mac-address mac-role
ZyXEL-mac description zyxel mac

3. Modify wlan-security-profile
Router(config)# wlan-security-profile secureWLAN1
Router(config-wlan-security default)# mac-auth activate
Router(config-wlan-security default)# mac-auth auth-method Auth1
Router(config-wlan-security default)# mac-auth delimiter account colon
Router(config-wlan-security default)# mac-auth case account upper
Router(config-wlan-security default)# exit
```

## 44.2.5 Additional User Commands

This table lists additional commands for users.

**Table 143** username/groupname Commands Summary: Additional

COMMAND	DESCRIPTION
show users {username   all   current}	Displays information about the users logged onto the system.
show lockout-users	Displays users who are currently locked out.
unlock lockout-users {ip   console}	Unlocks the specified IP address.
users force-logout username   ip	Logs out the specified login.

### 44.2.5.1 Additional User Command Examples

The following commands display the users that are currently logged in to the UAG and forces the logout of all logins from a specific IP address.

```
Router# configure terminal
Router(config)# show users all
No: 0
  Name: admin
  Type: admin
  From: console
  Service: console
  Session_Time: 25:46:00
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Type: re-auth-time
  Re_Auth_Timeout: unlimited
  Due_time: N/A
  User_Info: admin
No: 1
  Name: admin
  Type: admin
  From: 192.168.1.34
  Service: http/https
  Session_Time: 00:02:26
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Type: re-auth-time
  Re_Auth_Timeout: unlimited
  Due_time: N/A
  User_Info: admin
Router(config)# users force-logout 192.168.1.34
Logout user 'admin'(from 192.168.1.34 ): OK
Total 1 user has been forced logout
Router(config)# show users all
No: 0
  Name: admin
  Type: admin
  From: console
  Service: console
  Session_Time: 25:48:33
  Idle_Time: unlimited
  Lease_Timeout: unlimited
  Re_Auth_Type: re-auth-time
  Re_Auth_Timeout: unlimited
  Due_time: N/A
  User_Info: admin
```

The following commands display the users that are currently locked out and then unlocks the user who is displayed.

```
Router# configure terminal
Router(config)# show lockout-users
No.  Username Tried          From          Lockout Time Remaining
=====
No.  From          Failed Login Attempt  Record Expired Timer
=====1
172.16.1.5          2                46

Router(config)# unlock lockout-users 172.16.1.5
User from 172.16.1.5 is unlocked
Router(config)# show lockout-users
No.  Username Tried          From          Lockout Time Remaining
=====
No.  From          Failed Login Attempt  Record Expired Timer
=====
```

## Application Object

Check that you have the latest App Patrol signatures.

### 45.1 Application Object Commands Summary

The following table describes the values required for many application object commands. Other values are discussed with the corresponding commands.

**Table 144** Input Values for Application Object Commands

LABEL	DESCRIPTION
<i>object_name</i>	Type the name of the object.
<i>description</i>	This is a description of the object
<i>sid</i>	This is the associated IDP and App Patrol signature ID number.

#### 45.1.1 Application Object Commands

This table lists the application object commands.

**Table 145** application-object Commands

COMMAND	DESCRIPTION
show application-object <i>object_name</i>	Displays information on the named application object.
application-object <i>object_name</i>	Creates an object with the specified name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. The no command disables it.
[no] description <i>description</i>	Write a description of the object.
[no] application <i>sid</i>	Write a valid signature ID for the object. The no command disables it.
no application-object <i>object_name</i>	Deletes the object with the specified name.
application-object rename <i>object_name1</i> <i>object_name2</i>	Renames the specified object with a new name.



### 45.1.1.1 application-object Examples

These are some example usage commands.

```
Router(config)# show application-object
Name
Description                               Ref
Content
=====
tests
New Create                               1
Facebook Game (access)
Router(config)# show application-object tests
Name: tests
Description: New Create
Category                               Application
Application ID
=====
Social Network                           Facebook Game (access)
402685702
Router(config)#
```

### 45.1.2 Application Object Group Commands

This table lists the application object group commands.

**Table 146** object-group application Commands

COMMAND	DESCRIPTION
show object-group application <i>object_group_name</i>	Displays information on the named application object group.
object-group application <i>object_group_name</i>	Creates an application object group. with the specified name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. The no command disables it.
[no] description <i>description</i>	Write a description of the object group.
[no] application-object <i>object_name</i>	Adds the named application object to the object group. The no command removes it.
no object-group application <i>&lt;object_group_name</i>	Deletes the object group with the specified name.
object-group application rename <i>object_group_name1 object_group_name2</i>	Renames the specified object group with a new name.

### 45.1.2.1 object-group application Examples

These are some example usage commands.

```
Router(config)# show object-group application
Name
Description
Member
=====
Router(config)# object-group application may
Router(group-application)# description rinse after use
Router(group-application)# exit
Router(config)# show object-group application
Name
Description
Member
=====
may
rinse after use
tests
Router(config)#
```

# Addresses

This chapter describes how to set up addresses and address groups for the UAG.

## 46.1 Address Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

You can create IP address objects based on an interface's IP address, subnet, or gateway. The UAG automatically updates these objects whenever the interface's IP address settings change. This way every rule or setting that uses the object uses the updated IP address settings. For example, if you change the LAN1 interface's IP address, the UAG automatically updates the corresponding interface-based, LAN1 subnet address object. So any configuration that uses the LAN1 subnet address object is also updated.

Address objects and address groups are used in dynamic routes, firewall rules, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

## 46.2 Address Commands Summary

The following table describes the values required for many address object and address group commands. Other values are discussed with the corresponding commands.

**Table 147** Input Values for Address Commands

LABEL	DESCRIPTION
<i>object_name</i>	The name of the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>group_name</i>	The name of the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>interface_name</i>	The name of the interface. This depends on the UAG model. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.

The following sections list the address object and address group commands.

## 46.2.1 Address Object Commands

This table lists the commands for address objects.

**Table 148** address-object and address6-object Commands

COMMAND	DESCRIPTION
show {address-object   address6-object   service-object   schedule-object} [object_name]	Displays information about the specified object or all the objects of the specified type.
address-object object_name {ip   ip_range   ip_subnet   interface-ip   interface-subnet   interface-gateway} {interface}	Creates the specified IPv4 address object using the specified parameters.  ip_range: <1..255>.<0..255>.<0..255>.<1..255>-<1..255>.<0..255>.<0..255>.<1..255>  ip_subnet: <1..255>.<0..255>.<0..255>.<0..255>/<1..32>  interface: Specify an interface when you create an object based on an interface.
no address-object object_name	Deletes the specified address object.
address-object rename object_name object_name	Renames the specified address (first object_name) to the second object_name.

### 46.2.1.1 Address Object Command Examples

The following example creates three IPv4 address objects and then deletes one.

```
Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.1-192.168.1.20
Router(config)# address-object A2 192.168.1.0/24
Router(config)# show address-object
Object name          Type      Address                               Ref.
=====
A0                   HOST      192.168.1.1                          0
A1                   RANGE     192.168.1.1-192.168.1.20             0
A2                   SUBNET    192.168.1.0/24                       0
Router(config)# no address-object A2
Router(config)# show address-object
Object name          Type      Address                               Ref.
=====
A0                   HOST      192.168.1.1                          0
A1                   RANGE     192.168.1.1-192.168.1.20             0
```

## 46.2.2 Address Group Commands

This table lists the commands for address groups.

**Table 149** object-group Commands: Address Groups

COMMAND	DESCRIPTION
show object-group {address   address6} [group_name]	Displays information about the specified address group or about all address groups.
[no] object-group address group_name	Creates the specified address group if necessary and enters sub-command mode. The no command deletes the specified address group.

**Table 149** object-group Commands: Address Groups (continued)

COMMAND	DESCRIPTION
[no] address-object <i>object_name</i>	Adds the specified address to the specified address group. The no command removes the specified address from the specified group.
[no] object-group <i>group_name</i>	Adds the specified address group (second <i>group_name</i> ) to the specified address group (first <i>group_name</i> ). The no command removes the specified address group from the specified address group.
[no] description <i>description</i>	Sets the description to the specified value. The no command clears the description.  <i>description</i> : You can use alphanumeric and ( ) + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
object-group address rename <i>group_name</i> <i>group_name</i>	Renames the specified address group from the first <i>group_name</i> to the second <i>group_name</i> .

### 46.2.2.1 Address Group Command Examples

The following commands create three address objects A0, A1, and A2 and add A1 and A2 to address group RD.

```

Router# configure terminal
Router(config)# address-object A0 192.168.1.1
Router(config)# address-object A1 192.168.1.2-192.168.2.20
Router(config)# address-object A2 192.168.3.0/24
Router(config)# object-group address RD
Router(group-address)# address-object A1
Router(group-address)# address-object A2
Router(group-address)# exit
Router(config)# show object-group address
Group name          Reference
Description
=====
TW_TEAM             5
RD                  0

Router(config)# show object-group address RD
Object/Group name   Type   Reference
=====
A1                  Object 1
A2                  Object 1

```

## Services

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

### 47.1 Services Overview

See the appendices in the web configurator's User Guide for a list of commonly-used services.

### 47.2 Services Commands Summary

The following table describes the values required for many service object and service group commands. Other values are discussed with the corresponding commands.

**Table 150** Input Values for Service Commands

LABEL	DESCRIPTION
<i>group_name</i>	The name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>object_name</i>	The name of the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.

The following sections list the service object and service group commands.

#### 47.2.1 Service Object Commands

The first table lists the commands for service objects.

**Table 151** service-object Commands: Service Objects

COMMAND	DESCRIPTION
<code>show service-object [object_name]</code>	Displays information about the specified service or about all the services.
<code>no service-object object_name</code>	Deletes the specified service.
<code>service-object object_name {tcp   udp} {eq &lt;1..65535&gt;   range &lt;1..65535&gt; &lt;1..65535&gt;}</code>	Creates the specified TCP service or UDP service using the specified parameters.

**Table 151** service-object Commands: Service Objects (continued)

COMMAND	DESCRIPTION
<code>service-object object_name icmp icmp_value</code>	Creates the specified ICMP message using the specified parameters.  <i>icmp_value</i> : <0..255>   alternate-address   conversion-error   echo   echo-reply   information-reply   information-request   mask-reply   mask-request   mobile-redirect   parameter-problem   redirect   router-advertisement   router-solicitation   source-quench   time-exceeded   timestamp-reply   timestamp-request   unreachable
<code>service-object object_name protocol &lt;1..255&gt;</code>	Creates the specified user-defined service using the specified parameters.
<code>service-object rename object_name object_name</code>	Renames the specified service from the first <i>object_name</i> to the second <i>object_name</i> .

### 47.2.1.1 Service Object Command Examples

The following commands create four services, displays them, and then removes one of them.

```

Router# configure terminal
Router(config)# service-object TELNET tcp eq 23
Router(config)# service-object FTP tcp range 20 21
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# service-object MULTICAST protocol 2
Router(config)# show service-object
Object name          Protocol          Minmum port    Maxmum port    Ref.
=====
TELNET               TCP               23             23             0
FTP                  TCP               20             21             0
ICMP_ECHO            ICMP              0              0              0
MULTICAST            2                 0              0              0
Router(config)# no service-object ICMP_ECHO
Router(config)# show service-object
Object name          Protocol          Minmum port    Maxmum port    Ref.
=====
TELNET               TCP               23             23             0
FTP                  TCP               20             21             0
MULTICAST            2                 0              0              0

```

### 47.2.2 Service Group Commands

The first table lists the commands for service groups.

**Table 152** object-group Commands: Service Groups

COMMAND	DESCRIPTION
<code>show object-group service group_name</code>	Displays information about the specified service group.
<code>[no] object-group service group_name</code>	Creates the specified service group if necessary and enters sub-command mode. The <code>no</code> command removes the specified service group.
<code>[no] service-object object_name</code>	Adds the specified service to the specified service group. The <code>no</code> command removes the specified service from the specified group.
<code>[no] object-group group_name</code>	Adds the specified service group (second <i>group_name</i> ) to the specified service group (first <i>group_name</i> ). The <code>no</code> command removes the specified service group from the specified service group.

**Table 152** object-group Commands: Service Groups (continued)

COMMAND	DESCRIPTION
[no] description <i>description</i>	Sets the description to the specified value. The no command removes the description.  <i>description</i> : You can use alphanumeric and ()+/:=?!*#@\$_%- characters, and it can be up to 60 characters long.
object-group service rename <i>group_name</i> <i>group_name</i>	Renames the specified service group from the first <i>group_name</i> to the second <i>group_name</i> .

### 47.2.2.1 Service Group Command Examples

The following commands create service ICMP\_ECHO, create service group SG1, and add ICMP\_ECHO to SG1.

```

Router# configure terminal
Router(config)# service-object ICMP_ECHO icmp echo
Router(config)# object-group service SG1
Router(group-service)# service-object ICMP_ECHO
Router(group-service)# exit
Router(config)# show service-object ICMP_ECHO
Object name          Protocol          Minmum port    Maxmum port    Ref.
=====
ICMP_ECHO            ICMP              8              8              1
Router(config)# show object-group service SG1
Object/Group name    Type             Reference
=====
ICMP_ECHO            Object 1

```



## Schedules

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules, and content filtering.

### 48.1 Schedule Overview

The UAG supports two types of schedules: one-time and recurring. One-time schedules are effective only once, while recurring schedules usually repeat.

Note: Schedules are based on the current date and time in the UAG.

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

### 48.2 Schedule Commands Summary

The following table describes the values required for many schedule commands. Other values are discussed with the corresponding commands.

**Table 153** Input Values for Schedule Commands

LABEL	DESCRIPTION
<i>object_name</i>	The name of the schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>time</i>	24-hour time, hours and minutes; <0..23>:<0..59>.

The following table lists the schedule commands.

**Table 154** schedule Commands

COMMAND	DESCRIPTION
<code>show schedule-object</code>	Displays information about the schedules in the UAG.
<code>no schedule-object <i>object_name</i></code>	Deletes the schedule object.

**Table 154** schedule Commands (continued)

COMMAND	DESCRIPTION
<code>schedule-object object_name date time date time</code>	Creates or updates a one-time schedule. <i>date</i> : yyyy-mm-dd date format; yyyy-<01..12>-<01..31>
<code>schedule-object object_name time time [day] [day] [day] [day] [day] [day] [day]</code>	Creates or updates a recurring schedule. <i>day</i> : 3-character day of the week; sun   mon   tue   wed   thu   fri   sat

## 48.2.1 Schedule Command Examples

The following commands create recurring schedule SCHEDULE1 and one-time schedule SCHEDULE2 and then delete SCHEDULE1.

```
Router# configure terminal
Router(config)# schedule-object SCHEDULE1 11:00 12:00 mon tue wed thu fri
Router(config)# schedule-object SCHEDULE2 2006-07-29 11:00 2006-07-31 12:00
Router(config)# show schedule-object
Object name          Type          Start/End          Ref.
=====
SCHEDULE1            Recurring    11:00/12:00    ===MonTueWedThuFri=== 0
SCHEDULE2            Once         2006-07-29 11:00/2006-07-31 12:00 0

Router(config)# no schedule-object SCHEDULE1
Router(config)# show schedule-object
Object name          Type          Start/End          Ref.
=====
SCHEDULE2            Once         2006-07-29 11:00/2006-07-31 12:00 0
```

## AAA Server

This chapter introduces and shows you how to configure the UAG to use external authentication servers.

### 49.1 AAA Server Overview

You can use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network.

The following lists the types of authentication server the UAG supports.

- Local user database

The UAG uses the built-in local user database to authenticate administrative users logging into the UAG's web configurator or network access users logging into the network through the UAG. You can also use the local user database to authenticate VPN users.

- Directory Service (LDAP/AD)

LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

- RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

### 49.2 Authentication Server Command Summary

This section describes the commands for authentication server settings.

#### 49.2.1 ad-server Commands

The following table lists the `ad-server` commands you use to set the default AD server.

**Table 155** ad-server Commands

COMMAND	DESCRIPTION
<code>show ad-server</code>	Displays the default AD server settings.
<code>[no] ad-server basedn basedn</code>	Sets a base distinguished name (DN) for the default AD server. A base DN identifies an AD directory. The <code>no</code> command clears this setting.

**Table 155** ad-server Commands (continued)

COMMAND	DESCRIPTION
[no] ad-server binddn <i>binddn</i>	Sets the user name the UAG uses to log into the default AD server. The no command clears this setting.
[no] ad-server cn-identifier <i>uid</i>	Sets the unique common name (cn) to identify a record. The no command clears this setting.
[no] ad-server host <i>ad_server</i>	Sets the AD server address. Enter the IP address (in dotted decimal notation) or the domain name. The no command clears this setting.
[no] ad-server password <i>password</i>	Sets the bind password. This password will be encrypted when you use the show ad-server command to display. The no command clears this setting.
[no] ad-server password-encrypted <i>password</i>	Sets the encrypted password (less than 32 alphanumeric characters) in order to hide the real password from people behind you when you are configuring AD server password. This password is displayed as what you typed when you use the show ad-server command.
[no] ad-server port <i>port_no</i>	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
[no] ad-server search-time-limit <i>time</i>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting.
[no] ad-server ssl	Enables the UAG to establish a secure connection to the AD server. The no command disables this feature.

## 49.2.2 ldap-server Commands

The following table lists the ldap-server commands you use to set the default LDAP server.

**Table 156** ldap-server Commands

COMMAND	DESCRIPTION
show ldap-server	Displays current LDAP server settings.
[no] ldap-server basedn <i>basedn</i>	Sets a base distinguished name (DN) for the default LDAP server. A base DN identifies an LDAP directory. The no command clears this setting.
[no] ldap-server binddn <i>binddn</i>	Sets the user name the UAG uses to log into the default LDAP server. The no command clears this setting.
[no] ldap-server cn-identifier <i>uid</i>	Sets the unique common name (cn) to identify a record. The no command clears this setting.
[no] ldap-server host <i>ldap_server</i>	Sets the LDAP server address. Enter the IP address (in dotted decimal notation) or the domain name. The no command clears this setting.
[no] ldap-server password <i>password</i>	Sets the bind password. The no command clears this setting.
[no] ldap-server password-encrypted <i>password</i>	Sets an encrypted bind password. The no command clears this setting.
[no] ldap-server port <i>port_no</i>	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The no command clears this setting.
[no] ldap-server search-time-limit <i>time</i>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting.
[no] ldap-server ssl	Enables the UAG to establish a secure connection to the LDAP server. The no command disables this feature.

### 49.2.3 radius-server Commands

The following table lists the `radius-server` commands you use to set the default RADIUS server.

**Table 157** radius-server Commands

COMMAND	DESCRIPTION
<code>show radius-server</code>	Displays the default RADIUS server settings.
<code>[no] radius-server host radius_server auth-port auth_port</code>	Sets the RADIUS server address and service port number. Enter the IP address (in dotted decimal notation) or the domain name of a RADIUS server. The <code>no</code> command clears the settings.
<code>[no] radius-server key secret</code>	Sets a password (up to 15 alphanumeric characters) as the key to be shared between the RADIUS server and the UAG. The <code>no</code> command clears this setting.
<code>[no] radius-server timeout time</code>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The <code>no</code> command clears this setting.

### 49.2.4 radius-server Command Example

The following example sets the secret key and timeout period of the default RADIUS server (172.16.10.100) to "87643210" and 80 seconds.

```
Router# configure terminal
Router(config)# radius-server host 172.16.10.100 auth-port 1812
Router(config)# radius-server key 876543210
Router(config)# radius-server timeout 80
Router(config)# show radius-server
host                : 172.16.10.100
authentication port: 1812
key                 : 876543210
timeout             : 80
Router(config)#
```

### 49.2.5 aaa group server ad Commands

The following table lists the `aaa group server ad` commands you use to configure a group of AD servers.

**Table 158** aaa group server ad Commands

COMMAND	DESCRIPTION
<code>clear aaa group server ad [group-name]</code>	Deletes all AD server groups or the specified AD server group.  Note: You can NOT delete a server group that is currently in use.
<code>show aaa group server ad group-name</code>	Displays the specified AD server group settings.
<code>[no] aaa group server ad group-name</code>	Sets a descriptive name for an AD server group. Use this command to enter the sub-command mode.  The <code>no</code> command deletes the specified server group.
<code>aaa group server ad rename group-name group-name</code>	Changes the descriptive name for an AD server group.
<code>aaa group server ad group-name</code>	Enter the sub-command mode to configure an AD server group.
<code>[no] case-sensitive</code>	Specify whether or not the server checks the username case. Set this to be the same as the server's behavior.

**Table 158** aaa group server ad Commands (continued)

COMMAND	DESCRIPTION
[no] server alternative-cn-identifier <i>uid</i>	Sets the second type of identifier that the users can use to log in if any. For example "name" or "e-mail address". The <code>no</code> command clears this setting.
[no] server basedn <i>basedn</i>	Sets the base DN to point to the AD directory on the AD server group. The <code>no</code> command clears this setting.
[no] server binddn <i>binddn</i>	Sets the user name the UAG uses to log into the AD server group. The <code>no</code> command clears this setting.
[no] server cn-identifier <i>uid</i>	Sets the user name the UAG uses to log into the AD server group. The <code>no</code> command clears this setting.
[no] server description <i>description</i>	Sets the descriptive information for the AD server group. You can use up to 60 printable ASCII characters. The <code>no</code> command clears the setting.
[no] server group-attribute <i>group-attribute</i>	<p>Sets the name of the attribute that the UAG is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values.</p> <p>For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create an ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management". The <code>no</code> command clears the setting.</p>
[no] server host <i>ad_server</i>	Enter the IP address (in dotted decimal notation) or the domain name of an AD server to add to this group. The <code>no</code> command clears this setting.
[no] server password <i>password</i>	Sets the bind password (up to 15 alphanumeric characters). The <code>no</code> command clears this setting.
[no] server port <i>port_no</i>	Sets the AD port number. Enter a number between 1 and 65535. The default is 389. The <code>no</code> command clears this setting.
[no] server search-time-limit <i>time</i>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The <code>no</code> command clears this setting and set this to the default setting of 5 seconds.
[no] server ssl	Enables the UAG to establish a secure connection to the AD server. The <code>no</code> command disables this feature.

## 49.2.6 aaa group server ldap Commands

The following table lists the `aaa group server ldap` commands you use to configure a group of LDAP servers.

**Table 159** aaa group server ldap Commands

COMMAND	DESCRIPTION
<code>clear aaa group server ldap [group-name]</code>	<p>Deletes all LDAP server groups or the specified LDAP server group.</p> <p>Note: You can NOT delete a server group that is currently in use.</p>
<code>show aaa group server ldap group-name</code>	Displays the specified LDAP server group settings.
[no] <code>aaa group server ldap group-name</code>	<p>Sets a descriptive name for an LDAP server group. Use this command to enter the sub-command mode.</p> <p>The <code>no</code> command deletes the specified server group.</p>
<code>aaa group server ldap rename group-name group-name</code>	Changes the descriptive name for an LDAP server group.
<code>aaa group server ldap group-name</code>	Enter the sub-command mode.

**Table 159** aaa group server ldap Commands (continued)

COMMAND	DESCRIPTION
[no] case-sensitive	Specify whether or not the server checks the username case. Set this to be the same as the server's behavior.
[no] server alternative-cn-identifier <i>uid</i>	Sets the second type of identifier that the users can use to log in if any. For example "name" or "e-mail address". The <code>no</code> command clears this setting.
[no] server basedn <i>basedn</i>	Sets the base DN to point to the LDAP directory on the LDAP server group. The <code>no</code> command clears this setting.
[no] server binddn <i>binddn</i>	Sets the user name the UAG uses to log into the LDAP server group. The <code>no</code> command clears this setting.
[no] server cn-identifier <i>uid</i>	Sets the user name the UAG uses to log into the LDAP server group. The <code>no</code> command clears this setting.
[no] server description <i>description</i>	Sets the descriptive information for the LDAP server group. You can use up to 60 printable ASCII characters. The <code>no</code> command clears this setting.
[no] server group-attribute <i>group-attribute</i>	<p>Sets the name of the attribute that the UAG is to check to determine to which group a user belongs. The value for this attribute is called a group identifier; it determines to which group a user belongs. You can add ext-group-user user objects to identify groups based on these group identifier values.</p> <p>For example you could have an attribute named "memberOf" with values like "sales", "RD", and "management". Then you could also create an ext-group-user user object for each group. One with "sales" as the group identifier, another for "RD" and a third for "management". The <code>no</code> command clears the setting.</p>
[no] server host <i>ldap_server</i>	Enter the IP address (in dotted decimal notation) or the domain name of an LDAP server to add to this group. The <code>no</code> command clears this setting.
[no] server password <i>password</i>	Sets the bind password (up to 15 characters). The <code>no</code> command clears this setting.
[no] server port <i>port_no</i>	Sets the LDAP port number. Enter a number between 1 and 65535. The default is 389. The <code>no</code> command clears this setting.
[no] server search-time-limit <i>time</i>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The <code>no</code> command clears this setting and set this to the default setting of 5 seconds.
[no] server ssl	Enables the UAG to establish a secure connection to the LDAP server. The <code>no</code> command disables this feature.

## 49.2.7 aaa group server radius Commands

The following table lists the `aaa group server radius` commands you use to configure a group of RADIUS servers.

**Table 160** aaa group server radius Commands

COMMAND	DESCRIPTION
<code>clear aaa group server radius <i>group-name</i></code>	<p>Deletes all RADIUS server groups or the specified RADIUS server group.</p> <p><b>Note:</b> You can NOT delete a server group that is currently in use.</p>
<code>show aaa group server radius <i>group-name</i></code>	Displays the specified RADIUS server group settings.
[no] <code>aaa group server radius <i>group-name</i></code>	Sets a descriptive name for the RADIUS server group. The <code>no</code> command deletes the specified server group.
<code>aaa group server radius rename {<i>group-name-old</i>} <i>group-name-new</i></code>	Sets the server group name.

**Table 160** aaa group server radius Commands (continued)

COMMAND	DESCRIPTION
aaa group server radius <i>group-name</i>	Enter the sub-command mode.
[no] case-sensitive	Specify whether or not the server checks the username case. Set this to be the same as the server's behavior.
[no] server acct-address <i>radius_server</i> acct-port <i>auth_port</i>	Sets the IP address (in dotted decimal notation) or the domain name of a RADIUS accounting server to add to this server group. This also sets the port number (between 1 and 65535) on the RADIUS accounting server to which the UAG sends accounting information.  The no command clears this setting.
[no] server acct-interim activate	Sets the UAG to send subscriber status updates to the RADIUS server at the specified interval.  The no command sets the UAG to not send subscriber status updates to the RADIUS server.
[no] server acct-interim-interval <i>interval</i>	Sets the time interval for how often the UAG is to send a subscriber status update to the RADIUS server.  The no command clears this setting.
[no] server acct-retry-count <1-10>	At times the UAG may not be able to use the primary RADIUS accounting server. Sets the number of times the UAG should reattempt to use the primary RADIUS server before attempting to use the secondary RADIUS server. This also sets how many times the UAG will attempt to use the secondary RADIUS server.  If there is also no response from the secondary RADIUS server, the UAG stops attempting to authenticate the subscriber. The subscriber will see a message that says the RADIUS server was not found.  The no command clears this setting and sets this to the default setting.
[no] server acct-secret <i>secret</i>	Sets a password (up to 32 alphanumeric characters) as the key to be shared between the external accounting server and the UAG. The key is not sent over the network. This key must be the same on the external accounting server and the UAG.  The no command clears this setting.
[no] server nas-ip <i>NAS_ADDRESS</i>	Sets the Network Access Server (NAS) IP address attribute if the RADIUS server requires the UAG to provide it with a specific value.  The no command clears this setting.
[no] server nas-id <i>NAS_IDENTIFIER</i>	Sets the Network Access Server (NAS) identifier attribute if the RADIUS server requires the UAG to provide it with a specific value. You can use up to 64 characters.  The no command clears this setting.
[no] server description <i>description</i>	Sets the descriptive information for the RADIUS server group. You can use up to 60 printable ASCII characters. The no command clears the setting.
[no] server group-attribute <1-255>	Sets the value of an attribute that the UAG is used to determine to which group a user belongs.  This attribute's value is called a group identifier. You can add <b>ext-group-user</b> user objects to identify groups based on different group identifier values.  For example, you could configure attributes 1,10 and 100 and create a <b>ext-group-user</b> user object for each of them. The no command clears the setting.



**Table 160** aaa group server radius Commands (continued)

COMMAND	DESCRIPTION
[no] server host <i>radius_server</i> auth-port <i>auth_port</i>	Sets the IP address (in dotted decimal notation) or the domain name of a RADIUS server to add to this server group. This also sets the port number (between 1 and 65535) on the RADIUS server to which the UAG sends accounting information.  The no command clears this setting.
[no] server key <i>secret</i>	Sets a password (up to 32 alphanumeric characters) as the key to be shared between the RADIUS server(s) and the UAG. The no command clears this setting.
[no] server timeout <i>time</i>	Sets the search timeout period (in seconds). Enter a number between 1 and 300. The no command clears this setting and sets this to the default setting of 5 seconds.

## 49.2.8 aaa group server Command Example

The following example creates a RADIUS server group with two authentication members and sets the secret key to "12345678" and the timeout to 100 seconds. This example also sets two accounting members in this group. Then this example also shows how to view the RADIUS group settings.

```

Router> configure terminal
Router(config)# aaa group server radius RADIUSGroup1
Router(group-server-radius)# server host 192.168.1.100 auth-port 1812
Router(group-server-radius)# server host 172.16.12.100 auth-port 1812
Router(group-server-radius)# server key 12345678
Router(group-server-radius)# server timeout 100
Router(group-server-radius)# server acct-address 192.168.1.101 acct-port 1813
Router(group-server-radius)# server acct-address 172.16.13.100 acct-port 1813
Router(group-server-radius)# server acct-secret 12345678
Router(group-server-radius)# server acct-interim activate
Router(group-server-radius)# server acct-interim-interval 30
Router(group-server-radius)# exit
Router(config)# show aaa group server radius RADIUSGroup1
Key                               : 12345678
timeout                           : 100
description                        :
group attribute                    : 11
nas-ip                             : 127.0.0.1
nas-id                             :
acct-secret                        : 12345678
acct-retry-count                   : 3
acct-interim-interval              : 30
acct-interim-activate              : yes
case-sensitive                     : yes

No.  Host Member                               Auth. Port
=====
1    192.168.1.100                             1812
2    172.16.12.100                             1812

No.  Acct Member                               Acct. Port
=====
3    192.168.1.101                             1813
4    172.16.13.100                             1813

```

# Authentication Objects

This chapter shows you how to select different authentication methods for user authentication using the AAA servers or the internal user database.

## 50.1 Authentication Objects Overview

After you have created the AAA server objects, you can specify the authentication objects (containing the AAA server information) that the UAG uses to authenticate users (using VPN or managing through HTTP/HTTPS).

## 50.2 aaa authentication Commands

The following table lists the `aaa authentication` commands you use to configure an authentication profile.

**Table 161** aaa authentication Commands

COMMAND	DESCRIPTION
<code>aaa authentication rename <i>profile-name-old profile-name-new</i></code>	Changes the profile name.  <i>profile-name</i> : You may use 1-31 alphanumeric characters, underscores ( <code>_</code> ), or dashes ( <code>-</code> ), but the first character cannot be a number. This value is case-sensitive.
<code>clear aaa authentication <i>profile-name</i></code>	Deletes all authentication profiles or the specified authentication profile.  <b>Note:</b> You can NOT delete a profile that is currently in use.
<code>show aaa authentication {<i>group-name</i> default}</code>	Displays the specified authentication server profile settings.
<code>[no] aaa authentication <i>profile-name</i></code>	Sets a descriptive name for the authentication profile. The <code>no</code> command deletes a profile.
<code>[no] aaa authentication default <i>member1 [member2] [member3] [member4]</i></code>	Sets the default profile to use the authentication method(s) in the order specified.  <i>member</i> = group ad, group ldap, group radius, or local.  <b>Note:</b> You must specify at least one member for each profile. Each type of member can only be used once in a profile.  The <code>no</code> command clears the specified authentication method(s) for the profile.

**Table 161** aaa authentication Commands (continued)

COMMAND	DESCRIPTION
[no] aaa authentication <i>profile-name</i> <i>member1</i> [ <i>member2</i> ] [ <i>member3</i> ] [ <i>member4</i> ]	Sets the profile to use the authentication method(s) in the order specified.  <i>member</i> = group ad, group ldap, group radius, or local.  Note: You must specify at least one member for each profile. Each type of member can only be used once in a profile.  The no command clears the specified authentication method(s) for the profile.
aaa authentication [no] match- default-group	Enable this to treat a user successfully authenticated by a remote auth server as a default-ext-user. If the remote authentication server is LDAP, the default-ext-user account is an ldap-user. If the remote authentication server is AD, the default-ext-user account is an ad-user. If the remote authentication server is RADIUS, the default-ext-user account is a radius-user.

## 50.2.1 aaa authentication Command Example

The following example creates an authentication profile to authentication users using the LDAP server group and then the local user database.

```
Router# configure terminal
Router(config)# aaa authentication LDAPuser group ldap local
Router(config)# show aaa authentication LDAPuser
No.  Method
=====
0    ldap
1    local
Router(config)#
```

## 50.3 test aaa Command

The following table lists the test aaa command you use to test a user account on an authentication server.

**Table 162** test aaa Command

COMMAND	DESCRIPTION
test aaa {server secure-server} {ad ldap} host {hostname ipv4-address} [host {hostname ipv4- address}] port <1..65535> base-dn <i>base-dn-string</i> [bind-dn <i>bind-dn-string</i> password <i>password</i> ] login- name-attribute <i>attribute</i> [alternative-login-name- attribute <i>attribute</i> ] account <i>account-name</i>	Tests whether a user account exists on the specified authentication server.

### 50.3.1 Test a User Account Command Example

The following example shows how to test whether a user account named userABC exists on the AD authentication server which uses the following settings:

- IP address: 172.16.50.1
- Port: 389
- Base-dn: DC=ZyXEL,DC=com

- Bind-dn: zyxel\engineerABC
- Password: abcdefg
- Login-name-attribute: sAMAccountName

The result shows the account exists on the AD server. Otherwise, the UAG responds an error.

```
Router> test aaa server ad host 172.16.50.1 port 389 base-dn DC=ZyXEL,DC=com bind-dn
zyxel\engineerABC password abcdefg login-name-attribute sAMAccountName account
userABC

dn:: Q049MTIzNzco546L5aOr56uRKsXPVT1XaXRoTWFpbCxEQz1aeVhFTcxEQz1jb20=
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn:: MTIzNzco546L5aOr56uRKQ==
sn: User
l: 2341100
-----SNIP!-----
```

# Certificates

This chapter explains how to use the **Certificates**.

## 51.1 Certificates Overview

The UAG can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the UAG to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

## 51.2 Certificate Commands

This section describes the commands for configuring certificates.

## 51.3 Certificates Commands Input Values

The following table explains the values you can input with the `certificate` commands.

**Table 163** Certificates Commands Input Values

LABEL	DESCRIPTION
<i>certificate_name</i>	The name of a certificate. You can use up to 31 alphanumeric and ;'~!@#\$\$%^&()_+[]{}',.- characters.
<i>cn_address</i>	A common name IP address identifies the certificate's owner. Type the IP address in dotted decimal notation.
<i>cn_domain_name</i>	A common name domain name identifies the certificate's owner. The domain name is for identification purposes only and can be any string. The domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.
<i>cn_email</i>	A common name e-mail address identifies the certificate's owner. The e-mail address is for identification purposes only and can be any string. The e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore.
<i>organizational_unit</i>	Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.

**Table 163** Certificates Commands Input Values (continued)

LABEL	DESCRIPTION
<i>organization</i>	Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
<i>country</i>	Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore.
<i>key_length</i>	Type a number to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
<i>password</i>	When you have the UAG enroll for a certificate immediately online, the certification authority may want you to include a key (password) to identify your certification request. Use up to 31 of the following characters. a-zA-Z0-9; `~!@#\$%^&*()_+ \{ } ' : , / < > = -
<i>ca_name</i>	When you have the UAG enroll for a certificate immediately online, you must have the certification authority's certificate already imported as a trusted certificate. Specify the name of the certification authority's certificate. It can be up to 31 alphanumeric and ;'~!@#\$%^&*()_+ [ ] { } ' , . = - characters.
<i>url</i>	When you have the UAG enroll for a certificate immediately online, enter the IP address (or URL) of the certification authority server. You can use up to 511 of the following characters. a-zA-Z0-9'()+,/.:.=?;!*#@\$_%-

## 51.4 Certificates Commands Summary

The following table lists the commands that you can use to display and manage the UAG's summary list of certificates and certification requests. You can also create certificates or certification requests. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

**Table 164** ca Commands Summary

COMMAND	DESCRIPTION
<code>ca enroll cmp name <i>certificate_name</i> cn-type {ip cn <i>cn_address</i> fqdn cn <i>cn_domain_name</i> mail cn <i>cn_email</i>} [ou <i>organizational_unit</i>] [o <i>organization</i>] [c <i>country</i>] key-type {rsa dsa} key-len <i>key_length</i> num &lt;0..99999999&gt; password <i>password</i> ca <i>ca_name</i> url <i>url</i>;</code>	Enrolls a certificate with a CA using Certificate Management Protocol (CMP). The certification authority may want you to include a reference number and key (password) to identify your certification request.
<code>ca enroll scep name <i>certificate_name</i> cn-type {ip cn <i>cn_address</i> fqdn cn <i>cn_domain_name</i> mail cn <i>cn_email</i>} [ou <i>organizational_unit</i>] [o <i>organization</i>] [c <i>country</i>] key-type {rsa dsa} key-len <i>key_length</i> password <i>password</i> ca <i>ca_name</i> url <i>url</i></code>	Enrolls a certificate with a CA using Simple Certificate Enrollment Protocol (SCEP). The certification authority may want you to include a key (password) to identify your certification request.
<code>ca generate pkcs10 name <i>certificate_name</i> cn-type {ip cn <i>cn_address</i> fqdn cn <i>cn_domain_name</i> mail cn <i>cn_email</i>} [ou <i>organizational_unit</i>] [o <i>organization</i>] [c <i>country</i>] key-type {rsa dsa} key-len <i>key_length</i></code>	Generates a PKCS#10 certification request.
<code>ca generate pkcs12 name <i>name</i> password <i>password</i></code>	Generates a PKCS#12 certificate.
<code>ca generate x509 name <i>certificate_name</i> cn-type {ip cn <i>cn_address</i> fqdn cn <i>cn_domain_name</i> mail cn <i>cn_email</i>} [ou <i>organizational_unit</i>] [o <i>organization</i>] [c <i>country</i>] key-type {rsa dsa} key-len <i>key_length</i></code>	Generates a self-signed x509 certificate.
<code>ca rename category {local remote} <i>old_name</i> <i>new_name</i></code>	Renames a local (my certificates) or remote (trusted certificates) certificate.

**Table 164** ca Commands Summary (continued)

COMMAND	DESCRIPTION
<code>ca validation remote_certificate</code>	Enters the sub command mode for validation of certificates signed by the specified remote (trusted) certificates.
<code>cdp {activate deactivate}</code>	Turns certificate revocation on or off. When it is turned on, the UAG validates a certificate by getting a Certificate Revocation List (CRL) through HTTP or LDAP (can be configured after activating the LDAP checking option) and online responder (can be configured after activating the OSCP checking option). You also need to configure the OSCP or LDAP server details.
<code>ldap {activate deactivate}</code>	Has the UAG check (or not check) incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) on a LDAP (Lightweight Directory Access Protocol) directory server.
<code>ldap ip {ip fqdn} port &lt;1..65535&gt; [id name password password] [deactivate]</code>	<p>Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses LDAP.</p> <p><i>ip</i>: Type the IP address (in dotted decimal notation) or the domain name of the directory server. The domain name can use alphanumeric characters, periods and hyphens. Up to 255 characters.</p> <p><i>port</i>: Specify the LDAP server port number. You must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.</p> <p>The UAG may need to authenticate itself in order to access the CRL directory server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash.</p> <p>Type the password (up to 31 characters) from the entity maintaining the CRL directory server (usually a certification authority). You can use the following characters: a-zA-Z0-9; `~!@#\$\$%^&amp;*()_+{\}':./&lt;&gt;=-</p>
<code>ocsp {activate deactivate}</code>	Has the UAG check (or not check) incoming certificates that are signed by this certificate against a directory server that uses OSCP (Online Certificate Status Protocol).
<code>ocsp url url [id name password password] [deactivate]</code>	<p>Sets the validation configuration for the specified remote (trusted) certificate where the directory server uses OSCP.</p> <p><i>url</i>: Type the protocol, IP address and pathname of the OSCP server.</p> <p><i>name</i>: The UAG may need to authenticate itself in order to access the OSCP server. Type the login name (up to 31 characters) from the entity maintaining the server (usually a certification authority). You can use alphanumeric characters, the underscore and the dash.</p> <p><i>password</i>: Type the password (up to 31 characters) from the entity maintaining the OSCP server (usually a certification authority). You can use the following characters: a-zA-Z0-9; `~!@#\$\$%^&amp;*()_+{\}':./&lt;&gt;=-</p>
<code>no ca category {local remote} certificate_name</code>	Deletes the specified local (my certificates) or remote (trusted certificates) certificate.
<code>no ca validation name</code>	Removes the validation configuration for the specified remote (trusted) certificate.

**Table 164** ca Commands Summary (continued)

COMMAND	DESCRIPTION
<code>show ca category {local remote} name <i>certificate_name</i> certpath</code>	Displays the certification path of the specified local (my certificates) or remote (trusted certificates) certificate.
<code>show ca category {local remote} [name <i>certificate_name</i> format {text pem}]</code>	Displays a summary of the certificates in the specified category (local for my certificates or remote for trusted certificates) or the details of a specified certificate.
<code>show ca validation name <i>name</i></code>	Displays the validation configuration for the specified remote (trusted) certificate.
<code>show ca spaceusage</code>	Displays the storage space in use by certificates.



## 51.5 Certificates Commands Examples

The following example creates a self-signed X.509 certificate with IP address 10.0.0.58 as the common name. It uses the RSA key type with a 512 bit key. Then it displays the list of local certificates. Finally it deletes the pkcs12request certification request.

```
Router# configure terminal
Router(config)# ca generate x509 name test_x509 cn-type ip cn 10.0.0.58 key-type rsa
key-len 512
Router(config)# show ca category local
certificate: default
  type: SELF
  subject: CN=UAG_Factory_Default_Certificate
  issuer: CN=UAG_Factory_Default_Certificate
  status: VALID
  ID: UAG_Factory_Default_Certificate
  type: EMAIL
  valid from: 2003-01-01 00:38:30
  valid to: 2022-12-27 00:38:30
certificate: test
  type: REQ
  subject: CN=1.1.1.1
  issuer: none
  status: VALID
  ID: 1.1.1.1
  type: IP
  valid from: none
  valid to: none
certificate: pkcs12request
  type: REQ
  subject: CN=1.1.1.2
  issuer: none
  status: VALID
  ID: 1.1.1.2
  type: IP
  valid from: none
  valid to: none
certificate: test_x509
  type: SELF
  subject: CN=10.0.0.58
  issuer: CN=10.0.0.58
  status: VALID
  ID: 10.0.0.58
  type: IP
  valid from: 2006-05-29 10:26:08
  valid to: 2009-05-28 10:26:08
Router(config)# no ca category local pkcs12request
```

## ISP Accounts

Use ISP accounts to manage Internet Service Provider (ISP) account information for PPPoE and PPTP interfaces.

### 52.1 ISP Accounts Overview

An ISP account is a profile of settings for Internet access using PPPoE, or PPTP.

#### 52.1.1 PPPoE and PPTP Account Commands

The following table lists the PPPoE and PPTP ISP account commands.

**Table 165** PPPoE and PPTP ISP Account Commands

COMMAND	DESCRIPTION
<code>show account [pppoe <i>profile_name</i>   pptp <i>profile_name</i>]</code>	Displays information about the specified account(s).
<code>[no] account {pppoe   pptp} <i>profile_name</i></code>	Creates a new ISP account with name <i>profile_name</i> if necessary and enters sub-command mode. The <code>no</code> command deletes the specified ISP account.  <i>profile_name</i> : use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<code>encrypted-password <i>ciphertext</i></code>	Sets an encrypted secret for the specified ISP account.  <i>ciphertext</i> : You can use up to 128 printable ASCII characters. Spaces are not allowed.
<code>[no] user <i>username</i></code>	Sets the username for the specified ISP account. The <code>no</code> command clears the username.  <i>username</i> : You can use alphanumeric, underscores (_), dashes (-), commas (,), and /@\$ characters, and it can be up to 64 characters long.
<code>[no] password <i>password</i></code>	Sets the password for the specified ISP account. The <code>no</code> command clears the password.  <i>password</i> : You can use up to 63 printable ASCII characters. Spaces are not allowed.
<code>[no] authentication {chap-pap   chap   pap   mschap   mschap-v2}</code>	Sets the authentication for the specified ISP account. The <code>no</code> command sets the authentication to chap-pap.
<code>[no] compression {yes   no}</code>	Turns compression on or off for the specified ISP account. The <code>no</code> command turns off compression.
<code>[no] idle &lt;0..360&gt;</code>	Sets the idle timeout for the specified ISP account. The <code>no</code> command sets the idle timeout to zero.

**Table 165** PPPoE and PPTP ISP Account Commands (continued)

COMMAND	DESCRIPTION
<pre>[no] service-name {ip   hostname   service_name}</pre>	<p>Sets the service name for the specified PPPoE ISP account. The <code>no</code> command clears the service name.</p> <p><i>hostname</i>: You may use up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.</p> <p><i>service_name</i>: You can use up to 63 alphanumeric characters, underscores (_), dashes (-), and @\$./ characters.</p>
<pre>[no] server ip</pre>	<p>Sets the PPTP server for the specified PPTP ISP account. The <code>no</code> command clears the server name.</p>
<pre>[no] encryption {nomppe   mppe-40   mppe-128}</pre>	<p>Sets the encryption for the specified PPTP ISP account. The <code>no</code> command sets the encryption to <code>nomppe</code>.</p>
<pre>[no] connection-id connection_id</pre>	<p>Sets the connection ID for the specified PPTP ISP account. The <code>no</code> command clears the connection ID.</p> <p><i>connection_id</i>: You can use up to 31 alphanumeric characters, underscores (_), dashes (-), and colons (:).</p>

# SSL Application

This chapter describes how to configure SSL application objects for use in SSL VPN.

## 53.1 SSL Application Overview

Configure an SSL application object to specify a service and a corresponding IP address of the server on the local network. You can apply one or more SSL application objects in the **VPN > SSL VPN** screen for a user account/user group.

### 53.1.1 SSL Application Object Commands

This table lists the commands for creating SSL application objects. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 166** SSL Application Object Commands

COMMAND	DESCRIPTION
<code>show sslvpn application [application_object]</code>	Displays SSL VPN application objects.
<code>[no] sslvpn application application_object</code>	Enters the sub-command mode to create an SSL VPN application object.
<code>server-type rdp server-address server-address [starting-port &lt;1..65535&gt; ending-port &lt;1..65535&gt;] [program-path program-path]</code>	<p>Creates an SSL application object to allow users to manage LAN computers that have Remote Desktop Protocol remote desktop server software installed.</p> <p>Specify the listening ports of the LAN computer(s) running remote desktop server software. The UAG uses a port number from this range to send traffic to the LAN computer that is being remotely managed.</p> <p><i>program-path</i>: specify an application to open when a remote user logs into the remote desktop application, for example, C:\Program Files\application\application.exe.</p>
<code>server-type vnc server-address server-address [starting-port &lt;1..65535&gt; ending-port &lt;1..65535&gt;]</code>	<p>Creates an SSL application object to allow users to manage LAN computers that have Virtual Network Computing remote desktop server software installed.</p> <p>Specify the listening ports of the LAN computer(s) running remote desktop server software. The UAG uses a port number from this range to send traffic to the LAN computer that is being remotely managed.</p>

**Table 166** SSL Application Object Commands

COMMAND	DESCRIPTION
<code>server-type weblink url url</code>	<p>Sets this to create a link to a web site you specified that you expect the SSL VPN users to commonly use.</p> <p><i>url</i>: Enter the fully qualified domain name (FQDN) or IP address of the application server. You must enter the "http://" or "https://" prefix. For example, <code>https://1.2.3.4</code>. SSL VPN users are restricted to access only web pages or files in this directory. For example, if you enter "\remote\" in this field, emote users can only access web pages or files in the "remote" directory.</p> <p>If a link contains a file that is not within this domain, then SSL VPN users cannot access it.</p>
<code>no server-type</code>	Remove the type of service configuration for this SSL application.
<code>[no] webpage-encrypt</code>	Turn on web encrypt to prevent users from saving the web content.

### 53.1.2 SSL Application Command Examples

The following commands create and display a server-type SSL application object named example for a link to the website at `http://www.example.com`.

```

Router(config)# sslvpn application example
Router(sslvpn application)# server-type weblink url http://www.example.com
Router(sslvpn application)# exit
Router(config)# show sslvpn application
SSL Application: example
  Server Type: weblink
  URL: http://www.example.com
  Entry Point:
  Encrypted URL: ~aHR0cDovL2luZm8v/
  Web Page Encryption: yes
  Reference: 0
  Server Address:
  Starting Port:
  Ending Port:
  Program Path:
Router(config)#

```

# Endpoint Security

This chapter describes how to configure endpoint security objects for use in authentication policy and SSL VPN.

## 54.1 Endpoint Security Overview

Use Endpoint Security (EPS), also known as endpoint control, to make sure users' computers comply with defined corporate policies before they can access the network or an SSL VPN tunnel. After a successful user authentication, a user's computer must meet the endpoint security object's Operating System (OS) option and security requirements to gain access. You can configure the endpoint security object to require a user's computer to match just one of the endpoint security object's checking criteria or all of them. Configure endpoint security objects to use with the authentication policy and SSL VPN features.

### What Endpoint Security Can Check

The settings endpoint security can check vary depending on the OS of the user's computer. Depending on the OS, EPS can check user computers for the following:

- Operating System (Windows, Linux, Mac OSX, or others)
- Windows version and service pack version
- Windows Auto Update setting and installed security patches
- Personal firewall installation and activation
- Anti-virus installation and activation
- Windows registry settings
- Processes that the endpoint must execute
- Processes that the endpoint cannot execute
- The size and version of specific files

### Multiple Endpoint Security Objects

You can configure an authentication policy or SSL VPN policy to use multiple endpoint security objects. This allows checking of computers with different OSs or security settings. When a client attempts to log in, the UAG checks the client's computer against the endpoint security objects one-by-one. The client's computer must match one of the force authentication or SSL VPN policy's endpoint security policies in order to gain access.

## Requirements

User computers must have Sun's Java (Java Runtime Environment or 'JRE') installed and enabled with a minimum version of 1.4.

### 54.1.1 Endpoint Security Commands Summary

The following table describes the values required for many endpoint security object commands. Other values are discussed with the corresponding commands.

**Table 167** Input Values for Endpoint Security Commands

LABEL	DESCRIPTION
<i>profile_name</i>	The name of the endpoint security object. You may use 1-31 characters ("0-9", "a-z", "A-Z", "-", "_", "." with no spaces allowed).
<i>file_path</i>	This is a file with the full directory path in quotation marks ". For example, "C:\Program Files\Internet Explorer\iexplore.exe".

The following sections list the endpoint security object commands.

### 54.1.2 Endpoint Security Object Commands

This table lists the commands for creating endpoint security objects. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 168** Endpoint Security Object Commands

COMMAND	DESCRIPTION
[no] <code>eps failure-messages</code> <i>failure_messages</i>	Specify a message to display when a user's computer fails the endpoint security check. Use up to 1023 characters (0-9a-zA-Z;/?:@=+\$\._!*'()%,"). For example, "Endpoint Security checking failed. Please contact your network administrator for help.". The <code>no</code> command removes the setting.
<code>show eps failure-messages</code>	Displays the message to display when a user's computer fails the endpoint security check.
[no] <code>eps profile profile_name</code>	Enters the sub-command mode. The <code>no</code> command removes an endpoint security object.
[no] { <code>anti-virus</code>   <code>personal-firewall</code> } <code>activate</code>	If you set <code>windows</code> as the operating system (using the <code>os-type</code> command), you can set whether or not the user's computer is required to have anti-virus or personal firewall software installed.
[no] <code>anti-virus</code> <i>anti_virus_software_name</i> <code>detect-auto-protection</code> { <code>enable</code>   <code>disable</code>   <code>ignore</code> }	Sets a permitted anti-virus software package. If you want to enter multiple anti-virus software packages, use this command for each of them. Use the <code>list signature anti-virus</code> command to view the available anti-virus software package options.  <code>detect-auto-protection</code> : Set this to <code>enable</code> if the specified anti-virus software is not only detectable for the installation but also detectable for the activation status. You can check the settings for each anti-virus software by using the <code>show eps signature anti-virus</code> command.  The user's computer must have one of the listed anti-virus software packages to pass this checking item. For some anti-virus software the UAG can also detect whether or not the anti-virus software is activated; in those cases it must also be activated.

**Table 168** Endpoint Security Object Commands

COMMAND	DESCRIPTION
[no] personal-firewall <i>personal_firewall_software_name</i> detect-auto-protection {enable   disable   ignore}	<p>Sets a permitted personal firewall. If you want to enter multiple personal firewalls, use this command for each of them. Use the <code>list signature personal-firewall</code> command to view the available personal firewall software package options.</p> <p><code>detect-auto-protection</code>: Set this to enable if the specified firewall software is not only detectable for the installation but also detectable for the activation status. You can check the settings for each firewall software by using the <code>show eps signature personal-firewall</code> command.</p> <p>The user's computer must have one of the listed personal firewalls to pass this checking item. For some personal firewalls the UAG can also detect whether or not the firewall is activated; in those cases it must also be activated.</p>
[no] application forbidden-process <i>process_name</i>	<p>If you selected windows or linux as the operating system (using the <code>os-type</code> command), you can use this command to set an application that a user's computer is not permitted to have running. If you want to enter multiple applications, use this command for each of them.</p> <p>The user's computer must not have any of the forbidden applications running to pass this checking item.</p> <p>Include the filename extension for Linux operating systems.</p>
[no] application trusted-process <i>process_name</i>	<p>If you selected windows or linux as the operating system (using the <code>os-type</code> command), you can use this command to set an application that a user's computer must be running.</p> <p>The user's computer must have all of the trusted applications running to pass this checking item.</p> <p>Include the filename extension for Linux operating systems.</p>
[no] description <i>description</i>	Type a description for this endpoint security object. You can use alphanumeric and ()+/:=?!*#@\$_%- characters, and it can be up to 60 characters long.
[no] file-info file-path <i>file_path</i>	<p>If you selected windows or linux as the operating system (using the <code>os-type</code> command), you can use this command to check details of specific files on the user's computer.</p> <p>The user's computer must pass one of the file information checks to pass this checking item.</p>
[no] file-info file-path <i>file_path</i> {eq   gt   lt   ge   le   neq} file-size <1..1073741824>	Sets whether the size of the file on the user's computer has to be equal to (eq), greater than (gt), less than (lt), greater than or equal to (ge), less than or equal to (le), or not equal to (neq) the size of the file specified.
[no] file-info file-path <i>file_path</i> {eq   gt   lt   ge   le   neq} file-version <i>file_version</i>	Sets whether the version of the file on the user's computer has to be equal to (eq), greater than (gt), less than (lt), greater than or equal to (ge), less than or equal to (le), or not equal to (neq) the version of the file specified.
[no] file-info file-path <i>file_path</i> {eq   gt   lt   ge   le   neq} file-size <1..1073741824> {eq   gt   lt   ge   le   neq} file-version <i>file_version</i>	Sets whether the size and version of the file on the user's computer has to be equal to (eq), greater than (gt), less than (lt), greater than or equal to (ge), less than or equal to (le), or not equal to (neq) the size and version of the file specified.
os-type {windows   linux   mac-osx   others}	<p>Select the type of operating system the user's computer must be using. Use the <code>windows-version</code> command to configure the checking items according to the set operating system. If you set this to <code>mac-osx</code>, there are no other checking items.</p> <p><code>others</code> allows access for computers not using Windows, Linux, or Mac OSX operating systems. For example you create Windows, Linux, and Mac OSX endpoint security objects to apply to your LAN users. An "others" policy allows access for LAN computers using Solaris, HP, Android, or other operating systems.</p>



**Table 168** Endpoint Security Object Commands

COMMAND	DESCRIPTION
<code>windows-version {windows-2000   windows-xp   windows-2003   windows-2008   windows-vista   windows-7   windows-2008r2}</code>	If you set <code>windows</code> as the operating system (using the <code>os-type</code> command), use this command to set the version of Windows.
<code>matching-criteria {any   all}</code>	Select whether the user's computer has to match just one of the endpoint security object's checking criteria or all of them.
<code>list signature {anti-virus   personal-firewall   status}</code>	Displays all the anti-virus software packages, personal firewall software packages or EPS signature information respectively.  The <code>status</code> command displays the EPS signature version, release date and the total number of software packages for which the UAG's endpoint security can check.
<code>[no] windows-auto-update {enable   disable   ignore}</code>	If you set <code>windows</code> as the operating system (using the <code>os-type</code> command), you can use <code>enable</code> with this command if the user's computer must have the Windows Auto Update feature installed and activated; use <code>disable</code> if the Windows Auto Update feature must be installed but deactivated; use <code>ignore</code> if the Windows Auto Update feature must be installed but does not matter if it is activated or not.  The <code>no</code> command does not check the Windows Auto Update feature.
<code>[no] windows-service-pack &lt;1..10&gt;</code>	If you set <code>windows</code> as the operating system (using the <code>os-type</code> command), you can enter the minimum Windows service pack number the user's computer must have installed. The user's computer must have this service pack or higher. For example, "2" means service pack 2. The <code>no</code> command means to have the UAG ignore the Windows service pack number.
<code>[no] windows-security-patch security_patch</code>	If you set <code>windows</code> as the operating system (using the <code>os-type</code> command), you can use this command to set a Windows security patch that the user's computer must have installed. If you want to enter multiple security patches, use this command for each of them.  The user's computer must have all of the set Windows security patches installed to pass the checking item.
<code>[no] windows-registry registry_key {eq   gt   lt   ge   le   neq} registry_value</code>	If you set <code>windows</code> as the operating system (using the <code>os-type</code> command), you can use this command to set a Windows registry value to check on the user's computer. If you want to enter multiple registry values, use this command for each of them.  Set whether the value for the registry item in the user's computer has to be equal to ( <code>eq</code> ), greater than ( <code>gt</code> ), less than ( <code>lt</code> ), greater than or equal to ( <code>ge</code> ), less than or equal to ( <code>le</code> ), or not equal to ( <code>neq</code> ) the value specified.  The user's computer must pass all of the set Windows registry value checks to pass the checking item.
<code>show eps profile [profile_name]</code>	Displays the settings of all or the specified endpoint security object.
<code>show eps profile profile_name signature {anti-virus   personal-firewall}</code>	Displays Anti-Virus or personal firewall signatures that have been added to the specified endpoint security object.
<code>show eps signature {anti-virus   personal-firewall   status}</code>	Displays all the anti-virus software packages, personal firewall software packages or EPS signature information respectively.  The <code>status</code> command displays the EPS signature version, release date and the total number of software packages for which the UAG's endpoint security can check.
<code>[no] eps rename profile_name new_profile_name</code>	Changes an endpoint security object name.

### 54.1.3 Endpoint Security Object Command Example

Peter wants to create and display an endpoint security object named EPS-Example. Only the computers that match the following criteria can access the company's SSL VPN:

- Operating system: Windows XP
- Windows auto update: enabled
- Windows service pack: 2 or above
- Personal firewall: Windows firewall installed and enabled
- Anti-Virus: Kaspersky Anti-Virus v2011 installed and enabled

However, he needs to check the Anti-Virus software name defined on the UAG. The following example shows how to check all available Anti-Virus software packages for which the UAG's endpoint security can check. Copy and paste the name of the output item 17 for the setting later.

```
Router> configure terminal
Router(config)# show eps signature anti-virus
No.  Name                                                                 Detection
=====
1    Norton_Anti-Virus_v2010                                               no
2    Norton_Internet_Security_v2010                                       no
3    Norton_360_v3                                                         no
4    Microsoft_Security_Center                                             yes
5    TrendMicro_PC-cillin_AntiVirus_v2010                                 yes
6    TrendMicro_PC-cillin_Internet_Security_v2010                       yes
7    TrendMicro_PC-cillin_Internet_Security_Pro_v2010                   yes
8    Avira_Antivir_Personal_v2009                                          no
9    Kaspersky_Anti-Virus_v2010                                           yes
10   Kaspersky_Internet_Security_v2010                                    yes
11   Kaspersky_Anti-Virus_v2009                                           yes
12   Kaspersky_Internet_Security_v2009                                    yes
13   Norton_Anti-Virus_v2011                                              no
14   Norton_Internet_Security_v2011                                       no
15   Norton_360_v4                                                         no
16   Norton_360_v5                                                         no
17   Kaspersky_Anti-Virus_v2011                                           yes
18   Kaspersky_Anti-Virus_v2012                                          no
19   Kaspersky_Internet_Security_v2011                                    yes
20   Kaspersky_Internet_Security_v2012                                    no
21   TrendMicro_PC-cillin_v2011_Cloud                                     yes
22   Avira_Antivir_Personal_v2010                                          no
23   Avira_Antivir_Premium_2009                                           no
24   Avira_Antivir_Premium_v10                                           no
Router(config)#
```

Then he also needs to check the personal firewall software name defined on the UAG. Copy and paste the name of the output item 4 for the setting later.

```
Router(config)# show eps signature personal-firewall
No.  Name                                                                 Detection
=====
1    Kaspersky_Internet_Security_v2009                                     yes
2    Kaspersky_Internet_Security_v2010                                     yes
3    Microsoft_Security_Center                                           yes
4    Windows_Firewall                                                     yes
5    TrendMicro_PC-cillin_Internet_Security_v2010                       yes
6    TrendMicro_PC-cillin_Internet_Security_Pro_v2010                   yes
7    Windows_Firewall_Public                                              yes
8    Kaspersky_Internet_Security_v2011                                    yes
9    Kaspersky_Internet_Security_v2012                                    no
Router(config)#
```

Now Peter can create the EPS object profile as the example shown next. Note that he uses the `matching-criteria all` command to make sure all users' computers have the required software installed and settings being configured before they access the company's SSL VPN.

```
Router(config)# eps profile EPS-Example
Router(eps EPS-Example)# windows-version windows-xp
Router(eps EPS-Example)# personal-firewall activate
Router(eps EPS-Example)# anti-virus activate
Router(eps EPS-Example)# windows-auto-update enable
Router(eps EPS-Example)# windows-service-pack 2
Router(eps EPS-Example)# personal-firewall Windows_Firewall detect-auto-protection
enable
Router(eps EPS-Example)# anti-virus Kaspersky_Anti-Virus_v2011 detect-auto-
protection enable
Router(eps EPS-Example)# matching-criteria all
Router(eps EPS-Example)# exit
Router(config)#
```

Then he leaves the sub-command mode and uses the `show` command to view the EPS object settings.

```
Router(eps EPS-Example)# exit
Router(config)# show eps profile
name: EPS-Example
  description:
    os type: windows
    windows version: windows-xp
    matching criteria: all
    anti-virus activation: yes
    anti-virus: 1
      name: Kaspersky_Anti-Virus_v2011
      detect auto-protection: enable
    personal firewall activation: yes
    personal firewall: 1
      name: Windows_Firewall
      detect auto-protection: enable
    windows update: enable
    windows service pack: 2
    windows security patch:
    windows registry:
    trusted application:
    forbidden application:
    file information:
      reference count: 1
Router(config)#
```

See [Chapter 41 on page 205](#) for how to configure an SSL VPN using this EPS object .

For users who fail the endpoint security checking, Peter decides to show them an error message of "Endpoint Security checking failed. Contact helpdesk at #7777 if you have any questions." The following shows how to configure the error message.

```
Router(config)# eps failure-messages "Endpoint Security checking failed. Contact
helpdesk at #7777 if you have any questions."
Router(config)#
```

# Dynamic Guest Accounts

## 55.1 Dynamic Guest Accounts Overview

Dynamic guest accounts are guest accounts, but are created dynamically and stored in the UAG's local user database. A dynamic guest account has a dynamically-created user name and password. A dynamic guest account user can access the UAG's services only within a given period of time and will become invalid after the expiration date/time.

There are three types of dynamic guest accounts depending on how they are created or authenticated: billing-users, ua-users and trial-users.

billing-users are guest account created with the `dynamic-guest generate` command or the guest manager account or an external printer and paid by cash or created and paid via the on-line payment service.

ua-users are users that log in from the user agreement page.

trial-users are free guest accounts that are created with the `dynamic-guest generate-freeuser` command or the Free Time function.

## 55.2 Dynamic-guest Commands

This table lists the `dynamic-guest` commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 169** dynamic-guest Commands

COMMAND	DESCRIPTION
<code>dynamic-guest freeuser user_name</code>	Creates a free dynamic guest account (trial-user) with the specified user name and enters the <code>dynamic-guest</code> sub-command mode to set the password and timeout settings. See <a href="#">Table 170 on page 270</a> for the sub-commands.
<code>dynamic-guest generate</code>	Sets the UAG to automatically create a dynamic guest account (billing-user) and enters the <code>dynamic-guest</code> sub-command mode to set the password and timeout settings. See <a href="#">Table 170 on page 270</a> for the sub-commands.
<code>dynamic-guest generate-freeuser</code>	Sets the UAG to automatically create a free dynamic guest account (trial-user) and enters the <code>dynamic-guest</code> sub-command mode to set the password and timeout settings. See <a href="#">Table 170 on page 270</a> for the sub-commands.

**Table 169** dynamic-guest Commands (continued)

COMMAND	DESCRIPTION
[no] dynamic-guest <i>user_name</i>	Creates a dynamic guest account (billing-user) with the specified user name and enters the dynamic-guest sub-command mode to set the password and timeout settings. See <a href="#">Table 170 on page 270</a> for the sub-commands.  The <code>no</code> command removes the specified dynamic-guest account.
show dynamic-guest log	Displays all the dynamic guest accounts which are either active or expired.
show dynamic-guest log create-time begin <i>yyyy-mm-dd hh:mm</i> end <i>yyyy-mm-dd hh:mm</i>	Displays all the active and/or expired dynamic guest accounts that were generated within a specified period of time.
show dynamic-guest users	Displays all the active dynamic guest accounts on the UAG.

## 55.2.1 dynamic-guest Sub-commands

The following table describes the sub-commands for several dynamic-guest commands. Note that not all rule commands use all the sub-commands listed here.

**Table 170** dynamic-guest Sub-commands

COMMAND	DESCRIPTION
bandwidth {upload   download} <0..1048576> priority <1..7>	Specifies the maximum bandwidth allowed for the user account in kilobits per second and types a number between 1 and 7 to set the priority for the user's traffic. The smaller the number, the higher the priority.  upload refers to the traffic the UAG sends out from a user.  download refers to the traffic the UAG sends to a user.
[no] bandwidth activate	Turns on bandwidth management for the user account.  The <code>no</code> command disables bandwidth management for the user account.
charge <i>price</i>	Sets the account's price, up to 99999999.99, per time unit.
create-time <i>yyyy-mm-dd hh:mm</i>	Sets the date and time the account is created.
expire-time <i>yyyy-mm-dd hh:mm</i>	Sets the date and time the account becomes invalid.
password <i>password</i>	Sets the password for the account.
payment-info {cash   payment-service}	Sets the method of payment for the account.
phone <i>phone_number</i>	Sets the mobile phone number for the account.
quota {total   upload   download} megabytes <0..1023>	Sets how much downstream and/or upstream data in Megabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
quota {total   upload   download} gigabytes <0..100>	Sets how much downstream and/or upstream data in Gigabytes can be transmitted through the external interface before the account expires. 0 means there is no data limit for the user account.
quota type {total   upload-download}	Sets a limit for the user account. This only applies to user's traffic that is received or transmitted through the external interface.  <b>Note:</b> When the limit is exceeded, the user is not allowed to access the Internet through the UAG.  total: set a limit on the total traffic in both directions.  upload-download: set a limit on the upstream traffic and downstream traffic respectively.

**Table 170** dynamic-guest Sub-commands (continued)

COMMAND	DESCRIPTION
remaining-time <1..25920000>	Sets the amount of Internet access time (in seconds) remaining for the account.
time-period <1..432000>	Sets the total account of time (in minutes) the account can use to access the Internet through the UAG.

## 55.2.2 Dynamic-guest Command Example

This example shows how to create a dynamic guest account, configure the account related settings and displays the account information.

```

Router# configure terminal
Router(config)# dynamic-guest generate
[dynamic guest] username:gn0ti7, password:ihzun7
Router(config-dynamic-guest)# charge 5
Router(config-dynamic-guest)# expire-time 2013-06-26 14:00
Router(config-dynamic-guest)# payment-info cash
Router(config-dynamic-guest)# phone 0912345678
Router(config-dynamic-guest)# time-period 1440
Router(config-dynamic-guest)# remaining-time 86400
Router(config-dynamic-guest)# create-time 2013-06-25 14:03
Router(config-dynamic-guest)# exit
Router(config)# show dynamic-guest users
No.   Status   Username   Create Time           Expiration Time
      Time Period   Remaining Time       Charge      ayment Info   Phone Num
      User Role
=====
1     Unused   gn0ti7    2013-06-25 14:03     2013-06-26 14:00
      1day 00:00:00   1day 00:00:00       eur 5,00     cash          0912345678
      billing-users
Router(config)#

```

This chapter provides information on the commands that correspond to what you can configure in the system screens.

## 56.1 System Overview

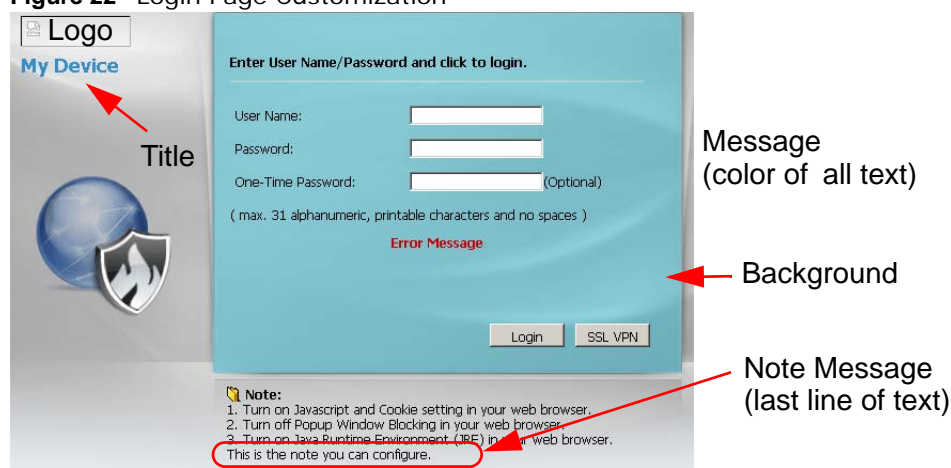
Use these commands to configure general UAG information, the system time and the console port connection speed for a terminal emulation program. They also allow you to configure DNS settings and determine which services/protocols can access which UAG zones (if any) from which computers.

## 56.2 Customizing the WWW Login Page

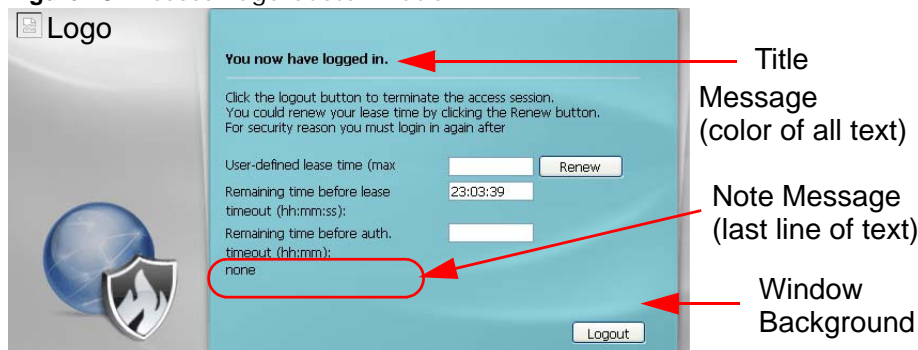
Use these commands to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet. See [Chapter 44 on page 224](#) for more on access user accounts.

The following figures identify the parts you can customize in the login and access pages.

**Figure 22** Login Page Customization





**Figure 23** Access Page Customization

You can specify colors in one of the following ways:

- *color-rgb*: Enter red, green, and blue values in parenthesis and separate by commas. For example, use "rgb(0,0,0)" for black.
- *color-name*: Enter the name of the desired color.
- *color-number*: Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use "#000000" for black.

The following table describes the commands available for customizing the Web Configurator login screen and the page that displays after an access user logs into the Web Configurator to access network services like the Internet. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 171** Command Summary: Customization

COMMAND	DESCRIPTION
[no] <code>access-page color-window-background</code>	Sets whether or not the access page uses a colored background.
<code>access-page message-color {color-rgb   color-name   color-number}</code>	Sets the color of the message text on the access page.
[no] <code>access-page message-text message</code>	Sets a note to display below the access page's title. Use up to 64 printable ASCII characters. Spaces are allowed.
<code>access-page title title</code>	Sets the title for the top of the access page. Use up to 64 printable ASCII characters. Spaces are allowed.
<code>access-page window-color {color-rgb   color-name   color-number}</code>	Sets the color of the access page's colored background.
<code>login-page background-color {color-rgb   color-name   color-number}</code>	Sets the color of the login page's background.
[no] <code>login-page color-background</code>	Sets the login page to use a solid colored background.
[no] <code>login-page color-window-background</code>	Sets the login page's window to use a solid colored background.
<code>login-page message-color {color-rgb   color-name   color-number}</code>	Sets the color of the message text on the login page.
[no] <code>login-page message-text % message</code>	Sets a note to display at the bottom of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
<code>login-page title title</code>	Sets the title for the top of the login screen. Use up to 64 printable ASCII characters. Spaces are allowed.
<code>login-page title-color {color-rgb   color-name   color-number}</code>	Sets the title text color of the login page.

**Table 171** Command Summary: Customization (continued)

COMMAND	DESCRIPTION
<code>login-page window-color {color-rgb   color-name   color-number}</code>	Sets the color of the login page's window border.
<code>logo background-color {color-rgb   color-name   color-number}</code>	Sets the color of the logo banner across the top of the login screen and access page.
<code>show access-page settings</code>	Lists the current access page settings.
<code>show login-page default-title</code>	Lists the factory default title for the login page.
<code>show login-page settings</code>	Lists the current login page settings.
<code>show logo settings</code>	Lists the current logo background (banner) and floor (line below the banner) settings.
<code>show page-customization</code>	Lists whether the UAG is set to use custom login and access pages or the default ones.

## 56.3 Host Name Commands

The following table describes the commands available for the hostname and domain name. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 172** Command Summary: Host Name

COMMAND	DESCRIPTION
<code>[no] domainname domain_name</code>	Sets the domain name. The <code>no</code> command removes the domain name.  <i>domain_name</i> : This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
<code>[no] hostname hostname</code>	Sets a descriptive name to identify your UAG. The <code>no</code> command removes the host name.
<code>show fqdn</code>	Displays the fully qualified domain name.

## 56.4 Time and Date

For effective scheduling and logging, the UAG system time must be accurate. The UAG's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server.

## 56.4.1 Date/Time Commands

The following table describes the commands available for date and time setup. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 173** Command Summary: Date/Time

COMMAND	DESCRIPTION
<code>clock date yyyy-mm-dd time hh:mm:ss</code>	Sets the new date in year, month and day format manually and the new time in hour, minute and second format.
<code>[no] clock daylight-saving</code>	Enables daylight saving. The <code>no</code> command disables daylight saving.
<code>[no] clock saving-interval begin {apr aug dec feb jan jul jun mar may nov oct sep} {1 2 3 4 last} {fri mon sat sun thu tue wed} hh:mm end {apr aug dec feb jan jul jun mar may nov oct sep} {1 2 3 4 last} {fri mon sat sun thu tue wed} hh:mm offset</code>	Configures the day and time when Daylight Saving Time starts and ends. The <code>no</code> command removes the day and time when Daylight Saving Time starts and ends.  offset: a number from 1 to 5.5 (by 0.5 increments)
<code>clock time hh:mm:ss</code>	Sets the new time in hour, minute and second format.
<code>[no] clock time-zone {- +hh}</code>	Sets your time zone. The <code>no</code> command removes time zone settings.
<code>[no] ntp</code>	Saves your date and time and time zone settings and updates the data and time every 24 hours. The <code>no</code> command stops updating the data and time every 24 hours.
<code>[no] ntp server {fqdn w.x.y.z}</code>	Sets the IP address or URL of your NTP time server. The <code>no</code> command removes time server information.
<code>ntp sync</code>	Gets the time and date from a NTP time server.
<code>show clock date</code>	Displays the current date of your UAG.
<code>show clock status</code>	Displays your time zone and daylight saving settings.
<code>show clock time</code>	Displays the current time of your UAG.
<code>show ntp server</code>	Displays time server settings.

## 56.5 Console Port Speed

This section shows you how to set the console port speed when you connect to the UAG via the console port using a terminal emulation program. The following table describes the console port commands. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 174** Command Summary: Console Port Speed

COMMAND	DESCRIPTION
<code>[no] console baud baud_rate</code>	Sets the speed of the console port. The <code>no</code> command resets the console port speed to the default (115200).  <i>baud_rate</i> : 9600, 19200, 38400, 57600 or 115200.
<code>show console</code>	Displays console port speed.

## 56.6 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

### 56.6.1 Domain Zone Forwarder

A domain zone forwarder contains a DNS server's IP address. The UAG can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

### 56.6.2 DNS Commands

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 175** Input Values for General DNS Commands

LABEL	DESCRIPTION
<i>address_object</i>	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>interface_name</i>	The name of the interface. This depends on the UAG model. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.

The following table describes the commands available for DNS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 176** Command Summary: DNS

COMMAND	DESCRIPTION
[no] ip dns server a-record <i>fqdn</i> <i>w.x.y.z</i>	Sets an A record that specifies the mapping of a fully qualified domain name (FQDN) to an IP address. The <code>no</code> command deletes an A record.
ip dns server cache-flush	Clears the DNS records.
ip dns server max-ttl <10..3600>	Sets the maximum TTL (Time to Live) value for DNS records.
[no] ip dns server mx-record <i>domain_name</i> { <i>w.x.y.z</i>   <i>fqdn</i> }	Sets a MX record that specifies a mail server that is responsible for handling the mail for a particular domain. The <code>no</code> command deletes a MX record.
ip dns server rule {<1..32> append insert <1..32>} access-group {ALL  <i>address_object</i> } zone {ALL  <i>address_object</i> } action {accept deny}	Sets a service control rule for DNS requests.
ip dns server rule move <1..32> to <1..32>	Changes the number of a service control rule.

**Table 176** Command Summary: DNS (continued)

COMMAND	DESCRIPTION
[no] ip dns server zone-forwarder {<1..32> append insert <1..32>} {domain_zone_name *} interface interface_name	Sets a domain zone forwarder record that specifies a fully qualified domain name. You can also use a star (*) if all domain zones are served by the specified DNS server(s).  <i>domain_zone_name</i> : This is a domain zone, not a host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the UAG receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.  <i>interface_name</i> : This is the interface through which the ISP provides a DNS server. The interface should be activated and set to be a DHCP client.  The no command deletes a zone forwarder record.
ip dns server zone-forwarder {<1..32> append insert <1..32>} {domain_zone_name *} user-defined w.x.y.z [private   interface {interface_name   auto}]	Sets a domain zone forwarder record that specifies a DNS server's IP address.  private   interface: Use private if the UAG connects to the DNS server through a VPN tunnel. Otherwise, use the interface command to set the interface through which the UAG sends DNS queries to a DNS server. The auto means any interface that the UAG uses to send DNS queries to a DNS server according to the routing rule.
ip dns server zone-forwarder move <1..32> to <1..32>	Changes the index number of a zone forwarder record.
no ip dns server rule <1..32>	Deletes a service control rule.
show ip dns server interface_name	Displays DNS entries for the specified interface.
show ip dns server database	Displays all configured records.
show ip dns server status	Displays whether this service is enabled or not.

### 56.6.3 DNS Command Example

This command sets an A record that specifies the mapping of a fully qualified domain name (www.abc.com) to an IP address (210.17.2.13).

```
Router# configure terminal
Router(config)# ip dns server a-record www.abc.com 210.17.2.13
```

## 56.7 Authentication Server Overview

The UAG can also work as a RADIUS server to exchange messages with other APs for user authentication and authorization.

## 56.7.1 Authentication Server Commands

The following table lists the authentication server commands you use to configure the UAG's built-in authentication server settings.

**Table 177** Command Summary: Authentication Server

COMMAND	DESCRIPTION
[no] <code>auth-server activate</code>	Sets the UAG to act as an authentication server for other RADIUS clients, such as APs. The <code>no</code> command sets the UAG to not act as an authentication server for other APs.
<code>auth-server authentication</code> <code>auth_method</code>	Specifies an authentication method used by the authentication server.
<code>no auth-server authentication</code>	Resets the authentication method used by the authentication server to the factory default ( <code>default</code> ).
[no] <code>auth-server cert</code> <code>certificate_name</code>	Specifies a certificate used by the authentication server (UAG). The <code>no</code> command resets the certificate used by the authentication server to the factory default ( <code>default</code> ).  <i>certificate_name</i> : The name of the certificate. You can use up to 31 alphanumeric and ;~!@#\$\$%^&()_+[]{}',.- characters.
[no] <code>auth-server trusted-client</code> <code>profile_name</code>	Creates a trusted RADIUS client profile. The <code>no</code> command deletes the specified profile.  <i>profile-name</i> : You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
[no] <code>activate</code>	Enables the client profile. The <code>no</code> command disables the profile.
[no] <code>ip address ip</code> <code>subnet_mask</code>	Sets the client's IP address and subnet mask. The <code>no</code> command clears this setting.
[no] <code>secret secret</code>	Sets a password as the key to be shared between the UAG and the client. The <code>no</code> command clears this setting.
[no] <code>description description</code>	Sets the description for the profile. The <code>no</code> command clears this setting.  <i>description</i> : You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 60 characters long.
<code>show auth-server status</code>	Displays the UAG's authentication server settings.
<code>show auth-server trusted-client</code>	Displays all RADIUS client profile settings.
<code>show auth-server trusted-client</code> <code>profile_name</code>	Displays the specified RADIUS client profile settings.

## 56.7.2 Authentication Server Command Examples

The following example shows you how to enable the authentication server feature on the UAG and sets a trusted RADIUS client profile. This example also shows you the authentication server and client profile settings.

```
Router# configure terminal
Router(config)# auth-server activate
Router(config)# auth-server trusted-client AP-1
Router(config-trusted-client-AP-1)# activate
Router(config-trusted-client-AP-1)# ip address 10.10.1.2 255.255.255.0
Router(config-trusted-client-AP-1)# secret 12345678
Router(config-trusted-client-AP-1)# exit
Router(config)# show auth-server status
activation: yes
authentication method: default
certificate: default
Router(config)# show auth-server trusted-client AP-1
Client: AP-1
  Activation: yes
  Description:
  IP: 10.10.1.2
  Netmask: 255.255.255.0
  Secret: VQEg907jWB8=
Router(config)#
```

## 56.8 ZON Overview

The ZyXEL One Network (ZON) utility uses the ZyXEL Discovery Protocol (ZDP) for discovering and configuring ZDP-aware ZyXEL devices in the same broadcast domain as the computer on which ZON is installed.

The ZON Utility issues requests via ZDP and in response to the query, the ZyXEL device responds with basic information including IP address, firmware version, location, system and model name. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at [www.zyxel.com](http://www.zyxel.com) and install it on a computer.

### 56.8.1 LLDP

LLDP is a layer-2 protocol that allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps you discover network changes and perform necessary network reconfiguration and management.

## 56.8.2 ZON Commands

The following table describes the commands available for ZON. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 178** Command Summary: ZON

COMMAND	DESCRIPTION
<code>zon lldp server</code>	Activates LLDP discovery on the UAG.  This allows you to use Link Layer Discovery Protocol (LLDP) for discovering and configuring LLDP-aware devices in the same broadcast domain as the UAG that you are logged into using the web configurator.
<code>zon lldp server tx-hold &lt;1..10&gt;</code>	Sets the multiplier used to calculate the TTL (Time To Live) value for the transmitted LLDP packets. The TTL value determines how long the device information can be saved on the neighbors.  LLDP TTL = the multiplier * the LLDP transmission interval
<code>zon lldp server tx-interval &lt;1..600&gt;</code>	Sets the interval (in seconds) at which the UAG sends a LLDP packet to the neighbor.
<code>zon zdp server</code>	Activates ZDP discovery on the UAG.
<code>show zon lldp neighbors</code>	Displays the the UAG's neighboring devices via LLDP.
<code>show zon lldp server config</code>	Displays the LLDP settings.
<code>show zon lldp server statistics</code>	Displays the LLDP traffic statistics.
<code>show zon lldp server status</code>	Displays whether LLDP discovery is enabled.
<code>show zon zdp server status</code>	Displays whether ZDP discovery is enabled.

## 56.8.3 ZON Examples

This example enables LLDP discovery and displays whether LLDP discovery is enabled on the UAG.

```
Router(config)# zon lldp server
Router(config)# zon lldp server status
status: active
Router(config)#
```



# System Remote Management

This chapter shows you how to determine which services/protocols can access which UAG zones (if any) from which computers.

Note: To access the UAG from a specified computer using a service, make sure no service control rules or to-Device firewall rules block that traffic.

## 57.1 Remote Management Overview

You may manage your UAG from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN&WAN&DMZ)
- DMZ only

To disable remote management of a service, deselect **Enable** in the corresponding service screen.

### 57.1.1 Remote Management Limitations

Remote management will not work when:

- 1 You have disabled that service in the corresponding screen.
- 2 The accepted IP address in the **Service Control** table does not match the client IP address. If it does not match, the UAG will disconnect the session immediately.
- 3 There is a firewall rule that blocks it.

### 57.1.2 System Timeout

There is a lease timeout for administrators. The UAG automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the UAG for authentication again when the reauthentication time expires.

## 57.2 Common System Command Input Values

The following table identifies the values required for many of these commands. Other input values are discussed with the corresponding commands.

**Table 179** Input Values for General System Commands

LABEL	DESCRIPTION
<i>address_object</i>	The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
<i>rule_number</i>	The number of a service control rule. 1 - <i>X</i> where <i>X</i> is the highest number of rules the UAG model supports.
<i>zone_object</i>	The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.  The UAG uses pre-defined zone names like DMZ, LAN1, LAN2, SSL VPN, IPSec VPN, and WAN.

## 57.3 HTTP/HTTPS Commands

The following table describes the commands available for HTTP/HTTPS. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 180** Command Summary: HTTP/HTTPS

COMMAND	DESCRIPTION
[no] ip http authentication <i>auth_method</i>	Sets an authentication method used by the HTTP/HTTPS server. The <code>no</code> command resets the authentication method used by the HTTP/HTTPS server to the factory default ( <code>default</code> ).  <i>auth_method</i> : The name of the authentication method. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.
[no] ip http port <1..65535>	Sets the HTTP service port number. The <code>no</code> command resets the HTTP service port number to the factory default (80).
[no] ip http secure-port <1..65535>	Sets the HTTPS service port number. The <code>no</code> command resets the HTTPS service port number to the factory default (443).
[no] ip http secure-server	Enables HTTPS access to the UAG web configurator. The <code>no</code> command disables HTTPS access to the UAG web configurator.
[no] ip http secure-server auth-client	Sets the client to authenticate itself to the HTTPS server. The <code>no</code> command sets the client not to authenticate itself to the HTTPS server.

**Table 180** Command Summary: HTTP/HTTPS (continued)

COMMAND	DESCRIPTION
[no] ip http secure-server cert <i>certificate_name</i>	Specifies a certificate used by the HTTPS server. The <code>no</code> command resets the certificate used by the HTTPS server to the factory default (default).  <i>certificate_name</i> : The name of the certificate. You can use up to 31 alphanumeric and ;'~!@#\$\$%^&()_+[]{}',.- characters.
[no] ip http secure-server force-redirect	Redirects all HTTP connection requests to a HTTPS URL. The <code>no</code> command disables forwarding HTTP connection requests to a HTTPS URL.
ip http secure-server table {admin user} rule { <i>rule_number</i>  append insert <i>rule_number</i> } access-group {ALL  <i>address_object</i> } zone {ALL  <i>zone_object</i> } action {accept deny}	Sets a service control rule for HTTPS service.
ip http secure-server table {admin user} rule move <i>rule_number</i> to <i>rule_number</i>	Changes the index number of a HTTPS service control rule.
ip http secure-server cipher-suite { <i>cipher_algorithm</i> } [ <i>cipher_algorithm</i> ] [ <i>cipher_algorithm</i> ] [ <i>cipher_algorithm</i> ]	Sets the encryption algorithms (up to four) that the UAG uses for the SSL in HTTPS connections and the sequence in which it uses them. The <i>cipher_algorithm</i> can be any of the following.  rc4: RC4 (RC4 may impact the UAG's CPU performance since the UAG's encryption accelerator does not support it).  aes: AES  des: DES  3des: Triple DES.
no ip http secure-server cipher-suite { <i>cipher_algorithm</i> }	Has the UAG not use the specified encryption algorithm for the SSL in HTTPS connections.
[no] ip http server	Allows HTTP access to the UAG web configurator. The <code>no</code> command disables HTTP access to the UAG web configurator.
ip http server table {admin user} rule { <i>rule_number</i>  append insert <i>rule_number</i> } access-group {ALL  <i>address_object</i> } zone {ALL  <i>zone_object</i> } action {accept deny}	Sets a service control rule for HTTP service.
ip http server table {admin user} rule move <i>rule_number</i> to <i>rule_number</i>	Changes the number of a HTTP service control rule.
no ip http secure-server table {admin user} rule <i>rule_number</i>	Deletes a service control rule for HTTPS service.
no ip http server table {admin user} rule <i>rule_number</i>	Deletes a service control rule for HTTP service.
show ip http server status	Displays HTTP settings.
show ip http server secure status	Displays HTTPS settings.

## 57.3.1 HTTP/HTTPS Command Examples

The following example adds a service control rule that allowed an administrator from the computers with the IP addresses matching the Marketing address object to access the WAN zone using HTTP service.

```
Router# configure terminal
Router(config)# ip http server table admin rule append access-group Marketing zone WAN
action accept
```

This command sets an authentication method used by the HTTP/HTTPS server to authenticate the client(s).

```
Router# configure terminal
Router(config)# ip http authentication Example
```

The following example sets a certificate named MyCert used by the HTTPS server to authenticate itself to the SSL client.

```
Router# configure terminal
Router(config)# ip http secure-server cert MyCert
```

## 57.4 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

### 57.4.1 SSH Implementation on the UAG

Your UAG supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the UAG for remote management on port 22 (by default).

### 57.4.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the UAG over SSH.

### 57.4.3 SSH Commands

The following table describes the commands available for SSH. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 181** Command Summary: SSH

COMMAND	DESCRIPTION
<code>[no] ip ssh server</code>	Allows SSH access to the UAG CLI. The <code>no</code> command disables SSH access to the UAG CLI.
<code>[no] ip ssh server cert <i>certificate_name</i></code>	Sets a certificate whose corresponding private key is to be used to identify the UAG for SSH connections. The <code>no</code> command resets the certificate used by the SSH server to the factory default (default).  <i>certificate_name</i> : The name of the certificate. You can use up to 31 alphanumeric and ;~!@#%&()_+[]{}',.- characters.
<code>[no] ip ssh server port &lt;1..65535&gt;</code>	Sets the SSH service port number. The <code>no</code> command resets the SSH service port number to the factory default (22).
<code>ip ssh server rule {<i>rule_number</i> append insert <i>rule_number</i>} access-group {ALL <i>address_object</i>} zone {ALL <i>zone_object</i>} action {accept deny}</code>	Sets a service control rule for SSH service.  <i>address_object</i> : The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.  <i>zone_object</i> : The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.  The UAG uses pre-defined zone names like DMZ, LAN1, LAN2, SSL VPN, IPsec VPN, and WAN.
<code>ip ssh server rule move <i>rule_number</i> to <i>rule_number</i></code>	Changes the index number of a SSH service control rule.
<code>[no] ip ssh server v1</code>	Enables remote management using SSH v1. The <code>no</code> command stops the UAG from using SSH v1.
<code>no ip ssh server rule <i>rule_number</i></code>	Deletes a service control rule for SSH service.
<code>show ip ssh server status</code>	Displays SSH settings.

### 57.4.4 SSH Command Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SSH service.

```
Router# configure terminal
Router(config)# ip ssh server rule 2 access-group Marketing zone WAN action accept
```

This command sets a certificate (Default) to be used to identify the UAG.

```
Router# configure terminal
Router(config)# ip ssh server cert Default
```

## 57.5 Telnet

You can configure your UAG for remote Telnet access.

## 57.6 Telnet Commands

The following table describes the commands available for Telnet. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 182** Command Summary: Telnet

COMMAND	DESCRIPTION
<code>[no] ip telnet server</code>	Allows Telnet access to the UAG CLI. The <code>no</code> command disables Telnet access to the UAG CLI.
<code>[no] ip telnet server port &lt;1..65535&gt;</code>	Sets the Telnet service port number. The <code>no</code> command resets the Telnet service port number back to the factory default (23).
<code>ip telnet server rule {rule_number append insert rule_number} access-group {ALL address_object} zone {ALL zone_object} action {accept deny}</code>	Sets a service control rule for Telnet service.  <i>address_object</i> : The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.  <i>zone_object</i> : The name of the zone. Use up to 31 characters (a-zA-Z0-9_). The name cannot start with a number. This value is case-sensitive.  The UAG uses pre-defined zone names like DMZ, LAN1, LAN2, SSL VPN, IPsec VPN, and WAN.
<code>ip telnet server rule move rule_number to rule_number</code>	Changes the index number of a service control rule.
<code>no ip telnet server rule rule_number</code>	Deletes a service control rule for Telnet service.
<code>show ip telnet server status</code>	Displays Telnet settings.

### 57.6.1 Telnet Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using Telnet service.

```
Router# configure terminal
Router(config)# ip telnet server rule 11 access-group RD zone LAN action
-> accept
```

This command displays Telnet settings.

```
Router# configure terminal
Router(config)# show ip telnet server status
active      : yes
port       : 23
service control:
No.  Zone                Address                Action
=====
Router(config)#
```

## 57.7 Configuring FTP

You can upload and download the UAG's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

### 57.7.1 FTP Commands

The following table describes the commands available for FTP. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 183** Command Summary: FTP

COMMAND	DESCRIPTION
<code>[no] ip ftp server</code>	Allows FTP access to the UAG. The <code>no</code> command disables FTP access to the UAG.
<code>[no] ip ftp server cert <i>certificate_name</i></code>	Sets a certificate to be used to identify the UAG. The <code>no</code> command resets the certificate used by the FTP server to the factory default.
<code>[no] ip ftp server port &lt;1..65535&gt;</code>	Sets the FTP service port number. The <code>no</code> command resets the FTP service port number to the factory default (21).
<code>[no] ip ftp server tls-required</code>	Allows FTP access over TLS. The <code>no</code> command disables FTP access over TLS.
<code>ip ftp server rule {<i>rule_number</i> append insert <i>rule_number</i>} access-group {ALL <i>address_object</i>} zone {ALL <i>zone_object</i>} action {accept deny}</code>	<p>Sets a service control rule for FTP service.</p> <p><i>address_object</i>: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p> <p><i>zone_object</i>: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.</p> <p>The UAG uses pre-defined zone names like DMZ, LAN1, LAN2, SSL VPN, IPsec VPN, and WAN.</p>
<code>ip ftp server rule move <i>rule_number</i> to <i>rule_number</i></code>	Changes the index number of a service control rule.
<code>no ip ftp server rule <i>rule_number</i></code>	Deletes a service control rule for FTP service.
<code>show ip ftp server status</code>	Displays FTP settings.

### 57.7.2 FTP Commands Examples

This command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using FTP service.

```
Router# configure terminal
Router(config)# ip ftp server rule 4 access-group Sales zone WAN action accept
```

This command displays FTP settings.

```

Router# configure terminal
Router(config)# show ip ftp server status
active      : yes
port       : 21
certificate: default
TLS        : no
service control:
No.  Zone                Address                Action
=====

```

## 57.8 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your UAG supports SNMP agent functionality, which allows a manager station to manage and monitor the UAG through the network. The UAG supports SNMP version one (SNMPv1) and version two (SNMPv2c).

### 57.8.1 Supported MIBs

The UAG supports MIB II that is defined in RFC-1213 and RFC-1215. The UAG also supports private MIBs (enterprise.mib and private.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the UAG's MIBs from [www.zyxel.com](http://www.zyxel.com).

### 57.8.2 SNMP Traps

The UAG will send traps to the SNMP manager when any one of the following events occurs:

**Table 184** SNMP Traps

OBJECT LABEL	OBJECT ID	DESCRIPTION
Cold Start	1.3.6.1.6.3.1.1.5.1	This trap is sent when the UAG is turned on or an agent restarts.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when an SNMP request comes from non-authenticated hosts.



### 57.8.3 SNMP Commands

The following table describes the commands available for SNMP. You must use the `configure` terminal command to enter the configuration mode before you can use these commands.

**Table 185** Command Summary: SNMP

COMMAND	DESCRIPTION
<code>[no] snmp-server</code>	Allows SNMP access to the UAG. The <code>no</code> command disables SNMP access to the UAG.
<code>[no] snmp-server community <i>community_string</i> {ro rw}</code>	Enters up to 64 characters to set the password for read-only (ro) or read-write (rw) access. The <code>no</code> command resets the password for read-only (ro) or read-write (rw) access to the default.
<code>[no] snmp-server contact <i>description</i></code>	Sets the contact information (of up to 60 characters) for the person in charge of the UAG. The <code>no</code> command removes the contact information for the person in charge of the UAG.
<code>[no] snmp-server enable {informs traps}</code>	Enables all SNMP notifications (informs or traps). The <code>no</code> command disables all SNMP notifications (informs or traps).
<code>[no] snmp-server host {w.x.y.z} [<i>community_string</i>]</code>	Sets the IPv4 address of the host that receives the SNMP notifications. The <code>no</code> command removes the host that receives the SNMP notifications.
<code>[no] snmp-server location <i>description</i></code>	Sets the geographic location (of up to 60 characters) for the UAG. The <code>no</code> command removes the geographic location for the UAG.
<code>[no] snmp-server port &lt;1..65535&gt;</code>	Sets the SNMP service port number. The <code>no</code> command resets the SNMP service port number to the factory default (161).
<code>snmp-server rule {<i>rule_number</i> append insert <i>rule_number</i>} access-group {ALL <i>address_object</i>} zone {ALL <i>zone_object</i>} action {accept deny}</code>	<p>Sets a service control rule for SNMP service.</p> <p><i>address_object</i>: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p> <p><i>zone_object</i>: The name of the zone. Use up to 31 characters (a-zA-Z0-9_-). The name cannot start with a number. This value is case-sensitive.</p> <p>The UAG uses pre-defined zone names like DMZ, LAN1, LAN2, SSL VPN, IPsec VPN, and WAN.</p>
<code>snmp-server rule move <i>rule_number</i> to <i>rule_number</i></code>	Changes the index number of a service control rule.
<code>no snmp-server rule <i>rule_number</i></code>	Deletes a service control rule for SNMP service.
<code>show snmp status</code>	Displays SNMP Settings.

### 57.8.4 SNMP Commands Examples

The following command sets a service control rule that allowed the computers with the IP addresses matching the specified address object to access the specified zone using SNMP service.

```
Router# configure terminal
Router(config)# snmp-server rule 11 access-group Example zone WAN action accept
```

The following command sets the password (secret) for read-write (rw) access.

```
Router# configure terminal
Router(config)# snmp-server community secret rw
```

The following command sets the IP address of the host that receives the SNMP notifications to 172.16.15.84 and the password (sent with each trap) to qwerty.

```
Router# configure terminal
Router(config)# snmp-server host 172.16.15.84 qwerty
```

## 57.9 ICMP Filter

The `ip icmp-filter` commands are obsolete. See [Chapter 33 on page 171](#) to configure firewall rules for ICMP traffic going to the UAG to discard or reject ICMP packets destined for the UAG.

Configure the ICMP filter to help keep the UAG hidden from probing attempts. You can specify whether or not the UAG is to respond to probing for unused ports.

You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 186** Command Summary: ICMP Filter

COMMAND	DESCRIPTION
<code>[no] ip icmp-filter activate</code>	Turns the ICMP filter on or off.
<code>ip icmp-filter rule {&lt;1..32&gt; append insert &lt;1..32&gt;} access-group {ALL ADDRESS_OBJECT} zone {ALL ZONE_OBJECT} icmp-type {ALL echo-reply destination-unreachable source-quench redirect echo-request router-advertisement router-solicitation time-exceeded parameter-problem timestamp-request timestamp-reply address-mask-request address-mask-reply} action {accept deny}</code>	<p>Sets an ICMP filter rule.</p> <p>ADDRESS_OBJECT: The name of the IP address (group) object. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p> <p>ZONE_OBJECT: The name of the zone. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.</p>
<code>no ip icmp-filter rule &lt;1..64&gt;</code>	Deletes an ICMP filter rule.
<code>ip icmp-filter rule move &lt;1..64&gt; to &lt;1..64&gt;</code>	Changes the index number of an ICMP filter rule.
<code>show ip icmp-filter status</code>	Displays ICMP filter settings.

## File Manager

This chapter covers how to work with the UAG's firmware, certificates, configuration files, packet trace results, shell scripts and temporary files.

### 58.1 File Directories

The UAG stores files in the following directories.

**Table 187** FTP File Transfer Notes

DIRECTORY	FILE TYPE	FILE NAME EXTENSION
A	Firmware (upload only)	bin
cert	Non-PKCS#12 certificates	cer
conf	Configuration files	conf
packet_trace	Packet trace results (download only)	
script	Shell scripts	.zysh
tmp	Temporary system maintenance files and crash dumps for technical support use (download only)	

A. After you log in through FTP, you do not need to change directories in order to upload the firmware.

### 58.2 Configuration Files and Shell Scripts Overview

You can store multiple configuration files and shell script files on the UAG.

When you apply a configuration file, the UAG uses the factory default settings for any features that the configuration file does not include. Shell scripts are files of commands that you can store on the UAG and run when you need them. When you run a shell script, the UAG only applies the commands that it contains. Other settings do not change.

You can edit configuration files or shell scripts in a text editor and upload them to the UAG. Configuration files use a .conf extension and shell scripts use a .zysh extension.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

**Figure 24** Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure wan1
interface wan1
ip address 172.16.13.240 255.255.255.0
ip gateway 172.16.13.254 metric 1
exit
# create address objects for remote management / to-Device firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.16.13.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-Device firewall for TW_TEAM for remote management
firewall WAN Device insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the UAG applies configuration files differently than it runs shell scripts. This is explained below.

**Table 188** Configuration Files and Shell Scripts in the UAG

Configuration Files (.conf)	Shell Scripts (.zysh)
<ul style="list-style-type: none"> <li>Resets to default configuration.</li> <li>Goes into CLI <b>Configuration</b> mode.</li> <li>Runs the commands in the configuration file.</li> </ul>	<ul style="list-style-type: none"> <li>Goes into CLI <b>Privilege</b> mode.</li> <li>Runs the commands in the shell script.</li> </ul>

You have to run the example in [Table 24 on page 292](#) as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode. (See [Section 1.5 on page 30](#) for more information about CLI modes.)

## 58.2.1 Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use “#” or “!” as the first character of a command line to have the UAG treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the UAG exit sub command mode.

Note: “exit” or “!” must follow sub commands if it is to make the UAG exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface wan1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface wan1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2006/06/05
interface wan1
ip address dhcp
!
```

## 58.2.2 Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the UAG processes the file line-by-line. The UAG checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the UAG finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The UAG ignores any errors in the configuration file or shell script and applies all of the valid commands. The UAG still generates a log for any errors.

## 58.2.3 UAG Configuration File Details

You can store multiple configuration files on the UAG. You can also have the UAG use a different configuration file without the UAG restarting.

- When you first receive the UAG, it uses the **system-default.conf** configuration file of default settings.
- When you change the configuration, the UAG creates a **startup-config.conf** file of the current configuration.
- The UAG checks the **startup-config.conf** file for errors when it restarts. If there is an error in the **startup-config.conf** file, the UAG copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file.

- When the UAG reboots, if the **startup-config.conf** file passes the error check, the UAG keeps a copy of the **startup-config.conf** file as the **lastgood.conf** configuration file for you as a back up file. If you upload and apply a configuration file with an error, you can apply **lastgood.conf** to return to a valid configuration.

## 58.2.4 Configuration File Flow at Restart

If there is not a **startup-config.conf** when you restart the UAG (whether through a management interface or by physically turning the power off and back on), the UAG uses the **system-default.conf** configuration file with the UAG's default settings.

If there is a **startup-config.conf**, the UAG checks it for errors and applies it. If there are no errors, the UAG uses it and copies it to the **lastgood.conf** configuration file. If there is an error, the UAG generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the UAG applies the **system-default.conf** configuration file.

You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The UAG ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The UAG still generates a log for any errors.

## 58.3 File Manager Commands Input Values

The following table explains the values you can input with the file manager commands.

**Table 189** File Manager Command Input Values

LABEL	DESCRIPTION
<i>file_name</i>	The name of a file. Use up to 25 characters (including a-zA-Z0-9;~!@#%&()_+[]{}',.=).

## 58.4 File Manager Commands Summary

The following table lists the commands that you can use for file management.

**Table 190** File Manager Commands Summary

COMMAND	DESCRIPTION
<code>apply /conf/file_name.conf [ignore-error] [rollback]</code>	<p>Has the UAG use a specific configuration file. You must still use the <code>write</code> command to save your configuration changes to the flash (“non-volatile” or “long term”) memory.</p> <p>Use this command without specify both <code>ignore-error</code> and <code>rollback</code>: this is not recommended because it would leave the rest of the configuration blank. If the interfaces were not configured before the first error, the console port may be the only way to access the device.</p> <p>Use <code>ignore-error</code> without <code>rollback</code>: this applies the valid parts of the configuration file and generates error logs for all of the configuration file’s errors. This lets the UAG apply most of your configuration and you can refer to the logs for what to fix.</p> <p>Use both <code>ignore-error</code> and <code>rollback</code>: this applies the valid parts of the configuration file, generates error logs for all of the configuration file’s errors, and starts the UAG with a fully valid configuration file.</p> <p>Use <code>rollback</code> without <code>ignore-error</code>: this gets the UAG started with a fully valid configuration file as quickly as possible.</p> <p>You can use the “<code>apply /conf/system-default.conf</code>” command to reset the UAG to go back to its system defaults.</p>
<code>copy {/cert   /conf   /packet_trace   /script   /tmp}file_name-a.conf {/cert   /conf   /packet_trace   /script   /tmp}/file_name-b.conf</code>	<p>Saves a duplicate of a file on the UAG from the source file name to the target file name.</p> <p>Specify the directory and file name of the file that you want to copy and the directory and file name to use for the duplicate. Always copy the file into the same directory.</p>
<code>copy running-config startup-config</code>	<p>Saves your configuration changes to the flash (“non-volatile” or “long term”) memory. The UAG immediately uses configuration changes made via commands, but if you do not use this command or the <code>write</code> command, the changes will be lost when the UAG restarts.</p>
<code>copy running-config /conf/file_name.conf</code>	<p>Saves a duplicate of the configuration file that the UAG is currently using. You specify the file name to which to copy.</p>
<code>delete {/cert   /conf   /packet_trace   /script   /tmp}/file_name</code>	<p>Removes a file. Specify the directory and file name of the file that you want to delete.</p>
<code>dir {/cert   /conf   /packet_trace   /script   /tmp}</code>	<p>Displays the list of files saved in the specified directory.</p>
<code>rename {/cert   /conf   /packet_trace   /script   /tmp}/old-file_name {/cert   /conf   /packet_trace   /script   /tmp}/new-file_name</code>	<p>Changes the name of a file.</p> <p>Specify the directory and file name of the file that you want to rename. Then specify the directory again followed by the new file name.</p>
<code>rename /script/old-file_name /script/new-file_name</code>	<p>Changes the name of a shell script.</p>
<code>run /script/file_name.zysh</code>	<p>Has the UAG execute a specific shell script file. You must still use the <code>write</code> command to save your configuration changes to the flash (“non-volatile” or “long term”) memory.</p>
<code>schedule-run 1 file_name.zysh {daily   monthly   weekly} time {date   sun   mon   tue   wed   thu   fri   sat}</code>	<p>Has the UAG execute the specified specific shell script file at the the specified time. You must still use the <code>write</code> command to save your configuration changes to the flash (“non-volatile” or “long term”) memory.</p>

**Table 190** File Manager Commands Summary (continued)

COMMAND	DESCRIPTION
<code>show running-config</code>	Displays the settings of the configuration file that the system is using.
<code>[no] backup-startup activate</code>	Sets the UAG to back up the <code>startup-conf.conf</code> file when it is performing firmware upgrade.  The <code>no</code> command disables the backup function.
<code>show backup-startup status</code>	Displays whether the startup configuration backup function is enabled or not.
<code>setenv-startup stop-on-error off</code>	Has the UAG ignore any errors in the <code>startup-config.conf</code> file and apply all of the valid commands.
<code>show setenv-startup</code>	Displays whether or not the UAG is set to ignore any errors in the <code>startup-config.conf</code> file and apply all of the valid commands.
<code>write</code>	Saves your configuration changes to the flash (“non-volatile” or “long term”) memory. The UAG immediately uses configuration changes made via commands, but if you do not use the <code>write</code> command, the changes will be lost when the UAG restarts.

## 58.5 File Manager Command Examples

This example saves a back up of the current configuration before applying a shell script file.

```
Router(config)# copy running-config /conf/backup.conf
Router(config)# run /script/vpn_setup.zysh
```

These commands run the `aaa.zysh` script at noon every day, on the first day of every month, and on every Monday, Wednesday, and Friday.

```
Router> configure terminal
Router(config)# schedule-run 1 aaa.zysh daily 12:00
Router(config)# schedule-run 1 aaa.zysh monthly 12:00 01
Router(config)# schedule-run 1 aaa.zysh weekly 12:00 mon wed fri
Router(config)#
```

## 58.6 FTP File Transfer

You can use FTP to transfer files to and from the UAG for advanced maintenance and support.

### 58.6.1 Command Line FTP File Upload

- 1 Connect to the UAG.
- 2 Enter “bin” to set the transfer mode to binary.
- 3 You can upload the firmware after you log in through FTP. To upload other files, use “cd” to change to the corresponding directory.



- 4 Use "put" to transfer files from the computer to the UAG.<sup>1</sup> For example:  
 In the conf directory, use "put config.conf today.conf" to upload the configuration file (config.conf) to the UAG and rename it "today.conf".  
 "put 1.00(XL.0).bin" transfers the firmware (1.00(XL.0).bin) to the UAG.

**The firmware update can take up to five minutes. Do not turn off or reset the UAG while the firmware update is in progress! If you lose power during the firmware upload, you may need to refer to [Section 58.8 on page 299](#) to recover the firmware.**

## 58.6.2 Command Line FTP Configuration File Upload Example

The following example transfers a configuration file named tomorrow.conf from the computer and saves it on the UAG as next.conf.

Note: Uploading a custom signature file named "custom.rules", overwrites all custom signatures on the UAG.

**Figure 25** FTP Configuration File Upload Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (UAG) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> cd conf
250 CWD command successful
ftp> bin
200 Type set to I
ftp> put tomorrow.conf next.conf
200 PORT command successful
150 Opening BINARY mode data connection for next.conf
226-Post action ok!!
226 Transfer complete.
ftp: 20231 bytes sent in 0.00Seconds 20231000.00Kbytes/sec.
```

## 58.6.3 Command Line FTP File Download

- 1 Connect to the UAG.
- 2 Enter "bin" to set the transfer mode to binary.
- 3 Use "cd" to change to the directory that contains the files you want to download.
- 4 Use "dir" or "ls" if you need to display a list of the files in the directory.
- 5 Use "get" to download files. For example:  
 "get vpn\_setup.zysh vpn.zysh" transfers the vpn\_setup.zysh configuration file on the UAG to your computer and renames it "vpn.zysh."

1. When you upload a custom signature, the UAG appends it to the existing custom signatures stored in the "custom.rules" file.

## 58.6.4 Command Line FTP Configuration File Download Example

The following example gets a configuration file named `today.conf` from the UAG and saves it on the computer as `current.conf`.

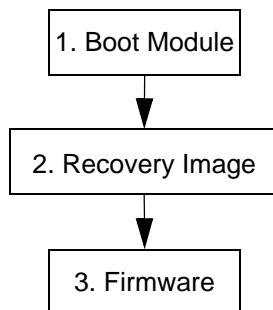
**Figure 26** FTP Configuration File Download Example

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (UAG) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> bin
200 Type set to I
ftp> cd conf
250 CWD command successful
ftp> get today.conf current.conf
200 PORT command successful
150 Opening BINARY mode data connection for conf/today.conf (20220
bytes)
226 Transfer complete.
ftp: 20220 bytes received in 0.03Seconds 652.26Kbytes/sec.
```

## 58.7 UAG File Usage at Startup

The UAG uses the following files at system startup.

**Figure 27** UAG File Usage at Startup



- 1 The boot module performs a basic hardware test. You cannot restore the boot module if it is damaged. The boot module also checks and loads the recovery image. The UAG notifies you if the recovery image is damaged.
- 2 The recovery image checks and loads the firmware. The UAG notifies you if the firmware is damaged.

## 58.8 Notification of a Damaged Recovery Image or Firmware

The UAG's recovery image and/or firmware could be damaged, for example by the power going off during a firmware upgrade. This section describes how the UAG notifies you of a damaged recovery image or firmware file. Use this section if your device has stopped responding for an extended period of time and you cannot access or ping it. Note that the UAG does not respond while starting up. It takes less than five minutes to start up with the default configuration, but the start up time increases with the complexity of your configuration.

- 1 Use a console cable and connect to the UAG via a terminal emulation program (such as HyperTerminal). Your console session displays the UAG's startup messages. If you cannot see any messages, check the terminal emulation program's settings (see [Section 1.2.1 on page 25](#)) and restart the UAG.
- 2 The system startup messages display followed by "Press any key to enter debug mode within 1 seconds."

Note: Do not press any keys at this point. Wait to see what displays next.

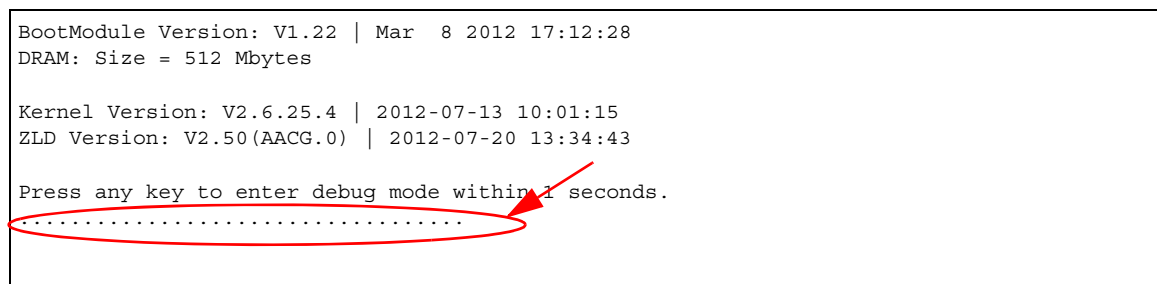
**Figure 28** System Startup Stopped

```

BootModule Version: V1.22 | Mar  8 2012 17:12:28
DRAM: Size = 512 Mbytes

Kernel Version: V2.6.25.4 | 2012-07-13 10:01:15
ZLD Version: V2.50(AACG.0) | 2012-07-20 13:34:43

Press any key to enter debug mode within 1 seconds.
.....
  
```

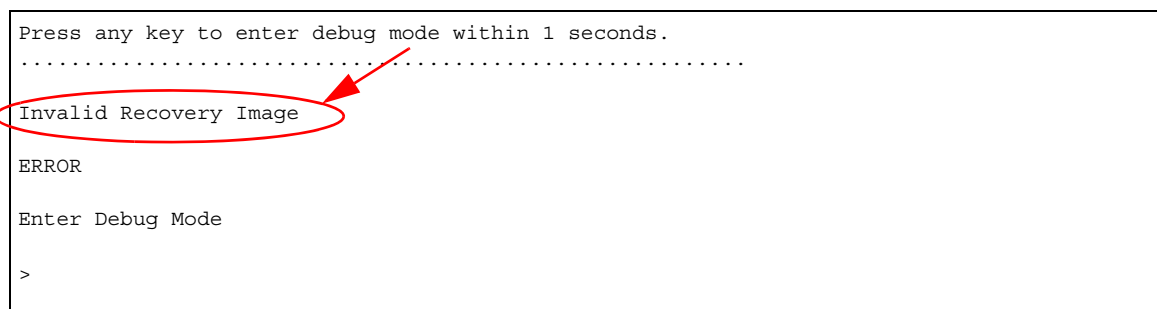


- 3 If the console session displays "Invalid Firmware", or "Invalid Recovery Image", or the console freezes at "Press any key to enter debug mode within 1 seconds" for more than one minute, go to [Section 58.9 on page 300](#) to restore the recovery image.

**Figure 29** Recovery Image Damaged

```

Press any key to enter debug mode within 1 seconds.
.....
Invalid Recovery Image
ERROR
Enter Debug Mode
>
  
```



- 4 If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, the firmware file is damaged. Use the procedure in [Section 58.10 on page 302](#) to restore it. If the message does not display, the firmware is OK and you do not need to use the firmware recovery procedure.

**Figure 30** Firmware Damaged

```
Building ...
Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

## 58.9 Restoring the Recovery Image

This procedure requires the UAG's recovery image. Download the firmware package from [www.zyxel.com](http://www.zyxel.com) and unzip it. The recovery image uses a .ri extension, for example, "1.01(XL.0)C0.ri". Do the following after you have obtained the recovery image file.

Note: You only need to use this section if you need to restore the recovery image.

- 1 Restart the UAG.
- 2 When “Press any key to enter debug mode within 1 seconds.” displays, press a key to enter debug mode.

**Figure 31** Enter Debug Mode

```
BootModule Version: V1.22 | Mar 8 2012 17:12:28
DRAM: Size = 512 Mbytes

Kernel Version: V2.6.25.4 | 2012-07-13 10:01:15
ZLD Version: V2.50(AACG.0) | 2012-07-20 13:34:43

Press any key to enter debug mode within 1 seconds.
.....
Enter Debug Mode

>
```

- 3 Enter atuk to initialize the recovery process. If the screen displays “ERROR”, enter atur to initialize the recovery process.



- 7 Enter `atgo`. The UAG starts up. If “Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file” displays on the screen, the firmware file is damaged and you need to use the procedure in [Section 58.10 on page 302](#) to recover the firmware.

**Figure 36** atgo Debug Command

```
> atgo
Booting ...
```

## 58.10 Restoring the Firmware

This procedure requires the UAG's firmware. Download the firmware package from [www.zyxel.com](http://www.zyxel.com) and unzip it. The firmware file uses a .bin extension, for example, "250AACG0C0.bin". Do the following after you have obtained the firmware file.

Note: This section is not for normal firmware uploads. You only need to use this section if you need to recover the firmware.

- 1 Connect your computer to the UAG's port **1** (only port **1** can be used).
- 2 The UAG's FTP server IP address for firmware recovery is 192.168.1.1, so set your computer to use a static IP address from 192.168.1.2 ~192.168.1.254.
- 3 Use an FTP client on your computer to connect to the UAG. For example, in the Windows command prompt, type `ftp 192.168.1.1`. Keep the console session connected in order to see when the firmware recovery finishes.
- 4 Enter your user name when prompted.
- 5 Enter your password as requested.
- 6 Set the transfer mode to binary (type `bin`).
- 7 Transfer the firmware file from your computer to the UAG. Type `put` followed by the path and name of the firmware file. This examples uses `put C:\ftproot\UAG_FW\250AACG0C0.bin`.

**Figure 37** FTP Firmware Transfer Command

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (UAG) [192.168.1.1]
User (192.168.1.1:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> bin
200 Type set to I
ftp> put C:\ftproot\UAG_FW\250AACG0C0.bin
```

- 8 Wait for the file transfer to complete.

- 9 Enter "quit" to exit the ftp prompt.

**Figure 38** FTP Firmware Transfer Complete

```
200 PORT command successful
150 Opening BINARY mode data connection for 250AACG0C0.bin
226-firmware verifying...
226-firmware updating...
226-Please Wait about 5 minutes!!
226-Do not poweroff or reset,
226-system will reboot automatically after finished updating.
226 Transfer complete.
ftp: 42923922 bytes sent in 3.50Seconds 12260.47Kbytes/sec.
ftp> quit
```

- 10 The console session displays "done" when the firmware recovery is complete. Then the UAG automatically restarts.

**Figure 39** Firmware Recovery Complete and Restart

```
BM cmd line: console=ttyS0,115200 root=/dev/ram init=zyinit "-r /dev/sda", address: 0x100000

intird start:000000008425E000 size:00000000000EAF4E

vmlinux start:0000000084006000 size:00000000002575CD

Uncompressing Linux...done.
Start to check file system...
/dev/sda2: 30/17640 files (6.7% non-contiguous), 47365/70432 blocks
/dev/sda3: 96/112224 files (2.1% non-contiguous), 8231/224192 blocks
Done
INIT: version 2.86 booting
Initializing Debug Account Authentication Seed (DAAS)... done.
```

- 11 The username prompt displays after the UAG starts up successfully. The firmware recovery process is now complete and the UAG is ready to use.

**Figure 40** Restart Complete

```
Setting the System Clock using the Hardware Clock as reference...System Clock set
INIT: Entering runlevel: 313:48:37 UTC 2012
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting ZLD Wrapper Daemon....
Starting uam daemon.
Starting periodic command scheduler: cron.
Start UAG715 system daemon....
.....
Got LINK_CHANGE
Port [1] Copper is up --> Group [1] is up
.....
Got LINK_CHANGE
Port [2] Copper is up --> Group [2] is up
Applying system configuration file, please wait...
.Device system is configured successfully with startup-config.conf

Welcome to UAG715

Username:
```

This chapter provides information about the UAG's logs.

Note: When the system log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

See the User's Guide for the maximum number of system log messages in the UAG.

## 59.1 Log Commands Summary

The following table describes the values required for many log commands. Other values are discussed with the corresponding commands.

**Table 191** Input Values for Log Commands

LABEL	DESCRIPTION
<i>interface_name</i>	The name of the interface. This depends on the UAG model. See <a href="#">Table 37 on page 86</a> for detailed information about the interface name.
<i>module_name</i>	The name of the category; <code>kernel</code> , <code>syslog</code> , .... The default category includes debugging messages generated by open source software. The <code>all</code> category includes all messages in all categories.
<i>protocol</i>	The name of a protocol such as TCP, UDP, ICMP.

The following sections list the logging commands.

### 59.1.1 Log Entries Commands

This table lists the commands to look at log entries.

**Table 192** logging Commands: Log Entries

COMMAND	DESCRIPTION
<code>show logging entries [priority <i>pri</i>] [category <i>module_name</i>] [srcip <i>ip</i>] [dstip <i>ip</i>] [service <i>service_name</i>] [begin &lt;1..512&gt; end &lt;1..512&gt;] [keyword <i>keyword</i>] [srciface <i>interface_name</i>] [dstiface <i>interface_name</i>] [protocol <i>protocol</i>]</code>	Displays the specified entries in the system log.  <i>pri</i> : alert   crit   debug   emerg   error   info   notice   warn  <i>keyword</i> : You can use alphanumeric and ()+/:=?!*#@\$_%- characters, and it can be up to 63 characters long. This searches the message, source, destination, and notes fields.
<code>show logging entries field <i>field</i> [begin &lt;1..512&gt; end &lt;1..512&gt;]</code>	Displays the specified fields in the system log.  <i>field</i> : time   msg   src   dst   note   pri   cat   all



## 59.1.2 System Log Commands

This table lists the commands for the system log settings.

**Table 193** logging Commands: System Log Settings

COMMAND	DESCRIPTION
show logging status system-log	Displays the current settings for the system log.
logging system-log category <i>module_name</i> {disable   level normal   level all}	Specifies what kind of information, if any, is logged in the system log and debugging log for the specified category.
[no] logging system-log suppression interval <10..600>	Sets the log consolidation interval for the system log. The no command sets the interval to ten.
[no] logging system-log suppression	Enables log consolidation in the system log. The no command disables log consolidation in the system log.
[no] connectivity-check continuous-log activate	Has the UAG generate a log for each connectivity check. The no command has the UAG only log the first connectivity check.
show connectivity-check continuous-log status	Displays whether or not the UAG generates a log for each connectivity check.
clear logging system-log buffer	Clears the system log.

### 59.1.2.1 System Log Command Examples

The following command displays the current status of the system log.

```
Router# configure terminal
Router(config)# show logging status system-log
58 events logged
suppression active : yes
suppression interval: 10
category settings :
  content-filter      : normal , content-filter-forward: no      ,
  forward-web-sites  : no      , blocked-web-sites : normal ,
  warning-web-sites  : normal , user                : normal ,
  myZyXEL.com        : normal , zysh                : normal ,
  bwm                 : normal , ike                 : normal ,
  ipsec               : normal , firewall            : normal ,
  sessions-limit     : normal , policy-route        : normal ,
  built-in-service   : normal , system              : normal ,
  system-monitoring  : no      , connectivity-check: normal ,
  routing-protocol   : normal , nat                 : normal ,
  pki                 : normal , interface           : normal ,
  interface-statistics: no      , account             : normal ,
  port-grouping      : normal , ssl-vpn             : normal ,
  traffic-log        : no      , file-manage         : normal ,
  adp                 : normal , usb-storage         : normal ,
  daily-report       : normal , ipmac-binding       : normal ,
  dhcp               : normal , eps                 : normal ,
  web-authentication: normal , smtp-redirect       : normal ,
  vpn-1-1-mapping    : normal , default             : all      ,
Router(config)#
```

### 59.1.3 Debug Log Commands

This table lists the commands for the debug log settings.

**Table 194** logging Commands: Debug Log Settings

COMMAND	DESCRIPTION
show logging debug status	Displays the current settings for the debug log.
show logging debug entries [priority <i>pri</i> ] [category <i>module_name</i> ] [srcip <i>ip</i> ] [dstip <i>ip</i> ] [service <i>service_name</i> ] [srciface <i>interface_name</i> ] [dstiface <i>interface_name</i> ] [protocol <i>protocol</i> ] [begin <1..512> end <1..512>] [keyword <i>keyword</i> ]	Displays the specified entries in the system log.  <i>pri</i> : alert   crit   debug   emerg   error   info   notice   warn  <i>keyword</i> : You can use alphanumeric and () + / : = ? ! * # @ \$ _ % - characters, and it can be up to 63 characters long. This searches the message, source, destination, and notes fields.
show logging debug entries field <i>field</i> [begin <1..1024> end <1..1024>]	Displays the specified field in the debug log.  <i>field</i> : time   msg   src   dst   note   pri   cat   all
[no] logging debug suppression	Enables log consolidation in the debug log. The no command disables log consolidation in the debug log.
[no] logging debug suppression interval <10..600>	Sets the log consolidation interval for the debug log. The no command sets the interval to ten.
clear logging debug buffer	Clears the debug log.

This table lists the commands for the remote syslog server settings.

**Table 195** logging Commands: Remote Syslog Server Settings

COMMAND	DESCRIPTION
show logging status syslog	Displays the current settings for the remote servers.
[no] logging syslog <1..4>	Enables the specified remote server. The no command disables the specified remote server.
[no] logging syslog <1..4> address { <i>ip</i>   <i>hostname</i> }	Sets the URL or IP address of the specified remote server. The no command clears this field.  <i>hostname</i> : You may up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
[no] logging syslog <1..4> {disable   level normal   level all}	Specifies what kind of information, if any, is logged for the specified category.
[no] logging syslog <1..4> facility {local_1   local_2   local_3   local_4   local_5   local_6   local_7}	Sets the log facility for the specified remote server. The no command sets the facility to local_1.
[no] logging syslog <1..4> format cef	Sets the format of the log information.  <i>cef</i> : Common Event Format, syslog-compatible format.
[no] logging syslog <1..4> port <1..65535>	Sets the port number of the specified remote server. The no command clears this field.

## 59.1.4 E-mail Profile Commands

This table lists the commands for the e-mail profile settings.

**Table 196** logging Commands: E-mail Profile Settings

COMMAND	DESCRIPTION
show logging status mail	Displays the current settings for the e-mail profiles.
[no] logging mail <1..2>	Enables the specified e-mail profile. The no command disables the specified e-mail profile.
[no] logging mail <1..2> address {ip   hostname}	Sets the URL or IP address of the mail server for the specified e-mail profile. The no command clears the mail server field.  <i>hostname</i> : You may use up to 63 alphanumeric characters, dashes (-), or periods (.), but the first character cannot be a period.
logging mail <1..2> sending_now	Sends mail for the specified e-mail profile immediately, according to the current settings.
[no] logging mail <1..2> authentication	Enables SMTP authentication. The no command disables SMTP authentication.
[no] logging mail <1..2> authentication username <i>username</i> password <i>password</i>	Sets the username and password required by the SMTP mail server. The no command clears the username and password fields.  <i>username</i> : You can use alphanumeric characters, underscores (_), and dashes (-), and it can be up to 31 characters long.  <i>password</i> : You can use most printable ASCII characters. You cannot use square brackets [ ], double quotation marks ("), question marks (?), tabs or spaces. It can be up to 31 characters long.
[no] logging mail <1..2> category <i>module_name</i> level {alert   all}	Specifies what kind of information is logged for the specified category. The no command disables logging for the specified category.
[no] logging mail <1..2> port <1..65535>	Sets the port number of the mail server for the specified e-mail profile.
[no] logging mail <1..2> {send-log-to   send-alerts-to} <i>e_mail</i>	Sets the e-mail address for logs or alerts. The no command clears the specified field.  <i>e_mail</i> : You can use up to 63 alphanumeric characters, underscores (_), or dashes (-), and you must use the @ character.
[no] logging mail <1..2> subject <i>subject</i>	Sets the subject line when the UAG mails to the specified e-mail profile. The no command clears this field.  <i>subject</i> : You can use up to 60 alphanumeric characters, underscores (_), dashes (-), or !@#\$%*()+=;: ',./ characters.
[no] logging mail <1..2> schedule {full   hourly}	Sets the e-mail schedule for the specified e-mail profile. The no command clears the schedule field.
logging mail <1..2> schedule daily hour <0..23> minute <0..59>	Sets a daily e-mail schedule for the specified e-mail profile.
logging mail <1..2> schedule weekly day <i>day</i> hour <0..23> minute <0..59>	Sets a weekly e-mail schedule for the specified e-mail profile.  <i>day</i> : sun   mon   tue   wed   thu   fri   sat

**Table 196** logging Commands: E-mail Profile Settings (continued)

COMMAND	DESCRIPTION
[no] logging mail <1..2> tls activate	Sets the UAG to use Transport Layer Security (TLS) to have encrypted communications between the mail server and the UAG.  The no command disables TLS in communications between the mail server and the UAG.
[no] logging mail <1..2> tls authenticate-server	Sets the UAG to authenticate the mail server in the TLS handshake.  The no command sets the UAG to not authenticate the mail server in the TLS handshake.

### 59.1.4.1 E-mail Profile Command Examples

The following commands set up e-mail log 1.

```
Router# configure terminal
Router(config)# logging mail 1 address mail.zyxel.com.tw
Router(config)# logging mail 1 subject AAA
Router(config)# logging mail 1 authentication username lachang.li password XXXXXX
Router(config)# logging mail 1 send-log-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 send-alerts-to lachang.li@zyxel.com.tw
Router(config)# logging mail 1 from lachang.li@zyxel.com.tw
Router(config)# logging mail 1 schedule weekly day mon hour 3 minute 3
Router(config)# logging mail 1
```

### 59.1.5 Console Port Logging Commands

This table lists the commands for the console port settings.

**Table 197** logging Commands: Console Port Settings

COMMAND	DESCRIPTION
show logging status console	Displays the current settings for the console log. (This log is not discussed above.)
[no] logging console	Enables the console log. The no command disables the console log.
logging console category <i>module_name</i> level {alert   crit   debug   emerg   error   info   notice   warn}	Controls whether or not debugging information for the specified priority is displayed in the console log, if logging for this category is enabled.
[no] logging console category <i>module_name</i>	Enables logging for the specified category in the console log. The no command disables logging.

## Reports and Reboot

This chapter provides information about the report associated commands and how to restart the UAG using commands. It also covers the daily report e-mail feature.

### 60.1 Report Commands Summary

The following sections list the report, session, and packet size statistics commands.

#### 60.1.1 Report Commands

This table lists the commands for reports.

**Table 198** report Commands

COMMAND	DESCRIPTION
<code>[no] report</code>	Begins data collection. The <code>no</code> command stops data collection.
<code>show report status</code>	Displays whether or not the UAG is collecting data and how long it has collected data.
<code>clear report [interface_name]</code>	Clears the report for the specified interface or for all interfaces.
<code>show report [interface_name {ip   service   url}]</code>	Displays the traffic report for the specified interface and controls the format of the report. Formats are:  <code>ip</code> - traffic by IP address and direction  <code>service</code> - traffic by service and direction  <code>url</code> - hits by URL

## 60.1.2 Report Command Examples

The following commands start collecting data, display the traffic reports, and stop collecting data.

```
Router# configure terminal
Router(config)# show report lan1 ip
No. IP Address      User                Amount              Direction
=====
1  192.168.1.4      admin              1273 (bytes)       Outgoing
2  192.168.1.4      admin              711 (bytes)        Incoming
Router(config)# show report lan1 service
No. Proto    Port  Service          Amount              Direction
=====
1  tcp       80    www              5.920 (MBytes)     Outgoing
2  tcp       80    www              224.363 (KBytes)   Incoming
Router(config)# show report lan1 url
No. Hit      URL
=====
1  1          140.114.79.60
Router(config)# show report status
Report status: on
Collect Statistics: since 2012-07-24 Tue 13:49:06 to 2012-07-24 Tue 14:12:46
```

## 60.1.3 Session Commands

This table lists the commands to display the current sessions for debugging or statistical analysis.

**Table 199** Session Commands

COMMAND	DESCRIPTION
show conn [user {username any unknown}] [service {service-name any unknown}] [source {ip any}] [destination {ip any}] [begin <1..128000>] [end <1..128000>]	Displays information about the selected sessions or about all sessions. You can look at all the active sessions or filter the information by user name, service object, source IP, destination IP, or session number(s). any means all users, services and IP addresses respectively. unknow means unknown users and services respectively.
show conn ip-traffic destination	Displays information about traffic session sorted by the destination.
show conn ip-traffic source	Displays information about traffic session sorted by the source.
show conn status	Displays the number of active sessions.

## 60.2 Email Daily Report Commands

The following table identifies the values used in some of these commands. Other input values are discussed with the corresponding commands.

**Table 200** Input Values for Email Daily Report Commands

LABEL	DESCRIPTION
e_mail	An e-mail address. You can use up to 80 alphanumeric characters, underscores (_), periods (.), or dashes (-), and you must use the @ character.

Use these commands to have the UAG e-mail you system statistics every day. You must use the `configure terminal` command to enter the configuration mode before you can use these commands.

**Table 201** Email Daily Report Commands

COMMAND	DESCRIPTION
<code>show daily-report status</code>	Displays the e-mail daily report settings.
<code>daily-report</code>	Enters the sub-command mode for configuring daily e-mail reports settings.
<code>[no] activate</code>	Turns daily e-mail reports on or off.
<code>draw-usage-graphics</code>	Has the report e-mail include usage graphs.
<code>smtp-address {ip   hostname}</code>	Sets the SMTP mail server IP address or domain name.
<code>[no] smtp-auth activate</code>	Enables or disables SMTP authentication.
<code>smtp-auth username username password password</code>	Sets the username and password for SMTP authentication.
<code>no smtp-address</code>	Resets the SMTP mail server configuration.
<code>no smtp-auth username</code>	Resets the authentication configuration.
<code>[no] smtp-port &lt;1..65535&gt;</code>	Sets the SMTP authentication port. The <code>no</code> command deletes the setting.
<code>mail-subject set subject</code>	Configures the subject of the report e-mails. Spaces are allowed.
<code>no mail-subject set</code>	Clears the configured subject for the report e-mails.
<code>[no] mail-subject append system-name</code>	Determines whether the system name will be appended to the subject of the report e-mails.
<code>[no] mail-subject append date-time</code>	Determines whether the sending date-time will be appended at subject of the report e-mails.
<code>[no] mail-from e_mail</code>	Sets the sender e-mail address of the report e-mails.
<code>[no] mail-to-1 e_mail</code>	Sets to whom the UAG sends the report e-mails (up to five recipients).
<code>[no] mail-to-2 e_mail</code>	See above.
<code>[no] mail-to-3 e_mail</code>	See above.
<code>[no] mail-to-4 e_mail</code>	See above.
<code>[no] mail-to-5 e_mail</code>	See above.
<code>[no] item cf-report</code>	Determines whether or not content filtering statistics are included in the report e-mails.
<code>[no] item cpu-usage</code>	Determines whether or not CPU usage statistics are included in the report e-mails.
<code>[no] item mem-usage</code>	Determines whether or not memory usage statistics are included in the report e-mails.
<code>[no] item port-usage</code>	Determines whether or not port usage statistics are included in the report e-mails.
<code>[no] item session-usage</code>	Determines whether or not session usage statistics are included in the report e-mails.
<code>[no] item traffic-report</code>	Determines whether or not network traffic statistics are included in the report e-mails.
<code>schedule hour &lt;0..23&gt; minute &lt;00..59&gt;</code>	Sets the time for sending out the report e-mails.
<code>[no] reset-counter</code>	Determines whether or not to discard all report data and starts all of the report statistics data counters over at zero after successfully sending out a report e-mail.

**Table 201** Email Daily Report Commands (continued)

COMMAND	DESCRIPTION
<code>send-now</code>	Sends the daily e-mail report immediately.
<code>[no] smtp-tls activate</code>	Sets the UAG to use Transport Layer Security (TLS) to have encrypted communications between the mail server and the UAG.  The <code>no</code> command disables TLS in communications between the mail server and the UAG.
<code>[no] smtp-tls authenticate-server</code>	Sets the UAG to authenticate the mail server in the TLS handshake.  The <code>no</code> command sets the UAG to not authenticate the mail server in the TLS handshake.
<code>reset-counter-now</code>	Discards all report data and starts all of the report statistics data counters over at zero.
<code>exit</code>	Leaves the sub-command mode.

## 60.2.1 Email Daily Report Example

This example sets the following about sending a daily report e-mail:

- Disables the reporting.
- Specifies `example-SMTP-mail-server.com` as the address of the SMTP mail server.
- Sets the subject of the report e-mails to `test`.
- Stops the system name from being appended to the mail subject.
- Appends the date and time to the mail subject.
- Sets the sender as `my-email@example.com`.
- Sets `example-administrator@example.com` as the first account to which to send the mail.
- Has the UAG not use the second and third mail-to options.
- Sets `my-email@example.com` as the fourth mail-to option.
- Has the UAG not use the fifth mail-to option.
- Has the UAG provide username `12345` and password `12345` to the SMTP server for authentication.
- Sets the UAG to send the report at 1:57 PM.
- Has the UAG not reset the counters after sending the report.
- Has the report include CPU, memory, port, and session usage along with traffic statistics.



- Turns on the daily e-mail reporting.

```

Router(config)# daily-report
Router(config-daily-report)# no activate
Router(config-daily-report)# smtp-address example-SMTP-mail-server.com
Router(config-daily-report)# mail-subject set test
Router(config-daily-report)# no mail-subject append system-name
Router(config-daily-report)# mail-subject append date-time
Router(config-daily-report)# mail-from my-email@example.com
Router(config-daily-report)# mail-to-1 example-administrator@example.com
Router(config-daily-report)# no mail-to-2
Router(config-daily-report)# no mail-to-3
Router(config-daily-report)# mail-to-4 my-email@example.com
Router(config-daily-report)# no mail-to-5
Router(config-daily-report)# smtp-auth activate
Router(config-daily-report)# smtp-auth username 12345 password pass12345
Router(config-daily-report)# schedule hour 13 minutes 57
Router(config-daily-report)# no reset-counter
Router(config-daily-report)# item cpu-usage
Router(config-daily-report)# item mem-usage
Router(config-daily-report)# item port-usage
Router(config-daily-report)# item session-usage
Router(config-daily-report)# item traffic-report
Router(config-daily-report)# activate
Router(config-daily-report)# exit
Router(config)#

```

This displays the email daily report settings and has the UAG send the report.

```

Router(config)# show daily-report status
email daily report status
=====
activate: yes
scheduled time: 13:57
reset counter: no
smtp address: example-SMTP-mail-server.com
smtp port: 25
smtp auth: yes
smtp username: 12345
smtp password: pass12345
mail subject: test subject
append system name: no
append date time: yes
mail from: my-email@example.com
mail-to-1: example-administrator@example.com
mail-to-2:
mail-to-3:
mail-to-4: my-email@example.com
mail-to-5:
cpu-usage: yes
mem-usage: yes
session-usage: yes
port-usage: yes
traffic-report: yes

Router(config)# daily-report send-now

```

## 60.3 Reboot

Use this to restart the device (for example, if the device begins behaving erratically).

If you made changes in the CLI, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Use the `reboot` command to restart the device.

## Session Timeout

Use these commands to modify and display the session timeout values. You must use the `configure terminal` command before you can use these commands.

**Table 202** Session Timeout Commands

COMMAND	DESCRIPTION
<code>session timeout {udp-connect &lt;1..300&gt;   udp-deliver &lt;1..300&gt;   icmp &lt;1..300&gt;}</code>	Sets the timeout for UDP sessions to connect or deliver and for ICMP sessions.
<code>session timeout {tcp-established   tcp-synrecv   tcp-close   tcp-finwait   tcp-synsent   tcp-closewait   tcp-lastack   tcp-timewait} &lt;1..300&gt;</code>	Sets the timeout for TCP sessions in the ESTABLISHED, SYN_RECV, FIN_WAIT, SYN_SENT, CLOSE_WAIT, LAST_ACK, or TIME_WAIT state.
<code>show session timeout {icmp   tcp   udp}</code>	Displays ICMP, TCP, and UDP session timeouts.

The following example sets the UDP session connect timeout to 10 seconds, the UDP deliver session timeout to 15 seconds, and the ICMP timeout to 15 seconds.

```
Router(config)# session timeout udp-connect 10
Router(config)# session timeout udp-deliver 15
Router(config)# session timeout icmp 15
Router(config)# show session timeout udp
UDP session connect timeout: 10 seconds
UDP session deliver timeout: 15 seconds
Router(config)# show session timeout icmp
ICMP session timeout: 15 seconds
```

# Diagnostics

This chapter covers how to use the diagnostics feature.

## 62.1 Diagnostics

The diagnostics feature provides an easy way for you to generate a file containing the UAG's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

## 62.2 Diagnosis Commands

The following table lists the commands that you can use to have the UAG collect diagnostics information. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

**Table 203** diagnosis Commands

COMMAND	DESCRIPTION
<code>diag-info collect</code>	Has the UAG create a new diagnostic file.
<code>diag-info cancel</code>	Stops the on-going diagnostic information collection.
<code>show diag-info</code>	Displays the name, size, and creation date (in yyyy-mm-dd hh:mm:ss format) of the diagnostic file.

## 62.3 Diagnosis Commands Example

The following example creates a diagnostic file and displays its name, size, and creation date.

```
Router# configure terminal
Router(config)# diag-info collect
Please wait, collecting information
Router(config)# show diag-info
Filename   : diaginfo-20070423.tar.bz2
File size  : 1259 KB
Date       : 2007-04-23 09:55:09
```

## Packet Flow Explore

This chapter covers how to use the packet flow explore feature.

### 63.1 Packet Flow Explore

Use this to get a clear picture on how the UAG determines where to forward a packet and how to change the source IP address of the packet according to your current settings. This function provides you a summary of all your routing and SNAT settings and helps troubleshoot the related problems.

### 63.2 Packet Flow Explore Commands

The following table lists the commands that you can use to have the UAG display routing and SNAT related settings.

**Table 204** Packet Flow Explore Commands

COMMAND	DESCRIPTION
<code>show ip route static-dynamic</code>	Displays activated static-dynamic routes.
<code>show route order</code>	Displays the order of routing related functions the UAG checks for packets. Once a packet matches the criteria of a routing rule, the UAG takes the corresponding action and does not perform any further flow checking.
<code>show system snat order</code>	Displays the order of SNAT related functions the UAG checks for packets. Once a packet matches the criteria of an SNAT rule, the UAG uses the corresponding source IP address and does not perform any further flow checking.
<code>show system route policy-route</code>	Displays activated policy routes.
<code>show system route nat-1-1</code>	Displays activated 1-to-1 NAT rules.
<code>show system route site-to-site-vpn</code>	Displays activated site-to-site VPN rules.
<code>show system route dynamic-vpn</code>	Displays activated dynamic VPN rules.
<code>show system route default-wan-trunk</code>	Displays the default WAN trunk settings.
<code>show system route vpn-1-1-map</code>	Displays activated VPN 1-1 mapping rules.
<code>show system snat policy-route</code>	Displays activated policy routes which use SNAT.
<code>show system snat nat-1-1</code>	Displays activated NAT rules which use SNAT.
<code>show system snat nat-loopback</code>	Displays activated activated NAT rules which use SNAT with NAT loopback enabled.
<code>show system snat default-snat</code>	Displays the default WAN trunk settings.
<code>show system snat vpn-1-1-map</code>	Displays activated VPN 1-1 mapping rules which use SNAT.

## 63.3 Packet Flow Explore Commands Example

The following example shows all routing related functions and their order.

```
Router> show route order
route order: Direct Route, Policy Route, VPN 1-1 Mapping Route, 1-1 SNAT, SiteTo
Site VPN, Dynamic VPN, Static-Dynamic Route, Default WAN Trunk, Main Route
```

The following example shows all SNAT related functions and their order.

```
Router> show system snat order
snat order: Policy Route SNAT, VPN 1-1 Mapping SNAT, 1-1 SNAT, Loopback SNAT, De
fault SNAT
```

The following example shows all activated policy routes.

```
Router> show system route policy-route
No. PR NO. Source Destination Incoming DSCP Service Nexthop Type
Nexthop Info
=====
```

The following example shows all activated 1-to-1 SNAT rules.

```
Router> show system route nat-1-1
No. VS Name Source Destination Outgoing Gateway
=====
```

The following example shows all activated site-to-site VPN rules.

```
Router> show system route site-to-site-vpn
No. Source Destination VPN Tunnel
=====
```

The following example shows all activated dynamic VPN rules.

```
Router> show system route dynamic-vpn
No. Source Destination VPN Tunnel
=====
```

The following example shows the default WAN trunk's settings.

```
Router> show system route default-wan-trunk
No. Source Destination Trunk
=====
1 any any SYSTEM_DEFAULT_WAN_TRUNK
```

The following example shows all activated dynamic VPN rules.

```
Router> show system route dynamic-vpn
No.  Source          Destination          VPN Tunnel
=====
```

The following example shows all activated VPN 1-1 mapping rules.

```
Router> sshow system route vpn-1-1-map
No.  Source          Destination  Outgoing  Gateway
=====
```

The following example shows all activated static-dynamic VPN rules.

```
Router> show ip route static-dynamic
Flags: A - Activated route, S - Static route, C - directly Connected
       O - OSPF derived, R - RIP derived, G - selected Gateway
       ! - reject, B - Black hole, L - Loop

IP Address/Netmask  Gateway          IFace          Metric  Flags  Persist
=====
0.0.0.0/0           10.1.1.254      wan1           0       ASG    -
```

The following example shows all activated policy routes which use SNAT.

```
Router> show system snat policy-route
No.  PR NO. Outgoing  SNAT
=====
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name  Source  Destination  Outgoing  SNAT
=====
```

The following example shows all activated policy routes which use SNAT and enable NAT loopback..

```
Router> show system snat nat-loopback
Note: Loopback SNAT will be only applied only when the initiator is located at the
network which the server locates at

No.  VS Name  Source  Destination  SNAT
=====
```

The following example shows all activated 1-to-1 NAT rules.

```
Router> show system snat nat-1-1
No.  VS Name      Source      Destination  Outgoing      SNAT
=====
```

The following example shows the default WAN trunk settings.

```
Router> show system snat default-snat
Incoming      Outgoing      SNAT
=====
Internal Interface  External Interface  Outgoing Interface IP

Internal Interfaces: lan1, lan2, dmz
External Interfaces: wan1, wan2, wan1_ppp, wan2_ppp
Router>
```



## Maintenance Tools

Use the maintenance tool commands to check the conditions of other devices through the UAG. The maintenance tools can help you to troubleshoot network problems.

Here are maintenance tool commands that you can use in privilege mode.

**Table 205** Maintenance Tools Commands in Privilege Mode

COMMAND	DESCRIPTION
<pre>packet-trace [interface <i>interface_name</i>] [ip-proto {&lt;0..255&gt;   <i>protocol_name</i>   any}] [src-host {<i>ip</i>   <i>hostname</i>   any}] [dst-host {<i>ip</i>   <i>hostname</i>   any}] [port {&lt;1..65535&gt;   any}] [file] [duration &lt;1..3600&gt;] [extension-filter <i>filter_extension</i>]</pre>	<p>Sniffs traffic going through the specified interface with the specified protocol, source address, destination address, and/or port number.</p> <p>If you specify <i>file</i>, the UAG dumps the traffic to <code>/packet_trace/packet_trace_interface</code>. Use FTP to retrieve the files (see <a href="#">Section 58.6 on page 296</a>).</p> <p>If you do not assign the duration, the UAG keeps dumping traffic until you use Ctrl-C.</p> <p>Use the extension filter to extend the use of this command.</p> <p><i>protocol_name</i>: You can use the name, instead of the number, for some IP protocols, such as <code>tcp</code>, <code>udp</code>, <code>icmp</code>, and so on. The names consist of 1-16 alphanumeric characters or dashes (-). The first character cannot be a number.</p> <p><i>hostname</i>: You can use up to 252 alphanumeric characters, dashes (-), or periods (.). The first character cannot be a period.</p> <p><i>filter_extension</i>: You can use 1-256 alphanumeric characters, spaces, or <code>'()+,/:=?!*#@\$_%.-</code> characters.</p>
<pre>traceroute {<i>ip</i>   <i>hostname</i>}</pre>	<p>Displays the route taken by packets to the specified destination. Use Ctrl+C to return to the prompt.</p>
<pre>Ping {<i>ipv4</i>   <i>hostname</i>} [source <i>ipv4</i>] [size &lt;0..65507&gt;] [forever  count &lt;1..4096&gt;]</pre>	<p>Sends an ICMP ECHO_REQUEST to test the reachability of a host on an IPv4 network and to measure the round-trip time for a message sent from the originating host to the destination computer.</p> <p><i>size</i>: specifies the number of data bytes to be sent</p> <p><i>count</i>: Stop after sending this number of ECHO_REQUEST packets.</p> <p><i>forever</i>: keep sending ECHO_REQUEST packets until you use Ctrl+c to stop.</p>
<pre>show packet-capture status</pre>	<p>Displays whether a packet capture is ongoing.</p>
<pre>show packet-capture config</pre>	<p>Displays current packet capture settings.</p>

Here are maintenance tool commands that you can use in configure mode.

**Table 206** Maintenance Tools Commands in Privilege Mode

COMMAND	DESCRIPTION
[no] packet-capture activate	Performs a packet capture that captures network traffic going through the set interface(s). Studying these packet captures may help you identify network problems.  The no command stops the running packet capture on the UAG.  <b>Note:</b> Use the packet-capture configure command to configure the packet-capture settings before using this command.
packet-capture configure	Enters the sub-command mode.
duration <0..300>	Sets a time limit in seconds for the capture. The UAG stops the capture and generates the capture file when either this period of time has passed or the file reaches the size specified using the files-size command below. 0 means there is no time limit.
file-suffix <profile_name>	Specifies text to add to the end of the file name (before the dot and filename extension) to help you identify the packet capture files. Modifying the file suffix also avoids making new capture files that overwrite existing files of the same name.  The file name format is "interface name-file suffix.cap", for example "vlan2-packet-capture.cap".
files-size <1..10000>	Specifies a maximum size limit in megabytes for the total combined size of all the capture files on the UAG, including any existing capture files and any new capture files you generate.  The UAG stops the capture and generates the capture file when either the file reaches this size or the time period specified ( using the duration command above) expires.
host-ip {ip-address   profile_name   any>	Sets a host IP address or a host IP address object for which to capture packets. any means to capture packets for all hosts.
host-port <0..65535>	Specifies the port number of traffic to capture.
iface {add   del} {interface_name   virtual_interface_name}	Adds or deletes an interface or a virtual interface for which to capture packets to the capture interfaces list.
snaplen <68..1512>	Specifies the maximum number of bytes to capture per packet. The UAG automatically truncates packets that exceed this size. As a result, when you view the packet capture files in a packet analyzer, the actual size of the packets may be larger than the size of captured packets.
storage <internal usbstorage>	Sets to have the UAG only store packet capture entries on the UAG (internal) or on a USB storage connected to the UAG.
ring-buffer <enable disable>	Enables or disables the ring buffer used as a temporary storage.
split-size <1..2048>	Specifies a maximum size limit in megabytes for individual packet capture files. After a packet capture file reaches this size, the UAG starts another packet capture file.
show packet-capture status	Displays whether a packet capture is ongoing.
show packet-capture config	Displays current packet capture settings.

## 64.1 Maintenance Command Examples

Some packet-trace command examples are shown below.

```
Router# packet-trace duration 3
tcpdump: listening on eth0
19:24:43.239798 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:43.240199 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:44.258823 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:44.259219 192.168.1.1 > 192.168.1.10: icmp: echo reply
19:24:45.268839 192.168.1.10 > 192.168.1.1: icmp: echo request
19:24:45.269238 192.168.1.1 > 192.168.1.10: icmp: echo reply

6 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface lan1 ip-proto icmp file extension-filter -s
-> 500 -n
tcpdump: listening on eth1
07:24:07.898639 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:07.900450 192.168.105.40 > 192.168.105.133: icmp: echo reply
07:24:08.908749 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:24:08.910606 192.168.105.40 > 192.168.105.133: icmp: echo reply

8 packets received by filter
0 packets dropped by kernel
```

```
Router# packet-trace interface lan1 ip-proto icmp file extension-filter
-> and src host 192.168.105.133 and dst host 192.168.105.40 -s 500 -n
tcpdump: listening on eth1
07:26:51.731558 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:52.742666 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:53.752774 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)
07:26:54.762887 192.168.105.133 > 192.168.105.40: icmp: echo request (DF)

8 packets received by filter
0 packets dropped by kernel
```

```
Router# traceroute www.zyxel.com
traceroute to www.zyxel.com (203.160.232.7), 30 hops max, 38 byte packets
 1 172.13.37.254  3.049 ms  1.947 ms  1.979 ms
 2 172.13.6.253  2.983 ms  2.961 ms  2.980 ms
 3 172.13.6.1    5.991 ms  5.968 ms  6.984 ms
 4 * * *
```

Here are maintenance tool commands that you can use in configure mode.

**Table 207** Maintenance Tools Commands in Configuration Mode

COMMAND	DESCRIPTION
show arp-table	Displays the current Address Resolution Protocol table.

**Table 207** Maintenance Tools Commands in Configuration Mode (continued)

COMMAND	DESCRIPTION
<code>arp IP mac_address</code>	Edits or creates an ARP table entry.
<code>no arp ip</code>	Removes an ARP table entry.

The following example creates an ARP table entry for IP address 192.168.1.10 and MAC address 01:02:03:04:05:06. Then it shows the ARP table and finally removes the new entry.

```
Router# arp 192.168.1.10 01:02:03:04:05:06
Router# show arp-table
Address          HWtype  HWaddress          Flags Mask          Iface
192.168.1.10    ether   01:02:03:04:05:06 CM                   lan1
172.16.19.254   ether   00:04:80:9B:78:00 C                     wan1
Router# no arp 192.168.1.10
Router# show arp-table
Address          HWtype  HWaddress          Flags Mask          Iface
192.168.1.10    (incomplete)
172.16.19.254   ether   00:04:80:9B:78:00 C                     wan1
```

### 64.1.1 Packet Capture Command Example

The following examples show how to configure packet capture settings and perform a packet capture. First you have to check whether a packet capture is running. This example shows no other packet capture is running. Then you can also check the current packet capture settings.

```
Router(config)# show packet-capture status
capture status: off
Router(config)#
Router(config)# show packet-capture config
iface: None
host-port: 0
host-ip: any
file-suffix: -packet-capture
snaplen: 1500
duration: 0
file-size: 10
split-size: 2
ring-buffer: 0
storage: 0
```

Then configure the following settings to capture packets going through the UAG's WAN1 interface only.

- IP address: any
- Host IP: any
- Host port: any (then you do not need to configure this setting)
- File suffix: Example
- File size: 10 megabytes
- Duration: 150 seconds
- Save the captured packets to: USB storage device
- Use the ring buffer: no

- The maximum size of a packet capture file: 100 megabytes

```
Router(config)# packet-capture configure
Router(packet-capture)# iface add wan1
Router(packet-capture)# ip-type any
Router(packet-capture)# host-ip any
Router(packet-capture)# file-suffix Example
Router(packet-capture)# files-size 10
Router(packet-capture)# duration 150
Router(packet-capture)# storage usbstorage
Router(packet-capture)# ring-buffer disable
Router(packet-capture)# split-size 100
Router(packet-capture)#
```

Exit the sub-command mode and have the UAG capture packets according to the settings you just configured.

```
Router(packet-capture)# exit
Router(config)# packet-capture activate
Router(config)#
```

Manually stop the running packet capturing.

```
Router(config)# no packet-capture activate
Router(config)#
```

Check current packet capture status and list all stored packet captures.

```
Router(config)# show packet-capture status
capture status: off
Router(config)# dir /packet_trace
File Name                               Size      Modified Time
=====
wan1-Example.cap                       575160    2009-11-24 09:06:59
Router(config)#
```

You can use FTP to download a capture file. Open and study it using a packet analyzer tool (for example, Ethereal or Wireshark).

# Watchdog Timer

This chapter provides information about the UAG's watchdog timers.

## 65.1 Hardware Watchdog Timer

The hardware watchdog has the system restart if the hardware fails.

**The `hardware-watchdog-timer` commands are for support engineers. It is recommended that you not modify the hardware watchdog timer settings.**

**Table 208** hardware-watchdog-timer Commands

COMMAND	DESCRIPTION
[no] hardware-watchdog-timer <4..37>	Sets how long the system's hardware can be unresponsive before resetting. The no command turns the timer off.
show hardware-watchdog-timer status	Displays the settings of the hardware watchdog timer.

## 65.2 Software Watchdog Timer

The software watchdog has the system restart if the core firmware fails.

**The `software-watchdog-timer` commands are for support engineers. It is recommended that you not modify the software watchdog timer settings.**

**Table 209** software-watchdog-timer Commands

COMMAND	DESCRIPTION
[no] software-watchdog-timer <10..600>	Sets how long the system's core firmware can be unresponsive before resetting. The no command turns the timer off.
show software-watchdog-timer status	Displays the settings of the software watchdog timer.
show software-watchdog-timer log	Displays a log of when the software watchdog timer took effect.

## 65.3 Application Watchdog

The application watchdog has the system restart a process that fails. These are the `app-watchdog` commands. Use the `configure terminal` command to enter the configuration mode to be able to use these commands.

**Table 210** app-watchdog Commands

COMMAND	DESCRIPTION
<code>[no] app-watch-dog activate</code>	Turns the application watchdog timer on or off.
<code>[no] app-watch-dog auto-recover</code>	If <code>app-watch-dog</code> detects a dead process, <code>app-watch-dog</code> will try to auto recover. The <code>no</code> command turns off auto-recover
<code>[no] app-watch-dog console-print {always once}</code>	Display debug messages on the console (every time they occur or once). The <code>no</code> command changes the setting back to the default.
<code>[no] app-watch-dog cpu-threshold min &lt;1..100&gt; max &lt;1..100&gt;</code>	Sets the percentage thresholds for sending a CPU usage alert. The UAG starts sending alerts when CPU usage exceeds the maximum (the second threshold you enter). The UAG stops sending alerts when the CPU usage drops back below the minimum threshold (the first threshold you enter). The <code>no</code> command changes the setting back to the default.
<code>[no] app-watch-dog interval &lt;6..300&gt;</code>	Sets how frequently (in seconds) the UAG checks the system processes. The <code>no</code> command changes the setting back to the default.
<code>[no] app-watch-dog retry-count &lt;1..5&gt;</code>	Set how many times the UAG is to re-check a process before considering it failed. The <code>no</code> command changes the setting back to the default.
<code>[no] app-watch-dog alert</code>	Has the UAG send an alert the user when the system is out of memory or disk space.
<code>[no] app-watch-dog disk-threshold min &lt;1..100&gt; max &lt;1..100&gt;</code>	Sets the percentage thresholds for sending a disk usage alert. The UAG starts sending alerts when disk usage exceeds the maximum (the second threshold you enter). The UAG stops sending alerts when the disk usage drops back below the minimum threshold (the first threshold you enter). The <code>no</code> command changes the setting back to the default.
<code>[no] app-watch-dog mem-threshold min &lt;1..100&gt; max &lt;1..100&gt;</code>	Sets the percentage thresholds for sending a memory usage alert. The UAG starts sending alerts when memory usage exceeds the maximum (the second threshold you enter). The UAG stops sending alerts when the memory usage drops back below the minimum threshold (the first threshold you enter). The <code>no</code> command changes the setting back to the default.
<code>app-watch-dog reboot-log flush</code>	Flushes the reboot log record.
<code>[no] app-watch-dog sys-reboot</code>	If auto recover fail reaches the maximum retry count, <code>app-watch-dog</code> reboots the device. The <code>no</code> command turns off system auto reboot.
<code>show app-watch-dog config</code>	Displays the application watchdog timer settings.
<code>show app-watch-dog monitor-list</code>	Display the list of applications that the application watchdog is monitoring.
<code>show app-watch-dog reboot-log</code>	Displays the application watchdog reboot log.

### 65.3.1 Application Watchdog Commands Example

The following example displays the application watchdog configuration and lists the processes that the application watchdog is monitoring.



```

Application Watch Dog Setting:
activate: yes
alert: yes
console print: always
retry count: 3
auto recover: yes
system reboot: yes
interval: 60 seconds
mem threshold: 80% ~ 90%
cpu threshold: 80% ~ 90%
disk threshold: 80% ~ 90%
Router(config)# show app-watch-dog monitor-list
#app_name      min_process_count      max_process_count      (-1 unlimited)      recover_enable      recover_reboot      recover_always      recover_max_try_count      recover_max_fail_count
uamnd          1                       1                       -1                   1                   1                   1                   1                   1
firewalld      1                       1                       -1                   0                   1                   1                   1                   1
policyd        1                       1                       -1                   1                   1                   1                   1                   1
contftd        1                       1                       -1                   1                   1                   1                   1                   1
classify       1                       1                       -1                   0                   1                   1                   1                   1
ospfd          1                       1                       -1                   0                   1                   1                   1                   1
ripd           1                       1                       -1                   0                   1                   1                   1                   1
resd           1                       1                       -1                   0                   1                   1                   1                   1
zyshd_wd       1                       1                       -1                   0                   1                   1                   1                   1
zyshd          1                       1                       -1                   0                   1                   1                   1                   1
htctpd        1                       1                       -1                   1                   1                   1                   1                   1
dhcpcd         1                       1                       -1                   1                   1                   1                   1                   1
sshsecpm       1                       1                       -1                   1                   1                   1                   1                   1
zylgd          1                       1                       -1                   0                   1                   1                   1                   1
syslog-ng      1                       1                       -1                   0                   1                   1                   1                   1
zylodger       1                       1                       -1                   0                   1                   1                   1                   1
dnsmasq        1                       1                       -1                   0                   1                   1                   1                   1
tpd            1                       1                       -1                   0                   1                   1                   1                   1
wtdtd         1                       1                       -1                   0                   1                   1                   1                   1
zebra          1                       1                       -1                   0                   1                   1                   1                   1
link_updown    1                       1                       -1                   0                   1                   1                   1                   1
faulthd        1                       1                       -1                   0                   1                   1                   1                   1
pro            1                       1                       -1                   0                   1                   1                   1                   1
signal_wrapper 1                       1                       -1                   0                   1                   1                   1                   1
asd            1                       1                       -1                   0                   1                   1                   1                   1
ctipd.bin      1                       1                       -1                   1                   1                   1                   1                   1
ipmonitord     1                       1                       -1                   0                   1                   1                   1                   1

```

# List of Commands (Alphabetical)

This section lists the commands and sub-commands in alphabetical order. Commands and subcommands appear at the same level.

[no] {anti-virus   personal-firewall} activate .....	263
[no] {firewall secure-policy} activate .....	173
[no] {firewall secure-policy} asymmetrical-route activate .....	172
[no] {ipv4   ipv4_cidr   ipv4_range   wildcard_domainname   tld} .....	217
[no] 2g-scan-channel wireless_channel_2g .....	65
[no] 5g-scan-channel wireless_channel_5g .....	65
[no] aaa authentication default member1 [member2] [member3] [member4] .....	250
[no] aaa authentication profile-name .....	250
[no] aaa authentication profile-name member1 [member2] [member3] [member4] .....	251
[no] aaa group server ad group-name .....	245
[no] aaa group server ldap group-name .....	246
[no] aaa group server radius group-name .....	247
[no] access-page color-window-background .....	273
[no] access-page message-text message .....	273
[no] account {pppoe   pptp} profile_name .....	258
[no] account e-mail .....	183
[no] account profile_name .....	101
[no] activate .....	143
[no] activate .....	154
[no] activate .....	154
[no] activate .....	161
[no] activate .....	167
[no] activate .....	174
[no] activate .....	176
[no] activate .....	178
[no] activate .....	191
[no] activate .....	203
[no] activate .....	206
[no] activate .....	278
[no] activate .....	311
[no] activate .....	60
[no] activate .....	65
[no] activate .....	71
[no] activate .....	74
[no] additional-ddns-options {--dyndns_system   --ip_server_name} .....	130
[no] address address_object .....	176
[no] address-object object_name .....	237
[no] ad-server basedn basedn .....	243
[no] ad-server binddn binddn .....	244
[no] ad-server cn-identifier uid .....	244
[no] ad-server host ad_server .....	244
[no] ad-server password password .....	244
[no] ad-server password-encrypted password .....	244
[no] ad-server port port_no .....	244
[no] ad-server search-time-limit time .....	244
[no] ad-server ssl .....	244
[no] advertisement activate .....	168
[no] advertisement name description url url .....	168
[no] agreement-url url .....	164
[no] ampdu .....	61

[no] amsdu .....	62
[no] anti-virus <i>anti_virus_software_name</i> detect-auto-protection {enable   disable   ignore} 263 .....	
[no] app log <i>sid</i> .....	211
[no] app <i>profile_name</i> .....	211
[no] app statistics collect .....	211
[no] application <i>application_object</i> .....	206
[no] application forbidden-process <i>process_name</i> .....	264
[no] application <i>sid</i> .....	232
[no] application trusted-process <i>process_name</i> .....	264
[no] application-object <i>object_name</i> .....	233
[no] app-watch-dog activate .....	327
[no] app-watch-dog alert .....	327
[no] app-watch-dog auto-recover .....	327
[no] app-watch-dog console-print {always once} .....	327
[no] app-watch-dog cpu-threshold min <1..100> max <1..100> .....	327
[no] app-watch-dog disk-threshold min <1..100> max <1..100> .....	327
[no] app-watch-dog interval <6..300> .....	327
[no] app-watch-dog mem-threshold min <1..100> max <1..100> .....	327
[no] app-watch-dog retry-count <1..5> .....	327
[no] app-watch-dog sys-reboot .....	327
[no] area IP [{stub   nssa}] .....	123
[no] area IP authentication .....	123
[no] area IP authentication authentication-key <i>authkey</i> .....	123
[no] area IP authentication message-digest .....	123
[no] area IP authentication message-digest-key <1..255> md5 <i>authkey</i> .....	123
[no] area IP virtual-link IP .....	123
[no] area IP virtual-link IP authentication .....	123
[no] area IP virtual-link IP authentication authentication-key <i>authkey</i> .....	123
[no] area IP virtual-link IP authentication message-digest .....	123
[no] area IP virtual-link IP authentication message-digest-key <1..255> md5 <i>authkey</i> ....	123
[no] area IP virtual-link IP authentication same-as-area .....	123
[no] area IP virtual-link IP authentication-key <i>authkey</i> .....	123
[no] authentication {chap-pap   chap   pap   mschap   mschap-v2} .....	258
[no] authentication {force   required} .....	161
[no] authentication mode {md5   text} .....	122
[no] authentication string <i>authkey</i> .....	122
[no] auth-server activate .....	278
[no] auth-server cert <i>certificate_name</i> .....	278
[no] auth-server trusted-client <i>profile_name</i> .....	278
[no] auto-destination .....	115
[no] auto-disable .....	115
[no] auto-healing activate .....	82
[no] backmx .....	130
[no] backup-custom <i>ip</i> .....	129
[no] backup-iface <i>interface_name</i> .....	130
[no] backup-startup activate .....	296
[no] bandwidth <1..1048576> priority <1..1024> [maximize-bandwidth-usage] .....	115
[no] bandwidth activate .....	179
[no] bandwidth activate .....	270
[no] billing discount activate .....	177
[no] billing discount unit <2..10> price <i>price</i> .....	178
[no] billing profile <i>profile_name</i> .....	178
[no] billing tax-rate activate .....	178
[no] billing wlan-ssid-profile <i>profile_name</i> .....	178
[no] bind <i>interface_name</i> .....	101
[no] block .....	126
[no] block-ack .....	62
[no] block-intra .....	67

[no] bwm activate .....	115
[no] bwm activate .....	190
[no] bypass-firewall activate .....	148
[no] cache-clean activate .....	206
[no] case-sensitive .....	245
[no] case-sensitive .....	247
[no] case-sensitive .....	248
[no] client-identifier <i>mac_address</i> .....	91
[no] client-name <i>host_name</i> .....	91
[no] clock daylight-saving .....	275
[no] clock saving-interval begin { <i>apr aug dec feb jan jul jun mar may nov oct sep</i> } {1 2 3 4 last} { <i>fri mon sat sun thu tue wed</i> } <i>hh:mm</i> end { <i>apr aug dec feb jan jul jun mar may nov oct sep</i> } {1 2 3 4 last} { <i>fri mon sat sun thu tue wed</i> } <i>hh:mm</i> offset .....	275
[no] clock time-zone {- + <i>hh</i> } .....	275
[no] compression { <i>yes   no</i> } .....	258
[no] conn-check activate .....	115
[no] connection-id <i>connection_id</i> .....	259
[no] connectivity { <i>nail-up   dial-on-demand</i> } .....	101
[no] connectivity-check continuous-log activate .....	305
[no] connectivity-check continuous-log activate .....	97
[no] connlimit max-per-host <1..8192> .....	172
[no] console baud <i>baud_rate</i> .....	275
[no] contain <i>ap_mac</i> .....	74
[no] content-filter active .....	216
[no] content-filter block message <i>message</i> .....	216
[no] content-filter block redirect <i>redirect_url</i> .....	216
[no] content-filter bypass-vpn .....	216
[no] content-filter cache-timeout <i>_timeout</i> .....	216
[no] content-filter cache-timeout <i>_timeout</i> .....	220
[no] content-filter default block .....	216
[no] content-filter license <i>license</i> .....	216
[no] content-filter policy <i>policy_number address schedule filtering_profile</i> .....	216
[no] content-filter profile <i>filtering_profile</i> .....	218
[no] content-filter profile <i>filtering_profile</i> commtouch-url category { <i>category_name</i> } ..	219
[no] content-filter profile <i>filtering_profile</i> custom .....	218
[no] content-filter profile <i>filtering_profile</i> custom activex .....	218
[no] content-filter profile <i>filtering_profile</i> custom cookie .....	218
[no] content-filter profile <i>filtering_profile</i> custom java .....	218
[no] content-filter profile <i>filtering_profile</i> custom proxy .....	218
[no] content-filter profile <i>filtering_profile</i> custom trust-allow-features .....	218
[no] content-filter profile <i>filtering_profile</i> custom trust-only .....	218
[no] content-filter profile <i>filtering_profile</i> url category { <i>category_name</i> } .....	218
[no] content-filter profile <i>filtering_profile</i> url url-server .....	219
[no] content-filter report deactivate .....	217
[no] content-filter report server { <i>ipv4   domain_name</i> } .....	217
[no] content-filter service-timeout <i>service_timeout</i> .....	219
[no] content-filter statistics collect .....	221
[no] corefile copy usb-storage .....	103
[no] crypto ignore-df-bit .....	199
[no] crypto map <i>map_name</i> .....	199
[no] crypto <i>map_name</i> .....	203
[no] crypto <i>profile_name</i> .....	126
[no] ctmatch { <i>dnat   snat</i> } .....	174
[no] ctrsts <0..2347> .....	61
[no] custom ip .....	129
[no] dcs activate .....	77
[no] ddns-server <i>fqdn</i> .....	130
[no] deactivate .....	115

[no] default-router <i>ip</i> .....	91
[no] description <i>description</i> .....	115
[no] description <i>description</i> .....	155
[no] description <i>description</i> .....	161
[no] description <i>description</i> .....	174
[no] description <i>description</i> .....	176
[no] description <i>description</i> .....	191
[no] description <i>description</i> .....	206
[no] description <i>description</i> .....	211
[no] description <i>description</i> .....	226
[no] description <i>description</i> .....	232
[no] description <i>description</i> .....	233
[no] description <i>description</i> .....	237
[no] description <i>description</i> .....	240
[no] description <i>description</i> .....	264
[no] description <i>description</i> .....	278
[no] description <i>description</i> .....	87
[no] description <i>description</i> .....	91
[no] destination { <i>address_object</i>   <i>group_name</i> } .....	161
[no] destination { <i>address_object</i>  any} .....	115
[no] destination <i>address_object</i> .....	191
[no] destinationip <i>address_object</i> .....	174
[no] diag-info copy usb-storage .....	103
[no] disable-dfs-switch .....	60
[no] domainname <i>domain_name</i> .....	274
[no] domain-name <i>domain_name</i> .....	91
[no] dot11n-disable-coexistence .....	61
[no] dot1x-eap .....	69
[no] downstream <0..1048576> .....	87
[no] dpd .....	197
[no] dscp <{0..63}   any   class {af11   af12   af13   af21   af22   af23   af31   af32   af33   af41   af42   af43   cs0   cs1   cs2   cs3   cs4   cs5   cs6   cs7   default   wmm_be0   wmm_be24   wmm_bk16   wmm_bk8   wmm_vi32   wmm_vi40   wmm_vo48   wmm_vo56}} .....	191
[no] dscp {any   <0..63>} .....	115
[no] dscp class {default   <i>dscp_class</i> } .....	116
[no] duplex <full   half> .....	99
[no] dynamic-guest <i>user_name</i> .....	270
[no] encryption {nomppe   mppe-40   mppe-128} .....	259
[no] eps <1..8> <i>eps_object_name</i> .....	161
[no] eps <1..8> <i>eps_profile_name</i> .....	206
[no] eps activate .....	161
[no] eps activate .....	206
[no] eps failure-messages <i>failure_messages</i> .....	263
[no] eps periodical-check <1..1440> .....	161
[no] eps periodical-check <1..1440> .....	207
[no] eps periodical-check activate .....	206
[no] eps profile <i>profile_name</i> .....	263
[no] eps rename <i>profile_name</i> <i>new_profile_name</i> .....	265
[no] error-url <i>url</i> .....	160
[no] fall-back .....	197
[no] file-info file-path <i>file_path</i> .....	264
[no] file-info file-path <i>file_path</i> {eq   gt   lt   ge   le   neq} file-size <1..1073741824> 264 .....	264
[no] file-info file-path <i>file_path</i> {eq   gt   lt   ge   le   neq} file-size <1..1073741824> {eq   gt   lt   ge   le   neq} file-version <i>file_version</i> .....	264
[no] file-info file-path <i>file_path</i> {eq   gt   lt   ge   le   neq} file-version <i>file_version</i> 264 .....	264
[no] first-dns-server { <i>ip</i>   <i>interface_name</i> {1st-dns   2nd-dns   3rd-dns}   Device} .....	92
[no] first-wins-server <i>ip</i> .....	92

[no] <i>forbid_hosts</i> .....	218
[no] <i>force</i> .....	161
[no] <i>force vlan</i> .....	56
[no] <i>frag</i> <256..2346> .....	61
[no] <i>frame-capture activate</i> .....	76
[no] <i>free-time activate</i> .....	186
[no] <i>free-time deliver-method onscreen</i> .....	186
[no] <i>free-time deliver-method sms</i> .....	186
[no] <i>free-time maximum-register-number</i> <1..5> .....	186
[no] <i>free-time reset-register</i> <i>hh:mm</i> .....	186
[no] <i>free-time time-period</i> <i>time_period</i> .....	186
[no] <i>from zone_object</i> .....	174
[no] <i>groupname groupname</i> .....	226
[no] <i>groupname groupname</i> .....	226
[no] <i>ha-iface interface_name</i> .....	130
[no] <i>hardware-address mac_address</i> .....	91
[no] <i>hardware-watchdog-timer</i> <4..37> .....	326
[no] <i>hidden</i> .....	167
[no] <i>hide</i> .....	67
[no] <i>host hostname</i> .....	129
[no] <i>host ip</i> .....	91
[no] <i>hostname hostname</i> .....	274
[no] <i>htprotection</i> .....	63
[no] <i>https activate</i> .....	130
[no] <i>identity-token identity_token</i> .....	183
[no] <i>idle</i> <0..360> .....	258
[no] <i>idle-detection</i> [timeout <1..60>] .....	162
[no] <i>idle-detection</i> [timeout <1..60>] .....	164
[no] <i>inbound ceiling</i> {<0..1048576>   <i>maximize-bandwidth-usage</i> } .....	191
[no] <i>inbound guarantee-bandwidth</i> <0..1048576> <i>priority</i> <1..7> .....	191
[no] <i>inbound-dscp-mark</i> {<0..63>   <i>class</i> { <i>af11</i>   <i>af12</i>   <i>af13</i>   <i>af21</i>   <i>af22</i>   <i>af23</i>   <i>af31</i>   <i>af32</i>   <i>af33</i>   <i>af41</i>   <i>af42</i>   <i>af43</i>   <i>cs0</i>   <i>cs1</i>   <i>cs2</i>   <i>cs3</i>   <i>cs4</i>   <i>cs5</i>   <i>cs6</i>   <i>cs7</i>   <i>default</i>   <i>wmm_be0</i>   <i>wmm_be24</i>   <i>wmm_bk16</i>   <i>wmm_bk8</i>   <i>wmm_vi32</i>   <i>wmm_vi40</i>   <i>wmm_vo48</i>   <i>wmm_vo56</i> }} .....	191
[no] <i>incoming-interface</i> { <i>interface interface_name</i>   <i>trunk group_name</i> } .....	192
[no] <i>in-dnat activate</i> .....	200
[no] <i>in-snat activate</i> .....	200
[no] <i>interface</i> { <i>interface_name</i>   <i>any</i> } .....	143
[no] <i>interface</i> { <i>num</i> / <i>interface-name</i> } .....	107
[no] <i>interface interface_name</i> .....	116
[no] <i>interface interface_name</i> .....	126
[no] <i>interface interface_name</i> .....	154
[no] <i>interface interface_name</i> .....	156
[no] <i>interface interface_name</i> .....	87
[no] <i>interface-group group-name</i> .....	107
[no] <i>internal-page-customization</i> .....	164
[no] <i>internal-welcome-url url</i> .....	160
[no] <i>internal-welcome-url url</i> .....	162
[no] <i>ip address dhcp</i> .....	87
[no] <i>ip address ip subnet_mask</i> .....	278
[no] <i>ip address ip subnet_mask</i> .....	87
[no] <i>ip ddns profile profile_name</i> .....	129
[no] <i>ip dhcp pool profile_name</i> .....	90
[no] <i>ip dhcp-pool profile_name</i> .....	92
[no] <i>ip dns server a-record fqdn w.x.y.z</i> .....	276
[no] <i>ip dns server mx-record domain_name</i> { <i>w.x.y.z</i>   <i>fqdn</i> } .....	276
[no] <i>ip dns server zone-forwarder</i> {<1..32>  <i>append</i>   <i>insert</i> <1..32>} { <i>domain_zone_name</i>  *} <i>interface interface_name</i> .....	277
[no] <i>ip ftp server</i> .....	287

[no] ip ftp server cert <i>certificate_name</i>	287
[no] ip ftp server port <1..65535>	287
[no] ip ftp server tls-required	287
[no] ip gateway <i>ip</i>	87
[no] ip helper-address <i>ip</i>	92
[no] ip http authentication <i>auth_method</i>	282
[no] ip http port <1..65535>	282
[no] ip http secure-port <1..65535>	282
[no] ip http secure-server	282
[no] ip http secure-server auth-client	282
[no] ip http secure-server cert <i>certificate_name</i>	283
[no] ip http secure-server force-redirect	283
[no] ip http server	283
[no] ip ipnp activate	156
[no] ip load-balancing link-sticking activate	110
[no] ip load-balancing link-sticking timeout <i>timeout</i>	110
[no] ip ospf authentication-key <i>password</i>	95
[no] ip ospf cost <1..65535>	95
[no] ip ospf dead-interval <1..65535>	96
[no] ip ospf hello-interval <1..65535>	95
[no] ip ospf priority <0..255>	95
[no] ip ospf retransmit-interval <1..65535>	96
[no] ip rip {send   receive} version <1..2>	95
[no] ip rip v2-broadcast	95
[no] ip route {w.x.y.z} {w.x.y.z} {interface w.x.y.z} <0..127>	119
[no] ip route control-virtual-server-rules activate	119
[no] ip ssh server	285
[no] ip ssh server cert <i>certificate_name</i>	285
[no] ip ssh server port <1..65535>	285
[no] ip ssh server v1	285
[no] ip telnet server	286
[no] ip telnet server port <1..65535>	286
[no] ip-address <i>ip</i>	155
[no] ip-select {iface   auto   custom}	129
[no] ip-select-backup {iface   auto   custom}	129
[no] isakmp policy <i>policy_name</i>	197
[no] item cf-report	311
[no] item cpu-usage	311
[no] item mem-usage	311
[no] item port-usage	311
[no] item session-usage	311
[no] item traffic-report	311
[no] join <i>interface_name</i>	105
[no] keyword	218
[no] ldap-server basedn <i>basedn</i>	244
[no] ldap-server binddn <i>binddn</i>	244
[no] ldap-server cn-identifier <i>uid</i>	244
[no] ldap-server host <i>ldap_server</i>	244
[no] ldap-server password <i>password</i>	244
[no] ldap-server password-encrypted <i>password</i>	244
[no] ldap-server port <i>port_no</i>	244
[no] ldap-server search-time-limit <i>time</i>	244
[no] ldap-server ssl	244
[no] lease {<0..365> [<0..23> [<0..59>]]   infinite}	92
[no] limit <0..8192>	176
[no] listen-interface <i>interface_name</i>	148
[no] load-balancing activate	79
[no] load-balancing kickout	79
[no] local-address <i>ip</i>	101

[no] log [alert]	174
[no] log [alert]	192
[no] logging console	308
[no] logging console category <i>module_name</i>	308
[no] logging debug suppression	306
[no] logging debug suppression interval <10..600>	306
[no] logging mail <1..2>	307
[no] logging mail <1..2> {send-log-to   send-alerts-to} <i>e_mail</i>	307
[no] logging mail <1..2> address { <i>ip</i>   <i>hostname</i> }	307
[no] logging mail <1..2> authentication	307
[no] logging mail <1..2> authentication username <i>username</i> password <i>password</i>	307
[no] logging mail <1..2> category <i>module_name</i> level {alert   all}	307
[no] logging mail <1..2> port <1..65535>	307
[no] logging mail <1..2> schedule {full   hourly}	307
[no] logging mail <1..2> subject <i>subject</i>	307
[no] logging mail <1..2> tls activate	308
[no] logging mail <1..2> tls authenticate-server	308
[no] logging syslog <1..4>	306
[no] logging syslog <1..4> {disable   level normal   level all}	306
[no] logging syslog <1..4> address { <i>ip</i>   <i>hostname</i> }	306
[no] logging syslog <1..4> facility {local_1   local_2   local_3   local_4   local_5   local_6   local_7}	306
[no] logging syslog <1..4> format cef	306
[no] logging syslog <1..4> port <1..65535>	306
[no] logging system-log suppression	305
[no] logging system-log suppression interval <10..600>	305
[no] logging usb-storage	103
[no] login-page color-background	273
[no] login-page color-window-background	273
[no] login-page message-text % <i>message</i>	273
[no] login-url <i>url</i>	160
[no] logout-ip <i>ipv4_address</i>	160
[no] logout-url <i>url</i>	160
[no] MAC description <i>description2</i>	70
[no] mac-auth database mac <i>mac_address</i> type ext-mac-address mac-role <i>username</i> description <i>description</i>	228
[no] mac-auth database mac <i>mac_address</i> type int-mac-address mac-role <i>username</i> description <i>description</i>	228
[no] mac-auth database mac <i>oui</i> type ext-oui mac-role <i>username</i> description <i>description</i>	229
[no] mac-auth database mac <i>oui</i> type int-oui mac-role <i>username</i> description <i>description</i>	229
[no] macfilter <i>macfilterprofile</i>	67
[no] mail-from <i>e_mail</i>	311
[no] mail-subject append date-time	311
[no] mail-subject append system-name	311
[no] mail-to-1 <i>e_mail</i>	311
[no] mail-to-2 <i>e_mail</i>	311
[no] mail-to-3 <i>e_mail</i>	311
[no] mail-to-4 <i>e_mail</i>	311
[no] mail-to-5 <i>e_mail</i>	311
[no] metric <0..15>	87
[no] mss <536..1452>	102
[no] mss <536..1460>	87
[no] mtu <576..1500>	87
[no] multicast-to-unicast	62
[no] mx { <i>ip</i>   <i>domain_name</i> }	129
[no] nail-up	200
[no] name <i>description</i>	167
[no] nat-pmp activate	149
[no] natt	198



[no] negotiation auto .....	99
[no] netbios-broadcast .....	200
[no] network interface area IP .....	123
[no] network interface_name .....	122
[no] network interface_name .....	94
[no] network interface_name area ip .....	95
[no] network-extension {activate   ip-pool address_object   1st-dns {address_object   ip }   2nd-dns {address_object   ip }   1st-wins {address_object   ip }   2nd-wins {address_object   ip }   network address_object} .....	207
[no] network-extension traffic-enforcement .....	207
[no] next-hop {auto gateway address object   interface interface_name  trunk trunk_name tunnel tunnel_name} .....	116
[no] ntp .....	275
[no] ntp server {fqdn w.x.y.z} .....	275
[no] object-group address group_name .....	236
[no] object-group group_name .....	237
[no] object-group group_name .....	239
[no] object-group service group_name .....	239
[no] outbound ceiling {<0..1048576>   maximize-bandwidth-usage} .....	192
[no] outbound guarantee-bandwidth <0..1048576> priority <1..7> .....	192
[no] outbound-dscp-mark {<0..63>   class {af11   af12   af13   af21   af22   af23   af31   af32   af33   af41   af42   af43   cs0   cs1   cs2   cs3   cs4   cs5   cs6   cs7   default   wmm_be0   wmm_be24   wmm_bk16   wmm_bk8   wmm_vi32   wmm_vi40   wmm_vo48   wmm_vo56}} 192	
[no] outgoing-interface {interface interface_name   trunk group_name} .....	192
[no] outonly-interface interface_name .....	122
[no] outonly-interface interface_name .....	94
[no] out-snat activate .....	200
[no] packet-capture activate .....	322
[no] passive-interface interface_name .....	122
[no] passive-interface interface_name .....	122
[no] passive-interface interface_name .....	94
[no] passive-interface interface_name .....	95
[no] password password .....	188
[no] password password .....	258
[no] payment-service activate .....	181
[no] payment-service page-customization .....	182
[no] personal-firewall personal_firewall_software_name detect-auto-protection {enable   dis- able   ignore} .....	264
[no] ping-check activate .....	97
[no] policy controll-ipsec-dynamic-rules activate .....	117
[no] policy controll-virtual-server-rules activate .....	117
[no] policy override-direct-route activate .....	117
[no] policy-enforcement .....	200
[no] pool profile_name .....	139
[no] port interface_name .....	104
[no] printer-manager activate .....	184
[no] printer-manager encrypt activate .....	184
[no] printer-manager printer <1..10> .....	184
[no] radius-server host radius_server auth-port auth_port .....	245
[no] radius-server key secret .....	245
[no] radius-server timeout time .....	245
[no] reauth <30..30000> .....	69
[no] redistribute {static   ospf} .....	122
[no] redistribute {static   rip} .....	122
[no] redistribute {static   rip} metric-type <1..2> metric <0..16777214> .....	122
[no] remote-address ip .....	101
[no] replay-detection .....	200
[no] report .....	309

[no] reset-counter .....	311
[no] router-id IP .....	122
[no] rssi-thres .....	60
[no] rtls ekahau activate .....	170
[no] schedule <i>schedule_name</i> .....	162
[no] schedule <i>schedule_object</i> .....	116
[no] schedule <i>schedule_object</i> .....	174
[no] schedule <i>schedule_object</i> .....	192
[no] second-dns-server { <i>ip</i>   <i>interface_name</i> {1st-dns   2nd-dns   3rd-dns}   Device} .....	92
[no] second-wins-server <i>ip</i> .....	92
[no] secret <i>secret</i> .....	278
[no] server { <i>domain_name</i>   <i>ip</i> } .....	143
[no] server acct-address <i>radius_server</i> acct-port <i>auth_port</i> .....	248
[no] server acct-interim activate .....	248
[no] server acct-interim-interval <i>interval</i> .....	248
[no] server acct-retry-count <1-10> .....	248
[no] server acct-secret <i>secret</i> .....	248
[no] server alternative-cn-identifier <i>uid</i> .....	246
[no] server alternative-cn-identifier <i>uid</i> .....	247
[no] server basedn <i>basedn</i> .....	246
[no] server basedn <i>basedn</i> .....	247
[no] server binddn <i>binddn</i> .....	246
[no] server binddn <i>binddn</i> .....	247
[no] server cn-identifier <i>uid</i> .....	246
[no] server cn-identifier <i>uid</i> .....	247
[no] server description <i>description</i> .....	246
[no] server description <i>description</i> .....	247
[no] server description <i>description</i> .....	248
[no] server group-attribute <1-255> .....	248
[no] server group-attribute <i>group-attribute</i> .....	246
[no] server group-attribute <i>group-attribute</i> .....	247
[no] server host <i>ad_server</i> .....	246
[no] server host <i>ldap_server</i> .....	247
[no] server host <i>radius_server</i> auth-port <i>auth_port</i> .....	249
[no] server <i>ip</i> .....	259
[no] server key <i>secret</i> .....	249
[no] server nas-id NAS_IDENTIFIER .....	248
[no] server nas-ip NAS_ADDRESS .....	248
[no] server password <i>password</i> .....	246
[no] server password <i>password</i> .....	247
[no] server port <i>port_no</i> .....	246
[no] server port <i>port_no</i> .....	247
[no] server search-time-limit <i>time</i> .....	246
[no] server search-time-limit <i>time</i> .....	247
[no] server ssl .....	246
[no] server ssl .....	247
[no] server timeout <i>time</i> .....	249
[no] server-auth <1..2> .....	69
[no] server-auth <1..2> activate .....	69
[no] service { <i>service_name</i>  any} .....	116
[no] service <i>service_name</i> .....	174
[no] service service-object { <i>service_name</i>   any} .....	193
[no] service-name { <i>ip</i>   <i>hostname</i>   <i>service_name</i> } .....	259
[no] service-object <i>object_name</i> .....	239
[no] service-type {dyndns   dyndns_static   dyndns_custom   dynu-basic   dynu-premium   no-ip   peanut-hull   3322-dyn   3322-static} .....	129
[no] session-limit activate .....	176
[no] session-url <i>url</i> .....	160
[no] shutdown .....	87

[no] sms-service activate	188
[no] smtp-auth activate	311
[no] smtp-port <1..65535>	311
[no] smtp-redirect <1..16>	143
[no] smtp-redirect activate	143
[no] smtp-tls activate	312
[no] smtp-tls authenticate-server	312
[no] snat {outgoing-interface pool {address_object}}	116
[no] snmp-server	289
[no] snmp-server community community_string {ro rw}	289
[no] snmp-server contact description	289
[no] snmp-server enable {informs traps}	289
[no] snmp-server host {w.x.y.z} [community_string]	289
[no] snmp-server location description	289
[no] snmp-server port <1..65535>	289
[no] software-watchdog-timer <10..600>	326
[no] source {address_object   group_name}	162
[no] source {address_object any}	116
[no] source {address_object any}	143
[no] source address_object	193
[no] sourceip address_object	174
[no] sourceport {tcp udp} {eq <1..65535> range <1..65535> <1..65535>}	174
[no] speed <100,10>	99
[no] ssid-profile wlan_interface_index ssid_profile	63
[no] sslvpn application application_object	260
[no] sslvpn profile_name	126
[no] sslvpn tunnel_name	116
[no] starting-address ip pool-size <1..65535>	92
[no] stop-rekeying	200
[no] system default-snat	107
[no] terms-of-service	161
[no] terms-of-service	162
[no] third-dns-server {ip   interface_name {1st-dns   2nd-dns   3rd-dns}   Device}	92
[no] to {zone_object Device}	175
[no] trigger <1..8> incoming service_name trigger service_name	116
[no] trust_hosts	218
[no] tunnel tunnel_name	116
[no] type {per-user   shared}	193
[no] upnp-igd activate	149
[no] upstream <0..1048576>	88
[no] url url	130
[no] url url	167
[no] usb-storage activate	102
[no] user {user_name any}	139
[no] user {user_name any}	143
[no] user user_name	117
[no] user user_name	175
[no] user user_name	176
[no] user user_name	193
[no] user user_name	207
[no] user username	226
[no] user username	258
[no] user-agreement idle-detection [timeout <1..60>]	163
[no] user-agreement welcome-url <url>	163
[no] username e-mail	188
[no] username username password password	129
[no] users idle-detection	228
[no] users idle-detection timeout <1..60>	228
[no] users kick-previous [billing]	227

[no] users lockout-period <1..65535>	227
[no] users retry-count <1..99>	227
[no] users retry-limit	227
[no] users simultaneous-logon {administration   access   billing-account} enforce	228
[no] users simultaneous-logon {administration   access   billing-account} limit <i>login_number</i>	228
[no] users update-lease automation	228
[no] version <1..2>	122
[no] vlan-id <1..4094>	104
[no] <i>vlan_interface</i>	57
[no] vlan-support	67
[no] vpn-1-1-map activate	137
[no] vpn-1-1-map pool <i>profile_name</i>	137
[no] vpn-1-1-map rule <1..16>	137
[no] vpn-concentrator <i>profile_name</i>	202
[no] vpn-configuration-provision activate	203
[no] walled-garden activate	166
[no] walled-garden rule <1..20>	166
[no] wan-host <i>ipv4_address</i>	112
[no] wan-iface <i>interface_name</i>	129
[no] web-auth activate	158
[no] webpage-encrypt	261
[no] web-portal error-url <i>url</i>	163
[no] web-portal logout-url <i>url</i>	163
[no] web-portal session-url <i>url</i>	164
[no] web-portal welcome-url <i>url</i>	164
[no] welcome-url < <i>url</i> >	164
[no] welcome-url <i>url</i>	161
[no] wildcard	130
[no] windows-auto-update {enable   disable   ignore}	265
[no] windows-registry <i>registry_key</i> {eq   gt   lt   ge   le   neq} <i>registry_value</i>	265
[no] windows-security-patch <i>security_patch</i>	265
[no] windows-service-pack <1..10>	265
[no] wlan-macfilter-profile <i>macfilter_profile_name</i>	70
[no] wlan-monitor-profile <i>monitor_profile_name</i>	65
[no] wlan-radio-profile <i>radio_profile_name</i>	60
[no] wlan-security-profile <i>security_profile_name</i>	68
[no] wlan-ssid-profile <i>ssid_profile_name</i>	66
[no] wpa2-preauth	69
[no] xauth type {server <i>xauth_method</i>   client name <i>username</i> password <i>password</i> }	198
[no] zone <i>profile_name</i>	126
{firewall secure-policy} append	173
{firewall secure-policy} default-rule action {allow   deny   reject} { no log   log [alert] }	173
{firewall secure-policy} delete <i>rule_number</i>	173
{firewall secure-policy} flush	173
{firewall secure-policy} insert <i>rule_number</i>	173
{firewall secure-policy} move <i>rule_number</i> to <i>rule_number</i>	173
{firewall secure-policy} <i>profile_name</i> {zone_object Device} append	173
{firewall secure-policy} <i>profile_name</i> {zone_object Device} delete <1..5000>	173
{firewall secure-policy} <i>profile_name</i> {zone_object Device} flush	173
{firewall secure-policy} <i>profile_name</i> {zone_object Device} insert <i>rule_number</i>	173
{firewall secure-policy} <i>profile_name</i> {zone_object Device} move <i>rule_number</i> to <i>rule_number</i>	173
{firewall secure-policy} <i>profile_name</i> {zone_object Device} <i>rule_number</i>	172
{firewall secure-policy} <i>rule_number</i>	172
uint32 <0..4294967295>   ip <i>ipv4</i> [ <i>ipv4</i> [ <i>ipv4</i> ] ]   fqdn <i>fqdn</i> [ <i>fqdn</i> [ <i>fqdn</i> ] ]   text <i>text</i>   hex <i>hex</i>   vivc <i>enterprise_id</i> <i>hex_s</i> [ <i>enterprise_id</i> <i>hex_s</i> ]   vivs <i>enterprise_id</i> <i>hex_s</i> [ <i>enterprise_id</i> <i>hex_s</i> ]	91

2g-basic-speed wlan_2g_basic_speed	62
2g-channel wireless_channel_2g	62
2g-mcs-speed {disable   wlan_mcs_speed}	62
2g-multicast-speed wlan_2g_support_speed	62
2g-support-speed {disable   wlan_2g_support_speed}	62
5g-basic-speed wlan_5g_basic_speed	62
5g-channel wireless_channel_5g	62
5g-mcs-speed {disable   wlan_mcs_speed}	62
5g-multicast-speed {wlan_5g_basic_speed}	62
5g-support-speed {disable   wlan_5g_support_speed}	63
aaa authentication [no] match-default-group	251
aaa authentication rename profile-name-old profile-name-new	250
aaa group server ad group-name	245
aaa group server ad rename group-name group-name	245
aaa group server ldap group-name	246
aaa group server ldap rename group-name group-name	246
aaa group server radius group-name	248
aaa group server radius rename {group-name-old} group-name-new	247
access-page message-color {color-rgb   color-name   color-number}	273
access-page title title	273
access-page window-color {color-rgb   color-name   color-number}	273
action {allow deny reject}	174
activate	112
activate	138
activate	185
activate	197
activate	199
address address_object	138
address-object object_name {ip   ip_range   ip_subnet   interface-ip   interface-subnet   interface-gateway} {interface}	236
address-object rename object_name object_name	236
adjust-mss {auto   <200..1500>}	199
advertisement flush	168
advertisement rename description_old description_new	168
algorithm {wrr llf spill-over}	107
ap_mac	71
ap_mac	74
app rename profile_name_old profile_name_new	211
app statistics flush	211
application profile_name action {forward drop reject} {no log log [alert]}	211
application-object object_name	232
application-object rename object_name1 object_name2	232
apply	37
apply /conf/file_name.conf [ignore-error] [rollback]	295
app-profile app_profile_name {[no log]   [log by-profile]}{activate deactivate}	174
app-watch-dog reboot-log flush	327
area IP virtual-link IP message-digest-key <1..255> md5 authkey	123
arp IP mac_address	324
atse	37
authentication {pre-share   rsa-sig}	197
authentication key <1..255> key-string authkey	122
auth_method	278
auth-server authentication	278
auto-healing activate: yes	83
auto-healing healing threshold: -85 dBm	83
auto-healing healing-interval interval	82
auto-healing healing-threshold	82
auto-healing interval: 10	83
auto-healing margin	83

auto-healing margin: 0	83
auto-healing power threshold: -70 dBm	83
auto-healing power-threshold <-50~-80>	82
auto-healing update	83
band {2.4G   5G} [band-mode {11n   bg   a}]	60
bandselect check-sta-interval <1..60000>	66
bandselect drop-authentication <1..16>	66
bandselect drop-probe-request <1..32>	66
bandselect min-sort-interval <1..60000>	66
bandselect mode {disable   force   standard}	66
bandselect time-out-period <1..256>	66
bandwidth {upload   download} <0..1048576> priority <1..7>	178
bandwidth {upload   download} <0..1048576> priority <1..7>	270
beacon-interval <40..1000>	61
billing accounting-method {accumulation   time-to-finish }	177
billing accumulation idle-detection timeout <1..60>	177
billing accumulation-expire {day <1..360>   hour <1..24>}	177
billing currency {eur   gbp   usd   user-define currency_code }	177
billing decimal-places <2>	177
billing decimal-symbol {comma   dot}	177
billing discount button {a   b   c} [charge-by-level]	177
billing profile rename profile_name profile_name	178
billing tax-rate <0..100>	178
billing unused-expire {day <1..30>   hour <1..24>   minute <30..60>}	178
billing username-password-length <4..6>	178
bwm <1..127>	190
bwm append	190
bwm default inbound priority <1..7>	190
bwm default outbound priority <1..7>	190
bwm delete <1..127>	190
bwm insert <1..127>	190
bwm modify <1..127>	190
bwm move <1..127> to <1..127>	191
ca enroll cmp name certificate_name cn-type {ip cn cn_address fqdn cn cn_domain_name mail cn cn_email} [ou organizational_unit] [o organization] [c country] key-type {rsa dsa} key-len key_length num <0..99999999> password password ca ca_name url url;	254
ca enroll scep name certificate_name cn-type {ip cn cn_address fqdn cn cn_domain_name mail cn cn_email} [ou organizational_unit] [o organization] [c country] key-type {rsa dsa} .. key-len key_length password password ca ca_name url url	254
ca generate pkcs10 name certificate_name cn-type {ip cn cn_address fqdn cn cn_domain_name mail cn cn_email} [ou organizational_unit] [o organization] [c country] key-type {rsa dsa} key-len key_length	254
ca generate pkcs12 name name password password	254
ca generate x509 name certificate_name cn-type {ip cn cn_address fqdn cn cn_domain_name mail cn cn_email} [ou organizational_unit] [o organization] [c country] key-type {rsa dsa} key-len key_length	254
ca rename category {local remote} old_name new_name	254
ca validation remote_certificate	255
capwap ap add ap_mac [ap_model]	56
capwap ap ap_mac	56
capwap ap fallback disable	56
capwap ap fallback enable	56
capwap ap fallback interval <30..86400>	56
capwap ap kick {all   ap_mac}	56
capwap ap reboot ap_mac	56
capwap manual-add {enable   disable}	56
capwap show statistic	56
capwap station kick sta_mac	56
cdp {activate deactivate}	255

certificate <i>certificate-name</i> .....	197
cf-profile <i>cf_profile_name</i> {[no log]   [log by-profile]}{activate deactivate} .....	174
charge <i>price</i> .....	270
ch-width <i>wlan_htcw</i> .....	62
clear .....	37
clear aaa authentication <i>profile-name</i> .....	250
clear aaa group server ad [ <i>group-name</i> ] .....	245
clear aaa group server ldap [ <i>group-name</i> ] .....	246
clear aaa group server radius <i>group-name</i> .....	247
clear ip dhcp binding { <i>ip</i>   *} .....	92
clear logging debug buffer .....	306
clear logging system-log buffer .....	305
clear report [ <i>interface_name</i> ] .....	309
clock date <i>yyyy-mm-dd</i> time <i>hh:mm:ss</i> .....	275
clock time <i>hh:mm:ss</i> .....	275
configure .....	37
conn-check {IPv4   FQDN } method {icmp   tcp} period <5..600> timeout <1..10> fail-tolerance <1..10> [port <1..65535>] .....	115
conn-check {IPv4   FQDN   first-and-last} method {icmp   tcp} period <5..600> timeout <1..10> fail-tolerance <1..10> action {log   no-log} [port <1..65535>] .....	201
content-filter common-list {trust forbid} .....	216
content-filter passed warning flush .....	216
content-filter passed warning timeout <1..1440> .....	216
content-filter policy <i>policy_number</i> shutdown .....	216
content-filter profile <i>filtering_profile</i> commtouch-url match {block   log   pass} .....	219
content-filter profile <i>filtering_profile</i> commtouch-url match-unsafe {block   log   warn   pass} 219	
content-filter profile <i>filtering_profile</i> commtouch-url offline {block   log   warn   pass} 219	
content-filter profile <i>filtering_profile</i> commtouch-url unrate {block   log   warn   pass} 219	
content-filter profile <i>filtering_profile</i> custom-list forbid .....	218
content-filter profile <i>filtering_profile</i> custom-list keyword .....	218
content-filter profile <i>filtering_profile</i> custom-list trust .....	218
content-filter profile <i>filtering_profile</i> url match {block   log   warn   pass} .....	219
content-filter profile <i>filtering_profile</i> url match-unsafe {block   log   pass} .....	218
content-filter profile <i>filtering_profile</i> url offline {block   log   warn   pass} .....	219
content-filter profile <i>filtering_profile</i> url unrate {block   log   warn   pass} .....	219
content-filter statistics flush .....	221
content-filter url-cache test .....	220
content-filter url-server test bluecoat .....	216
content-filter url-server test commtouch .....	216
content-filter zsb port <1..65535> .....	216
copy .....	37
copy {/cert   /conf   /packet_trace   /script   /tmp} <i>file_name-a.conf</i> {/cert   /conf   / packet_trace   /script   /tmp}/ <i>file_name-b.conf</i> .....	295
copy running-config /conf/ <i>file_name.conf</i> .....	295
copy running-config startup-config .....	295
create-time <i>yyyy-mm-dd hh:mm</i> .....	270
crypto map dial <i>map_name</i> .....	199
crypto map <i>map_name</i> .....	202
crypto map rename <i>map_name map_name</i> .....	201
crypto <i>map_name</i> .....	203
currency <i>currency_code</i> .....	183
customize .....	163
daily-report .....	311
dcs 2g-selected-channel <i>2.4g_channels</i> .....	77
dcs 5g-selected-channel <i>5g_channels</i> .....	77
dcs channel-deployment {3-channel 4-channel} .....	78
dcs client-aware {enable disable} .....	78

dcx dcs-2g-method {auto manual}	78
dcx dcs-5g-method {auto manual}	78
dcx dfs-aware {enable disable}	78
dcx invoke	78
dcx sensitivity-level {high  medium  low}	78
dcx time-interval <i>interval</i>	78
deactivate	138
deactivate	185
deactivate	197
deactivate	199
debug (*)	37
debug [cmdexec corefile ip  kernel mac-id-rewrite observer switch  system zyinetpkt zysh-ipt- op] (*)	40
debug [remoteWTP   remoteWTP-cmd] (*)	40
debug alg	38
debug billing show shm (*)	38
debug ca (*)	38
debug capwap (*)	39
debug content-filter	39
debug dns-query (*)	39
debug dynamic-guest (*)	39
debug eps	39
debug force-auth (*)	39
debug free-time show shm	39
debug gui (*)	39
debug hardware (*)	39
debug interface	39
debug interface ifconfig [interface]	39
debug interface-group	39
debug ip dns	39
debug ip virtual-server	39
debug ipsec	39
debug l2-isolation (*)	39
debug logging	39
debug manufacture	39
debug myzyxel server (*)	39
debug myzyxel2 show (*)	39
debug myzyxel2 show sms shm	39
debug network arpignore (*)	39
debug no myzyxel server (*)	39
debug payment-service (*)	39
debug policy-route (*)	39
debug printer-manager debug-info (*)	39
debug reset content-filter profiling	39
debug service-register	39
debug show content-filter server	39
debug show ipset	39
debug show myzyxel server status	39
debug show myzyxel server status	39
debug sms-service (*)	39
debug smtp-redirect show (*)	39
debug sslvpn	39
debug update server (*)	40
debug vpn-1-1-map (*)	40
debug web-auth (*)	40
delete	37
delete {/cert   /conf   /packet_trace   /script   /tmp}/file_name	295
description ap_description	56
description description	185



description	description	65
description2		71
details		37
device-register	checkuser user_name	49
device-register	username user_name password password [e-mail user@domainname] [country-code country_code] [reseller-name name] [reseller-mail email-address] [reseller-phone phone-number] [vat vat-number]	49
dhcp-option	<1..254> option_name {boolean <0..1>  uint8 <0..255>   uint16 <0..65535>}	91
diag		37
diag-info		37
diag-info	cancel	316
diag-info	collect	316
dir		37
dir	{/cert   /conf   /packet_trace   /script   /tmp}	295
disable		37
downlink-rate-limit	data_rate	67
dpd-interval	<15..60>	197
draw-usage-graphics		311
dscp-marking	<0..63>	116
dscp-marking	class {default   dscp_class}	116
dtim-period	<1..255>	61
duration	<0..300>	322
dynamic-guest	freeuser user_name	269
dynamic-guest	generate	269
dynamic-guest	generate-freeuser	269
eap	{external   internal auth_method}	69
enable		37
encapsulation	{tunnel   transport}	199
encrypted-password	ciphertext	258
eps	insert <1..8> eps_object_name	162
eps	insert <1..8> eps_profile_name	206
eps	move <1..8> to <1..8>	162
eps	move <1..8> to <1..8>	206
exit		107
exit		112
exit		116
exit		138
exit		138
exit		143
exit		160
exit		176
exit		203
exit		216
exit		216
exit		217
exit		218
exit		218
exit		218
exit		218
exit		220
exit		312
exit		38
exit		56
exit		63
exit		65
exit		67
exit		69
exit		70
exit		72
exit		74

exit	76
exit	87
exit	99
expire-time <i>yyyy-mm-dd hh:mm</i>	270
fall-back-check-interval <60..86400>	197
<i>file_name</i>	75
file-prefix <i>file_name</i>	76
files-size <1..10000>	322
files-size <i>mon_dir_size</i>	76
file-suffix < <i>profile_name</i> >	322
filter-action {allow   deny}	70
flush	107
flush pool	138
frame-capture configure	76
friendly-ap <i>ap_mac description2</i>	72
gateway url	183
group1	198
group2	198
group5	198
group-key <30..30000>	69
groupname rename <i>groupname groupname</i>	226
guard-interval <i>wlan_htgi</i>	62
host-ip { <i>ip-address</i>   <i>profile_name</i>   any}	322
host-port <0..65535>	322
htm	38
idle <30..30000>	69
iface {add   del} { <i>interface_name</i>   <i>virtual_interface_name</i> }	322
in-dnat <1..10> protocol {all   tcp   udp} original-ip <i>address_name</i> <0..65535> <0..65535> mapped-ip <i>address_name</i> <0..65535> <0..65535>	200
in-dnat append protocol {all   tcp   udp} original-ip <i>address_name</i> <0..65535> <0..65535> mapped- ip <i>address_name</i> <0..65535> <0..65535>	200
in-dnat delete <1..10>	200
in-dnat insert <1..10> protocol {all   tcp   udp} original-ip <i>address_name</i> <0..65535> <0..65535> mapped-ip <i>address_name</i> <0..65535> <0..65535>	200
in-dnat move <1..10> to <1..10>	200
in-snat source <i>address_name</i> destination <i>address_name</i> snat <i>address_name</i>	200
interface	38
interface { <i>num</i>  append insert <i>num</i> } <i>interface-name</i> [weight <1..10> limit <1..2097152> passive] 107	
interface dial <i>interface_name</i>	101
interface disconnect <i>interface_name</i>	101
interface <i>interface_name</i>	101
interface <i>interface_name</i>	104
interface <i>interface_name</i>	105
interface <i>interface_name</i>	138
interface <i>interface_name</i>	161
interface <i>interface_name</i>	92
interface <i>interface_name</i>	94
interface <i>interface_name</i>	95
interface <i>interface_name</i>	97
interface <i>interface_name</i>	98
interface reset { <i>interface_name</i>   <i>virtual_interface_name</i>  all}	88
interface send statistics interval <15..3600>	88
interface-name { <i>ppp_interface</i>   <i>ethernet_interface</i> } <i>user_defined_name</i>	88
interface-rename <i>old_user_defined_name</i> <i>new_user_defined_name</i>	88
interval	77
interval	82
ip dhcp pool rename <i>profile_name profile_name</i>	90
ip dns server cache-flush	276

ip dns server max-ttl <10..3600> .....	276
ip dns server rule {<1..32> append insert <1..32>} access-group {ALL address_object} zone {ALL address_object} action {accept deny} .....	276
ip dns server rule move <1..32> to <1..32> .....	276
ip dns server zone-forwarder {<1..32> append insert <1..32>} {domain_zone_name *} user-defined w.x.y.z [private   interface {interface_name   auto}] .....	277
ip dns server zone-forwarder move <1..32> to <1..32> .....	277
ip drop-in .....	112
ip ftp server rule {rule_number append insert rule_number} access-group {ALL address_object} zone {ALL zone_object} action {accept deny} .....	287
ip ftp server rule move rule_number to rule_number .....	287
ip gateway ip metric <0..15> .....	87
ip http secure-server cipher-suite {cipher_algorithm} [cipher_algorithm] [cipher_algorithm] [cipher_algorithm] .....	283
ip http secure-server table {admin user} rule {rule_number append insert rule_number} access-group {ALL address_object} zone {ALL zone_object} action {accept deny} .....	283
ip http secure-server table {admin user} rule move rule_number to rule_number .....	283
ip http server table {admin user} rule {rule_number append insert rule_number} access-group {ALL address_object} zone {ALL zone_object} action {accept deny} .....	283
ip http server table {admin user} rule move rule_number to rule_number .....	283
ip http-redirect activate description .....	140
ip http-redirect deactivate description .....	141
ip http-redirect description interface interface_name redirect-to w.x.y.z <1..65535> ...	140
ip http-redirect description interface interface_name redirect-to w.x.y.z <1..65535> deactivate	140
ip http-redirect flush .....	141
ip ipnp config .....	156
ip ospf authentication .....	95
ip ospf authentication message-digest .....	95
ip ospf authentication same-as-area .....	95
ip ospf message-digest-key <1..255> md5 password .....	95
ip route replace {w.x.y.z} {w.x.y.z} {interface w.x.y.z} <0..127> with {w.x.y.z} {w.x.y.z} {interface w.x.y.z} <0..127> .....	119
ip ssh server rule {rule_number append insert rule_number} access-group {ALL address_object} zone {ALL zone_object} action {accept deny} .....	285
ip ssh server rule move rule_number to rule_number .....	285
ip telnet server rule {rule_number append insert rule_number} access-group {ALL address_object} zone {ALL zone_object} action {accept deny} .....	286
ip telnet server rule move rule_number to rule_number .....	286
ip virtual-server {activate   deactivate} profile_name .....	133
ip virtual-server delete profile_name .....	133
ip virtual-server flush .....	133
ip virtual-server insert rule_number .....	133
ip virtual-server move rule_number to rule_number .....	133
ip virtual-server profile_name interface interface_name original-ip {any   ip   address_object} map-to {address_object   ip} map-type any [nat-loopback [nat-1-1-map] [deactivate]   nat-1-1-map [deactivate]   deactivate] .....	132
ip virtual-server profile_name interface interface_name original-ip {any   IP   address_object} map-to {address_object   ip} map-type original-service service_object mapped-service service_object [nat-loopback [nat-1-1-map] [deactivate]   nat-1-1-map [deactivate]   deactivate] .....	133
ip virtual-server profile_name interface interface_name original-ip {any   IP   address_object} map-to {address_object   ip} map-type port protocol {any   tcp   udp} original-port <1..65535> mapped-port <1..65535> [nat-loopback [nat-1-1-map] [deactivate]   nat-1-1-map [deactivate]   deactivate] .....	132
ip virtual-server profile_name interface interface_name original-ip {any   IP   address_object} map-to {address_object   ip} map-type ports protocol {any   tcp   udp} original-port-begin <1..65535> original-port-end <1..65535> mapped-port-begin <1..65535> [nat-loopback [nat-1-1-map] [deactivate]   nat-1-1-map [deactivate]   deactivate] .....	132

ip virtual-server rename <i>profile_name profile_name</i>	133
<i>ip_address</i>	75
ipsec-isakmp <i>policy_name</i>	199
isakmp keepalive <2..60>	197
isakmp policy rename <i>policy_name policy_name</i>	198
keystring <i>pre_shared_key</i>	198
l2-isolation	154
<i>lan_port</i> {activate   inactivate} pvid <1..4094>	57
lan-provision ap <i>ap_mac</i>	56
ldap {activate deactivate}	255
ldap ip { <i>ip fqdn</i> } port <1..65535> [ <i>id name password password</i> ] [ <i>deactivate</i> ]	255
lifetime <180..3000000>	198
limit-ampdu <100..65535>	61
limit-amsdu <2290..4096>	62
link-sticking outgoing interface { <i>interface_name</i>   all}	148
list signature {anti-virus   personal-firewall   status}	265
load-balancing alpha <1..255>	79
load-balancing beta <1..255>	79
load-balancing kickInterval <1..255>	80
load-balancing liInterval <1..255>	80
load-balancing max sta <1..127>	80
load-balancing mode {station   traffic}	80
load-balancing sigma <51..100>	80
load-balancing timeout <1..255>	80
load-balancing traffic level {high   low   medium}	80
loadbalancing-index <inbound outbound total>	107
local-id type {ip <i>ip</i>   fqdn <i>domain_name</i>   mail <i>e_mail</i>   dn <i>distinguished_name</i> }	198
local-ip {ip { <i>ip</i>   <i>domain_name</i> }   interface <i>interface_name</i> }	198
local-ip <i>ip</i>	202
local-policy <i>address_name</i>	200
logging console category <i>module_name</i> level {alert   crit   debug   emerg   error   info   notice   warn}	308
logging mail <1..2> schedule daily hour <0..23> minute <0..59>	307
logging mail <1..2> schedule weekly day <i>day</i> hour <0..23> minute <0..59>	307
logging mail <1..2> sending_now	307
logging system-log category <i>module_name</i> {disable   level normal   level all}	305
logging usb-storage category <i>category</i> disable	103
logging usb-storage category <i>category</i> level <all normal>	103
logging usb-storage flushThreshold <1..100>	103
login-page background-color { <i>color-rgb</i>   <i>color-name</i>   <i>color-number</i> }	273
login-page message-color { <i>color-rgb</i>   <i>color-name</i>   <i>color-number</i> }	273
login-page title <i>title</i>	273
login-page title-color { <i>color-rgb</i>   <i>color-name</i>   <i>color-number</i> }	273
login-page window-color { <i>color-rgb</i>   <i>color-name</i>   <i>color-number</i> }	274
logo background-color { <i>color-rgb</i>   <i>color-name</i>   <i>color-number</i> }	274
logon-re-auth-time <0..1440>	162
logon-re-auth-time <0..1440>	164
mac <i>mac</i>	98
mail-subject set <i>subject</i>	311
matching-criteria {any   all}	265
mode {main   aggressive}	197
mode {none   wep   wpa   wpa2   wpa2-mix}	68
mode {normal trunk}	107
<i>mon_dir_size</i>	75
monitoring flush	72
<i>monitor_profile_name</i>	64
move <1..8> to <1..8>	107
mtu <576..1492>	102
network ip <i>mask</i>	91

network IP/<1..32>	91
no address-object <i>object_name</i>	236
no application-object <i>object_name</i>	232
no application-object <i>profile_name</i>	211
no area IP virtual-link IP message-digest-key <1..255>	123
no arp <i>ip</i>	324
no authentication key	122
no auth-server authentication	278
no ca category {local remote} <i>certificate_name</i>	255
no ca validation <i>name</i>	255
no content-filter profile <i>filtering_profile</i> commtouch-url match {log}	220
no content-filter profile <i>filtering_profile</i> commtouch-url match-unsafe {log}	219
no content-filter profile <i>filtering_profile</i> commtouch-url offline {log}	220
no content-filter profile <i>filtering_profile</i> commtouch-url unrate {log}	220
no content-filter profile <i>filtering_profile</i> url match {log}	219
no content-filter profile <i>filtering_profile</i> url match-unsafe {log}	219
no content-filter profile <i>filtering_profile</i> url offline {log}	219
no content-filter profile <i>filtering_profile</i> url unrate {log}	219
no dhcp-option <1..254>	91
no dscp-marking	116
no friendly-ap <i>ap_mac</i>	72
no ip dns server rule <1..32>	277
no ip drop-in activate	112
no ip ftp server rule <i>rule_number</i>	287
no ip http secure-server cipher-suite { <i>cipher_algorithm</i> }	283
no ip http secure-server table {admin user} rule <i>rule_number</i>	283
no ip http server table {admin user} rule <i>rule_number</i>	283
no ip http-redirect <i>description</i>	141
no ip ospf authentication	95
no ip ospf message-digest-key	95
no ip ssh server rule <i>rule_number</i>	285
no ip telnet server rule <i>rule_number</i>	286
no ip virtual-server <i>profile_name</i>	132
no l2-isolation activate	154
no l2-isolation white-list activate	154
no l2-isolation white-list <i>rule_number</i>	154
no mac	98
no mail-subject set	311
no network	91
no object-group application < <i>object_group_name</i> >	233
no packet-trace	38
no port <1..x>	99
no rogue-ap <i>ap_mac</i>	72
no sa spi <i>spi</i>	204
no sa tunnel-name <i>map_name</i>	204
no schedule	63
no schedule-object <i>object_name</i>	241
no server-type	261
no service-object <i>object_name</i>	238
no <i>slot_name</i> ap-profile	56
no <i>slot_name</i> monitor-profile	56
no smtp-address	311
no smtp-auth username	311
no snmp-server rule <i>rule_number</i>	289
no sslvpn policy <i>profile_name</i>	207
no use-defined-mac	99
no user	203
no username <i>username</i>	225
nslookup	38

ntp sync	275
object-group address rename <i>group_name group_name</i>	237
object-group application <i>object_group_name</i>	233
object-group application rename <i>object_group_name1 object_group_name2</i>	233
object-group service rename <i>group_name group_name</i>	240
ocsp {activate deactivate}	255
ocsp url <i>url</i> [ <i>id name password password</i> ] [deactivate]	255
os-type {windows   linux   mac-osx   others}	264
output-power <i>wlan_power</i>	63
out-snat source <i>address_name</i> destination <i>address_name</i> snat <i>address_name</i>	200
packet-capture configure	322
packet-trace	38
packet-trace [interface <i>interface_name</i> ] [ip-proto {<0..255>   <i>protocol_name</i>   any}] [src-host { <i>ip</i>   <i>hostname</i>   any}] [dst-host { <i>ip</i>   <i>hostname</i>   any}] [port {<1..65535>   any}] [file] [duration <1..3600>] [extension-filter <i>filter_extension</i> ]	321
password <i>password</i>	270
payment-info {cash   payment-service}	270
payment-service account-delivery onscreen {activate   deactivate}	181
payment-service account-delivery sms {activate   deactivate}	181
payment-service check payment-all-currency	181
payment-service check payment-currency	181
payment-service check paypal-currency	181
payment-service fail-page failed-message <i>message</i>	181
payment-service profile-page selection-message <i>message</i>	182
payment-service provider paypal	182
payment-service provider select paypal	182
payment-service sms-page info-message <i>message</i>	182
payment-service success-page account-message <i>message</i>	182
payment-service success-page format-date {dd-mm-yyyy   mm-dd-yyyy   yyyy-mm-dd} format-time {12-hour   24-hour}	182
payment-service success-page notification-message <i>message</i>	182
payment-service success-page notification-message-color {#00FF00   <i>color_name</i>   rgb(0,0,255)}	182
payment-service success-page successful-message <i>message</i>	182
peer-id type {any   ip <i>ip</i>   fqdn <i>domain_name</i>   mail <i>e_mail</i>   dn <i>distinguished_name</i> }	198
peer-ip { <i>ip</i>   <i>domain_name</i> } [ <i>ip</i>   <i>domain_name</i> ]	198
peer-ip <i>ip</i>	202
phone <i>phone_number</i>	270
ping	38
Ping { <i>ipv4</i>   <i>hostname</i> } [source <i>ipv4</i> ] [size <0..65507>] [forever  count <1..4096>]	321
ping-check { <i>domain_name</i>   <i>ip</i>   default-gateway}	97
ping-check { <i>domain_name</i>   <i>ip</i>   default-gateway} fail-tolerance <1..10>	97
ping-check { <i>domain_name</i>   <i>ip</i>   default-gateway} method {icmp   tcp}	97
ping-check { <i>domain_name</i>   <i>ip</i>   default-gateway} period <5..30>	97
ping-check { <i>domain_name</i>   <i>ip</i>   default-gateway} port <1..65535>	97
ping-check { <i>domain_name</i>   <i>ip</i>   default-gateway} timeout <1..10>	97
policy { <i>policy_number</i>   append   insert <i>policy_number</i> }	115
policy default-route	117
policy delete <i>policy_number</i>	117
policy flush	117
policy list table	117
policy move <i>policy_number</i> to <i>policy_number</i>	117
port <1..65535> ending-port <1..65535>]	260
port <1..65535> ending-port <1..65535>] [program-path <i>program-path</i> ]	260
port status Port<1..x>	99
port-grouping <i>interface_name</i> port <1..x>	99
price <i>price</i>	179
printer-ip <i>ipv4_address</i>	185
printer-manager button {a   b   c} <i>profile_name</i>	184

printer-manager discover	184
printer-manager encrypt secret-key <i>secret_key</i>	184
printer-manager multi-printout <1..3>	184
printer-manager port <1..65535>	184
printer-manager printer append	184
printer-manager printout-type {customized   default}	184
psm	38
qos wlan_qos	67
quota {total   upload   download} gigabytes <0..100>	179
quota {total   upload   download} gigabytes <0..100>	270
quota {total   upload   download} megabytes <0..1023>	179
quota {total   upload   download} megabytes <0..1023>	270
quota type {total   upload-download}	179
quota type {total   upload-download}	270
reboot	38
redistribute {static   ospf} metric <0..16>	122
release	38
release dhcp <i>interface-name</i>	92
remaining-time <1..25920000>	271
remote-policy <i>address_name</i>	200
rename	38
rename {/cert   /conf   /packet_trace   /script   /tmp}/old-file_name {/cert   /conf   / packet_trace   /script   /tmp}/new-file_name	295
rename /script/old-file_name /script/new-file_name	295
renew	38
renew dhcp <i>interface-name</i>	92
reset-counter-now	312
ring-buffer <enable disable>	322
rogue-ap ap_mac <i>description2</i>	72
rogue-ap containment	74
rogue-ap detection	71
role ap	60
router ospf	122
router ospf	123
router ospf	123
router ospf	95
router rip	122
router rip	94
Router(config)#	280
Router(config)#	83
Router(config)# auto-healing activate	83
Router(config)# auto-healing power-threshold -70	83
Router(config)# show auto-healing config	83
Router(config)# zon lldp server	280
Router(config)# zon lldp server status	280
rsi-dbm <-20~-76>	60
rtls ekahau ip address <ip>	170
rtls ekahau ip port <1..65535>	170
run	38
run /script/ <i>file_name.zysh</i>	295
rx-mask <i>chain_mask</i>	63
scan-dwell <100..1000>	65
scan-method <i>scan_method</i>	65
scenario {site-to-site-static site-to-site-dynamic remote-access-server remote-access-cli- ent}	199
schedule hour <0..23> minute <00..59>	311
schedule <i>profile</i>	63
schedule-object <i>object_name date time date time</i>	242
schedule-object <i>object_name time time [day] [day] [day] [day] [day] [day] [day]</i>	242

schedule-run 1 <i>file_name.zysh</i> {daily   monthly   weekly} time {date   sun   mon   tue   wed   thu   fri   sat} .....	295
security <i>securityprofile</i> .....	67
send-now .....	312
server-auth <1..2> ip address <i>ipv4_address</i> port <1..65535> secret <i>secret</i> .....	69
server-type rdp server-address <i>server-address</i> [starting- .....	260
server-type vnc server-address <i>server-address</i> [starting- .....	260
server-type weblink url <i>url</i> .....	261
service-object <i>object_name</i> {tcp   udp} {eq <1..65535>   range <1..65535> <1..65535>} ...	238
service-object <i>object_name</i> icmp <i>icmp_value</i> .....	239
service-object <i>object_name</i> protocol <1..255> .....	239
service-object rename <i>object_name</i> <i>object_name</i> .....	239
service-register checkexpire .....	49
service-register service-type standard license-key <i>key_value</i> .....	49
service-register service-type trial service content-filter .....	49
session timeout {tcp-established   tcp-synrecv   tcp-close   tcp-finwait   tcp-synsent   tcp-closewait   tcp-lastack   tcp-timewait} <1..300> .....	315
session timeout {udp-connect <1..300>   udp-deliver <1..300>   icmp <1..300>} .....	315
session-limit append .....	176
session-limit delete <i>rule_number</i> .....	176
session-limit flush .....	176
session-limit insert <i>rule_number</i> .....	176
session-limit limit <0..8192> .....	176
session-limit move <i>rule_number</i> to <i>rule_number</i> .....	176
session-limit <i>rule_number</i> .....	176
set pfs {group1   group2   group5   none} .....	200
set security-association lifetime seconds <180..3000000> .....	200
set session-key {ah <256..4095> <i>auth_key</i>   esp <256..4095> [cipher <i>enc_key</i> ] authenticator <i>auth_key</i> } .....	202
setenv .....	38
setenv-startup stop-on-error off .....	296
show .....	162
show .....	193
show .....	226
show .....	38
show .....	90
show {address-object   address6-object   service-object   schedule-object} [ <i>object_name</i> ] .....	236
show {firewall secure-policy} .....	173
show {firewall secure-policy} any Device .....	173
show {firewall secure-policy} block_rules .....	173
show {firewall secure-policy} <i>profile_name</i> {zone_object Device} .....	173
show {firewall secure-policy} <i>profile_name</i> {zone_object Device} <i>rule_number</i> .....	173
show {firewall secure-policy} <i>rule_number</i> .....	173
show {firewall secure-policy} status .....	173
show aaa authentication { <i>group-name</i>  default} .....	250
show aaa group server ad <i>group-name</i> .....	245
show aaa group server ldap <i>group-name</i> .....	246
show aaa group server radius <i>group-name</i> .....	247
show access-page settings .....	274
show account [pppoe <i>profile_name</i>   pptp <i>profile_name</i> ] .....	258
show ad-server .....	243
show advertisement .....	168
show advertisement activation .....	168
show app profiles <i>profile_name</i> .....	211
show app profiles <i>profile_name</i> application .....	211
show app signatures date .....	211
show app signatures version .....	211
show app statistics collect .....	211
show app statistics summary .....	211



show application-object <i>object_name</i> .....	232
show app-watch-dog config .....	327
show app-watch-dog monitor-list .....	327
show app-watch-dog reboot-log .....	327
show arp-table .....	323
show auth-server status .....	278
show auth-server trusted-client .....	278
show auth-server trusted-client <i>profile_name</i> .....	278
show auto-healing config .....	83
show backup-startup status .....	296
show billing discount default rule .....	178
show billing discount rule .....	178
show billing discount status .....	178
show billing profile [ <i>profile_name</i> ] .....	178
show billing status .....	178
show boot status .....	45
show bridge available member .....	105
show bwm activation .....	117
show bwm activation .....	191
show bwm all .....	191
show bwm default .....	191
show bwm-usage < [ <i>policy-route policy_number</i> ]   [ <i>interface interface_name</i> ] .....	117
show ca category { <i>local remote</i> } [ <i>name certificate_name</i> format { <i>text pem</i> }] .....	256
show ca category { <i>local remote</i> } name <i>certificate_name</i> certpath .....	256
show ca spaceusage .....	256
show ca validation name <i>name</i> .....	256
show capwap ap { <i>all   ap_mac</i> } .....	57
show capwap ap { <i>all   ap_mac</i> } config status .....	57
show capwap ap all statistics .....	57
show capwap ap <i>ap_mac slot_name</i> detail .....	57
show capwap ap fallback .....	57
show capwap ap fallback interval .....	57
show capwap ap wait-list .....	57
show capwap manual-add .....	57
show capwap station all .....	57
show clock date .....	275
show clock status .....	275
show clock time .....	275
show comport status .....	45
show conn [ <i>user {username any unknown}</i> ] [ <i>service {service-name any unknown}</i> ] [ <i>source {ip any}</i> ] [ <i>destination {ip any}</i> ] [ <i>begin &lt;1..128000&gt;</i> ] [ <i>end &lt;1..128000&gt;</i> ] .....	310
show conn ip-traffic destination .....	310
show conn ip-traffic source .....	310
show conn status .....	310
show connectivity-check continuous-log status .....	305
show connectivity-check continuous-log status .....	97
show connlimit max-per-host .....	173
show console .....	275
show content-filter common-list { <i>trust forbid</i> } .....	217
show content-filter passed warning .....	217
show content-filter policy .....	217
show content-filter profile [ <i>filtering_profile</i> ] .....	220
show content-filter settings .....	217
show content-filter statistics collect .....	221
show content-filter statistics summary .....	221
show content-filter statistics summary .....	221
show content-filter url-cache .....	220
show content-filter url-cache [ <i>all-category</i> ] [ <i>begin url_cache_range</i> end <i>url_cache_range</i> ] [ <i>_count</i> ] .....	220

show corefile copy usb-storage .....	103
show cpu status .....	45
show crypto map [map_name] .....	199
show daily-report status .....	311
show dcs config .....	78
show ddns [profile_name] .....	129
show device-register status .....	49
show diag-info .....	316
show diag-info copy usb-storage .....	103
show disk .....	45
show dynamic-guest log .....	270
show dynamic-guest log create-time begin yyyy-mm-dd hh:mm end yyyy-mm-dd hh:mm .....	270
show dynamic-guest users .....	270
show eps failure-messages .....	263
show eps profile [profile_name] .....	265
show eps profile profile_name signature {anti-virus   personal-firewall} .....	265
show eps signature {anti-virus   personal-firewall   status} .....	265
show extension-slot .....	45
show fan-speed .....	45
show fqdn .....	274
show frame-capture config .....	76
show frame-capture status .....	76
show free-time status .....	186
show groupname [groupname] .....	226
show hardware-watchdog-timer status .....	326
show interface {ethernet   vlan   bridge   ppp   auxiliary} status .....	87
show interface {interface_name   ethernet   vlan   bridge   ppp   virtual ethernet   virtual vlan   virtual bridge   all} .....	87
show interface ppp system-default .....	102
show interface ppp user-define .....	102
show interface send statistics interval .....	87
show interface summary all .....	87
show interface summary all status .....	87
show interface-group {system-default user-define group-name} .....	107
show interface-name .....	88
show ip dhcp binding [ip] .....	92
show ip dhcp dhcp-options .....	90
show ip dhcp pool [profile_name] .....	90
show ip dhcp pool profile_name dhcp-options .....	90
show ip dns server database .....	277
show ip dns server interface_name .....	277
show ip dns server status .....	277
show ip drop-in status .....	112
show ip drop-in wan-host .....	112
show ip ftp server status .....	287
show ip http server secure status .....	283
show ip http server status .....	283
show ip http-redirect [description] .....	141
show ip ipnp activation .....	156
show ip ipnp interface .....	156
show ip load-balancing link-sticking status .....	110
show ip route [kernel   connected   static   ospf   rip   bgp] .....	124
show ip route control-virtual-server-rules .....	119
show ip route static-dynamic .....	317
show ip route-settings .....	119
show ip ssh server status .....	285
show ip telnet server status .....	286
show ip virtual-server [profile_name] .....	132
show isakmp keepalive .....	197

show isakmp policy [policy_name]	197
show isakmp sa	204
show l2-isolation	154
show l2-isolation activation	154
show l2-isolation white-list [rule_number]	154
show l2-isolation white-list activation	154
show lan-provision ap ap_mac interface {lan_port   vlan_interface   all   ethernet   uplink   vlan}	57
show ldap-server	244
show led status	45
show load-balancing config	80
show lockout-users	230
show logging debug entries [priority pri] [category module_name] [srcip ip] [dstip ip] [service service_name] [srciface interface_name] [dstiface interface_name] [protocol protocol] [begin <1..512> end <1..512>] [keyword keyword]	306
show logging debug entries field field [begin <1..1024> end <1..1024>]	306
show logging debug status	306
show logging entries [priority pri] [category module_name] [srcip ip] [dstip ip] [service service_name] [begin <1..512> end <1..512>] [keyword keyword] [srciface interface_name] [dstiface interface_name] [protocol protocol]	304
show logging entries field field [begin <1..512> end <1..512>]	304
show logging status console	308
show logging status mail	307
show logging status syslog	306
show logging status system-log	305
show logging status usb-storage	103
show login-page default-title	274
show login-page settings	274
show logo settings	274
show mac	45
show mem status	45
show ntp server	275
show object-group {address   address6} [group_name]	236
show object-group application object_group_name	233
show object-group service group_name	239
show ospf area IP virtual-link	123
show packet-capture config	321
show packet-capture config	322
show packet-capture status	321
show packet-capture status	322
show page-customization	274
show payment-service account-delivery	182
show payment-service activation	182
show payment-service fail-page settings	182
show payment-service page-customization	182
show payment-service profile-page settings	182
show payment-service provider paypal	182
show payment-service provider select	182
show payment-service sms-page settings	182
show payment-service success-page settings	182
show ping-check [interface_name   status]	97
show policy-route [policy_number]	117
show policy-route begin <1..200> end <1..200>	117
show policy-route conn-check [<1..5000>]	117
show policy-route conn-check status [<1..5000>]	117
show policy-route controll-ipsec-dynamic-rules	117
show policy-route controll-virtual-server-rules	117
show policy-route override-direct-route	117
show policy-route rule_count	117

show policy-route underlayer-rules	117
show port setting	99
show port status	99
show port vlan-id	104
show port-grouping	99
show printer-manager button	185
show printer-manager discover-printer-status	185
show printer-manager printer [<1..10>]	185
show printer-manager printerfw version	185
show printer-manager printer-status	185
show printer-manager printout-type	185
show printer-manager settings	185
show printer-manager workableIP	185
show radius-server	245
show ram-size	45
show redundant-power status	45
show reference object aaa authentication [default   auth_method]	43
show reference object account pppoe [object_name]	43
show reference object account pptp [object_name]	43
show reference object address [object_name]	43
show reference object ca category {local remote} [cert_name]	43
show reference object crypto map [crypto_name]	43
show reference object eps [object_name]	43
show reference object interface [interface_name   virtual_interface_name]	43
show reference object isakmp policy [isakmp_name]	43
show reference object schedule [object_name]	43
show reference object service [object_name]	43
show reference object sslvpn application [object_name]	43
show reference object sslvpn policy [object_name]	43
show reference object username [username]	43
show reference object zone [object_name]	43
show reference object-group aaa ad [group_name]	44
show reference object-group aaa ldap [group_name]	44
show reference object-group aaa radius [group_name]	44
show reference object-group address [object_name]	44
show reference object-group interface [object_name]	44
show reference object-group service [object_name]	44
show reference object-group username [username]	44
show report [interface_name {ip   service   url}]	309
show report status	309
show rip {global   interface {all   interface_name}}	95
show rogue-ap containment config	74
show rogue-ap containment list	74
show rogue-ap detection info	72
show rogue-ap detection list {rogue   friendly  all}	72
show rogue-ap detection monitoring	72
show rogue-ap detection status	72
show route order	317
show rtls ekahau cli	170
show rtls ekahau config	170
show running-config	296
show sa monitor [{begin <1..1000>   {end <1..1000>   {crypto-map regexp}   {policy regexp}   {rsort sort_order}   {sort sort_order}}	204
show schedule-object	241
show serial-number	45
show service-object [object_name]	238
show service-register reseller-info	49
show service-register server-type	49
show service-register status all	49

show service-register status all	50
show service-register status content-filter	49
show service-register status extension-user	50
show service-register status external-ap-control	50
show service-register status sms	50
show session-timeout {icmp   tcp   udp}	315
show session-limit	176
show session-limit begin <i>rule_number</i> end <i>rule_number</i>	176
show session-limit <i>rule_number</i>	176
show session-limit status	176
show setenv-startup	296
show sms-service	188
show sms-service activation	188
show sms-service default-country-code	188
show sms-service provider vianett	188
show smtp-redirect [<1..16>]	143
show smtp-redirect activation	143
show smtp-redirect begin <1..16> end <1..16>	143
show snmp status	289
show socket listen	45
show socket open	45
show software-watchdog-timer log	326
show software-watchdog-timer status	326
show sslvpn application [ <i>application_object</i> ]	260
show sslvpn monitor	206
show ssl-vpn network-extension local-ip	206
show sslvpn policy [ <i>profile_name</i> ]	206
show system default-interface-group	108
show system default-snat	108
show system route default-wan-trunk	317
show system route dynamic-vpn	317
show system route nat-1-1	317
show system route policy-route	317
show system route site-to-site-vpn	317
show system route vpn-1-1-map	317
show system snat default-snat	317
show system snat nat-1-1	317
show system snat nat-loopback	317
show system snat order	317
show system snat policy-route	317
show system snat vpn-1-1-map	317
show system uptime	45
show usb-storage	102
show username [ <i>username</i> ]	225
show users { <i>username</i>   all   current}	230
show users default-setting {all   user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user}}	227
show users idle-detection-settings	228
show users kick-previous-settings	227
show users retry-settings	227
show users simultaneous-logon-settings	227
show users update-lease-settings	228
show version	45
show vpn-1-1-map activation	137
show vpn-1-1-map pool [ <i>profile_name</i> ]	137
show vpn-1-1-map rule [<1..16>]	137
show vpn-1-1-map rule begin <1..16> end <1..16>	137
show vpn-1-1-map statistics summary	137
show vpn-1-1-map user-mapping summary	137

show vpn-concentrator [profile_name]	202
show vpn-configuration-provision activation	203
show vpn-configuration-provision authentication	203
show vpn-configuration-provision rules	203
show vpn-counters	204
show walled-garden activation	166
show walled-garden rule <1..20>	166
show web-auth activation	159
show web-auth default-rule	159
show web-auth exceptional-service	159
show web-auth method	159
show web-auth policy {<1..1024>   all}	159
show web-auth portal status	159
show web-auth status	159
show web-auth type {default-user-agreement   default-web-portal   summary}	159
show web-auth type customize-zip {user-agreement   web-portal}	159
show web-auth type profile profile_name	159
show web-auth user-agreement status	159
show wlan-macfilter-profile {all   macfilter_profile_name}	70
show wlan-monitor-profile {all   monitor_profile_name}	64
show wlan-radio-profile {all   radio_profile_name}	60
show wlan-security-profile {all   security_profile_name}	68
show wlan-ssid-profile {all   ssid_profile_name}	66
show workspace application	207
show workspace cifs	207
show zon lldp neighbors	280
show zon lldp server config	280
show zon lldp server statistics	280
show zon lldp server status	280
show zon zdp server status	280
show zone [profile_name]	126
show zone binding-iface	126
show zone default-binding	126
show zone none-binding	126
show zone system-default	126
show zone user-define	126
shutdown	38
slot_name ap-profile profile_name	56
slot_name monitor-profile profile_name	56
sms-service account-send phone phone_number account user_name password password	188
sms-service default-country-code country_code	188
sms-service provider vianett	188
sms-service provider-select vianett	188
sms-service test-send phone phone_number msg message	188
smtp-address {ip   hostname}	311
smtp-auth username username password password	311
smtp-redirect append	143
smtp-redirect flush	143
smtp-redirect insert <1..16>	143
smtp-redirect move <1..16> to <1..16>	143
snaplen <68..1512>	322
snmp-server rule {rule_number append insert rule_number} access-group {ALL address_object} zone {ALL zone_object} action {accept deny}	289
snmp-server rule move rule_number to rule_number	289
split-size <1..2048>	322
src-ip {add del} {ipv4_address / local}	76
ssid	67
sslvpn network-extension local-ip ip	206
sslvpn no connection username user_name	207

sslvpn policy { <i>profile_name</i>   <i>profile_name</i> append   <i>profile_name</i> insert <1..16>} .....	206
sslvpn policy move <1..16> to <1..16> .....	207
sslvpn policy rename <i>profile_name profile_name</i> .....	207
status: active .....	280
storage <internal usbstorage> .....	322
subframe-ampdu <2..64> .....	61
system default-interface-group <i>group-name</i> .....	107
telnet .....	38
test aaa .....	38
test aaa {server secure-server} {ad ldap} host {hostname ipv4-address} [host {hostname ipv4- address}] port <1..65535> base-dn base-dn-string [bind-dn bind-dn-string password pass- word] login-name-attribute attribute [alternative-login-name-attribute attribute] ac- count account-name .....	251
time-period {day <1..365>   hour <1..24>   minute <30..60>} .....	179
time-period <1..432000> .....	271
traceroute .....	38
traceroute {ip   hostname} .....	321
traffic-prioritize {tcp-ack content-filter dns ipsec-vpn ssl-vpn} bandwidth <0..1048576> pri- ority <1..7> [maximize-bandwidth-usage]; .....	87
traffic-prioritize {tcp-ack content-filter dns ipsec-vpn ssl-vpn} deactivate .....	88
transform-set <i>crypto_algo_ah</i> [ <i>crypto_algo_ah</i> [ <i>crypto_algo_ah</i> ]] .....	199
transform-set <i>crypto_algo_esp</i> [ <i>crypto_algo_esp</i> [ <i>crypto_algo_esp</i> ]] .....	199
transform-set isakmp-algo [ <i>isakmp_algo</i> [ <i>isakmp_algo</i> ]] .....	198
trigger append incoming <i>service_name</i> trigger <i>service_name</i> .....	116
trigger delete <1..8> .....	116
trigger insert <1..8> incoming <i>service_name</i> trigger <i>service_name</i> .....	116
trigger move <1..8> to <1..8> .....	116
tx-mask <i>chain_mask</i> .....	63
type {external   internal} .....	160
type {external   internal} .....	164
type {internal   external   general} .....	99
type {user-agreement   web-portal} .....	163
unlock lockout-users {ip   console} .....	230
uplink-rate-limit <i>data_rate</i> .....	67
url .....	220
url [ server <i>rating_server</i> ] [ timeout <i>query_timeout</i> ] .....	216
url timeout <i>query_timeout</i> .....	216
usb-storage mount .....	103
usb-storage umount .....	103
usb-storage warn <i>number</i> <percentage megabyte> .....	102
use-defined-mac .....	99
user <i>username</i> .....	203
user-agreement agreement-url <i>url</i> .....	163
user-agreement logon-re-auth-time <0..1440> .....	163
username rename <i>username username</i> .....	226
username <i>username</i> [no] description <i>description</i> .....	225
username <i>username</i> [no] logon-due-time <i>time</i> .....	225
username <i>username</i> [no] logon-lease-time <0..1440> .....	225
username <i>username</i> [no] logon-re-auth-time <0..1440> .....	226
username <i>username</i> logon-re-auth-type {due-time   re-auth-time} .....	226
username <i>username</i> logon-time-setting {default   manual} .....	226
username <i>username</i> nopassword user-type {admin   pre-subscriber   guest-manager   user   guest   limited-admin} .....	225
username <i>username</i> password <i>password</i> user-type {admin   pre-subscriber   guest-manager   user   guest   limited-admin} .....	225
username <i>username</i> user-type ext-group-user associated-aaa-server <i>server_profile</i> group-id <i>id</i> 225	
username <i>username</i> user-type ext-user .....	225
username <i>username</i> user-type mac-address .....	225

users default-setting [no] logon-lease-time <0..1440>	227
users default-setting [no] logon-re-auth-time <0..1440>	227
users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user}	227
users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user} logon-due-time <i>time</i>	227
users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user} logon-lease-time <0..1440>	227
users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user} logon-re-auth-time <0..1440>	227
users default-setting [no] user-type {admin   limited-admin   pre-subscriber   user   guest   ext-user   ext-group-user} logon-re-auth-type {due-time   re-auth-time}	227
users force-logout <i>username</i>   <i>ip</i>	230
vlan <1..4094> {tag   untag}	56
vlan-id <1..4094>	67
vlan_interface {activate   inactivate} vid <1..4094> join <i>lan_port</i> {tag   untag} [ <i>lan_port</i> {tag   untag}] [ <i>lan_port</i> {tag   untag}]	57
vpn-1-1-map pool rename <i>profile_name</i> <i>profile_name</i>	137
vpn-1-1-map rule append	137
vpn-1-1-map rule flush	137
vpn-1-1-map rule insert <1..16>	137
vpn-1-1-map rule move <1..16> to <1..16>	137
vpn-concentrator rename <i>profile_name</i> <i>profile_name</i>	203
vpn-configuration-provision authentication <i>auth_method</i>	203
vpn-configuration-provision rule { append   <i>conf_index</i>   insert <i>conf_index</i> }	203
vpn-configuration-provision rule { delete <i>conf_index</i>   move <i>conf_index</i> to <i>conf_index</i> }	203
walled-garden rule append	166
walled-garden rule flush	166
walled-garden rule insert <1..20>	166
walled-garden rule move <1..20> to <1..20>	166
wan-interface <i>interface_name</i> lan-interface <i>interface_name</i>	112
web-auth [no] exceptional-service <i>service_name</i>	158
web-auth default-rule authentication {required   unnecessary} {no log   log [alert]}	158
web-auth login setting	158
web-auth method {portal   user-agreement}	158
web-auth policy <1..1024>	158
web-auth policy append	159
web-auth policy delete <1..1024>	159
web-auth policy flush	159
web-auth policy insert <1..1024>	159
web-auth policy move <1..1024> to <1..1024>	159
web-auth type default-user-agreement	159
web-auth type default-web-portal	159
web-auth type profile <i>profile_name</i>	159
web-auth type rename <i>profile_name_old</i> <i>profile_name_new</i>	159
web-auth user-agreement	159
web-portal login-url <i>url</i>	163
wep <64   128> default-key <1..4>	68
wep-auth-type {open   share}	68
white-list activate	154
white-list append	154
white-list flush	154
white-list no activate	154
white-list <i>rule_number</i>	154
windows-version {windows-2000   windows-xp   windows-2003   windows-2008   windows-vista   windows-7   windows-2008r2}	265
wlan-macfilter-profile rename <i>macfilter_profile_name1</i> <i>macfilter_profile_name2</i>	70
wlan-monitor-profile rename <i>monitor_profile_name1</i> <i>monitor_profile_name2</i>	64
wlan-radio-profile rename <i>radio_profile_name1</i> <i>radio_profile_name2</i>	60



---

wlan-security-profile rename <i>security_profile_name1</i> <i>security_profile_name2</i> .....	68
wlan-ssid-profile rename <i>ssid_profile_name1</i> <i>ssid_profile_name2</i> .....	66
wpa-encrypt { <i>tkip</i>   <i>aes</i>   <i>auto</i> } .....	69
wpa-psk { <i>wpa_key</i> / <i>wpa_key_64</i> } .....	69
write .....	296
write .....	38
zon lldp server .....	280
zon lldp server tx-hold < <i>1..10</i> > .....	280
zon lldp server tx-interval < <i>1..600</i> > .....	280
zon zdp server .....	280
zone <i>profile_name</i> .....	126