

KEENETIC

CARRIER

AC1200 Dual Band Whole Home Wi-Fi Router
with Wireless Power Amplifiers, 5-port
Managed Switch, and Multifunction USB Port

Command Reference Guide

Model	Carrier (KN-1711)
OS Version	4.3
Edition	1.159 10.06.2025

Preface

This guide contains Command-Line Interface (CLI) commands to maintain the Carrier device. This guide provides a complete listing of all possible commands. The other chapters provide examples of how to implement the most common of these commands, general information on the interrelationships between the commands and the conceptual background of how to use them.

1 Readership

This guide is for the networking or computer technician responsible for configuring and maintaining the Carrier on-site. It is also intended for the operator who manages the Carrier. This manual cover high-level technical support procedures available to Root administrators and Carrier technical support personnel.

2 Organization

This manual covers the following topics:

Introduction to the CLI	Describes how to use the Carrier Command-Line Interface (CLI), its hierarchical structure, authorization levels and its help features.
Command Reference	Provides an alphabetical list of the available CLI commands that you can use to configure the Carrier device.

3 Document Conventions

Command descriptions use the following conventions:

boldface font	Commands and keywords are in boldface . Must be typed exactly as shown. Bold font is used as a user input in examples.
<i>italic</i> font	Arguments for which you supply values are in <i>italics</i> .
[<i>optional</i>]	Elements in square brackets are optional.
⟨ <i>replaceable</i> ⟩	Elements in angle brackets are replaceable.
(x y z)	Alternative keywords are grouped in round brackets and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Each command description is broken down into the following sub-sections:

Description	Description of what the command does.
Synopsis	The general format of the command.
Prefix no	The possibility of using no prefix with command.
Change settings	The ability of command to change the settings.
Multiple input	The possibility of multiple input.
Group entry	Name of the group that owns the command. If there is no group, this section does not displayed.
Interface type	Type of interface, which can be managed by the command. The section does not displayed, if this context has no meaning for the command. Interfaces used in the system and the relationships between them are shown in the diagrams below.
Arguments	List of arguments if they exists, and explanations to them.
Example	An illustration of how the command looks when invoked. Because the interface is straightforward, some of the examples are obvious, but they are included for clarity.

Notes, cautionary statements, and safety warnings use these conventions.

Note: Means "reader take note". Notes contain helpful suggestions or references to materials not contained in this manual.

Warning: Means "reader be careful". You are capable of doing something that might result in equipment damage or loss of data.

Contents Overview

Preface	3
Product Overview	33
Introduction to the CLI	35
Command Reference	41
Glossary	731
Interface Hierarchy	745
HTTP API	747
NVOX CLI commands	755
SNMP MIB	855
IPsec Encryption Levels	861

Table of Contents

Preface	3
1 Readership	3
2 Organization	3
3 Document Conventions	3
Table of Contents	5
Chapter 1	
Product Overview	33
1.1 Hardware Configuration	33
Chapter 2	
Introduction to the CLI	35
2.1 Enter commands in the CLI	35
2.1.1 Entering a group	36
2.2 Getting Help and auto-completion	36
2.3 Prefix no	37
2.4 Multiple input	38
2.5 Saving to startup settings	38
2.6 Delayed restart	39
Chapter 3	
Command Reference	41
3.1 Core commands	41
3.1.1 copy	41
3.1.2 erase	41
3.1.3 exit	42
3.1.4 grep	42
3.1.5 ls	45
3.1.6 mkdir	46
3.1.7 more	47
3.2 access	47
3.3 access-list	48
3.3.1 access-list auto-delete	49
3.3.2 access-list deny	49
3.3.3 access-list permit	51
3.3.4 access-list rule	54
3.4 afp	55
3.4.1 afp automount	55

3.4.2	afp permissive	56
3.4.3	afp share	56
3.5	cifs	57
3.5.1	cifs automount	58
3.5.2	cifs map-hidden	58
3.5.3	cifs master	59
3.5.4	cifs permissive	59
3.5.5	cifs share	60
3.6	cloud control2 security-level	61
3.7	components	61
3.7.1	components auto-update channel	62
3.7.2	components auto-update disable	62
3.7.3	components auto-update schedule	63
3.7.4	components check-update	64
3.7.5	components commit	64
3.7.6	components install	65
3.7.7	components list	65
3.7.8	components preset	66
3.7.9	components preview	67
3.7.10	components remove	68
3.7.11	components validity-period	68
3.8	crypto engine	69
3.9	crypto ike key	69
3.10	crypto ike mtu	70
3.11	crypto ike nat-keepalive	71
3.12	crypto ike policy	72
3.12.1	crypto ike policy lifetime	72
3.12.2	crypto ike policy mode	73
3.12.3	crypto ike policy negotiation-mode	74
3.12.4	crypto ike policy proposal	74
3.13	crypto ike proposal	75
3.13.1	crypto ike proposal aead	76
3.13.2	crypto ike proposal dh-group	76
3.13.3	crypto ike proposal encryption	77
3.13.4	crypto ike proposal integrity	78
3.13.5	crypto ike proposal prf	79
3.14	crypto ipsec incompatible	80
3.15	crypto ipsec profile	81
3.15.1	crypto ipsec profile authentication-local	81
3.15.2	crypto ipsec profile authentication-remote	82
3.15.3	crypto ipsec profile dpd-clear	83
3.15.4	crypto ipsec profile dpd-interval	83
3.15.5	crypto ipsec profile identity-local	84

3.15.6	crypto ipsec profile match-identity-remote	85
3.15.7	crypto ipsec profile mode	86
3.15.8	crypto ipsec profile policy	86
3.15.9	crypto ipsec profile preshared-key	87
3.15.10	crypto ipsec profile xauth	88
3.15.11	crypto ipsec profile xauth-identity	88
3.15.12	crypto ipsec profile xauth-password	89
3.16	crypto ipsec rekey delete-delay	90
3.17	crypto ipsec rekey make-before	91
3.18	crypto ipsec transform-set	91
3.18.1	crypto ipsec transform-set aead	92
3.18.2	crypto ipsec transform-set cypher	92
3.18.3	crypto ipsec transform-set dh-group	93
3.18.4	crypto ipsec transform-set hmac	94
3.18.5	crypto ipsec transform-set lifetime	95
3.19	crypto map	96
3.19.1	crypto map connect	96
3.19.2	crypto map enable	97
3.19.3	crypto map fallback-check-interval	97
3.19.4	crypto map force-encaps	98
3.19.5	crypto map l2tp-server dhcp route	99
3.19.6	crypto map l2tp-server enable	99
3.19.7	crypto map l2tp-server interface	100
3.19.8	crypto map l2tp-server ipv6cp	101
3.19.9	crypto map l2tp-server lcp echo	102
3.19.10	crypto map l2tp-server mru	102
3.19.11	crypto map l2tp-server mtu	103
3.19.12	crypto map l2tp-server multi-login	104
3.19.13	crypto map l2tp-server nat	104
3.19.14	crypto map l2tp-server range	105
3.19.15	crypto map l2tp-server session-logout	106
3.19.16	crypto map l2tp-server session-preempt	106
3.19.17	crypto map l2tp-server static-ip	107
3.19.18	crypto map nail-up	108
3.19.19	crypto map reauth-passive	108
3.19.20	crypto map set-peer	109
3.19.21	crypto map set-peer-fallback	109
3.19.22	crypto map set-profile	110
3.19.23	crypto map set-tcpmss	111
3.19.24	crypto map set-transform	112
3.19.25	crypto map traffic-selectors	112
3.19.26	crypto map tunnel-interface	113
3.19.27	crypto map virtual-ip dhcp route	114

3.19.28	crypto map virtual-ip dns-server	115
3.19.29	crypto map virtual-ip enable	115
3.19.30	crypto map virtual-ip interface	116
3.19.31	crypto map virtual-ip multi-login	117
3.19.32	crypto map virtual-ip nat	117
3.19.33	crypto map virtual-ip range	118
3.19.34	crypto map virtual-ip session-logout	118
3.19.35	crypto map virtual-ip session-preempt	119
3.19.36	crypto map virtual-ip static-ip	119
3.20	dlna	120
3.20.1	dlna container	121
3.20.2	dlna db-directory	121
3.20.3	dlna directory	122
3.20.4	dlna display-name	123
3.20.5	dlna interface	123
3.20.6	dlna port	124
3.20.7	dlna rescan	125
3.20.8	dlna sort	126
3.21	dns-proxy	126
3.21.1	dns-proxy filter assign host preset	127
3.21.2	dns-proxy filter assign host profile	128
3.21.3	dns-proxy filter assign interface preset	129
3.21.4	dns-proxy filter assign interface profile	129
3.21.5	dns-proxy filter engine	130
3.21.6	dns-proxy filter profile	131
3.21.7	dns-proxy filter profile description	132
3.21.8	dns-proxy filter profile dns53 upstream	132
3.21.9	dns-proxy filter profile https upstream	133
3.21.10	dns-proxy filter profile intercept enable	134
3.21.11	dns-proxy filter profile tls upstream	135
3.21.12	dns-proxy https upstream	136
3.21.13	dns-proxy intercept enable	137
3.21.14	dns-proxy max-ttl	138
3.21.15	dns-proxy proceed	138
3.21.16	dns-proxy rebind-protect	139
3.21.17	dns-proxy srr-reset	140
3.21.18	dns-proxy tls upstream	140
3.22	dnp accept	141
3.23	dyndns profile	142
3.23.1	dyndns profile domain	142
3.23.2	dyndns profile password	143
3.23.3	dyndns profile send-address	144
3.23.4	dyndns profile type	144

3.23.5	dyndns profile update-interval	145
3.23.6	dyndns profile url	146
3.23.7	dyndns profile username	147
3.24	easyconfig check	147
3.24.1	easyconfig check exclude-gateway	148
3.24.2	easyconfig check max-fails	148
3.24.3	easyconfig check period	149
3.25	easyconfig disable	150
3.26	eula accept	150
3.27	igmp-proxy	151
3.27.1	igmp-proxy fast-leave	151
3.27.2	igmp-proxy force	152
3.28	igmp-snooping disable	152
3.29	interface	153
3.29.1	interface atf disable	155
3.29.2	interface atf inbound	155
3.29.3	interface authentication chap	156
3.29.4	interface authentication eap-md5	156
3.29.5	interface authentication eap-mschapv2	157
3.29.6	interface authentication eap-ttls	157
3.29.7	interface authentication identity	158
3.29.8	interface authentication mschap	159
3.29.9	interface authentication mschap-v2	159
3.29.10	interface authentication pap	160
3.29.11	interface authentication password	161
3.29.12	interface authentication peap	161
3.29.13	interface authentication shared	162
3.29.14	interface authentication wpa-psk	162
3.29.15	interface auto-ssid	163
3.29.16	interface backhaul	164
3.29.17	interface band-steering	165
3.29.18	interface band-steering preference	165
3.29.19	interface ccp	166
3.29.20	interface channel	167
3.29.21	interface channel auto-rescan	168
3.29.22	interface channel width	168
3.29.23	interface chilli coaport	169
3.29.24	interface chilli dhcpif	170
3.29.25	interface chilli dns	170
3.29.26	interface chilli lease	171
3.29.27	interface chilli login	172
3.29.28	interface chilli logout	172
3.29.29	interface chilli macauth	173

3.29.30	interface chilli macpasswd	174
3.29.31	interface chilli nasip	174
3.29.32	interface chilli nasmac	175
3.29.33	interface chilli profile	176
3.29.34	interface chilli radius	177
3.29.35	interface chilli radiusacctport	177
3.29.36	interface chilli radiusauthport	178
3.29.37	interface chilli radiuslocationid	179
3.29.38	interface chilli radiuslocationname	179
3.29.39	interface chilli radiusnasid	180
3.29.40	interface chilli radiussecret	181
3.29.41	interface chilli uamallowed	181
3.29.42	interface chilli uamdomain	182
3.29.43	interface chilli uamhomepage	183
3.29.44	interface chilli uamport	184
3.29.45	interface chilli uamsecret	184
3.29.46	interface chilli uamserver	185
3.29.47	interface compatibility	186
3.29.48	interface connect	186
3.29.49	interface country-code	187
3.29.50	interface debug	188
3.29.51	interface description	188
3.29.52	interface down	189
3.29.53	interface duplex	189
3.29.54	interface dyndns nobind	190
3.29.55	interface dyndns profile	191
3.29.56	interface dyndns update	191
3.29.57	interface encryption anonymous-dh	192
3.29.58	interface encryption enable	192
3.29.59	interface encryption key	193
3.29.60	interface encryption mppe	194
3.29.61	interface encryption owe	194
3.29.62	interface encryption tkip hold-down	195
3.29.63	interface encryption wpa	196
3.29.64	interface encryption wpa2	196
3.29.65	interface encryption wpa3	197
3.29.66	interface encryption wpa3 suite-b	198
3.29.67	interface flowcontrol	198
3.29.68	interface follow	199
3.29.69	interface ft enable	200
3.29.70	interface ft mdid	200
3.29.71	interface ft otd	201
3.29.72	interface hide-ssid	202

3.29.73	interface iapp auto	202
3.29.74	interface iapp key	203
3.29.75	interface idle-timeout	203
3.29.76	interface igmp downstream	204
3.29.77	interface igmp fork	205
3.29.78	interface igmp upstream	205
3.29.79	interface include	206
3.29.80	interface inherit	206
3.29.81	interface ip access-group	207
3.29.82	interface ip address	208
3.29.83	interface ip address dhcp	209
3.29.84	interface ip adjust-ttl recv	210
3.29.85	interface ip adjust-ttl send	210
3.29.86	interface ip alias	211
3.29.87	interface ip dhcp client broadcast	212
3.29.88	interface ip dhcp client class-id	213
3.29.89	interface ip dhcp client debug	213
3.29.90	interface ip dhcp client displace	214
3.29.91	interface ip dhcp client dns-routes	215
3.29.92	interface ip dhcp client fallback	216
3.29.93	interface ip dhcp client hostname	216
3.29.94	interface ip dhcp client name-servers	217
3.29.95	interface ip dhcp client release	218
3.29.96	interface ip dhcp client renew	218
3.29.97	interface ip dhcp client routes	219
3.29.98	interface ip flow	219
3.29.99	interface ip global	220
3.29.100	interface ip mru	221
3.29.101	interface ip mtu	222
3.29.102	interface ip name-servers	223
3.29.103	interface ip nat loopback	223
3.29.104	interface ip remote	224
3.29.105	interface ip tcp adjust-mss	224
3.29.106	interface ipcp address	225
3.29.107	interface ipcp default-route	226
3.29.108	interface ipcp dns-routes	226
3.29.109	interface ipcp name-servers	227
3.29.110	interface ipcp vj	228
3.29.111	interface ipsec aggressive	228
3.29.112	interface ipsec encryption-level	229
3.29.113	interface ipsec force-encaps	230
3.29.114	interface ipsec ignore	231
3.29.115	interface ipsec ikev2	231

3.29.116	interface ipsec nail-up	232
3.29.117	interface ipsec name-servers	232
3.29.118	interface ipsec preshared-key	233
3.29.119	interface ipsec proposal lifetime	234
3.29.120	interface ipsec proposal local-id	235
3.29.121	interface ipsec proposal remote-id	235
3.29.122	interface ipsec transform-set lifetime	236
3.29.123	interface ipv6 address	237
3.29.124	interface ipv6 dhcp client pd hint	238
3.29.125	interface ipv6 id	238
3.29.126	interface ipv6 name-servers	239
3.29.127	interface ipv6 prefix	240
3.29.128	interface ipv6cp	240
3.29.129	interface lcp acfc	241
3.29.130	interface lcp echo	242
3.29.131	interface lcp pfc	242
3.29.132	interface ldpc	243
3.29.133	interface led wan	244
3.29.134	interface lldp disable	244
3.29.135	interface mac access-list address	245
3.29.136	interface mac access-list type	246
3.29.137	interface mac address	246
3.29.138	interface mac address factory	247
3.29.139	interface mac band	248
3.29.140	interface mac bssid	249
3.29.141	interface mac clone	249
3.29.142	interface mobile lte disable-band	250
3.29.143	interface mobile name-servers	250
3.29.144	interface mobile operator	251
3.29.145	interface mobile pdp	252
3.29.146	interface mobile roaming	252
3.29.147	interface mobile scan	253
3.29.148	interface mobile umts disable-band	254
3.29.149	interface modem connect	254
3.29.150	interface modem timeout	255
3.29.151	interface openconnect accept-addresses	256
3.29.152	interface openconnect accept-routes	256
3.29.153	interface openconnect authgroup	257
3.29.154	interface openconnect dtls	258
3.29.155	interface openconnect protocol fortinet	258
3.29.156	interface openvpn accept-routes	259
3.29.157	interface openvpn connect	259
3.29.158	interface openvpn name-servers	260

3.29.159	interface peer	261
3.29.160	interface peer-isolation	261
3.29.161	interface ping-check profile	262
3.29.162	interface ping-check restart	263
3.29.163	interface pmf	263
3.29.164	interface pmksa-lifetime	264
3.29.165	interface power	265
3.29.166	interface pppoe service	266
3.29.167	interface pppoe session auto-cleanup	266
3.29.168	interface preamble-short	267
3.29.169	interface proxy connect	267
3.29.170	interface proxy protocol	268
3.29.171	interface proxy socks5-udp	269
3.29.172	interface proxy upstream	269
3.29.173	interface reconnect-delay	270
3.29.174	interface rekey-interval	271
3.29.175	interface rename	272
3.29.176	interface rf e2p set	272
3.29.177	interface role	273
3.29.178	interface rrm	274
3.29.179	interface rssi-threshold	275
3.29.180	interface schedule	275
3.29.181	interface security-level	276
3.29.182	interface sim pin	277
3.29.183	interface sim slot	278
3.29.184	interface speed	279
3.29.185	interface speed nonegotiate	279
3.29.186	interface ssid	280
3.29.187	interface standby enable	281
3.29.188	interface storm-control disable	282
3.29.189	interface switchport access	282
3.29.190	interface switchport friend	283
3.29.191	interface switchport mode	284
3.29.192	interface switchport trunk	285
3.29.193	interface traffic-counter action disconnect	285
3.29.194	interface traffic-counter action sms-alert message	286
3.29.195	interface traffic-counter action sms-alert phone	286
3.29.196	interface traffic-counter enable	287
3.29.197	interface traffic-counter limit	288
3.29.198	interface traffic-counter monthly	288
3.29.199	interface traffic-counter set	289
3.29.200	interface traffic-counter threshold	290
3.29.201	interface traffic-shape	290

3.29.202	interface tty init	291
3.29.203	interface tty send	292
3.29.204	interface tunnel destination	293
3.29.205	interface tunnel eoip id	294
3.29.206	interface tunnel gre keepalive	294
3.29.207	interface tunnel source	295
3.29.208	interface tx-burst	296
3.29.209	interface tx-queue length	296
3.29.210	interface tx-queue scheduler cake	297
3.29.211	interface tx-queue scheduler fq_codel	298
3.29.212	interface up	298
3.29.213	interface usb acq	299
3.29.214	interface usb apn	299
3.29.215	interface usb device-id	300
3.29.216	interface usb port-id	301
3.29.217	interface usb power-cycle	302
3.29.218	interface usb power-fail	302
3.29.219	interface usb wwan-force-connected	303
3.29.220	interface vga-clamp	303
3.29.221	interface vlan qos egress map	304
3.29.222	interface web-api address	305
3.29.223	interface web-api login	306
3.29.224	interface web-api password	306
3.29.225	interface wireguard asc	307
3.29.226	interface wireguard listen-port	308
3.29.227	interface wireguard peer	309
3.29.228	interface wireguard private-key	315
3.29.229	interface wmm	315
3.29.230	interface wpa-eap radius secret	316
3.29.231	interface wpa-eap radius server	316
3.29.232	interface wps	317
3.29.233	interface wps auto-self-pin	318
3.29.234	interface wps button	318
3.29.235	interface wps peer	319
3.29.236	interface wps self-pin	319
3.29.237	interface zerotier accept-addresses	320
3.29.238	interface zerotier accept-routes	320
3.29.239	interface zerotier connect	321
3.29.240	interface zerotier network-id	322
3.30	ip arp	322
3.31	ip dhcp class	323
3.31.1	ip dhcp class option	324
3.32	ip dhcp host	324

3.33	ip dhcp pool	325
3.33.1	ip dhcp pool bind	326
3.33.2	ip dhcp pool bootfile	327
3.33.3	ip dhcp pool class	327
3.33.4	ip dhcp pool debug	329
3.33.5	ip dhcp pool default-router	329
3.33.6	ip dhcp pool dns-server	330
3.33.7	ip dhcp pool domain	330
3.33.8	ip dhcp pool enable	331
3.33.9	ip dhcp pool lease	331
3.33.10	ip dhcp pool next-server	332
3.33.11	ip dhcp pool option	333
3.33.12	ip dhcp pool range	334
3.33.13	ip dhcp pool update-dns	335
3.33.14	ip dhcp pool wpad	335
3.34	ip dhcp relay enable	336
3.35	ip dhcp relay lan	336
3.36	ip dhcp relay server	337
3.37	ip dhcp relay upstream interface	337
3.38	ip dhcp relay upstream server	338
3.39	ip dhcp relay wan	339
3.40	ip esp alg enable	340
3.41	ip flow-cache timeout active	340
3.42	ip flow-cache timeout inactive	341
3.43	ip flow-export destination	342
3.44	ip flow-export version	342
3.45	ip ftp	343
3.45.1	ip ftp client-charset	343
3.45.2	ip ftp lockout-policy	346
3.45.3	ip ftp permissive	347
3.45.4	ip ftp security-level	347
3.46	ip host	348
3.47	ip hotspot	349
3.47.1	ip hotspot auto-register disable	349
3.47.2	ip hotspot auto-scan interface	350
3.47.3	ip hotspot auto-scan interval	350
3.47.4	ip hotspot auto-scan passive	351
3.47.5	ip hotspot auto-scan timeout	352
3.47.6	ip hotspot default-policy	352
3.47.7	ip hotspot host	353
3.47.8	ip hotspot host conform	354
3.47.9	ip hotspot host priority	355
3.47.10	ip hotspot policy	356

3.47.11	ip hotspot priority	357
3.47.12	ip hotspot wake	358
3.48	ip http lockout-policy	358
3.49	ip http log access	359
3.50	ip http log auth	360
3.51	ip http log webdav	360
3.52	ip http port	361
3.53	ip http proxy	362
3.53.1	ip http proxy auth	362
3.53.2	ip http proxy dns-override	363
3.53.3	ip http proxy domain	364
3.53.4	ip http proxy domain ndns	364
3.53.5	ip http proxy force-host	365
3.53.6	ip http proxy preserve-host	366
3.53.7	ip http proxy preserve-origin	366
3.53.8	ip http proxy preserve-referer	367
3.53.9	ip http proxy security-level	367
3.53.10	ip http proxy ssl redirect	368
3.53.11	ip http proxy timeout	369
3.53.12	ip http proxy upstream	369
3.53.13	ip http proxy x-real-ip	370
3.54	ip http security-level	371
3.55	ip http ssl acme debug	454
3.56	ip http ssl acme ecdsa	372
3.57	ip http ssl acme get	373
3.58	ip http ssl acme revoke	373
3.59	ip http ssl acme list	374
3.60	ip http ssl enable	375
3.61	ip http ssl port	375
3.62	ip http ssl redirect	376
3.63	ip http webdav	376
3.63.1	ip http webdav enable	377
3.63.2	ip http webdav permissive	377
3.63.3	ip http webdav security-level	378
3.64	ip http x-frame-options	379
3.65	ip name-server	379
3.66	ip nat	380
3.67	ip nat full-cone	381
3.68	ip nat oc	382
3.69	ip nat restricted-cone	382
3.70	ip nat sstp	383
3.71	ip nat vpn	384
3.72	ip policy	384

3.72.1	ip policy description	385
3.72.2	ip policy ipv6 route	386
3.72.3	ip policy multipath	387
3.72.4	ip policy permit	387
3.72.5	ip policy permit auto	388
3.72.6	ip policy rate-limit input	389
3.72.7	ip policy rate-limit output	390
3.72.8	ip policy route	390
3.72.9	ip policy standalone	392
3.73	ip route	392
3.74	ip search-domain	394
3.75	ip sip alg direct-media	395
3.76	ip sip alg port	395
3.77	ip ssh	396
3.77.1	ip ssh cipher	396
3.77.2	ip ssh keygen	397
3.77.3	ip ssh lockout-policy	398
3.77.4	ip ssh port	399
3.77.5	ip ssh security-level	400
3.77.6	ip ssh session timeout	400
3.77.7	ip ssh sftp	401
3.78	ip static	403
3.79	ip static rule	405
3.80	ip telnet	406
3.80.1	ip telnet lockout-policy	407
3.80.2	ip telnet port	408
3.80.3	ip telnet security-level	408
3.80.4	ip telnet session max-count	409
3.80.5	ip telnet session timeout	410
3.81	ip traffic-shape host	410
3.82	ip traffic-shape unknown-host	412
3.83	ipv6 local-prefix	413
3.84	ipv6 name-server	413
3.85	ipv6 pass	415
3.86	ipv6 route	415
3.87	ipv6 static	416
3.88	ipv6 subnet	417
3.88.1	ipv6 subnet bind	418
3.88.2	ipv6 subnet dns-server	419
3.88.3	ipv6 subnet mode	420
3.88.4	ipv6 subnet number	420
3.88.5	ipv6 subnet prefix delegate	421
3.88.6	ipv6 subnet prefix length	421

3.89	isolate-private	422
3.90	kabinet	423
3.90.1	kabinet access-level	423
3.90.2	kabinet interface	424
3.90.3	kabinet password	425
3.90.4	kabinet port	425
3.90.5	kabinet protocol-version	426
3.90.6	kabinet server	427
3.91	known host	427
3.92	mdns	428
3.92.1	mdns reflector disable	428
3.92.2	mdns reflector enforce	429
3.93	mws acquire	429
3.94	mws auto-ap-shutdown	430
3.95	mws backhaul shutdown	431
3.96	mws log stp	431
3.97	mws member	432
3.98	mws member debug	433
3.99	mws member dpn-accept	433
3.100	mws member port access	434
3.101	mws member port disable	435
3.102	mws member reboot	435
3.103	mws member update channel	436
3.104	mws member update check	437
3.105	mws member update start	437
3.106	mws member update stop	438
3.107	mws reboot	438
3.108	mws revisit	439
3.109	mws stp priority	439
3.110	mws update start	440
3.111	mws update stop	441
3.112	mws zone	442
3.113	nextdns	442
3.113.1	nextdns assign	443
3.113.2	nextdns authenticate	444
3.113.3	nextdns authtoken	444
3.113.4	nextdns check-availability	445
3.114	ndns	445
3.114.1	ndns book-name	446
3.114.2	ndns check-name	448
3.114.3	ndns drop-name	449
3.114.4	ndns get-booked	450
3.114.5	ndns get-update	451

3.115	ntce	454
3.115.1	ntce debug	454
3.115.2	ntce filter assign host	455
3.115.3	ntce filter assign interface	455
3.115.4	ntce filter profile	456
3.115.5	ntce filter profile application	457
3.115.6	ntce filter profile description	458
3.115.7	ntce filter profile group	458
3.115.8	ntce filter profile schedule	459
3.115.9	ntce filter profile type	460
3.115.10	ntce memory-watcher	460
3.115.11	ntce qos category priority	461
3.115.12	ntce qos enable	462
3.115.13	ntce upstream rate-limit input	462
3.115.14	ntce upstream rate-limit output	463
3.116	ntp	464
3.117	ntp master	464
3.118	ntp server	465
3.119	ntp source	465
3.120	ntp sync-period	466
3.121	object-group fqdn	466
3.121.1	object-group fqdn exclude	467
3.121.2	object-group fqdn include	468
3.122	object-group ip	469
3.122.1	object-group ip exclude	469
3.122.2	object-group ip include	470
3.123	oc-server	471
3.123.1	oc-server camouflage	472
3.123.2	oc-server debug	472
3.123.3	oc-server interface	473
3.123.4	oc-server mtu	474
3.123.5	oc-server multi-login	474
3.123.6	oc-server pool-range	475
3.123.7	oc-server route	475
3.123.8	oc-server session-logout	476
3.123.9	oc-server session-preempt	477
3.123.10	oc-server static-ip	477
3.124	opkg chroot	478
3.125	opkg disk	479
3.126	opkg dns-override	479
3.127	opkg initrc	480
3.128	opkg timezone	481
3.129	ping-check profile	482

3.129.1	ping-check profile host	482
3.129.2	ping-check profile max-fails	483
3.129.3	ping-check profile min-success	484
3.129.4	ping-check profile mode	485
3.129.5	ping-check profile port	485
3.129.6	ping-check profile power-cycle	486
3.129.7	ping-check profile timeout	486
3.129.8	ping-check profile update-interval	487
3.129.9	ping-check profile uri	488
3.130	ppe	488
3.131	pppoe pass	489
3.132	printer	490
3.132.1	printer bidirectional	490
3.132.2	printer debug	491
3.132.3	printer firmware	492
3.132.4	printer name	492
3.132.5	printer port	493
3.132.6	printer status-polling	493
3.132.7	printer type	494
3.133	schedule	494
3.133.1	schedule action	495
3.133.2	schedule description	495
3.133.3	schedule led	496
3.134	service afp	497
3.135	service cifs	497
3.136	service dhcp	498
3.137	service dhcp-relay	498
3.138	service dlna	499
3.139	service dns-proxy	499
3.140	service ftp	500
3.141	service http	500
3.142	service igmp-proxy	501
3.143	service internet-checker	501
3.144	service ipsec	502
3.145	service kabinet	502
3.146	service mdns	503
3.147	service mws	503
3.148	service ntce	504
3.149	service ntp	504
3.150	service oc-server	505
3.151	service snmp	505
3.152	service ssh	506
3.153	service sstp-server	506

3.154	service telnet	507
3.155	service torrent	507
3.156	service udpxy	508
3.157	service upnp	508
3.158	service vpn-server	509
3.159	show	509
3.159.1	show access	510
3.159.2	show acme	510
3.159.3	show afp	511
3.159.4	show associations	512
3.159.5	show button	513
3.159.6	show button bindings	514
3.159.7	show button handlers	516
3.159.8	show chilli profiles	518
3.159.9	show cifs	519
3.159.10	show clock date	519
3.159.11	show clock timezone-list	520
3.159.12	show components status	521
3.159.13	show configurator status	521
3.159.14	show credits	522
3.159.15	show crypto ike key	530
3.159.16	show crypto map	531
3.159.17	show defaults	532
3.159.18	show dlna	533
3.159.19	show dns-proxy	534
3.159.20	show dns-proxy filter presets	535
3.159.21	show dns-proxy filter profiles	537
3.159.22	show dpn document	538
3.159.23	show dpn list	539
3.159.24	show dot1x	541
3.159.25	show drivers	542
3.159.26	show dyndns updaters	543
3.159.27	show easyconfig status	543
3.159.28	show eula document	544
3.159.29	show eula list	545
3.159.30	show interface	546
3.159.31	show interface antennas	548
3.159.32	show interface bands	549
3.159.33	show interface bridge	550
3.159.34	show interface cells	551
3.159.35	show interface channel-utilization rrd	552
3.159.36	show interface channels	553
3.159.37	show interface chilli	555

3.159.38	show interface country-codes	556
3.159.39	show interface mac	557
3.159.40	show interface name-server	558
3.159.41	show interface operators	560
3.159.42	show interface rf e2p	562
3.159.43	show interface rrd	562
3.159.44	show interface spectrum rrd	564
3.159.45	show interface stat	566
3.159.46	show interface traffic-counter	567
3.159.47	show interface wps pin	568
3.159.48	show interface wps status	569
3.159.49	show interface zerotier peers	570
3.159.50	show internet status	571
3.159.51	show ip arp	572
3.159.52	show ip dhcp bindings	573
3.159.53	show ip dhcp pool	573
3.159.54	show ip ftp	574
3.159.55	show ip hotspot	575
3.159.56	show ip hotspot rrd	576
3.159.57	show ip hotspot summary	579
3.159.58	show ip http proxy	580
3.159.59	show ip http webdav	581
3.159.60	show ip name-server	582
3.159.61	show ip nat	583
3.159.62	show ip neighbour	584
3.159.63	show ip policy	585
3.159.64	show ip route	587
3.159.65	show ip service	590
3.159.66	show ipsec	591
3.159.67	show ipv6 addresses	592
3.159.68	show ipv6 dhcp bindings	593
3.159.69	show ipv6 prefixes	594
3.159.70	show ipv6 route	594
3.159.71	show ipv6 subnets	596
3.159.72	show kabinet status	596
3.159.73	show last-change	597
3.159.74	show led	597
3.159.75	show led bindings	598
3.159.76	show led controls	601
3.159.77	show log	604
3.159.78	show media	605
3.159.79	show mws associations	606
3.159.80	show mws candidate	607

3.159.81	show mws log	609
3.159.82	show mws member	609
3.159.83	show ndns	611
3.159.84	show netfilter	612
3.159.85	show nextdns availability	612
3.159.86	show nextdns profiles	613
3.159.87	show ntce applications	613
3.159.88	show ntce attributes	615
3.159.89	show ntce filter profile	619
3.159.90	show ntce groups	620
3.159.91	show ntce groupsets	626
3.159.92	show ntce hosts	627
3.159.93	show ntce oses	631
3.159.94	show ntce status	633
3.159.95	show ntp status	634
3.159.96	show oc-server	635
3.159.97	show ping-check	635
3.159.98	show printers	636
3.159.99	show processes	637
3.159.100	show running-config	639
3.159.101	show schedule	645
3.159.102	show self-test	646
3.159.103	show site-survey	646
3.159.104	show snmp view	647
3.159.105	show ssh fingerprint	647
3.159.106	show ssh sftp	648
3.159.107	show sstp-server	649
3.159.108	show system	649
3.159.109	show system country	650
3.159.110	show system cpustat	651
3.159.111	show system zram	652
3.159.112	show tags	653
3.159.113	show threads	654
3.159.114	show torrent status	655
3.159.115	show upnp redirect	655
3.159.116	show usb	656
3.159.117	show version	657
3.159.118	show vpn-server	658
3.160	sms	658
3.160.1	sms delete	659
3.160.2	sms list	659
3.160.3	sms read	662
3.160.4	sms send	663

3.161	snmp community	663
3.162	snmp contact	664
3.163	snmp location	664
3.164	snmp view	665
3.165	snmp view exclude	666
3.166	snmp view include	666
3.167	sstp-server	667
3.167.1	sstp-server allow-bridging	667
3.167.2	sstp-server camouflage	668
3.167.3	sstp-server debug	668
3.167.4	sstp-server dhcp route	669
3.167.5	sstp-server interface	670
3.167.6	sstp-server ipv6cp	671
3.167.7	sstp-server lcp echo	671
3.167.8	sstp-server lcp force-pap	672
3.167.9	sstp-server mru	672
3.167.10	sstp-server mtu	673
3.167.11	sstp-server multi-login	674
3.167.12	sstp-server pool-range	674
3.167.13	sstp-server session-logout	675
3.167.14	sstp-server session-preempt	675
3.167.15	sstp-server static-ip	676
3.168	system	676
3.168.1	system button	677
3.168.2	system caption	678
3.168.3	system clock date	679
3.168.4	system clock timezone	680
3.168.5	system configuration factory-reset	680
3.168.6	system configuration fail-safe commit	681
3.168.7	system configuration fail-safe keep-alive	681
3.168.8	system configuration fail-safe rollback	681
3.168.9	system configuration fail-safe timer	682
3.168.10	system configuration save	683
3.168.11	system country	683
3.168.12	system debug	684
3.168.13	system description	684
3.168.14	system domainname	686
3.168.15	system eject	686
3.168.16	system hostname	687
3.168.17	system led	687
3.168.18	system led power schedule	688
3.168.19	system led power shutdown	689
3.168.20	system log clear	690

3.168.21	system log reduction	690
3.168.22	system log server	690
3.168.23	system log suppress	691
3.168.24	system mode	692
3.168.25	system mount	692
3.168.26	system ndss dump-report disable	693
3.168.27	system reboot	693
3.168.28	system set	694
3.168.29	system swap	695
3.168.30	system trace lock threshold	696
3.168.31	system usb power schedule	697
3.168.32	system usb power shutdown	697
3.168.33	system zram	698
3.169	tools	699
3.169.1	tools arping	699
3.169.2	tools ping	700
3.169.3	tools ping6	702
3.169.4	tools traceroute	703
3.170	torrent	705
3.170.1	torrent directory	705
3.170.2	torrent io-priority	706
3.170.3	torrent peer-port	707
3.170.4	torrent policy	707
3.170.5	torrent reset	708
3.170.6	torrent rpc-port	708
3.171	udpxy	709
3.171.1	udpxy buffer-size	709
3.171.2	udpxy buffer-timeout	710
3.171.3	udpxy interface	710
3.171.4	udpxy port	711
3.171.5	udpxy renew-interval	712
3.171.6	udpxy timeout	712
3.172	upnp forward	713
3.173	upnp lan	714
3.174	upnp redirect	715
3.175	user	716
3.175.1	user home	716
3.175.2	user password	717
3.175.3	user tag	718
3.176	ussd send	720
3.177	vpn-server	721
3.177.1	vpn-server dhcp route	721
3.177.2	vpn-server interface	722

3.177.3	vpn-server ipv6cp	723
3.177.4	vpn-server lcp echo	723
3.177.5	vpn-server lockout-policy	724
3.177.6	vpn-server mppe	725
3.177.7	vpn-server mppe-optional	726
3.177.8	vpn-server mru	726
3.177.9	vpn-server mtu	727
3.177.10	vpn-server multi-login	727
3.177.11	vpn-server pool-range	728
3.177.12	vpn-server session-logout	729
3.177.13	vpn-server session-preempt	729
3.177.14	vpn-server static-ip	730
	Glossary	731
	Appendix A	
	Interface Hierarchy	745
	Appendix B	
	HTTP API	747
B.1	REST Core Interface	747
B.1.1	Resource Location	747
B.1.2	Methods	747
B.1.3	Data Format	748
B.2	XML Core Interface	751
B.2.1	Command Request	752
B.2.2	Configuration Request	753
B.2.3	Request Packet	753
	Appendix C	
	NVOX CLI commands	755
C.1	nvox	756
C.2	nvox call-history clear	756
C.3	nvox call-history delete-call	757
C.4	nvox call-history directory	757
C.5	nvox call-history dump	758
C.6	nvox call-history filter	759
C.7	nvox call-history length	760
C.8	nvox fxs	760
C.8.1	nvox fxs country	761
C.8.2	nvox fxs echo-canc-mode	762
C.8.3	nvox fxs echo-canc-thresholds	763
C.8.4	nvox fxs force-calibration	763
C.8.5	nvox fxs init-timer	764
C.8.6	nvox fxs led-blinking-timer	765
C.8.7	nvox fxs port-paging	765

C.8.8	nvox fxs pulse-dial-mode	766
C.8.9	nvox fxs unmute-timer	767
C.9	nvox parallel accept	767
C.10	nvox parallel disable	768
C.11	nvox parallel call-external	769
C.12	nvox parallel call-internal	769
C.13	nvox parallel hold-resume	770
C.14	nvox parallel intercept	771
C.15	nvox parallel reject	772
C.16	nvox parallel release-active	772
C.17	nvox parallel release-passive	773
C.18	nvox parallel toggle	774
C.19	nvox parallel transfer	775
C.20	nvox phone	775
C.20.1	nvox phone cadence	776
C.20.2	nvox phone dial-digit-timer	777
C.20.3	nvox phone intercom-cadence	778
C.20.4	nvox phone offhook-timer	778
C.20.5	nvox phone paging-cadence	779
C.21	nvox phonebook delete	780
C.22	nvox phonebook handset-edit	780
C.23	nvox phonebook import	781
C.24	nvox phonebook last-name-first	782
C.25	nvox phonebook length	783
C.26	nvox phonebook match-length	783
C.27	nvox postdial key	784
C.28	nvox postdial mid-timer	785
C.29	nvox postdial post-timer	785
C.30	nvox postdial pre-timer	786
C.31	nvox sip	787
C.31.1	nvox sip audio-protocol	787
C.31.2	nvox sip blacklist	788
C.31.3	nvox sip cadence	789
C.31.4	nvox sip cadence-rule	790
C.31.5	nvox sip codec	791
C.31.6	nvox sip deny-interception	791
C.31.7	nvox sip deny-pickup	792
C.31.8	nvox sip digit-map	793
C.31.9	nvox sip disable	793
C.31.10	nvox sip disable-extended-keepalive	794
C.31.11	nvox sip disable-force-registration-retry	795
C.31.12	nvox sip disable-stun	795
C.31.13	nvox sip display-name	796

C.31.14	nvox sip dnd	796
C.31.15	nvox sip dnd-schedule	797
C.31.16	nvox sip domain	798
C.31.17	nvox sip dtmf-flash-signal	798
C.31.18	nvox sip dtmf-mode	799
C.31.19	nvox sip enable-blacklist	800
C.31.20	nvox sip enable-whitelist	800
C.31.21	nvox sip enable-whitelist-phonebook	801
C.31.22	nvox sip forward	802
C.31.23	nvox sip forward-if-busy	802
C.31.24	nvox sip forward-if-busy-schedule	803
C.31.25	nvox sip forward-if-timeout	804
C.31.26	nvox sip forward-if-timeout-schedule	804
C.31.27	nvox sip forward-schedule	805
C.31.28	nvox sip identity	806
C.31.29	nvox sip incoming-mask	806
C.31.30	nvox sip keepalive	807
C.31.31	nvox sip lock-codec	808
C.31.32	nvox sip login	808
C.31.33	nvox sip name	809
C.31.34	nvox sip outgoing-mask	810
C.31.35	nvox sip password	810
C.31.36	nvox sip priority	811
C.31.37	nvox sip proxy	812
C.31.38	nvox sip reg-timeout	813
C.31.39	nvox sip registration-first-retry	813
C.31.40	nvox sip registration-retry	814
C.31.41	nvox sip registration-uri	815
C.31.42	nvox sip sdp-nat-rewrite	815
C.31.43	nvox sip selection-id	816
C.31.44	nvox sip session-timer	817
C.31.45	nvox sip session-timer-mode	817
C.31.46	nvox sip substitute	818
C.31.47	nvox sip tls-security-mode	819
C.31.48	nvox sip transport	820
C.31.49	nvox sip whitelist	821
C.32	nvox sip-common	822
C.32.1	nvox sip-common 100rel	822
C.32.2	nvox sip-common agent	823
C.32.3	nvox sip-common disable-dns-srv	824
C.32.4	nvox sip-common disable-tls-validation	824
C.32.5	nvox sip-common g726-dynamic-payload	825
C.32.6	nvox sip-common outbound-proxy	826

C.32.7	nvox sip-common qos	826
C.32.8	nvox sip-common rtp-port	830
C.32.9	nvox sip-common sdp rtcp	830
C.32.10	nvox sip-common sdp tias	831
C.32.11	nvox sip-common stun-server	832
C.32.12	nvox sip-common tcp-keepalive	832
C.32.13	nvox sip-common tcp-port	833
C.32.14	nvox sip-common td-timeout	834
C.32.15	nvox sip-common tls-keepalive	835
C.32.16	nvox sip-common tls-port	835
C.32.17	nvox sip-common udp-port	836
C.32.18	nvox sip-common unescape-hash-char	837
C.33	show nvox active-calls	838
C.34	show nvox blacklist	839
C.35	show nvox cadences	839
C.36	show nvox call-history	841
C.37	show nvox fxs	843
C.38	show nvox fxs-ports	844
C.39	show nvox info	844
C.40	show nvox license	845
C.41	show nvox phonebook	846
C.42	show nvox sip-lines	847
C.43	show nvox sip-profiles	848
C.44	show nvox try-dial	850
C.45	show nvox try-dial-ext	851
C.46	show nvox whitelist	852
Appendix D		
SNMP MIB		855
D.1	SNMPv2-MIB	855
D.2	IF-MIB	855
D.3	IP-MIB	857
D.4	UDP-MIB	858
D.5	HOST-RESOURCES-MIB	858
D.6	UCD-SNMP-MIB	858
Appendix E		
IPsec Encryption Levels		861
E.1	weak	861
E.2	weak-pfs	862
E.3	normal	864
E.4	normal-pfs	865
E.5	normal-3des	866
E.6	normal-3des-pfs	867

E.7 high 868

E.8 strong 869

E.9 strong-aead 870

E.10 strong-aead-pfs 870

Product Overview

1.1 Hardware Configuration

CPU MediaTek MT7628AN MIPS® 24KEc 580 MHz

RAM ESMT M14D1G1664A 128MB DDR2

Flash Winbond 25Q256JVFQ 32MB SPI

Ethernet

Ports	Chipset	Notes
5	Integrated	

Label	Speed	Notes
0	100 Mbps	WAN port
1	100 Mbps	
2	100 Mbps	
3	100 Mbps	
4	100 Mbps	

USB

Label	Speed	Notes
1	USB 2.0	

Wi-Fi

Band	Chipset	Notes
2.4 GHz	MediaTek MT7603 (on-die)	802.11bgn 2x2
5 GHz	MediaTek MT7613AEN (PCIe Gen 2.1)	802.11an+ac 2x2, BF, MU-MIMO

Introduction to the CLI

This chapter describes how to use the Carrier Command-Line Interface (CLI), its hierarchical structure, authorization levels and its help features.

The primary tool for managing the Carrier router is the command line interface ([CLI](#)). System settings can be defined as a sequence of commands, which can be executed to bring the device to the specified condition.

Carrier has three types of settings:

Current settings	<i>running config</i> is a set of commands describing the current status of the system. Current settings are stored in RAM and reflect every change of the system settings. However, the content of RAM is lost when the device is turned off. To restore the settings after reboot, they must be saved in non-volatile memory.
Startup configuration	<i>startup config</i> is a sequence of commands, which is stored in a specific partition of the non-volatile memory. It is used to initialize the system immediately after startup.
Default settings	<i>default config</i> contains factory default settings of Carrier. RESET button is used to reset startup configuration to the factory default.

Files startup-config and running-config can be edited manually, without participation of the command line. It should be remembered that the lines with ! in the beginning are ignored by the parser and the arguments which contain spaces must be enclosed in double quotes (for example, ssid "Free Wi-Fi"). Quotes themselves are ignored by the parser.

Responsibility for the accuracy of the changes rests with their author.

2.1 Enter commands in the CLI

Command line interpreter in Carrier is designed for beginners as well as experts. All command names and options are clear and easy to remember.

Commands are divided into groups and arranged in a hierarchy. Thus, to do a setting, the operator needs to enter a sequence of nested command group names (node commands), and then enter the final command with parameters.

For example, IP-address of the FastEthernet0/Vlan2 network interface is set using the **address** command, which is located in the **interface** → **ip** group:

```
(config)>interface FastEthernet0/Vlan2 ip address 192.168.15.43/24
Network address saved.
```

2.1.1 Entering a group

Some of the node commands (containing a group of child commands) can be “entered” to allow direct executing of the child commands without typing the node name as prefix. In this case the prompt is changed to indicate the entered group.

The **exit** command or [Ctrl]+[D] key combination can be used to exit a group.

For example, after entering the interface group the command line prompt is changed to (config-if):

```
(config)>interface FastEthernet0/Vlan2
(config-if)>ip address 192.168.15.43/24
Network address saved.
(config-if)>[Ctrl]+[D]
(config)>
```

2.2 Getting Help and auto-completion

To make the configuring process as comfortable as possible, the CLI provides auto-completion of commands and parameters, hinting the operator, which commands are available at the current level of nesting. Auto-completion works by pressing [Tab]. Example:

```
(config)>in[Tab]

interface - network interface configuration

(config)> interface Fa[Tab]

Usage template:
interface {name}

Variants:
FastEthernet0
FastEthernet0/Vlan1
FastEthernet0/Vlan2

(config)> interface FastEthernet0[Tab]

Usage template:
interface {name}

Variants:
FastEthernet0/Vlan1
FastEthernet0/Vlan2

(config)> interface FastEthernet0[Enter]
(config-if)> ip[Tab]

address - set interface IP address
alias - add interface IP alias
dhcp - enable dhcp client
```

```

        mtu - set Maximum Transmit Unit size
        mru - set Maximum Receive Unit size
    access-group - bind access-control rules
        apn - set 3G access point name

(config-if)> ip ad[Tab]

        address - set interface IP address

(config-if)> ip address[Tab]

Usage template:
address {address} {mask}

(config-if)> ip address 192.168.15.43[Enter]
Configurator error[852002]: address: argument parse error.
(config-if)> ip address 192.168.15.43/24[Enter]
Network address saved.
(config-if)>

```

Hint for the current command can always be displayed by pressing [Tab]. Example:

```

(config)> interface FastEthernet0/Vlan2 [Tab]

        description - set interface description
        alias - add interface name alias
        mac-address - set interface MAC address
        dyndns - DynDns updates
        security-level - assign security level
        authentication - configure authentication
            ip - set interface IP parameters
            igmp - set interface IGMP parameters
            up - enable interface
            down - disable interface

(config)> interface FastEthernet0/Vlan2

```

2.3 Prefix no

Prefix **no** is used to negate a command.

For example, the command **interface** is responsible for creating a network interface with the given name. When used with this command, prefix **no** causes the opposite action — removing of the interface:

```

(config)> no interface PPPoE0

```

If the command is composite, **no** can be placed in front of any member. For example, **service dhcp** enables the *DHCP* service. It consists of two parts: **service** — the group name in the hierarchy of commands, and **dhcp** — the final command. Prefix **no** can be placed either at the beginning, or in the middle. The action is the same in both cases: stopping of the service.

```
(config)> no service dhcp
(config)> service no dhcp
```

2.4 Multiple input

Many commands have the property of *idempotence*, which means that multiple input of a command has the same effect as the single input. For example, entering **service http** adds a single line “service http” to the current settings, and re-entering does not change anything.

However, some of the commands allow you to add not a single, but multiple records, if they are entered with different arguments. For example, static routing table entries **ip route** or filters **access-list** are added sequentially and appear in the settings as a list:

Example 2.1. Using a command with multiple input

```
(config)> ip route 1.1.1.0/24 PPTP0
Network::RoutingTable: Added static route: 1.1.1.0/24 via PPTP0.
(config)> ip route 1.1.2.0/24 PPTP0
Network::RoutingTable: Added static route: 1.1.2.0/24 via PPTP0.
(config)> ip route 1.1.3.0/24 PPTP1
Network::RoutingTable: Added static route: 1.1.3.0/24 via PPTP1.
(config)> show running-config
...
ip route 1.1.1.0 255.255.255.0 PPTP0
ip route 1.1.2.0 255.255.255.0 PPTP0
ip route 1.1.3.0 255.255.255.0 PPTP1
...
```

Records from such tables can be removed one by one, using prefix **no** and arguments to identify the record you want to remove:

```
(config)> no ip route 1.1.2.0/24
Network::RoutingTable: Deleted static route: 1.1.2.0/24 via PPTP0.
(config)> show running-config
...
ip route 1.1.1.0 255.255.255.0 PPTP0
ip route 1.1.3.0 255.255.255.0 PPTP1
...
```

2.5 Saving to startup settings

Current and startup settings are stored in the files `running-config` and `startup-config`, respectively. To save the current settings in the non-volatile memory, copy them as shown below:

```
(config)> copy running-config startup-config
Copied: running-config -> startup-config
```

2.6 Delayed restart

If Carrier device is located away from the operator and is managed remotely, there is a risk to lose control over it because of a misoperation. In this case it will be difficult to reboot and return to the saved settings.

The **system reboot** command lets you set a delayed restart timer, perform “risky” settings, then turn off the timer and save the changes. If connection to the device is lost during configuration, the operator will be enough to wait for automatic reboot and connect to the device again.

Command Reference

3.1 Core commands

Core commands are used to manage files on your device.

3.1.1 copy

Description Copy the contents of one file to another. Used for the firmware updating, saving the current settings, resetting to factory, etc.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config)> copy <source> <destination>`

Arguments

Argument	Value	Description
source	<i>Filename</i>	Full path to the file to be copied in <file system>:<path> format
destination	<i>Filename</i>	Full path to the directory for the new file.

Example

Current settings can be saved as follows:

```
(config)> copy running-config startup-config
```

```
(config)> copy log MyPassport:/log.txt
```

File names in this example are aliases. Full names of the configuration files are system:running-config and flash:startup-config, respectively.

History

Version	Description
2.00	The copy command has been introduced.

3.1.2 erase

Description Delete a file from the Carrier device.

Prefix no No

Change settings Yes

Multiple input Yes

Synopsis `(config)> erase <filename>`

Arguments	Argument	Value	Description
	filename	<i>Filename</i>	Specifies the file to be removed.

Example `(config)> erase ext-opkg:/dlna_files.db`
FileSystem::Repository: "ext-opkg:/dlna_files.db" erased.

History	Version	Description
	2.00	The erase command has been introduced.

3.1.3 exit

Description Leave the command node.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config)> exit`

Example `(show)> exit`
Core::Configurator: Done.
`(config)>`

History	Version	Description
	2.00	The exit command has been introduced.

3.1.4 grep

Description Filter and search for lines containing a match to the given pattern in [show](#) command output.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(show)> <command> | grep [-A <a>] [-B <b>] [-C <c>] <pattern>
```

Arguments

Argument	Value	Description
command	<i>String</i>	Command name.
a	<i>String</i>	Number of lines to show after match.
b	<i>String</i>	Number of lines to show before match.
c	<i>String</i>	Nesting depth of XML context.
pattern	<i>String</i>	A regular expression to search for node names or values in the XML response from the system core.

Example

```
(show)> version | grep dual_image
```

```
ndw:
features: dual_image,usb_3,single_usb_port,
          led_control,wifi_button, wifi5ghz,vht2ghz,mimo2ghz,
          mimo5ghz,atf2ghz,atf5ghz,wifi6,wifi_ft,wpa3,hwnat,
          hwnat_mib,link_agg,lte
```

```
(show)> version | grep -A 1 dual_image
```

```
ndw:
version: 4.1.2.17.1
features: dual_image,wifi_button,usb_3,usb_3_first,
          led_control,wifi5ghz,vht2ghz,mimo2ghz,mimo5ghz,atf2ghz,
          atf5ghz,wifi6,wifi_ft,wpa3,wsa5ghz,hwnat,sfp
```

```
(show)> version | grep -B 1 dual_image
```

```
ndw:
features: dual_image,wifi_button,usb_3,usb_3_first,led_control,
          wifi5ghz,vht2ghz,mimo2ghz,mimo5ghz,atf2ghz,atf5ghz,
          wifi6,wifi_ft,wpa3,wsa5ghz,hwnat,sfp
components: acl,afp,base,chilli,cloudcontrol,corewireless,
            ddns,dhcpd,dlna,dns-filter,dns-https,dns-tls,dot1x,
            easyconfig,eoip,exfat,ext,fat,ftp,gre,hfsplus,igmp,
            ike-client,ip6,ipip,ipsec,kabinet,l2tp,lang-en,
            lang-ru,mdns,miniupnpd,monitor,mws,nathelper-esp,
            nathelper-ftp,nathelper-h323,nathelper-pptp,
            nathelper-rtsp,nathelper-sip,ndmp,ndns,netflow,
            nextdns,ntce,ntfs,nvox,ocserver,openvpn,opkg,
            opkg-kmod-audio,opkg-kmod-dvb-tuner,opkg-kmod-fs,
            opkg-kmod-netfilter,opkg-kmod-netfilter-addons,
            opkg-kmod-tc,opkg-kmod-usbip,opkg-kmod-video,
            pingcheck,ppe,pppoe,pptp,proxy,sftp,skydns,snmp,ssh,
            sstp,sstp-server,storage,trafficcontrol,
            transmission,tsmb,udpxy,usb,usbdsi,usblte,usbmodem,
            usbnet,usbnet-extra,usbqmi,usbserial-extra,
            vpnserver,vpnserver-l2tp,webdav,wireguard,wpa-eap,
            zerotier
```

```
(show)> version | grep -C 1 dual_image
```

```

    ndw:
    version: 4.1.2.17.1
    features: dual_image,wifi_button,usb_3,usb_3_first,led_control,
              wifi5ghz,vht2ghz,mimo2ghz,mimo5ghz,atf2ghz,atf5ghz,
              wifi6,wifi_ft,wpa3,wsa5ghz,hwnat,sfp
    components: acl,afp,base,chilli,cloudcontrol,corewireless,ddns,
                dhcpd,dlna,dns-filter,dns-https,dns-tls,dot1x,
                easyconfig,eoip,exfat,ext,fat,ftp,gre,hfsplus,igmp,
                ike-client,ip6,ipip,ipsec,kabinet,l2tp,lang-en,mdns,
                miniupnpd,monitor,mws,nathelper-esp,nathelper-ftp,
                nathelper-h323,nathelper-pptp,nathelper-rtsp,
                nathelper-sip,ndmp,ndns,netflow,nextdns,ntce,ntfs,
                nvox,ocserver,openvpn,opkg,opkg-kmod-audio,
                opkg-kmod-dvb-tuner,opkg-kmod-fs,opkg-kmod-netfilter,
                opkg-kmod-netfilter-addons,opkg-kmod-tc,
                opkg-kmod-usbip,opkg-kmod-video,pingcheck,ppe,pppoe,
                pptp,proxy,sftp,skydns,snmp,ssh,sstp,sstp-server,
                storage,trafficcontrol,transmission,tsmb,udpxy,usb,
                usbdsl,usblte,usbmodem,usbnet,usbnet-extra,usbqmi,
                usbserial-extra,vpnserver,vpnserver-l2tp,webdav,
                wireguard,wpa-eap,zerotier

```

```
(show)> version | grep -C 2 dual_image
```

```

    release: 4.02.A.7.0-0
    sandbox: draft
    title: 4.2 Alpha 7
    arch: mips

    ndm:
    exact: 0-0c7997d
    cdate: 27 Apr 2024

    bsp:
    exact: 0-844097c815
    cdate: 27 Apr 2024

    ndw:
    version: 4.1.2.17.1
    features: dual_image,wifi_button,usb_3,usb_3_first,led_control,
              wifi5ghz,vht2ghz,mimo2ghz,mimo5ghz,atf2ghz,atf5ghz,
              wifi6,wifi_ft,wpa3,wsa5ghz,hwnat,sfp
    components: acl,afp,base,chilli,cloudcontrol,corewireless,ddns,
                dhcpd,dlna,dns-filter,dns-https,dns-tls,dot1x,
                easyconfig,eoip,exfat,ext,fat,ftp,gre,hfsplus,igmp,
                ike-client,ip6,ipip,ipsec,kabinet,l2tp,lang-en,mdns,
                miniupnpd,monitor,mws,nathelper-esp,nathelper-ftp,
                nathelper-h323,nathelper-pptp,nathelper-rtsp,
                nathelper-sip,ndmp,ndns,netflow,nextdns,ntce,ntfs,
                nvox,ocserver,openvpn,opkg,opkg-kmod-audio,
                opkg-kmod-dvb-tuner,opkg-kmod-fs,opkg-kmod-netfilter,
                opkg-kmod-netfilter-addons,opkg-kmod-tc,

```

```
opkg-kmod-usbip,opkg-kmod-video,pingcheck,ppe,pppoe,
pptp,proxy,sftp,skydns,snmp,ssh,sstp,sstp-server,
storage,trafficcontrol,transmission,tsmb,udpxy,usb,
usbdsi,usbdlte,usbmodem,usbnet,usbnet-extra,usbqmi,
usbserial-extra,vpnserver,vpnserver-l2tp,webdav,
wireguard,wpa-eap,zerotier
```

```
ndw3:
  version: 1.73.1
```

```
manufacturer: Keenetic Ltd.
  vendor: Keenetic
  series: KN
  model: Giga (KN-1011)
hw_version: 11108000
  hw_type: router
  hw_id: KN-1011
  device: Giga
  region: EA
description: Keenetic Giga (KN-1011)
```

History

Version	Description
4.02	The grep filter has been introduced.

3.1.5 ls

Description

Display list of files from the specified directory.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(config)>  ls [ <directory> ]
```

Arguments

Argument	Value	Description
directory	<i>String</i>	Path to the directory. Must contain the name of the file system and path to the folder directly in the following format <file system>:<path>. Examples of file systems — flash, temp, proc, usb. etc.

Example

```
(config)>  ls FILES:
```

```
rel: FILES:
```

```
entry, type = D:
  name: com
```

```

entry, type = R:
    name: IMAX.mkv
    size: 1886912512

entry, type = D:
    name: speedfan

entry, type = D:
    name: portable

entry, type = D:
    name: video

entry, type = D:
    name: Новая папка

```

History

Version	Description
2.00	The ls command has been introduced.

3.1.6 mkdir

Description

Create a new directory.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(config)> mkdir <directory>
```

Arguments

Argument	Value	Description
directory	<i>String</i>	Path to the directory.

Example

```
(config)> mkdir SANDSK:/test
FileSystem::Repository: "SANDSK:/test" created.
```

```
(config)> mkdir SANDSK:/test/onetest
FileSystem::Repository: "SANDSK:/test/onetest" created.
```

History

Version	Description
2.12	The mkdir command has been introduced.

3.1.7 more

Description Display the contents of a text file line by line.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config)> more <filename>`

Arguments

Argument	Value	Description
filename	<i>Filename</i>	Full path to the file or alias.

Example

```
(config)> more temp:/resolv.conf
nameserver 127.0.0.1
options timeout:1 attempts:1 rotate
```

History

Version	Description
2.00	The more command has been introduced.

3.2 access

Description Set user access for directory on USB storage.

Command with **no** prefix denies access to the directory.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis `(config)> access <directory> <user> <mode> [ recursive ]`
`(config)> no access <directory> <user> [ recursive ]`

Arguments

Argument	Value	Description
directory	<i>String</i>	Name of directory on USB storage.
user	<i>String</i>	User name.
mode	forbidden	Access denied.
	read	Read-only access.
	write	Write-only access.
	read/write	Access to reading and writing.

Argument	Value	Description
	inherited	Access rights are inherited from a parent folder.
recursive	<i>Keyword</i>	Access rights applies to all subfolders.

Example

```
(config)> access 0D5F-1DB6:Downloads test read/write
```

```
(config)> no access 0D5F-1DB6:Downloads test
```

History

Version	Description
2.00	The access command has been introduced.

3.3 access-list

Description

Access to a group of commands to configure the selected list of packet filtering rules. If the list is not found, the command tries to create it. Such a list can be assigned to a network interface using [interface ip access-group](#) command.

Command with **no** prefix removes the list of rules.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Group entry

(config-acl)

Synopsis

```
(config)> access-list <name>
```

```
(config)> no access-list <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Filtering rules list name (Access Control List , ACL).

Example

```
(config)> access-list test_acl
Network::Acl: "test_acl" access list created.
(config-acl)>
```

```
(config)> no access-list test_acl
Network::Acl: "test_acl" access list removed.
```

History

Version	Description
2.00	The access-list command has been introduced.

3.3.1 access-list auto-delete

Description	Enable automatic deletion of the ACL rules when deleting an interface. The command is forced on access lists with the <code>_WEBADMIN_</code> prefix. The command cannot be enabled if there are no bound interfaces. The exception is reading the startup-config. Command with no prefix disables automatic deletion.				
Prefix no	Yes				
Change settings	Yes				
Multiple input	No				
Synopsis	<pre>(config-acl)> auto-delete (config-acl)> no auto-delete</pre>				
Example	<pre>(config-acl)> auto-delete Network::Acl: Enabled auto-deletion for "_WEBADMIN_Home" access ► group.</pre> <pre>(config-acl)> no auto-delete Network::Acl: Disabled auto-deletion for "_WEBADMIN_Home" access ► group.</pre>				
History	<table border="1"> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>3.09</td><td>The access-list auto-delete command has been introduced.</td></tr> </tbody> </table>	Version	Description	3.09	The access-list auto-delete command has been introduced.
Version	Description				
3.09	The access-list auto-delete command has been introduced.				

3.3.2 access-list deny

Description	Add a packet filtering deny rule into a specified ACL. Command with no prefix removes the rule.
Prefix no	Yes
Change settings	Yes
Multiple input	Yes
Synopsis	<pre>(config-acl)> deny (tcp udp) <source> <source-mask> [port((<src-port-operator> <source-port>) (range <source-port> <source-end-port>))] <destination> <destination-mask> [port((<dst-port-operator> <destination-port>) (range <destination-port> <destination-end-port>))]</pre>

```
(config-acl)> deny (icmp | esp | gre | ipip | ip) <source> <source-mask>
<destination> <destination-mask>
```

```
(config-acl)> no deny (tcp | udp) <source> <source-mask>
[ port( ( <src-port-operator> <source-port> ) |
( range <source-port> <source-end-port> ) ) ]
<destination> <destination-mask>
[ port( ( <dst-port-operator> <destination-port> ) |
( range <destination-port> <destination-end-port> ) ) ]
```

```
(config-acl)> no deny (icmp | esp | gre | ipip | ip) <source> <source-mask>
<destination> <destination-mask>
```

Arguments

Argument	Value	Description
tcp	Keyword	TCP protocol.
udp	Keyword	UDP protocol.
icmp	Keyword	ICMP protocol.
esp	Keyword	ESP protocol.
gre	Keyword	GRE protocol.
ipip	Keyword	IP in IP protocol.
ip	Keyword	IP protocol (include TCP , UDP , ICMP and other).
source	<i>IP address</i>	The source address in the header of IP-packet.
source-mask	<i>IP-mask</i>	Mask to be applied to the source address in the header of IP-packet before comparison with <i>source</i> . There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).
source-port	<i>Integer</i>	Source port in the TCP or UDP header.
source-end-port	<i>Integer</i>	The end of the source range of ports.
src-port-operator	lt	Operator “less” to compare the port with the specified <i>source-port</i> .
	eq	Operator “equal” to compare the port with the specified <i>source-port</i> .
	gt	Operator “greater” to compare the port with the specified <i>source-port</i> .
destination	<i>IP address</i>	The destination address in the header of IP-packet.
destination-mask	<i>IP-mask</i>	Mask to be applied to the destination address in the header of IP-packet before comparison with <i>destination</i> .

Argument	Value	Description
		There are two ways to enter the mask: in the canonical form (for example, 255.255.255.0) and in the form of prefix with bit length (for example, /24).
destination-port	<i>Integer</i>	Destination port in the <i>TCP</i> or <i>UDP</i> header.
destination-end-port	<i>Integer</i>	The end of the destination range of ports.
dst-port-operator	lt	Operator “less” to compare the port with the specified <i>destination-port</i> .
	eq	Operator “equal” to compare the port with the specified <i>destination-port</i> .
	gt	Operator “greater” to compare the port with the specified <i>destination-port</i> .

Example

```
(config-acl)> deny tcp 0.0.0.0/24 port eq 80 0.0.0.0/24 port ►
range 18 88
Network::Acl: Rule accepted.
```

```
(config-acl)> deny icmp 192.168.0.0 255.255.255.0 192.168.1.1 ►
255.255.255.0
Network::Acl: Rule accepted.
```

```
(config-acl)> no deny tcp 0.0.0.0/24 port eq 80 0.0.0.0/24 port ►
range 18 88
Network::Acl: Rule deleted.
```

```
(config-acl)> no deny icmp 192.168.0.0 255.255.255.0 192.168.1.1 ►
255.255.255.0
Network::Acl: Rule deleted.
```

History

Version	Description
2.00	The access-list deny command has been introduced.
2.06	New value ip was added to the protocol argument.
2.08	New protocols esp, gre and ipip were added.
2.09.A.2.1	Port ranges were added.

3.3.3 access-list permit

Description

Add a packet filtering permit rule into a specified *ACL*.

Command with **no** prefix removes the rule.

Prefix no

Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-acl)> permit (tcp | udp) <source> <source-mask>
[ port( ( <src-port-operator> <source-port> ) |
( range <source-port> <source-end-port> ) )]
<destination> <destination-mask>
[ port( ( <dst-port-operator> <destination-port> ) |
( range <destination-port> <destination-end-port> ) )]

(config-acl)> permit(icmp | esp | gre | ipip | ip)<source> <source-mask>
<destination> <destination-mask>

(config-acl)> no permit (tcp | udp) <source> <source-mask>
[ port( ( <src-port-operator> <source-port> ) |
( range <source-port> <source-end-port> ) )]
<destination> <destination-mask>
[ port( ( <dst-port-operator> <destination-port> ) |
( range <destination-port> <destination-end-port> ) )]

(config-acl)> no permit(icmp | esp | gre | ipip | ip)<source> <source-mask>
<destination> <destination-mask>
```

Arguments

Argument	Value	Description
tcp	Keyword	TCP protocol.
udp	Keyword	UDP protocol.
icmp	Keyword	ICMP protocol.
esp	Keyword	ESP protocol.
gre	Keyword	GRE protocol.
ipip	Keyword	IP in IP protocol.
ip	Keyword	IP protocol (include TCP , UDP , ICMP and other).
source	IP address	The source address in the header of IP-packet.
source-mask	IP-mask	Mask to be applied to the source address in the header of IP-packet before comparison with <i>source</i> . There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).
source-port	Integer	Source port in the TCP or UDP header.
source-end-port	Integer	The end of the source range of ports.
src-port-operator	lt	Operator "less" to compare the port with the specified <i>source-port</i> .

Argument	Value	Description
	eq	Operator “equal” to compare the port with the specified <i>source-port</i> .
	gt	Operator “greater” to compare the port with the specified <i>source-port</i> .
destination	<i>IP address</i>	The destination address in the header of IP-packet.
destination-mask	<i>IP-mask</i>	Mask to be applied to the destination address in the header of IP-packet before comparison with <i>destination</i> . There are two ways to enter the mask: in the canonical form (for example, 255.255.255.0) and in the form of prefix with bit length (for example, /24).
destination-port	<i>Integer</i>	Destination port in the <i>TCP</i> or <i>UDP</i> header.
destination-end-port	<i>Integer</i>	The end of the destination range of ports.
dst-port-operator	lt	Operator “less” to compare the port with the specified <i>destination-port</i> .
	eq	Operator “equal” to compare the port with the specified <i>destination-port</i> .
	gt	Operator “greater” to compare the port with the specified <i>destination-port</i> .

Example

```
(config-acl)> permit icmp 192.168.0.0 255.255.255.0 192.168.1.1 ►
255.255.255.0
Network::Acl: Rule accepted.
```

```
(config-acl)> permit tcp 0192.168.1.0/24 port eq 443 0.0.0.0/24 ►
port range 8080 9090
Network::Acl: Rule accepted.
```

```
(config-acl)> no permit icmp 192.168.0.0 255.255.255.0 ►
192.168.1.1 255.255.255.0
Network::Acl: Rule deleted.
```

```
(config-acl)> no permit tcp 0192.168.1.0/24 port eq 443 ►
0.0.0.0/24 port range 8080 9090
Network::Acl: Rule deleted.
```

History

Version	Description
2.00	The access-list permit command has been introduced.
2.06	New value ip was added to the protocol argument.
2.08	New protocols esp, gre and ipip were added.
2.09.A.2.1	Port ranges were added.

3.3.4 access-list rule

Description Disable, set operation time by schedule, change the order or set description for the [ACL](#) rule.

Command with **no** prefix enables the rule, removes schedule and description for [ACL](#) rule.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-acl)> rule <index> (disable | schedule <schedule> | order
<new-index> | description <description>)

(config-acl)> no rule <index> (disable | schedule | description)
```

Arguments

Argument	Value	Description
index	<i>Integer</i>	The ACL rule number.
disable	<i>Keyword</i>	Disable the ACL rule.
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.
order	<i>Integer</i>	New position of the ACL rule in the list.
description	<i>String</i>	The ACL rule description.

Example

```
(config-acl)> rule 0 disable
Network::Acl: Rule disabled.
```

```
(config-acl)> rule 0 schedule acl_schedule
Network::Acl: Rule schedule set to "acl_schedule".
```

```
(config-acl)> rule 0 description myacl
Network::Acl: Rule description set to "myacl".
```

```
(config-acl)> rule 0 order 1
Network::Acl: Rule 0 moved to position 1.
```

```
(config-acl)> no rule 0 disable
Network::Acl: Rule enabled.
```

```
(config-acl)> no rule 0 schedule
Network::Acl: Rule schedule removed.
```

```
(config-acl)> no rule 0 description
Network::Acl: Rule description removed.
```

History

Version	Description
2.08	The access-list rule command has been introduced.

3.4 afp

Description Access to a group of commands to manage [AFP](#) server service.

Prefix no No

Change settings No

Multiple input No

Group entry (config-afp)

Synopsis (config)> **afp**

Example (config)> **afp**
Core::Configurator: Done.
(config-afp)>

History

Version	Description
2.06	The afp command has been introduced.

3.4.1 afp automount

Description Enable automounting of USB storages to access via [AFP](#). By default, the function is enabled.

Command with **no** prefix disables the automounting function.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis (config-afp)> **automount**

(config-afp)> **no automount**

Example (config-afp)> **automount**
Afp::Server: Automount enabled.

(config-afp)> **no automount**
Afp::Server: Automount disabled.

History

Version	Description
2.06	The afp automount command has been introduced.

3.4.2 afp permissive

Description

Enable permissive mode, when all users can access the files on USB storage. By default, the setting is disabled.

Command with **no** prefix disables permissive mode, so access to the files have only users with "afp" tag.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-afp)> permissive
```

```
(config-afp)> no permissive
```

Example

```
(config-afp)> permissive
Afp::Server: Permissive mode enabled.
```

```
(config-afp)> no permissive
Afp::Server: Permissive mode disabled.
```

History

Version	Description
2.06	The afp permissive command has been introduced.

3.4.3 afp share

Description

Share directory on USB storage. By default, the timemachine attribute is enabled for all shares.

Command with **no** prefix removes share. If you use no argument, the entire list of shares will be removed.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-afp)> share <label> <mount> [ <description> ]
```

```
(config-afp)> no share [ <label> ]
```


Arguments

Argument	Value	Description
label	<i>String</i>	Share name for users.
mount	<i>String</i>	Name of root directory or name subdirectory to share.
description	<i>String</i>	Description of share.

Example

```
(config-afp)> share TEST MISC:/ timemachine
Afp::Server: Added share "TEST".
```

```
(config-afp)> share TEST MISC:/os/ timemachine
Afp::Server: Added share "TEST".
```

```
(config-afp)> no share TEST
Afp::Server: Removed share "TEST".
```

```
(config-afp)> no share
Afp::Server: All shares removed.
```

History

Version	Description
2.06	The afp share command has been introduced.
4.03	Argument timemachine was removed as obsolete.

3.5 cifs

Description

Access to a group of commands to manage *CIFS* service.

Prefix no

No

Change settings

No

Multiple input

No

Group entry

(config-cifs)

Synopsis

```
(config)> cifs
```

Example

```
(config)> cifs
Core::Configurator: Done.
(config-cifs)>
```

History

Version	Description
2.00	The cifs command has been introduced.

3.5.1 cifs automount

Description Enable automounting of USB storages to access via [CIFS](#). By default, the function is enabled.

Command with **no** prefix disables the automounting function.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-cifs)> automount
(config-cifs)> no automount
```

Example

```
(config-cifs)> automount
Cifs::ServerTsmb: Automount enabled.
```

```
(config-cifs)> no automount
Cifs::ServerTsmb: Automount disabled.
```

History

Version	Description
2.00	The cifs automount command has been introduced.

3.5.2 cifs map-hidden

Description Enable [ACL](#) and hidden files support for [CIFS](#). By default, the feature is disabled.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-cifs)> map-hidden
(config-cifs)> no map-hidden
```

Example

```
(config-cifs)> map-hidden
Cifs::ServerTsmb: Map hidden enabled.
```

```
(config-cifs)> no map-hidden
Cifs::ServerTsmb: Map hidden enabled.
```

History	Version	Description
	2.14	The cifs map-hidden command has been introduced.

3.5.3 cifs master

Description Enable *Master Browser* function for TSMB server. By default, the setting is enabled.

Command with **no** prefix disables *Master Browser* function.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-cifs)> master
(config-cifs)> no master
```

Example

```
(config-cifs)> master
Cifs::ServerTsmb: Master browser enabled.
```

```
(config-cifs)> no master
Cifs::ServerTsmb: Master browser disabled.
```

History	Version	Description
	2.00	The cifs master command has been introduced.
	2.04	The cifs master command was removed as obsolete.
	3.03	The cifs master command has been returned.

3.5.4 cifs permissive

Description Enable permissive mode, when all users can access the files on USB storage. By default, the setting is disabled.

Command with **no** prefix disables permissive mode, so access to the files have only users with "cifs" tag.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-cifs)> permissive
(config-cifs)> no permissive
```

Example

```
(config-cifs)> permissive
Cifs::ServerTsmB: Permissive mode enabled.
```

```
(config-cifs)> no permissive
Cifs::ServerTsmB: Permissive mode disabled.
```

History

Version	Description
2.00	The cifs permissive command has been introduced.

3.5.5 cifs share

Description

Share directory on USB storage.

Command with **no** prefix removes share. If you use no argument, the entire list of shares will be removed.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-cifs)> share <label> <mount> [ <description> ]
```

```
(config-cifs)> no share [ <label> ]
```

Arguments

Argument	Value	Description
label	<i>String</i>	Share name, that users will see.
mount	<i>String</i>	Name of directory to share.
description	<i>String</i>	Description of share.

Example

```
(config-cifs)> share MYHOME1 10A0CDE9A0CDD4FE:/
Cifs::ServerTsmB: Added share "MYHOME1".
```

```
(config-cifs)> share MYHOME 10A0CDE9A0CDD4FE:/Video/
Cifs::ServerTsmB: Added share "MYHOME".
```

```
(config-cifs)> no share MYHOME1
Cifs::ServerTsmB: Removed share "MYHOME1".
```

History

Version	Description
2.00	The cifs share command has been introduced.

3.6 cloud control2 security-level

Description Set Cloud Control2 service security level for Keenetic mobile application. By default, public value is set.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(config)> cloud control2 security-level (public | private)`

Arguments

Argument	Value	Description
public	<i>Keyword</i>	Access to the Cloud Control2 is allowed for public, private and protected interfaces.
private	<i>Keyword</i>	Access to the Cloud Control2 is allowed for private interfaces only.

Example

```
(config)> cloud control2 security-level public
CloudControl2::Agent: Security level changed to public.
```

```
(config)> cloud control2 security-level private
CloudControl2::Agent: Security level changed to private.
```

History

Version	Description
3.05	The cloud control2 security-level command has been introduced.

3.7 components

Description Access to a group of commands to manage firmware components.

Prefix no No

Change settings No

Multiple input No

Group entry (config-comp)

Synopsis `(config)> components`

History

Version	Description
2.00	The components command has been introduced.

3.7.1 components auto-update channel

Description Set source of components for auto-update feature. By default, value `stable` is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-comp)> auto-update channel <channel>
(config-comp)> no auto-update channel
```

Arguments

Argument	Value	Description
channel	stable	Components have been fully tested and recommended for installation. The web interface specifies this channel as Main.
	preview	Components contain the latest features and enhancements, but have not been fully tested yet. The web interface specifies this channel as Preview.
	draft	The components contain the latest features and are used for testing. The web interface specifies this channel as Dev.

Example

```
(config-comp)> auto-update channel preview
Components::Manager: Auto-update channel is "preview".
```

```
(config-comp)> no auto-update channel
Components::Manager: Reset an auto-update channel to default.
```

History

Version	Description
3.01	The components auto-update channel command has been introduced.

3.7.2 components auto-update disable

Description Components auto-update function. By default, automatic update is enabled.
Command with **no** prefix enables auto-update.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-comp)> auto-update disable
(config-comp)> no auto-update disable
```

Example

```
(config-comp)> auto-update disable
Components::Manager: Components auto-update disabled.

(config-comp)> no auto-update disable
Components::Manager: Components auto-update enabled.
```

History	Version	Description
	2.09	The components auto-update disable command has been introduced.

3.7.3 components auto-update schedule

Description Assign a schedule for the auto-update operation. Schedule must be created and customized with [schedule action](#) command before execution.

Command with **no** prefix unbinds the schedule.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-comp)> auto-update schedule <schedule>
(config-comp)> no auto-update schedule
```

Arguments	Argument	Value	Description
	schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(config-comp)> auto-update schedule Update
Components::Manager: Set auto-update schedule "Update".
```

```
(config-comp)> no auto-update schedule
Components::Manager: Schedule disabled.
```

History	Version	Description
	3.03	The components auto-update schedule command has been introduced.

3.7.4 components check-update

Description Check the firmware updates for the candidate or member of Modular Wi-Fi System.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config-comp)> check-update [ force ]`

Arguments

Argument	Value	Description
force	<i>Keyword</i>	Check for updates constantly.

Example

```
(config-comp)> check-update

release: 2.15.A.3.0-2
  sandbox: draft
  timestamp: Dec 17 18:58:55
  valid: no
```

```
(config-comp)> check-update force

release: 2.15.A.3.0-2
  sandbox: draft
  timestamp: Dec 17 18:58:55
  valid: no
```

History

Version	Description
2.14	The components check-update command has been introduced.

3.7.5 components commit

Description Apply the changes made by [components install](#) and [components remove](#) commands.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(config-comp)> commit`

History	Version	Description
	2.00	The components commit command has been introduced.

3.7.6 components install

Description Mark component to install. Final installation carried out with **components commit** command.

Prefix no No

Change settings Yes

Multiple input Yes

Synopsis `(config-comp)> install <component>`

Arguments	Argument	Value	Description
	component	<i>String</i>	Component name. List of available components for installation can be displayed with the components list command.

Example `(config-comp)> install ntfs`
Components::Manager: Component "ntfs" is queued for installation.

History	Version	Description
	2.00	The components install command has been introduced.

3.7.7 components list

Description Switch to the selected sandbox and mark for installation all the components that require changes to match the version in the sandbox. If you use no argument, the entire list of all components for current sandbox (installed and available) will be displayed. If there is no Internet connection, only the list of installed components will be displayed.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config-comp)> list [ sandbox ]`

Arguments	Argument	Value	Description
	sandbox	<i>String</i>	Remote sandbox, such as stable or beta.

Example

```
(config-comp)> list

    firmware:
        version: 2.13.C.0.0-1

    sandbox: stable

    local:
        sandbox: beta

    component:
        name: base

        priority: optional
        size: 35233
        version: 2.13.C.0.0-1
        hash: f65428af2a6fd636db779370deb58f40
        installed: 2.13.B.1.0-1

        preset: minimal
        preset: recommended
        queued: yes

    ...
```

History

Version	Description
2.00	The components list command has been introduced.
2.06.A.6	The <i>sandbox</i> parameter has been introduced. The command components list should be used in favour of components sync .

3.7.8 components preset

Description

Select a predefined set of components. Installation of preset is carried out with **components commit** command.

Before preset installation check the latest versions of components on the update server with **components list** command. Internet connection is required.

Prefix no

No

Change settings

Yes

Multiple input

No

Synopsis

```
(config-comp)>  preset <preset>
```

Arguments

Number and names of presets can be changed, so check the list of available presets with help of **preset [Tab]** command.

Argument	Value	Description
preset	minimal	Minimal set of components will be marked.
	recommended	Recommended set of components will be marked for installation.

Example

```
(config-comp)> preset [Tab]
```

```
Usage template:
  preset {preset}
```

```
Choose:
  minimal
  recommended
```

```
(config-comp)> preset recommended
```

```
lib::libndmComponents error[268369922]: updates are available ►
for this system.
```

```
(config-comp)> commit
```

```
Components::Manager: Update task started.
```

History

Version	Description
2.00	The components preset command has been introduced.

3.7.9 components preview

Description Show size of firmware as current set of components selected with **components install** command.

Prefix no No

Change settings Yes

Multiple input No

Synopsis (config-comp)> **preview**

Example (config-comp)> **preview**

```
preview:
  size: 7733308
```

History

Version	Description
2.06	The components preview command has been introduced.

3.7.10 components remove

Description Mark component to remove. Final removal carried out with **components commit** command.

Prefix no No

Change settings Yes

Multiple input Yes

Synopsis `(config-comp)> remove <component>`

Arguments

Argument	Value	Description
component	<i>String</i>	Component name. List of available components for removal can be displayed with the components list command.

Example

```
(config-comp)> remove ntfs
Components::Manager: Component "ntfs" is queued for removal.
```

History

Version	Description
2.00	The components remove command has been introduced.

3.7.11 components validity-period

Description Set a validity period of a local component list. After this time the command **components list** will be automatically executed to get actual list of components from update server. By default, value 1800 is used.

Command with **no** prefix resets period to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(config-comp)> validity-period <seconds>`

`(config-comp)> no validity-period`

Arguments

Argument	Value	Description
seconds	<i>Integer</i>	Validity period of a local component list in seconds. Can take values in the range from 0 to 604800 inclusively.

Example

```
(config-comp)> validity-period 500
Components::Manager: Validity period set to 500 seconds.
```

```
(config-comp)> no validity-period
Components::Manager: Validity period reset to 1800 seconds.
```

History	Version	Description
	2.03	The components validity-period command has been introduced.

3.8 crypto engine

Description Select the type of *ESP* packets processing with *IPsec*.
Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> crypto engine <type>
```

```
(config)> no crypto engine
```

Arguments	Argument	Value	Description
	type	software	Software mode.

Example

```
(config)> crypto engine software
IpSec::CryptoEngineManager: IPsec crypto engine set to "software".
```

```
(config)> no crypto engine
IpSec::CryptoEngineManager: IPsec crypto engine was disabled.
```

History	Version	Description
	2.06	The crypto engine command has been introduced.

3.9 crypto ike key

Description Add *IKE* key with remote side ID.
Command with **no** prefix removes specified key.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config)> crypto ike key <name> <psk> (<type> <id> | any)
```

```
(config)> no crypto ike key <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Name of the key. Latin letters, numbers, dots, hyphens and underscores are acceptable.
psk	<i>String</i>	Password for authentication. Password length can be from 6 to 96 characters.
type	address	ID type is IP address.
	fqdn	ID type is full domain name.
	dn	ID type is domain name.
	email	ID type is e-mail address.
id	<i>String</i>	Value of the remote side ID.
any	<i>Keyword</i>	Allow the key usage for any remote side.

Example

```
(config)> crypto ike key VirtualIPServer ▶  
adjs0C1gvWCs0iE4Ijhs+HRnNPiheGA478 any  
IpSec::Manager: "VirtualIPServer": crypto ike key successfully ▶  
added.
```

```
(config)> crypto ike key VirtualIPServer ▶  
adjs0C1gvWCs0iE4Ijhs+HRnNPiheGA478R4M6d4+054LLihe any  
IpSec::Manager: "VirtualIPServer": crypto ike key successfully ▶  
updated.
```

```
(config)> no crypto ike key VirtualIPServer  
IpSec::Manager: "VirtualIPServer": crypto ike key successfully ▶  
removed.
```

History

Version	Description
2.06	The crypto ike key command has been introduced.

3.10 crypto ike mtu

Description Set the *MTU* value to be transmitted to *IKE*. By default, the *MTU* value is inherited from the interface through which the Internet is accessed.

Command with **no** prefix resets the *MTU* value to default.

Prefix no Yes

Change settings	Yes						
Multiple input	No						
Synopsis	(config)> crypto ike mtu <i>(value)</i> (config)> no crypto ike mtu						
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td>value</td><td><i>Integer</i></td><td><i>MTU</i> value. Can take values in the range from 576 to 1500 inclusively.</td></tr></table>	Argument	Value	Description	value	<i>Integer</i>	<i>MTU</i> value. Can take values in the range from 576 to 1500 inclusively.
Argument	Value	Description					
value	<i>Integer</i>	<i>MTU</i> value. Can take values in the range from 576 to 1500 inclusively.					
Example	(config)> crypto ike mtu 1400 IpSec::Manager: IKE MTU value is set to 1400. (config)> no crypto ipsec mtu IpSec::Manager: Reset IKE MTU value.						
History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>3.08</td><td>The crypto ike mtu command has been introduced.</td></tr></table>	Version	Description	3.08	The crypto ike mtu command has been introduced.		
Version	Description						
3.08	The crypto ike mtu command has been introduced.						

3.11 crypto ike nat-keepalive

Description	Set the timeout between keepalive packets in case of NAT between the client and server <i>IPsec</i> . By default, 20 value is set. Command with no prefix resets setting to default.						
Prefix no	Yes						
Change settings	Yes						
Multiple input	No						
Synopsis	<pre>(config)> crypto ike nat-keepalive <nat-keepalive></pre> <pre>(config)> no crypto ike nat-keepalive</pre>						
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td>nat-keepalive</td><td>Integer</td><td>Timeout between keepalive packets in seconds. Can take values in the range from 5 to 3600 inclusively.</td></tr></table>	Argument	Value	Description	nat-keepalive	Integer	Timeout between keepalive packets in seconds. Can take values in the range from 5 to 3600 inclusively.
Argument	Value	Description					
nat-keepalive	Integer	Timeout between keepalive packets in seconds. Can take values in the range from 5 to 3600 inclusively.					
Example	<pre>(config)> crypto ike nat-keepalive 90</pre> IpSec::Manager: Set crypto ike nat-keepalive timeout to 90 s.						

```
(config)> no crypto ike nat-keepalive
IpSec::Manager: Reset crypto ike nat-keepalive timeout to 20 s.
```

History

Version	Description
2.06	The crypto ike nat-keepalive command has been introduced.

3.12 crypto ike policy

Description

Access to a group of commands to configure selected *IKE* policy. If *IKE* policy is not found, the command tries to create it.

Command with **no** prefix removes *IKE* policy. At the same time references to this *IKE* policy are automatically deleted from all *IPsec* profiles.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Group entry

(config-ike-policy)

Synopsis

```
(config)> crypto ike policy <name>
```

```
(config)> no crypto ike policy <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	<i>IKE</i> policy name. Latin letters, numbers, dots, hyphens and underscores are acceptable.

Example

```
(config)> crypto ike policy test
IpSec::Manager: "test": crypto ike policy successfully created.
```

```
(config)> no crypto ike policy test
IpSec::Manager: Crypto ike policy "test" removed.
```

History

Version	Description
2.06	The crypto ike policy command has been introduced.

3.12.1 crypto ike policy lifetime

Description

Set lifetime of *IPsec IKE* association. By default, the value 86400 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ike-policy)> lifetime lifetime
(config-ike-policy)> no lifetime
```

Arguments

Argument	Value	Description
lifetime	<i>Integer</i>	Lifetime of <i>IPsec IKE</i> association in seconds. Can take values in the range from 60 to 2147483647.

Example

```
(config-ike-policy)> lifetime 3600
IpSec::Manager: "test": crypto ike policy lifetime set to 3600 s.
```

```
(config-ike-policy)> no lifetime
IpSec::Manager: "test": crypto ike policy lifetime reset.
```

History

Version	Description
2.06	The crypto ike policy lifetime command has been introduced.

3.12.2 crypto ike policy mode

Description Set *IKE* protocol version. By default, the value ikev1 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ike-policy)> mode mode
(config-ike-policy)> no mode
```

Arguments

Argument	Value	Description
mode	ikev1	Protocol version IKEv1.
	ikev2	Protocol version IKEv2.

Example

```
(config-ike-policy)> mode ikev2
IpSec::Manager: "test": crypto ike policy mode set to "ikev2".
```

```
(config-ike-policy)> no mode
IpSec::Manager: "test": crypto ike policy mode reset.
```

History

Version	Description
2.06	The crypto ike policy mode command has been introduced.

3.12.3 crypto ike policy negotiation-mode

Description

Set exchange mode for IKEv1 (see [crypto ike policy mode](#) command). By default, the value main is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ike-policy)> negotiation-mode <negotiation-mode>
```

```
(config-ike-policy)> no negotiation-mode
```

Arguments

Argument	Value	Description
negotiation-mode	main	Main mode, protects the identity of the peers.
	aggressive	Aggressive mode, does not protect the identity of the peers.

Example

```
(config-ike-policy)> negotiation-mode aggressive
IpSec::Manager: "test": crypto ike policy negotiation-mode set ►
to "aggressive".
```

```
(config-ike-policy)> no negotiation-mode
IpSec::Manager: "test": crypto ike policy negotiation-mode reset.
```

History

Version	Description
2.06	The crypto ike policy negotiation-mode command has been introduced.

3.12.4 crypto ike policy proposal

Description

Add reference on existing [IKE](#) proposal to [IKE](#) policy. The order of adding has a value for data exchange on the [IKE](#) protocol.

Command with **no** prefix removes reference on *IKE* proposal.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ike-policy)> proposal <proposal>
(config-ike-policy)> no proposal <proposal>
```

Arguments

Argument	Value	Description
proposal	String	<i>IKE</i> proposal name. Latin letters, numbers, dots, hyphens and underscores are acceptable.

Example

```
(config-ike-policy)> proposal test
IpSec::Manager: "test": crypto ike proposal "test" successfully ►
added.
```

```
(config-ike-policy)> no proposal
IpSec::Manager: "test": crypto ike policy proposal "test" ►
successfully removed.
```

History

Version	Description
2.06	The crypto ike policy proposal command has been introduced.

3.13 crypto ike proposal

Description

Access to a group of commands to configure selected *IKE* proposal. If *IKE* proposal is not found, the command tries to create it.

A full list of encryption algorithms implemented in the system is provided in the [Appendix](#).

Command with **no** prefix removes *IKE* proposal. At the same time references to this *IKE* proposal are automatically deleted from all *IKE* policy.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry (config-ike-proposal)

Synopsis

```
(config)> crypto ike proposal <name>
```

```
(config)> no crypto ike proposal <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	<i>IKE</i> proposal name. Latin letters, numbers, dots, hyphens and underscores are acceptable.

Example

```
(config)> crypto ike proposal test
IpSec::Manager: "test": crypto ike proposal successfully created.
```

```
(config)> no crypto ike proposal test
IpSec::Manager: Crypto ike proposal "test" removed.
```

History

Version	Description
2.06	The crypto ike proposal command has been introduced.

3.13.1 crypto ike proposal aead

Description Enable *AEAD* cypher mode on *IKE* proposal.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(config-ike-proposal)> aead
```

Example

```
(config-ike-proposal)> aead
IpSec::Manager: "TEST": crypto ike proposal "TEST" enabled AEAD mode.
```

History

Version	Description
3.05	The crypto ike proposal aead command has been introduced.

3.13.2 crypto ike proposal dh-group

Description Add the selected *DH* group to *IKE* proposal to work in the *PFS* mode. The order of adding has a value for data exchange on the *IKE* protocol.

Command with **no** prefix removes the selected group.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ike-proposal)> dh-group <dh-group>
```

```
(config-ike-proposal)> no dh-group <dh-group>
```

Arguments

Argument	Value	Description
dh-group	1	<i>DH</i> group to work in the <i>PFS</i> mode.
	2	
	5	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	25	
	26	
	31	
	32	

Example

```
(config-ike-proposal)> dh-group 14
IpSec::Manager: "test": crypto ike proposal DH group "14" ►
successfully added.
```

```
(config-ike-proposal)> no dh-group 14
IpSec::Manager: "test": crypto ike proposal "test" group type ►
successfully removed.
```

History

Version	Description
2.06	The crypto ike proposal dh-group command has been introduced.

3.13.3 crypto ike proposal encryption

Description

Add the selected type of encryption to *IKE* proposal. The order of adding has a value for data exchange on the *IKE* protocol.

Command with **no** prefix removes the selected type of encryption.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ike-proposal)> encryption <encryption>
(config-ike-proposal)> no encryption <encryption>
```

Arguments

Argument	Value	Description
encryption	des	Type of <i>IKE</i> encryption.
	3des	
	aes-cbc-128	
	aes-cbc-192	
	aes-cbc-256	
	aes-ctr-128	
	aes-ctr-192	
	aes-ctr-256	

Example

```
(config-ike-proposal)> encryption des
IpSec::Manager: "test": crypto ike proposal encryption algorithm ►
"des" added.
```

```
(config-ike-proposal)> no encryption des
IpSec::Manager: "test": crypto ike proposal "test" encryption ►
type successfully removed.
```

History

Version	Description
2.06	The crypto ike proposal encryption command has been introduced.

3.13.4 crypto ike proposal integrity

Description Add the selected value of *HMAC* signature algorithm to *IKE* proposal. The order of adding has a value for data exchange on the *IKE* protocol.

Command with **no** prefix removes the selected algorithm.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ike-proposal)> integrity <integrity>
```

```
(config-ike-proposal)> no integrity <integrity>
```

Arguments

Argument	Value	Description
integrity	md5	HMAC signature algorithm of IKE messages.
	sha1	
	sha256	
	sha384	
	sha512	

Example

```
(config-ike-proposal)> integrity sha256
IpSec::Manager: "test": crypto ike proposal integrity algorithm ►
"sha256" successfully added.
```

```
(config-ike-proposal)> no integrity sha256
IpSec::Manager: "test": crypto ike proposal "test" integrity ►
type successfully removed.
```

History

Version	Description
2.06	The crypto ike proposal integrity command has been introduced.

3.13.5 crypto ike proposal prf

Description

Add the selected [PRF](#) group to [IKE](#) proposal.

Command with **no** prefix removes the selected algorithm.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-ike-proposal)> prf <prf>
```

```
(config-ike-proposal)> no prf <prf>
```

Arguments

Argument	Value	Description
prf	md5	HMAC signature algorithm of IKE messages.
	sha1	
	aes-xcbc	
	sha256	

Argument	Value	Description
	sha384	
	sha512	
	aes-cmac	

Example

```
(config-ike-proposal)> prf sha256
IpSec::Manager: "TEST": crypto ike proposal prf algorithm ►
"sha256" successfully added.
```

```
(config-ike-proposal)> no prf sha256
IpSec::Manager: "TEST": crypto ike proposal "TEST" prf type ►
successfully removed.
```

History

Version	Description
3.05	The crypto ike proposal prf command has been introduced.

3.14 crypto ipsec incompatible

Description

Disable *IPsec* tunnels compatibility checking. By default, the setting is disabled.

Command with **no** prefix enables the checking back.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> crypto ipsec incompatible
```

```
(config)> no crypto ipsec incompatible
```

Example

```
(config)> crypto ipsec incompatible
IpSec::Manager: Compatibility checks is disabled.
```

```
(config)> no crypto ipsec incompatible
IpSec::Manager: Compatibility checks is enabled.
```

History

Version	Description
2.10	The crypto ipsec incompatible command has been introduced.

3.15 crypto ipsec profile

Description Access to a group of commands to configure selected *IPsec* profile. If profile is not found, the command tries to create it.

Command with **no** prefix removes profile. At the same time references to this profile are automatically deleted from all *IPsec* crypto maps.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry (config-ipsec-profile)

Synopsis

```
(config)>  crypto ipsec profile <name>
(config)> no crypto ipsec profile <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	<i>IPsec</i> profile name. Latin letters, numbers, dots, hyphens and underscores are acceptable.

Example

```
(config)> crypto ipsec profile test
IpSec::Manager: "test": crypto ipsec profile successfully created.

(config)> no crypto ipsec profile test
IpSec::Manager: Crypto ipsec profile "test" removed.
```

History

Version	Description
2.06	The crypto ipsec profile command has been introduced.

3.15.1 crypto ipsec profile authentication-local

Description Set authentication type for local host. By default, value pre-share is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ipsec-profile)>  authentication-local <auth>
```

```
(config-ipsec-profile)> no authentication-local
```

Arguments

Argument	Value	Description
auth	pre-share	A single available type of authorization for now.

Example

```
(config-ipsec-profile)> authentication-local pre-share
IpSec::Manager: "test": crypto ipsec profile authentication-local ►
type "pre-share" is set.
```

```
(config-ipsec-profile)> no authentication-local
IpSec::Manager: "test": crypto ipsec profile authentication-local ►
reset.
```

History

Version	Description
2.06	The crypto ipsec profile authentication-local command has been introduced.

3.15.2 crypto ipsec profile authentication-remote

Description Set authentication type for remote host. By default, value pre-share is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ipsec-profile)> authentication-remote <auth>
```

```
(config-ipsec-profile)> no authentication-remote
```

Arguments

Argument	Value	Description
auth	pre-share	A single available type of authorization for now.

Example

```
(config-ipsec-profile)> authentication-remote pre-share
IpSec::Manager: "test": crypto ipsec profile ►
authentication-remote type "pre-share" is set.
```

```
(config-ipsec-profile)> no authentication-remote
IpSec::Manager: "test": crypto ipsec profile ►
authentication-remote reset.
```

History	Version	Description
	2.06	The crypto ipsec profile authentication-remote command has been introduced.

3.15.3 crypto ipsec profile dpd-clear

Description Set method of action when detecting a dead *IKE* peer. By default, the setting is enabled, which means deleting peer information.

Command with **no** prefix set action to restart.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ipsec-profile)> dpd-clear
(config-ipsec-profile)> no dpd-clear
```

Example

```
(config-ipsec-profile)> dpd-clear
IpSec::Manager: "VPNL2TPServer": crypto ipsec profile DPD action ►
set to "clear".

(config-ipsec-profile)> no dpd-clear
IpSec::Manager: "VPNL2TPServer": crypto ipsec profile DPD action ►
set to "restart".
```

History	Version	Description
	2.11	The crypto ipsec profile dpd-clear command has been introduced.

3.15.4 crypto ipsec profile dpd-interval

Description Set parameters of method to detect a dead *IKE* peer. By default, interval is set to 30, retry-count is set to 3.

Command with **no** prefix resets settings to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ipsec-profile)> dpd-interval <interval> [retry-count]
```

```
(config-ipsec-profile)> no dpd-interval
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	The interval of sending <i>DPD</i> packets in seconds. Can take values in the range from 2 to 3600.
retry-count	<i>Integer</i>	Number of attempts to send <i>DPD</i> packets. Can take values in the range from 3 to 60.

Example

```
(config-ipsec-profile)> dpd-interval 5 30
IpSec::Manager: "test": crypto ipsec profile dpd retry count is ►
set to 30.
```

```
(config-ipsec-profile)> no dpd-interval
IpSec::Manager: "test": crypto ipsec profile dpd retry count ►
reset.
```

History

Version	Description
2.06	The crypto ipsec profile dpd-interval command has been introduced.

3.15.5 crypto ipsec profile identity-local

Description

Set a local identifier of *IPsec* profile.

Command with **no** prefix removes the local identifier.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ipsec-profile)> identity-local <type> <id>
```

```
(config-ipsec-profile)> no identity-local
```

Arguments

Argument	Value	Description
type	address	ID type is IP address.
	fqdn	ID type is full domain name.
	dn	ID type is domain name.
	email	ID type is e-mail address.
id	<i>String</i>	Local ID value.

Example

```
(config-ipsec-profile)> identity-local address 10.10.10.5
IpSec::Manager: "test": crypto ipsec profile identity-local is ►
set to "10.10.10.5" with type "address".
```

```
(config-ipsec-profile)> no identity-local
IpSec::Manager: "test": crypto ipsec profile identity-local reset.
```

History

Version	Description
2.06	The crypto ipsec profile identity-local command has been introduced.

3.15.6 crypto ipsec profile match-identity-remote

Description

Set remote host identifier for *IPsec* profile.

Command with **no** prefix removes remote host ID.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ipsec-profile)> match-identity-remote ( <type> <id> | any )
```

```
(config-ipsec-profile)> no match-identity-remote
```

Arguments

Argument	Value	Description
type	address	ID type is IP address.
	fqdn	ID type is full domain name.
	dn	ID type is domain name.
	email	ID type is e-mail address.
id	<i>String</i>	Remote host ID value.
any	<i>Keyword</i>	Allow usage of any remote host.

Example

```
(config-ipsec-profile)> match-identity-remote any
IpSec::Manager: "test": crypto ipsec profile ►
match-identity-remote is set to any.
```

```
(config-ipsec-profile)> no match-identity-remote
IpSec::Manager: "test": crypto ipsec profile ►
match-identity-remote reset.
```

History

Version	Description
2.06	The crypto ipsec profile match-identity-remote command has been introduced.

3.15.7 crypto ipsec profile mode

Description Set the mode of operation *IPsec*. By default, tunnel value is set.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ipsec-profile)> mode mode
(config-ipsec-profile)> no mode
```

Arguments

Argument	Value	Description
mode	tunnel	Tunnel mode, when the entire IP packet is encrypted and/or authenticated.
	transport	Transport mode, when only the payload of the IP packet is encrypted and/or authenticated.

Example

```
(config-ipsec-profile)> mode transport
IpSec::Manager: "test": crypto ipsec profile mode set to ►
"transport".
```

```
(config-ipsec-profile)> no mode
IpSec::Manager: "test": crypto ipsec profile mode reset.
```

History

Version	Description
2.06	The crypto ipsec profile mode command has been introduced.

3.15.8 crypto ipsec profile policy

Description Set the reference to existing *IKE* policy (see [crypto ike policy](#) command).

Command with **no** prefix removes the reference.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ipsec-profile)> policy policy
```

```
(config-ipsec-profile)> no policy
```

Arguments

Argument	Value	Description
policy	<i>String</i>	<i>IKE</i> policy name. You can see the list of available policies with help of policy [Tab] command.

Example

```
(config-ipsec-profile)> policy [Tab]
Usage template:
    policy {name: {A-Z, a-z, 0-9, ., _, -}}
```

```
Choose:
VirtualIPServer
VPNL2TPServer
```

```
(config-ipsec-profile)> policy VirtualIPServer
IpSec::Manager: "TEST": crypto ipsec profile policy set to ►
"VirtualIPServer".
```

```
(config-ipsec-profile)> no policy
IpSec::Manager: "test": crypto ipsec profile policy reset.
```

History

Version	Description
2.06	The crypto ipsec profile policy command has been introduced.

3.15.9 crypto ipsec profile preshared-key

Description

Set pre-shared key for *IPsec* profile.

Command with **no** prefix removes pre-shared key.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ipsec-profile)> preshared-key <preshare-key>
```

```
(config-ipsec-profile)> no preshared-key
```

Arguments

Argument	Value	Description
preshare-key	<i>String</i>	Pre-shared key value.

Example

```
(config-ipsec-profile)> preshared-key testkey
IpSec::Manager: "test": crypto ipsec profile preshared key was ►
set.
```

```
(config-ipsec-profile)> no preshared-key
IpSec::Manager: "test": crypto ipsec profile preshared key reset.
```

History

Version	Description
2.06	The crypto ipsec profile preshared-key command has been introduced.

3.15.10 crypto ipsec profile xauth

Description

Enable additional authentication [XAuth](#) for IKEv1 mode. By default, function is disabled.

Command with **no** prefix disables additional authentication.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ipsec-profile)> xauth <type>
```

```
(config-ipsec-profile)> no xauth
```

Arguments

Argument	Value	Description
type	client	Client mode.
	server	Server mode.

Example

```
(config-ipsec-profile)> xauth client
IpSec::Manager: "test": crypto ipsec profile xauth set to ►
"client".
```

```
(config-ipsec-profile)> no xauth
IpSec::Manager: "test": crypto ipsec profile xauth is disabled.
```

History

Version	Description
2.06	The crypto ipsec profile xauth command has been introduced.

3.15.11 crypto ipsec profile xauth-identity

Description

Set login for additional authentication [XAuth](#) in client mode.

Command with **no** prefix removes the login.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ipsec-profile)> xauth-identity <identity>
(config-ipsec-profile)> no xauth-identity
```

Arguments

Argument	Value	Description
identity	<i>String</i>	Login for <i>XAuth</i> client mode.

Example

```
(config-ipsec-profile)> xauth-identity ident
IpSec::Manager: "test": crypto ipsec profile xauth-identity is ►
set to "ident".
```

```
(config-ipsec-profile)> no xauth-identity
IpSec::Manager: "test": crypto ipsec profile xauth identity is ►
deleted.
```

History

Version	Description
2.06	The crypto ipsec profile xauth-identity command has been introduced.

3.15.12 crypto ipsec profile xauth-password

Description Set password for additional authentication *XAuth* in client mode.

Command with **no** prefix removes the password.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ipsec-profile)> xauth-password <password>
(config-ipsec-profile)> no xauth-password
```

Arguments

Argument	Value	Description
password	<i>String</i>	Password for <i>XAuth</i> client mode.

Example

```
(config-ipsec-profile)> xauth-password password
IpSec::Manager: "test": crypto ipsec profile xauth-password is ►
set.
```

```
(config-ipsec-profile)> no xauth-password
IpSec::Manager: "test": crypto ipsec profile xauth password is ►
deleted.
```

History

Version	Description
2.06	The crypto ipsec profile xauth-password command has been introduced.

3.16 crypto ipsec rekey delete-delay

Description

Set interval before removing the IKE SA after receiving the DELETE command from the remote side. By default, the 10 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> crypto ipsec rekey delete-delay <delay>
```

```
(config)> no crypto ipsec rekey delete-delay
```

Arguments

Argument	Value	Description
delay	<i>Integer</i>	Delay value in seconds. Can take value in the range from 1 to 60.

Example

```
(config)> crypto ipsec rekey delete-delay 1
IpSec::Manager: Rekey delete-delay value is set to 1.
```

```
(config)> no crypto ipsec rekey delete-delay
IpSec::Manager: Rekey delete-delay value is set to 10.
```

History

Version	Description
2.11	The crypto ipsec rekey delete-delay command has been introduced.

3.17 crypto ipsec rekey make-before

Description Set the mode when new IKE SA creates before the breaking the old one. By default, the feature is disabled.

Command with **no** prefix disables the mode.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> crypto ipsec rekey make-before
(config)> no crypto ipsec rekey make-before
```

Example

```
(config)> crypto ipsec rekey make-before
IpSec::Manager: Enable make-before-brake scheme for IKEv2 rekey.

(config)> no crypto ipsec rekey make-before
IpSec::Manager: Disable make-before-brake scheme for IKEv2 rekey.
```

History

Version	Description
2.11	The crypto ipsec rekey make-before command has been introduced.

3.18 crypto ipsec transform-set

Description Access to a group of commands to configure selected *IPsec ESP* transformation during Phase 2. If transformation is not found, the command tries to create it.

Command with **no** prefix removes transformation. At the same time references to this transformation are automatically deleted from all *IPsec* crypto maps.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry (config-ipsec-transform)

Synopsis

```
(config)> crypto ipsec transform-set <name>
(config)> no crypto ipsec transform-set <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	<i>IPsec</i> transformation name. Latin letters, numbers, dots, hyphens and underscores are acceptable.

Example

```
(config)> crypto ipsec transform-set test
IpSec::Manager: "test": crypto ipsec transform-set successfully ►
created.
```

```
(config)> no crypto ipsec transform-set test
IpSec::Manager: Crypto ipsec transform-set "test" removed.
```

History

Version	Description
2.06	The crypto ipsec transform-set command has been introduced.

3.18.1 crypto ipsec transform-set aead

Description Enable *AEAD* cypher mode on *IPsec*.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config-ipsec-transform)> aead`

Example

```
(config-ipsec-transform)> dh-group 14
IpSec::Manager: "TEST": crypto ipsec transform-set "TEST" enabled ►
AEAD mode.
```

History

Version	Description
3.05	The crypto ipsec transform-set aead command has been introduced.

3.18.2 crypto ipsec transform-set cypher

Description Add the selected type of encryption to *IPsec* transformation. The order of adding has a value for data exchange on the *IKE* protocol.

Command with **no** prefix removes the selected type of encryption.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ipsec-transform)> cypher <cypher>
```

```
(config-ipsec-transform)> no cypher <cypher>
```

Arguments

Argument	Value	Description
cypher	esp-des	Type of <i>IPsec ESP</i> encryption.
	esp-3des	
	esp-aes-128	
	esp-aes-192	
	esp-aes-256	

Example

```
(config-ipsec-transform)> cypher esp-3des
IpSec::Manager: "test": crypto ipsec transform-set cypher ►
"esp-3des" successfully added.
```

```
(config-ipsec-transform)> no cypher esp-3des
IpSec::Manager: "test": crypto ipsec transform-set "test" cypher ►
successfully removed.
```

History

Version	Description
2.06	The crypto ipsec transform-set cypher command has been introduced.

3.18.3 crypto ipsec transform-set dh-group

Description

Add the selected *DH* group to *IPsec* transformation to work in the *PFS* mode. The order of adding has a value for data exchange on the *IKE* protocol.

Command with **no** prefix removes the selected group.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ipsec-transform)> dh-group <dh-group>
```

```
(config-ipsec-transform)> no dh-group <dh-group>
```

Arguments

Argument	Value	Description
dh-group	1	<i>DH</i> group to work in the <i>PFS</i> mode.
	2	

Argument	Value	Description
	5	
	14	
	15	
	16	
	17	
	18	

Example

```
(config-ipsec-transform)> dh-group 14
IpSec::Manager: "test": crypto ipsec transform-set dh-group "14" ►
successfully added.
```

```
(config-ipsec-transform)> no dh-group 14
IpSec::Manager: "test": crypto ipsec transform-set "test" ►
dh-group successfully removed.
```

History

Version	Description
2.06	The crypto ipsec transform-set dh-group command has been introduced.

3.18.4 crypto ipsec transform-set hmac

Description

Add the selected value of [HMAC](#) signature algorithm to [IPsec](#) transformation. The order of adding has a value for data exchange on the [IKE](#) protocol.

Command with **no** prefix removes the selected algorithm.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-ipsec-transform)> hmac <hmac>
```

```
(config-ipsec-transform)> no hmac <hmac>
```

Arguments

Argument	Value	Description
hmac	esp-md5-hmac	HMAC signature algorithm of IPsec ESP transformation.
	esp-sha1-hmac	
	esp-sha256-hmac	
	esp-sha512-hmac	
	esp-null-hmac	

Example

```
(config-ipsec-transform)> hmac esp-sha512-hmac
IpSec::Config::TransformSet: "TEST": added auth "esp-sha512-hmac".
```

```
(config-ipsec-transform)> no hmac esp-sha512-hmac
IpSec::Config::TransformSet: "TEST": removed auth ►
"esp-sha512-hmac".
```

History

Version	Description
2.06	The crypto ipsec transform-set hmac command has been introduced.
4.02	Added support for esp-sha512-hmac on IKE Phase II.

3.18.5 crypto ipsec transform-set lifetime

Description

Set lifetime of selected *IPsec* transformation. By default, the value 3600 is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ipsec-transform)> lifetime <lifetime>
```

```
(config-ipsec-transform)> no lifetime
```

Arguments

Argument	Value	Description
lifetime	<i>Integer</i>	Lifetime of <i>IPsec</i> transformation in seconds. Can take values in the range from 60 to 2147483647.

Example

```
(config-ipsec-transform)> lifetime 8640
IpSec::Manager: "test": crypto ipsec transform-set lifetime set ►
to 8640 s.
```

```
(config-ipsec-transform)> no lifetime
IpSec::Manager: "test": crypto ipsec transform-set lifetime reset.
```

History

Version	Description
2.06	The crypto ipsec transform-set lifetime command has been introduced.

3.19 crypto map

Description Access to a group of commands to configure selected *IPsec* crypto map. If crypto map is not found, the command tries to create it.

Command with **no** prefix removes crypto map.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry (config-crypto-map)

Synopsis

```
(config)> crypto map <name>
(config)> no crypto map <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	<i>IPsec</i> crypto map name. Latin letters, numbers, dots, hyphens and underscores are acceptable.

Example

```
(config)> crypto map test
IpSec::Manager: "test": crypto map successfully created.
```

```
(config)> no crypto map test
IpSec::Manager: Crypto map profile "test" removed.
```

History

Version	Description
2.06	The crypto map command has been introduced.

3.19.1 crypto map connect

Description Enable automatic unconditional *IPsec* connection to the remote host. Setting has no meaning if basic remote host was set to any (see [crypto map set-peer](#) command). By default, setting is disabled and connection is established when attempting to transmit traffic through the *IPsec ESP* transformation.

Command with **no** prefix disables automatic unconditional connection.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> connect
(config-crypto-map)> no connect
```

Example

```
(config-crypto-map)> connect
IpSec::Manager: "test": crypto map autoconnect enabled.

(config-crypto-map)> no connect
IpSec::Manager: "test": crypto map autoconnect disabled.
```

History	Version	Description
	2.06	The crypto map connect command has been introduced.

3.19.2 crypto map enable

Description Enable selected *IPsec* crypto map. By default, setting is enabled.
Command with **no** prefix disables crypto map.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> enable
(config-crypto-map)> no enable
```

Example

```
(config-crypto-map)> enable
IpSec::Manager: "test": crypto map enabled.

(config-crypto-map)> no enable
IpSec::Manager: "test": crypto map disabled.
```

History	Version	Description
	2.06	The crypto map enable command has been introduced.

3.19.3 crypto map fallback-check-interval

Description Enable periodic checking of basic host availability and return to it in case of presence basic and backup remote hosts both. By default, setting is disabled.
Command with **no** prefix disables checking.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> fallback-check-interval <interval-value>
(config-crypto-map)> no fallback-check-interval
```

Arguments

Argument	Value	Description
interval-value	<i>Integer</i>	Period of checking in seconds. Can take values in the range from 60 to 86400.

Example

```
(config-crypto-map)> fallback-check-interval 120
IpSec::Manager: "test": crypto map fallback check interval is ►
set to 120.
```

```
(config-crypto-map)> no fallback-check-interval
IpSec::Manager: "test": crypto map fallback check interval is ►
cleared.
```

History

Version	Description
2.06	The crypto map fallback-check-interval command has been introduced.

3.19.4 crypto map force-encaps

Description Enforce the [ESP](#) packet wrapping mode in [UDP](#) to bypass the firewall and NAT.
Command with **no** prefix disables the mode.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> force-encaps
(config-crypto-map)> no force-encaps
```

Example

```
(config-crypto-map)> force-encaps
IpSec::Manager: "test": crypto map force ESP in UDP encapsulation ►
enabled.
```

```
(config-crypto-map)> no force-encaps
IpSec::Manager: "test": crypto map force ESP in UDP encapsulation ►
disabled.
```

History

Version	Description
2.08	The crypto map force-encaps command has been introduced.

3.19.5 crypto map l2tp-server dhcp route

Description

Assign a route which is transmitted in DHCP INFORM messages to the [L2TP](#) server clients.

Command with **no** prefix cancels the specified route. If you use no arguments, the entire list of routes will be cleared.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-crypto-map)> l2tp-server dhcp route <address> <mask>
```

```
(config-crypto-map)> no l2tp-server dhcp route [ <address> <mask> ]
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	Network client address.
mask	<i>IP-mask</i>	Network client mask. There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).

Example

```
(config-crypto-map)> l2tp-server dhcp route 192.168.2.0/24  
IpSec::Manager: "VPNLTTPServer": crypto map L2TP/IPsec server ►  
added DHCP INFORM route to 192.168.2.0/255.255.255.0.
```

```
(config-crypto-map)> l2tp-server no dhcp route  
IpSec::Manager: "VPNLTTPServer": Cleared DHCP INFORM routes.
```

History

Version	Description
2.12	The crypto map l2tp-server dhcp route command has been introduced.

3.19.6 crypto map l2tp-server enable

Description

Enable [L2TP](#) server on [IPsec](#) crypto map. By default, the setting is enabled.

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings Yes**Multiple input** No

Synopsis

```
(config-crypto-map)> l2tp-server enable
```

```
(config-crypto-map)> no l2tp-server enable
```

Example

```
(config-crypto-map)> l2tp-server enable
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
enabled.
```

```
(config-crypto-map)> no l2tp-server enable
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
disabled.
```

History

Version	Description
2.11	The crypto map l2tp-server enable command has been introduced.

3.19.7 crypto map l2tp-server interface

Description Bind [L2TP](#) server to the specified interface.
Command with **no** prefix unbinds the server.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config-crypto-map)> l2tp-server interface <interface>
```

```
(config-crypto-map)> no l2tp-server interface
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full name or an alias of the interface. You can see the list of available interfaces with help of l2tp-server interface [Tab] command.

Example

```
(config-crypto-map)> l2tp-server interface [Tab]
```

```
Usage template:
    interface {interface}
```

```
Choose:
    GigabitEthernet1
```

```

ISP
WifiMaster0/AccessPoint2
WifiMaster1/AccessPoint1
WifiMaster0/AccessPoint3
WifiMaster0/AccessPoint0
AccessPoint
WifiMaster1/AccessPoint2
WifiMaster0/AccessPoint1
GuestWiFi

(config-crypto-map)> l2tp-server interface ISP
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
is bound to ISP.

(config-crypto-map)> no l2tp-server interface ISP
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
is unbound.

```

History

Version	Description
2.11	The crypto map l2tp-server interface command has been introduced.

3.19.8 crypto map l2tp-server ipv6cp

Description

Enable IPv6 support. DHCP IPv6 pools are created for each [L2TP](#) server. By default, the setting is disabled.

Command with **no** prefix disables IPv6 support.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-crypto-map)> l2tp-server ipv6cp
```

```
(config-crypto-map)> no l2tp-server ipv6cp
```

Example

```
(config-crypto-map)> l2tp-server ipv6cp
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
IPv6CP is enabled.
```

```
(config-crypto-map)> no l2tp-server ipv6cp
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
IPv6CP is disabled.
```

History

Version	Description
3.00	The crypto map l2tp-server ipv6cp command has been introduced.

3.19.9 crypto map l2tp-server lcp echo

Description Specify the testing rules of the *L2TP* server connections with *LCP* echo tools.
Command with **no** prefix disables *LCP* echo.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> l2tp-server lcp echo <interval> <count>
(config-crypto-map)> no l2tp-server lcp echo
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	Interval between sending <i>LCP</i> echo, in seconds. If within the specified time interval there is no <i>LCP</i> echo request from the remote location, the same request will be sent there asking for response <i>LCP</i> reply.
count	<i>Integer</i>	The number of consecutive requests <i>LCP</i> echo sent, for which no response <i>LCP</i> reply was received. If count of <i>LCP</i> echo requests goes unanswered, the connection is terminated.

Example

```
(config-crypto-map)> l2tp-server lcp echo 5 3
IpSec::Manager: "VPNLT2TPServer": crypto map L2TP/IPsec server ►
set LCP echo to "5" : "3".
```

```
(config-crypto-map)> no l2tp-server lcp echo
IpSec::Manager: "VPNLT2TPServer": crypto map L2TP/IPsec server ►
LCP echo disabled.
```

History

Version	Description
2.11	The crypto map l2tp-server lcp echo command has been introduced.

3.19.10 crypto map l2tp-server mru

Description Set *MRU* value to be transmitted to *L2TP* server. By default, 1200 value is used.
Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> l2tp-server mru <mr>
```

```
(config-crypto-map)> no l2tp-server mru
```

Arguments

Argument	Value	Description
mru	Integer	MRU value. Can take values in the range from 128 to 1500 inclusively.

Example

```
(config-crypto-map)> l2tp-server mru 1500  
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►  
set MRU to "1500".
```

```
(config-crypto-map)> no l2tp-server mru  
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►  
MRU reset to default.
```

History

Version	Description
2.11	The crypto map l2tp-server mru command has been introduced.

3.19.11 crypto map l2tp-server mtu

Description

Set [MTU](#) value to be transmitted to [L2TP](#) server. By default, 1400 value is used.

Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> l2tp-server mtu <mt>
```

```
(config-crypto-map)> no l2tp-server mtu
```

Arguments

Argument	Value	Description
mtu	Integer	MTU value. Can take values in the range from 576 to 1500 inclusively.

Example

```
(config-crypto-map)> l2tp-server mtu 1400  
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►  
set MTU to "1400".
```

```
(config-crypto-map)> no l2tp-server mtu
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
MTU reset to default.
```

History

Version	Description
2.11	The crypto map l2tp-server mtu command has been introduced.

3.19.12 crypto map l2tp-server multi-login

Description Allow connection to [L2TP](#) server for multiple users from one account.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> l2tp-server multi-login
```

```
(config-crypto-map)> no l2tp-server multi-login
```

Example

```
(config-crypto-map)> l2tp-server multi-login
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
multiple login is enabled.
```

```
(config-crypto-map)> no l2tp-server multi-login
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
multiple login is disabled.
```

History

Version	Description
2.11	The crypto map l2tp-server multi-login command has been introduced.

3.19.13 crypto map l2tp-server nat

Description Enable translation of addresses for [L2TP](#) server.

Command with **no** prefix disables the translation.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> l2tp-server nat
```

```
(config-crypto-map)> no l2tp-server nat
```

Example

```
(config-crypto-map)> l2tp-server nat
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
SNAT is enabled.
```

```
(config-crypto-map)> no l2tp-server nat
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
SNAT is disabled.
```

History

Version	Description
2.11	The crypto map l2tp-server nat command has been introduced.

3.19.14 crypto map l2tp-server range

Description

Assign a pool of addresses for the clients of [L2TP](#) server. By default, size 100 is used.

Command with **no** prefix removes a pool.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-crypto-map)> l2tp-server range <begin> <end> | <size>
```

```
(config-crypto-map)> no l2tp-server range
```

Arguments

Argument	Value	Description
begin	<i>IP address</i>	Start address of pool.
end	<i>IP address</i>	End address of pool.
size	<i>Integer</i>	Pool size.

Example

```
(config-crypto-map)> l2tp-server range 172.16.2.33 172.16.2.38
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
pool range set from "172.16.2.33" to "172.16.2.38".
```

```
(config-crypto-map)> l2tp-server range 172.16.2.33 100
IpSec::Manager: "VPNL2TPServer": crypto map L2TP/IPsec server ►
pool range set from "172.16.2.33" to "172.16.2.132".
```

```
(config-crypto-map)> no l2tp-server range
IpSec::Manager: "VPNLTTPServer": crypto map L2TP/IPsec server ►
pool range deleted.
```

History

Version	Description
2.11	The crypto map l2tp-server range command has been introduced.

3.19.15 crypto map l2tp-server session-logout

Description Terminate an active or stalled session on the [L2TP](#) server.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> session-logout <session>
```

Arguments

Argument	Value	Description
session	<i>Integer</i>	Identifier of the L2TP session (can be viewed using the show crypto map command).

Example

```
(config-crypto-map)> session-logout 3
IpSec::L2tp::Manager: Session "3" is terminated.
```

History

Version	Description
4.03	The crypto map l2tp-server session-logout command has been introduced.

3.19.16 crypto map l2tp-server session-preempt

Description Enable to preempt VPN sessions when [crypto map l2tp-server multi-login](#) option is disabled for the [L2TP](#) server.

Command with **no** prefix disables the preempt.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> l2tp-server session-preempt
```

```
(config-crypto-map)> no l2tp-server session-preempt
```

Example

```
(config-crypto-map)> l2tp-server session-preempt
IpSec::L2tp::Manager: Enabled session preemption.
```

```
(config-crypto-map)> no l2tp-server session-preempt
IpSec::L2tp::Manager: Disabled session preemption.
```

History

Version	Description
4.03	The crypto map l2tp-server session-preempt command has been introduced.

3.19.17 crypto map l2tp-server static-ip

Description

Bind IP address to the user. User account must have ipsec-l2tp tag.

Command with **no** prefix removes binding.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-crypto-map)> static-ip <user> <address>
```

```
(config-crypto-map)> no static-ip <user>
```

Arguments

Argument	Value	Description
user	<i>String</i>	Username.
address	<i>IP address</i>	IP address to bind.

Example

```
(config-crypto-map)> l2tp-server static-ip admin 172.16.2.33
IpSec::Manager: "VPNLTTPServer": crypto map L2TP/IPsec server ►
static IP "172.16.2.33" assigned to user "admin".
```

```
(config-crypto-map)> no l2tp-server static-ip admin
IpSec::Manager: "VPNLTTPServer": crypto map L2TP/IPsec server ►
static IP removed for user "admin".
```

History

Version	Description
2.11	The crypto map l2tp-server static-ip command has been introduced.

3.19.18 crypto map nail-up

Description Enable automatic renegotiation of *IPsec ESP* transformations at their obsolescence. By default, setting is disabled.

Command with **no** prefix disables automatic renegotiation.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> nail-up
(config-crypto-map)> no nail-up
```

Example

```
(config-crypto-map)> nail-up
IpSec::Manager: "test": crypto map SA renegotiation enabled.
```

```
(config-crypto-map)> no nail-up
IpSec::Manager: "test": crypto map SA renegotiation disabled.
```

History

Version	Description
2.06	The crypto map nail-up command has been introduced.

3.19.19 crypto map reauth-passive

Description Enable passive reauthentication of *IPsec* crypto map. By default, setting is disabled.

Command with **no** prefix disables passive reauthentication.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> reauth-passive
(config-crypto-map)> no reauth-passive
```

Example

```
(config-crypto-map)> reauth-passive
IpSec::Manager: "VPNLT2TPServer": crypto map SA passive ►
reauthentication enabled.
```

```
(config-crypto-map)> no reauth-passive
IpSec::Manager: "VPNLT2TPServer": crypto map SA passive ►
reauthentication disabled.
```

History	Version	Description
	2.11	The crypto map reauth-passive command has been introduced.

3.19.20 crypto map set-peer

Description Set basic remote host for *IPsec* connection.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> set-peer <remote-ip>
(config-crypto-map)> no set-peer
```

Arguments	Argument	Value	Description
	remote-ip	String	IP address or domain name of remote host.
		any	Accept any incoming connections.

Example

```
(config-crypto-map)> set-peer ipsec.test.com
IpSec::Manager: "test": crypto map primary remote peer is set ►
to "ipsec.test.com".

(config-crypto-map)> no set-peer
IpSec::Manager: "test": crypto map remote primary and fallback ►
peer reset.
```

History	Version	Description
	2.06	The crypto map set-peer command has been introduced.

3.19.21 crypto map set-peer-fallback

Description Set backup remote host for *IPsec* connection. This setting can be made after assignment of basic host (see **crypto map set-peer** command).

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> set-peer-fallback <remote-ip>
```

```
(config-crypto-map)> no set-peer-fallback
```

Arguments

Argument	Value	Description
remote-ip	<i>String</i>	IP address or domain name of remote host.

Example

```
(config-crypto-map)> set-peer-fallback test.com
IpSec::Manager: "test": crypto map fallback remote peer cannot ►
be set without primary peer.
```

```
(config-crypto-map)> no set-peer-fallback
IpSec::Manager: "test": crypto map fallback remote peer reset.
```

History

Version	Description
2.06	The crypto map set-peer-fallback command has been introduced.

3.19.22 crypto map set-profile

Description

Set the reference to existing *IPsec* profile (see [crypto ipsec profile](#) command).

Command with **no** prefix removes the reference.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-crypto-map)> set-profile <profile>
```

```
(config-crypto-map)> no set-profile
```

Arguments

Argument	Value	Description
profile	<i>String</i>	<i>IPsec</i> profile name. You can see the list of available profiles with help of set-profile [Tab] command.

Example

```
(config-crypto-map)> set-profile [Tab]
```

Usage template:

```
set-profile {name: {A-Z, a-z, 0-9, ., _, -}}
```

Choose:

```
TEST
MYMY
```

```
VirtualIPServer
VPNL2TPServer
```

```
(config-crypto-map)> set-profile test
IpSec::Manager: "test": crypto map ipsec profile is set to "test".
```

```
(config-crypto-map)> no set-profile
IpSec::Manager: "test": crypto map ipsec profile reset.
```

History

Version	Description
2.06	The crypto map set-profile command has been introduced.

3.19.23 crypto map set-tcpmss

Description

Set the limit on the segment size of outgoing *TCP* sessions within *IPsec* tunnel. If the *MSS* value, which is transmitted in the header of SYN-packets, exceeds the specified limit, command changes it. Path MTU Discovery mode allows automatically identify *MSS* limit.

Command with **no** prefix removes all limits from *MSS*.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-crypto-map)> set-tcpmss <mss-value>
```

```
(config-crypto-map)> no set-tcpmss
```

Arguments

Argument	Value	Description
mss-value	<i>Integer</i>	<i>MSS</i> upper limit. Can take values in the range from 576 to 1500.
	pmtu	Enable Path MTU Discovery mode.

Example

```
(config-crypto-map)> set-tcpmss 1280
IpSec::Manager: "test": crypto map tcpmss set to 1280.
```

```
(config-crypto-map)> no set-tcpmss
IpSec::Manager: "test": crypto map tcpmss reset.
```

History

Version	Description
2.06	The crypto map set-tcpmss command has been introduced.

3.19.24 crypto map set-transform

Description Set the reference to existing *IPsec ESP* transformation (see [crypto ipsec transform-set](#) command).

Command with **no** prefix removes the reference.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> set-transform <transform-set>
(config-crypto-map)> no set-transform
```

Arguments

Argument	Value	Description
transform-set	String	<i>IPsec</i> transformation name. You can see the list of available transformations with help of set-transform [Tab] command.

Example

```
(config-crypto-map)> set-transform [Tab]
Usage template:
  set-transform {name: {A-Z, a-z, 0-9, ., _, -}}

Choose:
VirtualIPServer
VPNL2TPServer
```

```
(config-crypto-map)> set-transform test
IpSec::Manager: "test": crypto map ipsec transform-set is set ►
to "test".
```

```
(config-crypto-map)> no set-transform
IpSec::Manager: "test": crypto map ipsec transform-set reset.
```

History

Version	Description
2.06	The crypto map set-transform command has been introduced.

3.19.25 crypto map traffic-selectors

Description Assign an object group as *IPsec* Phase 2 selectors.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> traffic-selectors <local> <remote>
```

```
(config-crypto-map)> no traffic-selectors
```

Arguments

Argument	Value	Description
local	<i>String</i>	Name of local object group.
remote	<i>String</i>	Name of remote object group.

Example

```
(config-crypto-map)> traffic-selectors ►
  _WEBADMIN_IPSEC_VPNL2TPServe-local ►
  _WEBADMIN_IPSEC_VPNL2TPServe-remote
IpSec::Config::CryptoMap: "test": set traffic-selectors to ►
  "_WEBADMIN_IPSEC_VPNL2TPServer-local": ►
  "_WEBADMIN_IPSEC_VPNL2TPServer-remote".
```

```
(config-crypto-map)> no traffic-selectors
IpSec::Config::CryptoMap: "test": reset traffic-selectors.
```

History

Version	Description
4.00	The crypto map traffic-selectors command has been introduced.

3.19.26 crypto map tunnel-interface

Description Assign the [XFRM](#) interface to a crypto map for site-to-site traffic routing.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> tunnel-interface <interface>
```

```
(config-crypto-map)> no tunnel-interface
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full name of the interface.

Example

```
(config-crypto-map)> tunnel-interface XFRM0
IpSec::Config::CryptoMap: "TEST": linked tunnel interface "XFRM0".
```

```
(config-crypto-map)> no tunnel-interface
IpSec::Config::CryptoMap: "TEST": reset tunnel interface.
```

History

Version	Description
4.01	The crypto map tunnel-interface command has been introduced.

3.19.27 crypto map virtual-ip dhcp route

Description

Assign a route which is transmitted in DHCP INFORM messages to the Virtual IP server clients.

Command with **no** prefix deletes the specified route. If you use no arguments, the entire list of routes will be cleared.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-crypto-map)> virtual-ip dhcp route <address> <mask>
```

```
(config-crypto-map)> no virtual-ip dhcp route [ <address> <mask> ]
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	Network client address.
mask	<i>IP-mask</i>	Network client mask. There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).

Example

```
(config-crypto-map)> virtual-ip dhcp route 192.168.2.0/24
IpSec::ManagerVirtualIp: "VirtualIPServerIKE2": crypto map ►
Virtual IP server added DHCP INFORM route to ►
192.168.2.0/255.255.255.0.
```

```
(config-crypto-map)> no virtual-ip dhcp route 192.168.2.0/24
IpSec::ManagerVirtualIp: "VirtualIPServerIKE2": crypto map ►
Virtual IP server DHCP INFORM route to 192.168.2.0/255.255.255.0 ►
removed.
```

```
(config-crypto-map)> no virtual-ip dhcp route
IpSec::ManagerVirtualIp: "VirtualIPServerIKE2": crypto map ►
Virtual IP server DHCP INFORM routes cleared.
```

History	Version	Description
	3.06	The crypto map virtual-ip dhcp route command has been introduced.

3.19.28 crypto map virtual-ip dns-server

Description Set [DNS](#) server issued to clients in Virtual IP server mode.

Command with **no** prefix deletes the address.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> virtual-ip dns-server <address>
(config-crypto-map)> no virtual-ip dns-server
```

Arguments	Argument	Value	Description
	address	<i>IP address</i>	IP address of DNS server.

Example

```
(config-crypto-map)> virtual-ip dns-server 10.5.5.5
IpSec::Manager: "test": crypto map Virtual IP DNS server set to ►
"10.5.5.5".
```

```
(config-crypto-map)> no virtual-ip dns-server
IpSec::Manager: "test": crypto map Virtual IP DNS server deleted.
```

History	Version	Description
	2.08	The crypto map virtual-ip dns-server command has been introduced.

3.19.29 crypto map virtual-ip enable

Description Enable Virtual IP server mode, when clients receive addresses from a given range. The value of a remote subnet, specified in the corresponding access-list, will be ignored. By default, the setting is disabled.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> virtual-ip enable
```

```
(config-crypto-map)> no virtual-ip enable
```

Example

```
(config-crypto-map)> virtual-ip enable  
IpSec::Manager: "test": crypto map Virtual IP mode enabled.
```

```
(config-crypto-map)> no virtual-ip enable  
IpSec::Manager: "test": crypto map Virtual IP mode disabled.
```

History

Version	Description
2.08	The crypto map virtual-ip enable command has been introduced.

3.19.30 crypto map virtual-ip interface

Description

Bind Virtual IP server to the specified interface.

Command with **no** prefix unbinds the interface.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-crypto-map)> virtual-ip interface interface
```

```
(config-crypto-map)> no virtual-ip interface
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(config-crypto-map)> virtual-ip interface Bridge0  
IpSec::VirtualIp::CryptoMap: "VirtualIPServerIKE2": bound to ► Bridge0.
```

```
(config-crypto-map)> no virtual-ip interface  
IpSec::VirtualIp::CryptoMap: "VirtualIPServerIKE2": unbound.
```

History

Version	Description
4.02	The crypto map virtual-ip interface command has been introduced.

3.19.31 crypto map virtual-ip multi-login

Description Allow connection to Virtual IP server for multiple users from one account.
Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> virtual-ip multi-login
(config-crypto-map)> no virtual-ip multi-login
```

Example

```
(config-crypto-map)> virtual-ip multi-login
IpSec::Manager: "VirtualIPServer": crypto map Virtual IP server ►
multiple login is enabled.

(config-crypto-map)> no virtual-ip multi-login
IpSec::Manager: "VirtualIPServer": crypto map Virtual IP server ►
multiple login is disabled.
```

History	Version	Description
	3.05	The crypto map virtual-ip multi-login command has been introduced.

3.19.32 crypto map virtual-ip nat

Description Enable translation for remote network of Virtual IP extension server.
Command with **no** prefix removes the rule.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> virtual-ip nat
(config-crypto-map)> no virtual-ip nat
```

Example

```
(config-crypto-map)> virtual-ip nat
IpSec::Manager: "test": crypto map Virtual IP remote pool SNAT ►
is enabled.

(config-crypto-map)> no virtual-ip nat
IpSec::Manager: "test": crypto map Virtual IP remote pool SNAT ►
is disabled.
```

History

Version	Description
2.08	The crypto map virtual-ip nat command has been introduced.

3.19.33 crypto map virtual-ip range

Description Configure the range of addresses issued to clients in Virtual IP server mode. Command with **no** prefix removes the range.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> virtual-ip range <begin> ( <end> | <size> )
(config-crypto-map)> no virtual-ip range
```

Arguments

Argument	Value	Description
begin	<i>IP address</i>	The beginning of the address range.
end	<i>IP address</i>	The end of the address range.
size	<i>Integer</i>	Address range size.

Example

```
(config-crypto-map)> virtual-ip range 10.5.0.0 20
IpSec::Manager: "test": crypto map Virtual IP pool range set ►
from "10.5.0.0" to "10.5.0.19" (CIDR 10.5.0.0/27).
```

```
(config-crypto-map)> no virtual-ip range
IpSec::Manager: "test": crypto map Virtual IP pool range deleted.
```

History

Version	Description
2.08	The crypto map virtual-ip range command has been introduced.

3.19.34 crypto map virtual-ip session-logout

Description Terminate an active or stalled session on the Virtual IP server.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(config-crypto-map)> session-logout <session>
```

Arguments

Argument	Value	Description
session	<i>Integer</i>	Identifier of the IKE session (can be viewed using the show crypto map command).

Example

```
(config-crypto-map)> session-logout 1
IpSec::VirtualIp::Manager: Session "1" is terminated.
```

History

Version	Description
4.03	The crypto map virtual-ip session-logout command has been introduced.

3.19.35 crypto map virtual-ip session-preempt

Description

Enable to preempt VPN sessions when [crypto map virtual-ip multi-login](#) option is disabled for the IKEv1 or IKEv2 [IPSec](#) server.

Command with **no** prefix disables the preempt.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-crypto-map)> virtual-ip session-preempt
```

```
(config-crypto-map)> no virtual-ip session-preempt
```

Example

```
(config-crypto-map)> virtual-ip session-preempt
IpSec::VirtualIp::CryptoMap: "VirtualIPServerIKE2": enable ►
session preemption.
```

```
(config-crypto-map)> no virtual-ip session-preempt
IpSec::VirtualIp::CryptoMap: "VirtualIPServerIKE2": disable ►
session preemption.
```

History

Version	Description
4.03	The crypto map virtual-ip session-preempt command has been introduced.

3.19.36 crypto map virtual-ip static-ip

Description

Bind IP address to the user. User account must have ipsec-xauth tag.

Command with **no** prefix removes binding.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-crypto-map)> virtual-ip static-ip <user> <address>
(config-crypto-map)> no virtual-ip static-ip <user>
```

Arguments

Argument	Value	Description
user	<i>String</i>	Username.
address	<i>IP address</i>	IP address to bind.

Example

```
(config-crypto-map)> virtual-ip static-ip admin 172.20.0.1
IpSec::ManagerVirtualIp: "VirtualIPServer": crypto map Virtual ►
IP server static address "172.20.0.1" assigned to user "admin".
```

```
(config-crypto-map)> no virtual-ip static-ip admin
IpSec::ManagerVirtualIp: "VirtualIPServer": crypto map Virtual ►
IP server static address removed for user "admin".
```

History

Version	Description
3.05	The crypto map virtual-ip static-ip command has been introduced.

3.20 dlna

Description Access to a group of commands to manage [DLNA](#) service.

Prefix no No

Change settings No

Multiple input No

Group entry (config-dlna)

Synopsis

```
(config)> dlna
```

Example

```
(config)> dlna
Core::Configurator: Done.
(config-dlna)>
```


History	Version	Description
	2.00	The dlna command has been introduced.

3.20.1 dlina container

Description Set default container for [DLNA](#) service.
Command with **no** prefix resets the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dlna)> container <container>
(config-dlna)> no container
```

Arguments	Argument	Value	Description
	container	browse	Show the content of browse container by default.
		music	Show the content of music container by default.
		video	Show the content of video container by default.
		images	Show the content of images container by default.

Example

```
(config-dlna)> container browse
Dlna::Server: Set default container to "browse".

(config-dlna)> no container
Dlna::Server: Reset default container.
```

History	Version	Description
	2.11	The dlina container command has been introduced.

3.20.2 dlina db-directory

Description Specify the directory with database of multimedia content.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dlna)> db-directory <directory>
```

```
(config-dlna)> no db-directory
```

Arguments

Argument	Value	Description
directory	<i>String</i>	Name of the directory with database.

Example

```
(config-dlna)> db-directory 46E243F4E243E6B1:/components/dlna/Dlna::Server: DB directory set.
```

```
(config-dlna)> no db-directory
Dlna::Server: DB directory removed.
```

History

Version	Description
2.06	The dlna db-directory command has been introduced.

3.20.3 dlna directory

Description

Specify the directory with media content.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-dlna)> directory <directory> [media-type]
```

```
(config-dlna)> no directory <directory>
```

Arguments

Argument	Value	Description
directory	<i>String</i>	Name of the directory with media content.
media-type	audio	Content type is audio.
	video	Content type is video.
	images	Content type is images.

Example

```
(config-dlna)> directory ►
46E243F4E243E6B1:/components/transmission/download/
Dlna::Server: ►
"46E243F4E243E6B1:/components/transmission/download/" directory ►
added.
```

```
(config-dlna)> no directory ►
46E243F4E243E6B1:/components/transmission/download/
```

```
Dlna::Server: ►
"46E243F4E243E6B1:/components/transmission/download/" directory ►
removed.
```

History

Version	Description
2.00	The dlna directory command has been introduced.
2.06	Parameter media-type was added.

3.20.4 dlna display-name

Description

Assign custom name to [DLNA](#) server.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-dlna)> display-name <display-name>
```

```
(config-dlna)> no display-name
```

Arguments

Argument	Value	Description
display-name	<i>String</i>	Server name to assign.

Example

```
(config-dlna)> display-name MYDLNA
Dlna::Server: Set a display name.
```

History

Version	Description
2.12	The dlna display-name command has been introduced.

3.20.5 dlna interface

Description

Set the router interface through which media content will be transmitted. You can enter up to 16 interfaces.

Command with **no** prefix removes the defined interface from the list. If you use no argument, the entire list of interfaces will be removed.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type IP**Synopsis**`(config-dlna)> interface <interface>``(config-dlna)> no interface <interface>`**Arguments**

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example`(config-dlna)> interface [Tab]`

Usage template:
 interface {interface}

Choose:

```

    GigabitEthernet1
    ISP
    WifiMaster0/AccessPoint2
    WifiMaster1/AccessPoint1
    WifiMaster0/AccessPoint3
    WifiMaster0/AccessPoint0
    AccessPoint
    WifiMaster1/AccessPoint2
    WifiMaster0/AccessPoint1
    GuestWiFi
  
```

`(config-dlna)> interface FastEthernet0/Vlan1``(config-dlna)> no interface FastEthernet0/Vlan1`**History**

Version	Description
2.00	The dlna interface command has been introduced.

3.20.6 dlna port

Description

Set DLNA server port for HTTP (descriptions, SOAP, media transfer) traffic. By default, value 8200 is used.

Command with **no** prefix resets port to default.

Prefix no Yes**Change settings** Yes**Multiple input** No**Synopsis**`(config-dlna)> port <port>`

```
(config-dlna)> no port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	The port number.

Example

```
(config-dlna)> port 8999
Dlna::Server: Port changed to 8999.
```

```
(config-dlna)> no port
Dlna::Server: Port reset to 8200.
```

History

Version	Description
2.00	The dlna port command has been introduced.

3.20.7 dlna rescan

Description

Renew info about files in the directory with media content.

Note: If keyword **full** is specified, deleting and recreating of the content database happens. This may take a long time, so it is recommended to do this when the content database structure is damaged.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(config-dlna)> rescan [ full ]
```

Arguments

Argument	Value	Description
full	<i>Keyword</i>	Specifies if rebuilding of database content is needed.

Example

```
(config-dlna)> rescan
```

```
(config-dlna)> rescan full
```

History

Version	Description
2.00	The dlna rescan command has been introduced.

3.20.8 dlna sort

Description Set the sort criteria for [DLNA](#) server files.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-dlna)> sort <key> [ <order> ]
```

```
(config-dlna)> no sort
```

Arguments

Argument	Value	Description
key	class	Sort by class of media content (audio, video, images).
	title	Sort by title.
	date	Sort by date.
	track	Sort by track.
	album	Sort by album.
order	ascending	Sort files in ascending order. The parameter is used by default.
	descending	Sort files in descending order.

Example

```
(config-dlna)> sort date
Dlna::Server: "date by ascending" sort criterion appended.
```

```
(config-dlna)> sort date ascending
Dlna::Server: "date by ascending" sort criterion appended.
```

```
(config-dlna)> no sort
Dlna::Server: Sort criteria removed.
```

History

Version	Description
2.11	The dlna sort command has been introduced.

3.21 dns-proxy

Description Access to a group of commands to manage DNS proxy service.

Prefix no No

Change settings No

Multiple input No

Group entry (config-dnspx)

Synopsis (config)> **dns-proxy**

Example

```
(config)> dns-proxy
Core::Configurator: Done.
(config-dnspx)>
```

History

Version	Description
2.04	The dns-proxy command has been introduced.

3.21.1 dns-proxy filter assign host preset

Description Assign a filtering preset to a network device.

See the list of presets you can with help of [show dns-proxy filter presets](#) command.

Command with **no** prefix removes the defined preset for host. If you use no argument, the entire list of presets will be cleared for hosts.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-dnspx)> filter assign host preset <host> <preset>
(config-dnspx)> no filter assign host preset [<host>]
```

Arguments

Argument	Value	Description
host	<i>MAC address</i>	Network device MAC address.
preset	<i>String</i>	Preset name.

Example

```
(config-dnspx)> filter assign host preset 04:d4:c1:51:b1:59 ►
opendns-family
Dns::Filter::Public: Associated host "04:d4:c1:51:b1:59" with ►
preset "opendns-family".

(config-dnspx)> no filter assign host preset 04:d4:c1:51:b1:59
Dns::Filter::Public: Removed preset for host "04:d4:c1:51:b1:59".

(config-dnspx)> no filter assign host preset
Dns::Filter::Public: Removed presets for hosts.
```

History

Version	Description
3.08	The dns-proxy filter assign host preset command has been introduced.

3.21.2 dns-proxy filter assign host profile

Description

Assign a filtering profile to a network device.

Add new profile you can with help of **dns-proxy filter profile** command.

See the list of profiles you can with help of **show dns-proxy filter profiles** command.

Command with **no** prefix removes the defined profile for host. If you use no argument, the entire list of profiles will be cleared for hosts.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-dnspx)> filter assign host profile <host> <profile>
```

```
(config-dnspx)> no filter assign host profile [host]
```

Arguments

Argument	Value	Description
host	<i>MAC address</i>	Network device MAC address.
profile	<i>String</i>	Profile name.

Example

```
(config-dnspx)> filter assign host profile 00:d2:c1:54:bc:59 test
Dns::Filter::Public: Associated host "00:d2:c1:54:bc:59" with ►
profile "test".
```

```
(config-dnspx)> no filter assign host profile 00:d2:c1:54:bc:59
Dns::Filter::Public: Removed profile for host "00:d2:c1:54:bc:59".
```

```
(config-dnspx)> no filter assign host profile
Dns::Filter::Public: Removed profiles for hosts.
```

History

Version	Description
3.08	The dns-proxy filter assign host profile command has been introduced.

3.21.3 dns-proxy filter assign interface preset

Description Assign a filtering preset to all devices on segment (exclude ones with already assigned profiles/presets).

See the list of presets you can with help of [show dns-proxy filter presets](#) command.

Command with **no** prefix removes the defined preset for interface. If you use no argument, the entire list of presets for interfaces will be cleared.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-dnspj)> filter assign interface preset <interface> <preset>
(config-dnspj)> no filter assign interface preset [ <interface> ]
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Network interface name. Must have a private or protected security level.
preset	<i>String</i>	Preset name.

Example

```
(config-dnspj)> filter assign interface preset Bridge0 ►
quad9-security
Dns::Filter::Public: Associated interface "Bridge0" with preset ►
"quad9-security".
```

```
(config-dnspj)> no filter assign interface preset Bridge0
Dns::Filter::Public: Removed preset for interface "Bridge0".
```

```
(config-dnspj)> no filter assign interface preset
Dns::Filter::Public: Removed presets for interfaces.
```

History

Version	Description
3.08	The dns-proxy filter assign interface preset command has been introduced.

3.21.4 dns-proxy filter assign interface profile

Description Assign a filtering profile to all devices on segment (exclude ones with already assigned profiles/presets).

Add new profile you can with help of [dns-proxy filter profile](#) command.

See the list of profiles you can with help of [show dns-proxy filter profiles](#) command.

Command with **no** prefix removes the defined profile for interface. If you use no argument, the entire list of profiles for interfaces will be cleared.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-dnspx)> filter assign interface profile <interface> <profile>
(config-dnspx)> no filter assign interface profile [ <interface> ]
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Network interface name. Must have a private or protected security level.
profile	<i>String</i>	Profile name.

Example

```
(config-dnspx)> filter assign interface profile ►
GigabitEthernet0/Vlan1 DnsProfile0
Dns::Filter::Public: Associated interface ►
"GigabitEthernet0/Vlan1" with profile "DnsProfile0".
```

```
(config-dnspx)> no filter assign interface profile ►
GigabitEthernet0/Vlan1
Dns::Filter::Public: Removed profile for interface ►
"GigabitEthernet0/Vlan1".
```

```
(config-dnspx)> no filter assign interface profile
Dns::Filter::Public: Removed profiles for interfaces.
```

History

Version	Description
3.08	The dns-proxy filter assign interface profile command has been introduced.

3.21.5 dns-proxy filter engine

Description Selects DNS engine.

Command with **no** prefix disables the feature. Config request will return empty value in case of disabled filter.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dnspx)> filter engine <engine>
```

```
(config-dnspx)> no filter engine
```

Arguments

Argument	Value	Description
engine	interceptor	One of available DNS filtering engines.
	public	
	nextdns	
	opkg	
	skydns	

Example

```
(config-dnspx)> filter engine interceptor  
Dns::Filter::Interceptor: Enabled.
```

```
(config-dnspx)> no filter engine  
Dns::Manager: Disabled filter engine.
```

History

Version	Description
3.08	The dns-proxy filter engine command has been introduced.

3.21.6 dns-proxy filter profile

Description

Create a custom DNS filtering profile.

Command with **no** prefix removes profile.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-dnspx)> filter profile <name>
```

```
(config-dnspx)> no filter profile <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Profile name in reduced form, not more than 32 characters. The maximum number of profiles is 8.

Example

```
(config-dnspx)> filter profile test  
Dns::Filter::Public: Created profile "test".
```

```
(config-dnspj)> no filter profile test
Dns::Filter::Public: Removed profile "test".
```

History

Version	Description
3.08	The dns-proxy filter profile command has been introduced.

3.21.7 dns-proxy filter profile description

Description

Assign description for DNS filtering profile.

Command with **no** prefix deletes the profile description.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-dnspj)> filter profile <name>description <description>
```

```
(config-dnspj)> no filter profile <name>description <description>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Profile name.
description	<i>String</i>	Arbitrary description of the profile.

Example

```
(config-dnspj)> filter profile test description MyProfile1
Dns::Filter::Public: Set description to profile "test".
```

```
(config-dnspj)> no filter profile test description
Dns::Filter::Public: Cleared description of profile "test".
```

History

Version	Description
3.08	The dns-proxy filter profile description command has been introduced.

3.21.8 dns-proxy filter profile dns53 upstream

Description

Add IP address of the DNS server to user-defined filtering profile. Number of servers are limited to 6.

Command with **no** prefix removes the defined server from the list. If you use no argument, the entire list of servers will be cleared.

Prefix no

Yes

Change settings

Multiple input

Synopsis

Arguments

Example

History

Yes

Yes

(config-dnspx)> filter profile <name>dns53 upstream <address>[:<port>]

(config-dnspx)> no filter profile <name>dns53 description [<address>[:<port>]]

Argument	Value	Description
name	String	Profile name.
address	IP address	IP address of the server.
port	Integer	The server port.

(config-dnspx)> filter profile test dns53 upstream 1.1.1.1

Dns::Filter::Public: Added DNS name server 1.1.1.1 to profile ► "test".

(config-dnspx)> no filter profile test dns53 upstream

Dns::Filter::Public: Removed DNS name server from profile "test".

(config-dnspx)> no filter profile test dns53 upstream 1.1.1.1

Dns::Filter::Public: Removed DNS name server 1.1.1.1 from profile ► "test".

Version	Description
3.08	The dns-proxy filter profile dns53 upstream command has been introduced.

3.21.9 dns-proxy filter profile https upstream

Description	Add DNS over HTTPS server to user-defined filtering profile. Number of servers are limited to 6. Command with no prefix removes the defined server from the list. If you use no argument, the entire list of servers will be cleared.
Prefix no	Yes
Change settings	Yes
Multiple input	Yes
Synopsis	<pre>(config-dnspx)> filter profile <name>https upstream <url> [spki <hash>]</pre> <pre>(config-dnspx)> no filter profile <name>https description [<url>]</pre>

Arguments

Argument	Value	Description
name	<i>String</i>	Profile name.
url	<i>String</i>	URL of DNS service.
hash	<i>String</i>	Hash TLS certificate.

Example

```
(config-dnspx)> filter profile test https upstream ►
https://dns.google/resolve
Dns::Filter::Public: Added DNS-over-HTTPS name server ►
https://dns.google/resolve to profile "test".
```

```
(config-dnspx)> no filter profile test https upstream ►
https://dns.google/resolve
Dns::Filter::Public: Removed DNS-over-HTTPS name server ►
https://dns.google/resolve from profile "test".
```

```
(config-dnspx)> no filter profile test https upstream
Dns::Filter::Public: Removed DNS-over-HTTPS name server from ►
profile "test".
```

History

Version	Description
3.08	The dns-proxy filter profile https upstream command has been introduced.

3.21.10 dns-proxy filter profile intercept enable

Description

Enable transit DNS requests interception for filtering profile. By default, the interception is disabled.

Command with **no** prefix disables the interception for filtering profile.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-dnspx)> filter profile <name>intercept enable
```

```
(config-dnspx)> no filter profile <name>intercept enable
```

Arguments

Argument	Value	Description
name	<i>String</i>	Filtering profile name.

Example

```
(config-dnspx)> filter profile DnsProfile0 intercept enable
Dns::Filter::Public: Enabled intercept in profile "DnsProfile0".
```

```
(config-dnspx)> no filter profile DnsProfile0 intercept enable
Dns::Filter::Public: Disabled intercept in profile "DnsProfile0".
```

History

Version	Description
3.09	The dns-proxy filter profile intercept enable command has been introduced.

3.21.11 dns-proxy filter profile tls upstream

Description

Add [DNS over TLS](#) server to user-defined filtering profile. Number of servers are limited to 6.

Command with **no** prefix removes the defined server from the list. If you use no argument, the entire list of servers will be cleared.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-dnspx)> filter profile <name>tls upstream <address> [ <port>
] [ sni <fqdn> ] [ spki <hash> ]
```

```
(config-dnspx)> no filter profile <name>tls description [ <address> ] [
<port> ]
```

Arguments

Argument	Value	Description
name	<i>String</i>	Profile name.
address	<i>IP address</i> <i>FQDN</i>	Address of the server.
port	<i>Integer</i>	The server port.
fqdn	<i>String</i>	Full domain name.
hash	<i>String</i>	Hash TLS certificate.

Example

```
(config-dnspx)> filter profile test tls upstream 1.1.1.1 8853 ►
sni cloudflare-dns.com
Dns::Filter::Public: Added DNS-over-TLS name server 1.1.1.1 to ►
profile "test".
```

```
(config-dnspx)> no filter profile test tls upstream 1.1.1.1 8853
Dns::Filter::Public: Removed DNS-over-TLS name server 1.1.1.1 ►
from profile "test".
```

```
(config-dnspx)> no filter profile test tls upstream
Dns::Filter::Public: Removed DNS-over-TLS name server from ►
profile "test".
```

History

Version	Description
3.08	The dns-proxy filter profile tls upstream command has been introduced.

3.21.12 dns-proxy https upstream

Description

Add [DNS over HTTPS](#) server.

Command with **no** prefix removes the defined server from the list. If you use no argument, the entire list of servers will be cleared.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-dnspx)> https upstream <url> [ <format> ] [ sni <hash> ] [ on
<interface> ] [ domain <domain> ]

(config-dnspx)> no https upstream [ <url> ]
```

Arguments

Argument	Value	Description
url	<i>String</i>	Custom URL of DNS service.
format	dnsm	The format to represent DNS data.
	json	
hash	<i>String</i>	Hash TLS certificate.
interface	<i>Interface</i>	Interface name to configure.
domain	<i>String</i>	The domain name.

Example

```
(config-dnspx)> https upstream ►
https://cloudflare-dns.com/dns-query?ct=application/dns-json json
Dns::Secure::ManagerDoh: DNS-over-HTTPS name server ►
"https://cloudflare-dns.com/dns-query?ct=application/dns-json" ►
(json) added.
```

```
(config-dnspx)> https upstream https://dns.adguard.com/dns-query ►
dnsm
Dns::Secure::ManagerDoh: DNS-over-HTTPS name server ►
"https://dns.adguard.com/dns-query" (dnsm) added.
```

```
(config-dnspx)> https upstream https://dns.adguard.com/dns-query ►
dnsm on ISP
Dns::Secure::ManagerDoh: DNS-over-HTTPS name server ►
"https://dns.adguard.com/dns-query" (dnsm) added.
```

```
(config-dnspx)> https upstream https://my.domain.com/dns-query ►
dnsm domain my.lib
```



```
Dns::Secure::ManagerDoh: DNS-over-HTTPS name server ►
"https://my.domain.com/dns-query" (dnsm) added.
```

```
(config-dnsp) > no https upstream ►
https://dns.adguard.com/dns-query
Dns::Secure::ManagerDoh: DNS-over-HTTPS name server ►
"https://dns.adguard.com/dns-query" deleted.
```

```
(config-dnsp) > no https upstream
Dns::Secure::ManagerDoh: DNS-over-HTTPS name servers cleared.
```

History

Version	Description
3.01	The dns-proxy https upstream command has been introduced.
3.08	The domain argument was added.

3.21.13 dns-proxy intercept enable

Description Enable transit DNS requests interception for system profile. By default, the interception is disabled.

Command with **no** prefix disables the interception for system profile.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dnsp) > intercept enable
(config-dnsp) > no intercept enable
```

Example

```
(config-dnsp) > intercept enable
Dns::Filter::Filter: Enable intercept for system profile.
(config-dnsp) > no intercept enable
Dns::Filter::Filter: Disable intercept for system profile.
```

History

Version	Description
3.06	The dns-proxy intercept enable command has been introduced.
3.08	The dns-proxy intercept enable command was removed as obsolete.
3.09	The dns-proxy intercept enable command has been added again.

3.21.14 dns-proxy max-ttl

Description Set maximum TTL for DNS proxy cached entries.

Command with **no** prefix removes maximum TTL value.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dnspx)> max-ttl <max-ttl>
```

```
(config-dnspx)> no max-ttl
```

Arguments

Argument	Value	Description
max-ttl	<i>Integer</i>	The maximum value of TTL. Can take values in the range from 1 to 604800000 milliseconds (1 week).

Example

```
(config-dnspx)> max-ttl 10000
Dns::Proxy: Dns-proxy set max-ttl to 10000.
```

```
(config-dnspx)> no max-ttl
Dns::Proxy: Dns-proxy max-ttl cleared.
```

History

Version	Description
2.05	The dns-proxy max-ttl command has been introduced.

3.21.15 dns-proxy proceed

Description Set interval between concurrent requests, which is sent by DNS proxy to multiple DNS servers. By default, 500 value is used.

Command with **no** prefix resets proceed to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dnspx)> proceed <proceed>
```

```
(config-dnspx)> no proceed
```

Arguments

Argument	Value	Description
proceed	<i>Integer</i>	The value of DNS proxy proceed in milliseconds. Can take values in the range from 1 to 50000.

Example

```
(config-dnspj)> proceed 600
Dns::Proxy: Dns-proxy set 600 msec. proceed.
```

```
(config-dnspj)> no proceed
Dns::Proxy: Dns-proxy proceed timeout reset.
```

History

Version	Description
2.04	The dns-proxy proceed command has been introduced.

3.21.16 dns-proxy rebind-protect

Description

Enable protect against [DNS rebinding](#) attacks. By default, auto mode is used.

Command with **no** prefix disables protection.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-dnspj)> rebind-protect (auto | strict)
```

```
(config-dnspj)> no rebind-protect
```

Arguments

Argument	Value	Description
auto	<i>Keyword</i>	Protect subnets for private interfaces.
strict	<i>Keyword</i>	Protect subnets from list IANA IPv4 Special-Purpose Address Registry ¹ .

Example

```
(config-dnspj)> rebind-protect auto
Dns::Manager: Enabled rebind protection.
(config-dnspj)> no rebind-protect
Dns::Manager: Disabled rebind protection.
```

History

Version	Description
3.04	The dns-proxy rebind-protect command has been introduced.

¹ <https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml>

3.21.17 dns-proxy srr-reset

Description Set DNS proxy send-response rating reset time. By default, value 600000 is used.

Command with **no** prefix resets time reset to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dnspx)> srr-reset <srr-reset>
(config-dnspx)> no srr-reset
```

Arguments

Argument	Value	Description
srr-reset	<i>Integer</i>	The value of time reset in milliseconds. Can take values in the range from 0 to 600000.

Example

```
(config-dnspx)> srr-reset 111
Dns::Manager: Set send-response rating reset time to 111 ms.
```

```
(config-dnspx)> no srr-reset
Dns::Manager: Reset send-response rating reset time to default.
```

History

Version	Description
2.12	The dns-proxy srr-reset command has been introduced.

3.21.18 dns-proxy tls upstream

Description Add [DNS over TLS](#) server.

Command with **no** prefix removes the defined server from the list. If you use no argument, the entire list of servers will be cleared.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-dnspx)> tls upstream <address> [ <port> ] [ sni <fqdn> ] [ spki
<hash> ] [ on <interface> ] [ domain <domain> ]
(config-dnspx)> no tls upstream [ <address> ] [ <port> ]
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	IP address of the server.
port	<i>Integer</i>	The server port.
fqdn	<i>String</i>	Full domain name.
hash	<i>String</i>	Hash TLS certificate.
interface	<i>Interface</i>	Interface name to configure.
domain	<i>String</i>	The domain name.

Example

```
(config-dnspx)> tls upstream 1.1.1.1 853 sni cloudflare-dns.com
Dns::Secure::ManagerDot: DNS-over-TLS name server 1.1.1.1:853 ►
added.
```

```
(config-dnspx)> tls upstream 1.1.1.1 853 sni cloudflare-dns.com ►
on ISP
Dns::Secure::ManagerDot: DNS-over-TLS name server 1.1.1.1:853 ►
added.
```

```
(config-dnspx)> tls upstream 144.144.144.143 853 sni ►
my.domain.com domain my.lib
Dns::Secure::ManagerDot: DNS-over-TLS name server ►
144.144.144.143:853 added.
```

```
(config-dnspx)> no tls upstream 1.1.1.1 853
Dns::Secure::ManagerDot: DNS-over-TLS name server 1.1.1.1:853 ►
deleted.
```

```
(config-dnspx)> no tls upstream
Dns::Secure::ManagerDot: DNS-over-TLS name servers cleared.
```

History

Version	Description
3.01	The dns-proxy tls upstream command has been introduced.
3.08	The domain argument was added.

3.22 dpn accept

Description Accept user agreement [DPN](#). Until the license is accepted, the configurator does not accept any command except READ_ONLY.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config)> dpn accept`

Example

```
(config)> dpn accept
Core::Legal: Accepted dpn version 20200330.
```

History

Version	Description
3.05	The dpn accept command has been introduced.

3.23 dyndns profile

Description

Access to a group of commands to configure DynDns profile. If the profile is not found, the command tries to create it. You can enter up to 32 profiles.

Command with **no** prefix removes DynDns profile.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Group entry

(config-dyndns)

Synopsis

```
(config)> dyndns profile <name>
```

```
(config)> no dyndns profile <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	The profile name. Maximum name length is 64 characters.

Example

```
(config)> dyndns profile _WEBADMIN
Core::Configurator: Done.
(config-dyndns)>
```

History

Version	Description
2.00	The dyndns profile command has been introduced.

3.23.1 dyndns profile domain

Description

Assign permanent domain name to the computer. You need to register this domain name on the site [dyndns.com](http://www.dyndns.com)² or [no-ip.com](http://www.no-ip.com)³ before execution.

Command with **no** prefix removes the setting.

Prefix no

Yes

² <http://www.dyndns.com>

³ <http://www.no-ip.com>

Change settings Yes**Multiple input** No

Synopsis

```
(config-dyndns)> domain <domain>
```

```
(config-dyndns)> no domain
```

Arguments	Argument	Value	Description
	domain	<i>String</i>	The domain name. Maximum domain name length is 254 characters.

Example

```
(config-dyndns)> domain support.ddns.net  
DynDns::Profile: "_WEBADMIN": domain saved..
```

```
(config-dyndns)> no domain  
ynDns::Profile: "_WEBADMIN" domain cleared.
```

History	Version	Description
	2.00	The dyndns profile domain command has been introduced.

3.23.2 dyndns profile password

Description Set password for access via DynDns.**Prefix no** Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config-dyndns)> password <password>
```

```
(config-dyndns)> no password
```

Arguments	Argument	Value	Description
	password	<i>String</i>	The password for authentication. Maximum password length is 64 characters.

Example

```
(config-dyndns)> password 123456789  
DynDns::Profile: "_WEBADMIN": password saved.
```

```
(config-dyndns)> no password  
DynDns::Profile: "_WEBADMIN" password cleared.
```

History

Version	Description
2.00	The dyndns profile password command has been introduced.

3.23.3 dyndns profile send-address

Description Enable the necessity of connection IP address indication in DynDns request.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dyndns)> send-address
(config-dyndns)> no send-address
```

Example

```
(config-dyndns)> send-address
DynDns::Profile: Send address is enabled.

(config-dyndns)> no send-address
DynDns::Profile: Send address is disabled.
```

History

Version	Description
2.03	The dyndns profile send-address command has been introduced.

3.23.4 dyndns profile type

Description Set DynDns type depending on the site where the domain name was registered.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dyndns)> type <type>
(config-dyndns)> no type
```


Arguments

Argument	Value	Description
type	dyndns	The domain name is registered on the account.dyn.com ⁴ site.
	noip	The domain name is registered on the noip.com ⁵ site.
	opendns	The domain name is registered on the opendns.com ⁶ site.
	dnsomatic	The domain name is registered on the dnsomatic.com ⁷ site.
	anydns	The domain name is registered on the anydns.info ⁸ site.
	dnshome	The domain name is registered on the dnshome.de ⁹ site.
	duckdns	The domain name is registered on the duckdns.org ¹⁰ site.
	dyndnsfree	The domain name is registered on the dyndnsfree.de ¹¹ site.
	desec	The domain name is registered on the desec.io ¹² site.
	custom	The domain name is registered on the other site (defined with dyndns profile url command).

Example

```
(config-dyndns)> type noip
DynDns::Profile: "_WEBADMIN": type saved.
```

```
(config-dyndns)> no type
DynDns::Profile: "_WEBADMIN": type cleared.
```

History

Version	Description
2.00	The dyndns profile type command has been introduced.

3.23.5 dyndns profile update-interval

Description

Set the address update interval for DynDns.

Command with **no** prefix cancels the ability to update.

⁴ <https://account.dyn.com>

⁵ <https://www.noip.com>

⁶ <https://www.opendns.com>

⁷ <https://dnsomatic.com>

⁸ <https://www.anydns.info>

⁹ <https://www.dnshome.de>

¹⁰ <https://www.duckdns.org>

¹¹ <https://www.dyndnsfree.de>

¹² <https://desec.io>

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config-dyndns)> update-interval <days> days [ <hours> hours ]
[ <minutes> minutes ] [ <seconds> seconds ]
```

```
(config-dyndns)> no update-interval
```

Arguments

Argument	Value	Description
days	<i>Integer</i>	Interval time in days.
hours	<i>Integer</i>	Interval time in hours.
minutes	<i>Integer</i>	Interval time in minutes.
seconds	<i>Integer</i>	Interval time in seconds.

Example

```
(config-dyndns)> update-interval 5 days 5 hours 5 minutes 5 ►  
seconds  
DynDns::Profile: Interval is set to 450305 seconds.
```

```
(config-dyndns)> update-interval 5 days  
DynDns::Profile: Interval is set to 432000 seconds.
```

```
(config-dyndns)> no update-interval  
DynDns::Profile: Periodic registration disabled.
```

History

Version	Description
2.03	The dyndns profile update-interval command has been introduced.

3.23.6 dyndns profile url

Description Set dynamic DNS service custom URL.**Prefix no** Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config-dyndns)> url <url>
```

```
(config-dyndns)> no url
```

Arguments

Argument	Value	Description
url	<i>String</i>	Custom URL of DNS service.

Example

```
(config-dyndns)> url http://members.dyndns.org/nic/update
DynDns::Profile: "_WEBADMIN": URL saved.
```

```
(config-dyndns)> no url
DynDns::Profile: "_WEBADMIN" URL cleared.
```

History	Version	Description
	2.05	The dyndns profile url command has been introduced.

3.23.7 dyndns profile username

Description Set username for access via DynDns.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dyndns)> username <username>
```

```
(config-dyndns)> no username
```

Arguments	Argument	Value	Description
	username	<i>String</i>	Username for authentication. Maximum name length is 64 characters.

Example

```
(config-dyndns)> username test@gmail.com
DynDns::Profile: "_WEBADMIN": username saved.
```

```
(config-dyndns)> no username
DynDns::Profile: "_WEBADMIN" username cleared.
```

History	Version	Description
	2.00	The dyndns profile username command has been introduced.

3.24 easyconfig check

Description Access to a group of commands to configure Internet access check. To check Internet access, first requests to the default gateway are sent. If the answer is received, then the remote hosts specified in the settings are polled. The duration and frequency of requests are also specified in the settings. If all the checks have been passed, then the Internet access is provided.

Prefix no No

Change settings No**Multiple input** No**Group entry** (ezconfig-check)**Synopsis** (config)> **easyconfig check****Example**
(config)> **easyconfig check**
(ezconfig-check)>**History**

Version	Description
2.00	The easyconfig check command has been introduced.

3.24.1 easyconfig check exclude-gateway

Description Disable default gateway check. By default, the setting is enabled.Command with **no** prefix enables the check back.**Prefix no** Yes**Change settings** Yes**Multiple input** No**Synopsis**
(ezconfig-check)> **exclude-gateway**
(ezconfig-check)> **no exclude-gateway****Example**
(ezconfig-check)> **exclude-gateway**
Network::InternetChecker: Gateway checking disabled.(ezconfig-check)> **no exclude-gateway**
Network::InternetChecker: Gateway checking enabled.**History**

Version	Description
2.05	The easyconfig check exclude-gateway command has been introduced.

3.24.2 easyconfig check max-fails

Description Specify the number of consecutive failed requests to the cloud service to conclude that the internet is unavailable. By default, value 3 is used.Command with **no** prefix resets setting to default.**Prefix no** Yes

Change settings Yes**Multiple input** No

Synopsis

```
(ezconfig-check)> max-fails <count>
```

```
(ezconfig-check)> no max-fails
```

Arguments

Argument	Value	Description
count	<i>Integer</i>	Amount of failed requests. Can take values in the range from 2 to 8 inclusively.

Example

```
(ezconfig-check)> max-fails 5
```

```
Network::InternetChecker: A new maximum fail count set to 5.
```

```
(ezconfig-check)> no max-fails
```

```
Network::InternetChecker: The maximum fail count reset to the ► default value (3).
```

History

Version	Description
2.00	The easyconfig check max-fails command has been introduced.

3.24.3 easyconfig check period

Description Set a period of checking. By default, the value 15 is used.Command with **no** prefix resets setting to default.**Prefix no** Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(ezconfig-check)> period <period>
```

```
(ezconfig-check)> no period
```

Arguments

Argument	Value	Description
period	<i>Integer</i>	Check interval in seconds. Can take values in the range from 10 to 60 inclusively.

Example

```
(ezconfig-check)> period 20
```

```
Network::InternetChecker: A new check period set to 20 seconds.
```

```
(ezconfig-check)> no period
Network::InternetChecker: Check period reset to default (15 ►
seconds).
```

History

Version	Description
2.00	The easyconfig check period command has been introduced.

3.25 easyconfig disable

Description

Disable initial setup wizard. By default, the setting is enabled.

Command with **no** prefix enables initial setup wizard.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> easyconfig disable
```

```
(config)> no easyconfig disable
```

Example

```
(config)> easyconfig disable
EasyConfig::Manager: Disabled.
```

```
(config)> no easyconfig disable
EasyConfig::Manager: Enabled.
```

History

Version	Description
3.01	The easyconfig disable command has been introduced.

3.26 eula accept

Description

Accept user agreement [EULA](#). Until the license is accepted, the configurator does not accept any command except READ_ONLY.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(config)> eula accept
```

Example (config)> **eula accept**
Core::Eula: "20181001" license accepted.

History	Version	Description
	2.15	The eula accept command has been introduced.

3.27 igmp-proxy

Description Access to a group of commands to configure [IGMP](#).

Prefix no No

Change settings No

Multiple input No

Group entry (igmp-proxy)

Synopsis (config)> **igmp-proxy**

Example (config)> **igmp-proxy**
(igmp-proxy)>

History	Version	Description
	2.06	The igmp-proxy command has been introduced.

3.27.1 igmp-proxy fast-leave

Description Enable the [IGMP](#) fast-leave to immediately remove a port from the forwarding entry for a multicast group when the port receives a leave message.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis (igmp-proxy)> **fast-leave**
(igmp-proxy)> **no fast-leave**

Example (igmp-proxy)> **fast-leave**
Igmp::Proxy: Enabled Fast Leave.

```
(igmp-proxy)> no fast-leave
Igmp::Proxy: Disabled Fast Leave.
```

History

Version	Description
3.09	The igmp-proxy fast-leave command has been introduced.

3.27.2 igmp-proxy force

Description

Force old version of *IGMP*. By default, the setting is disabled and the protocol version is selected in automatic mode.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(igmp-proxy)> force <protocol>
```

```
(igmp-proxy)> no force
```

Arguments

Argument	Value	Description
protocol	igmp-v1	Apply filtering to incoming packets.
	igmp-v2	Apply filtering to outgoing packets.

Example

```
(igmp-proxy)> force igmp-v1
Igmp::Proxy: Forced protocol: igmp-v1.
```

```
(igmp-proxy)> no force
Igmp::Proxy: Enabled IGMP auto-detect.
```

History

Version	Description
2.08	The igmp-proxy force command has been introduced.

3.28 igmp-snooping disable

Description

Disable IGMP snooping. Command is available in Client, Repeater or AP modes only.

Command with **no** prefix enables IGMP snooping.

Prefix no

Yes

Change settings Yes

Multiple input No

Synopsis `(config)> igmp-snooping disable`

Example `(config)> igmp-snooping disable`
 Igmp::Snooping: Disabled.

`(config)> no igmp-snooping disable`
 Igmp::Snooping: Enabled.

History

Version	Description
2.12	The igmp-snooping disable command has been introduced.

3.29 interface

Description Access to a group of commands to configure the selected interface. If the interface is not found, the command tries to create it.

The interface name specifies its class that inherits certain properties, see the diagrams in the [Appendix](#). The commands work in relation to classes. The corresponding interface class is specified in the command description.

Command with **no** prefix deletes the interface.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry `(config-if)`

Synopsis `(config)> interface <name>`

`(config)> no interface <name>`

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example `(config)> interface [Tab]`

Usage template:
 interface {name}

Choose:

```

Pvc
Vlan
CdcEthernet
UsbModem
RealtekEthernet
AsixEthernet
Davicom
UsbQmi
UsbLte
Yota
Bridge
PPPoE
SSTPEthernet
SSTP
PPTP
L2TP
ZeroTier
Wireguard
Proxy
OpenVPN
IPIP
XFRM
TunnelSixInFour
IKE
Gre
EoIP
Clat
MapT
DsLite
TunnelFourInSix
Chilli

```

History

Version	Description
2.00	The interface command has been introduced.

3.29.1 interface atf disable

Description Disable [ATF](#) for AP 5 GHz. By default, the setting is disabled.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFiMaster

Synopsis `(config-if)> atf disable`

```
(config-if)> no atf disable
```

Example

```
(config-if)> atf disable
Network::Interface::Rtx::WifiMaster: "WifiMaster1": Airtime ►
Fairness disabled.
```

```
(config-if)> no atf disable
Network::Interface::Rtx::WifiMaster: "WifiMaster1": Airtime ►
Fairness enabled.
```

History

Version	Description
3.02	The interface atf disable command has been introduced.

3.29.2 interface atf inbound

Description

Enable [ATF](#) for transferring inbound packets only for AP 5 GHz. By default, the setting is disabled.

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

WiFiMaster

Synopsis

```
(config-if)> atf inbound
```

```
(config-if)> no atf inbound
```

Example

```
(config-if)> atf inbound
Network::Interface::Rtx::WifiMaster: "WifiMaster0": Airtime ►
Fairness inbound is set.
```

```
(config-if)> atf inbound
Network::Interface::Rtx::WifiMaster: "WifiMaster1": Airtime ►
Fairness inbound is set.
```

```
(config-if)> no atf inbound
Network::Interface::Rtx::WifiMaster: "WifiMaster1": Airtime ►
Fairness inbound is unset.
```

History

Version	Description
3.02	The interface atf inbound command has been introduced.

3.29.3 interface authentication chap

Description	Enable <i>CHAP</i> authentication support. Command with no prefix disables <i>CHAP</i> .				
Prefix no	Yes				
Change settings	Yes				
Multiple input	No				
Interface type	Secure				
Synopsis	<pre>(config-if)> authentication chap</pre> <pre>(config-if)> no authentication chap</pre>				
Example	<pre>(config-if)> authentication chap</pre> <pre>Network::Interface::Supplicant: "PPTP0": added authentication: ►</pre> <pre>CHAP.</pre> <pre>(config-if)> no authentication chap</pre> <pre>Network::Interface::Supplicant: "PPTP0": removed authentication: ►</pre> <pre>CHAP.</pre>				
History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>2.00</td><td>The interface authentication chap command has been introduced.</td></tr></table>	Version	Description	2.00	The interface authentication chap command has been introduced.
Version	Description				
2.00	The interface authentication chap command has been introduced.				

3.29.4 interface authentication eap-md5

Description	Enable EAP-MD5 authentication support. Command with no prefix disables EAP-MD5.
Prefix no	Yes
Change settings	Yes
Multiple input	No
Interface type	Secure
Synopsis	<pre>(config-if)> authentication eap-md5</pre> <pre>(config-if)> no authentication eap-md5</pre>
Example	<pre>(config-if)> authentication eap-md5</pre> <pre>Network::Interface::Ethernet: "GigabitEthernet1": configured ►</pre> <pre>authentication: EAP-MD5.</pre>

```
(config-if)> no authentication eap-md5
Network::Interface::Supplicant: "GigabitEthernet1": removed ►
authentication: EAP-MD5.
```

History

Version	Description
2.00	The interface authentication eap-md5 command has been introduced.

3.29.5 interface authentication eap-mschapv2

Description

Enable EAP-MSCHAPv2 authentication support.

Command with **no** prefix disables EAP-MSCHAPv2, MS-CHAPv2.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> authentication eap-mschapv2
```

```
(config-if)> no authentication eap-mschapv2
```

Example

```
(config-if)> authentication eap-mschapv2
Network::Interface::Supplicant: "IKE0": authentication is ►
unchanged.
```

```
(config-if)> no authentication eap-mschapv2
Network::Interface::Supplicant: "IKE0": removed authentication: ►
EAP-MSCHAPv2, MS-CHAPv2.
```

History

Version	Description
3.05	The interface authentication eap-mschapv2 command has been introduced.

3.29.6 interface authentication eap-ttls

Description

Enable EAP-TTLS authentication support.

Command with **no** prefix disables EAP-TTLS.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type Secure

Synopsis

```
(config-if)> authentication eap-ttls
(config-if)> no authentication eap-ttls
```

Example

```
(config-if)> authentication eap-ttls
Network::Interface::Ethernet: "GigabitEthernet1": configured ►
authentication: EAP-TTLS.

(config-if)> no authentication eap-ttls
Network::Interface::Supplicant: "GigabitEthernet1": removed ►
authentication: EAP-TTLS.
```

History

Version	Description
2.00	The interface authentication eap-ttls command has been introduced.

3.29.7 interface authentication identity

Description Specify user name for device authentication on the remote system. Equally often used on PPTP, PPPoE, L2TP and Proxy connections, as well as for UsbQmi interfaces.

Command with **no** prefix deletes the previously specified user name.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Secure

Synopsis

```
(config-if)> authentication identity <identity>
(config-if)> no authentication identity
```

Arguments

Argument	Value	Description
identity	<i>String</i>	User name for authentication.

Example

```
(config-if)> authentication identity mylogin
Network::Interface::Supplicant: "PPTP0": identity saved.

(config-if)> no authentication identity
Network::Interface::Supplicant: "PPTP0": identity cleared.
```

History	Version	Description
	2.00	The interface authentication identity command has been introduced.

3.29.8 interface authentication mschap

Description Enable MS-CHAP authentication support.
Command with **no** prefix disables MS-CHAP.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Secure

Synopsis

```
(config-if)> authentication mschap
(config-if)> no authentication mschap
```

Example

```
(config-if)> authentication mschap
Network::Interface::Supplicant: "PPTP0": added authentication: ►
MS-CHAP.

(config-if)> no authentication mschap
Network::Interface::Supplicant: "PPTP0": removed authentication: ►
MS-CHAP.
```

History	Version	Description
	2.00	The interface authentication mschap command has been introduced.

3.29.9 interface authentication mschap-v2

Description Enable MS-CHAPv2 authentication support.
Command with **no** prefix disables MS-CHAPv2.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Secure

Synopsis

```
(config-if)> authentication mschap-v2
```

```
(config-if)> no authentication mschap-v2
```

Example

```
(config-if)> authentication mschap-v2
Network::Interface::Supplicant: "PPTP0": authentication is ►
unchanged.
```

```
(config-if)> no authentication mschap-v2
Network::Interface::Supplicant: "PPTP0": removed authentication: ►
MS-CHAPv2.
```

History

Version	Description
2.00	The interface authentication mschap-v2 command has been introduced.

3.29.10 interface authentication pap

Description

Enable [PAP](#) authentication support.

Command with **no** prefix disables [PAP](#).

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> authentication pap
```

```
(config-if)> no authentication pap
```

Example

```
(config-if)> authentication pap
Network::Interface::Supplicant: "PPTP0": added authentication: ►
PAP.
```

```
(config-if)> no authentication pap
Network::Interface::Supplicant: "PPTP0": removed authentication: ►
PAP.
```

History

Version	Description
2.00	The interface authentication pap command has been introduced.

3.29.11 interface authentication password

Description Specify password for device authentication on the remote system. Equally often used on PPTP, PPPoE, L2TP and Proxy connections.

Command with **no** prefix deletes the password.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Secure

Synopsis

```
(config-if)> authentication password <password>
(config-if)> no authentication password
```

Arguments

Argument	Value	Description
password	<i>String</i>	Password for authentication.

Example

```
(config-if)> authentication password Aihoi2cha1
Network::Interface::Supplicant: "PPTP0": password saved.
```

```
(config-if)> no authentication password
Network::Interface::Supplicant: "PPTP0": password cleared.
```

History

Version	Description
2.00	The interface authentication password command has been introduced.

3.29.12 interface authentication peap

Description Enable [EAP-PEAP](#) authentication support.

Command with **no** prefix disables [EAP-PEAP](#).

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Secure

Synopsis

```
(config-if)> authentication peap
(config-if)> no authentication peap
```

Example

```
(config-if)> authentication peap
Network::Interface::Ethernet: "WifiMaster1/AccessPoint0": ►
configured authentication: PEAP.
```

```
(config-if)> no authentication peap
Network::Interface::Supplicant: "WifiMaster1/AccessPoint0": ►
removed authentication: PEAP.
```

History

Version	Description
2.03	The interface authentication peap command has been introduced.

3.29.13 interface authentication shared

Description

Enable authentication with a *shared key*. This mode is used only in conjunction with *WEP* encryption. *Shared keys* are specified by **interface encryption key** command.

Command with **no** prefix turns authentication to open mode.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

WiFi

Synopsis

```
(config-if)> authentication shared
```

```
(config-if)> no authentication shared
```

Example

```
(config-if)> authentication shared
Network::Interface::Rtx::AccessPoint: "WifiMaster1/AccessPoint0": ►
shared authentication mode enabled.
```

```
(config-if)> no authentication shared
Network::Interface::Rtx::AccessPoint: "WifiMaster1/AccessPoint0": ►
shared authentication mode disabled.
```

History

Version	Description
2.00	The interface authentication shared command has been introduced.

3.29.14 interface authentication wpa-psk

Description

Specify the pre-agreed key for authentication via WPA-PSK protocol. It is possible to specify the key as a 256-bit hexadecimal number or as a string of

ASCII-characters. In the second case, the string is used as a code phrase to generate the key (passphrase).

Command with **no** prefix removes setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFi

Synopsis

```
(config-if)> authentication wpa-psk <psk>
```

```
(config-if)> no authentication wpa-psk
```

Arguments

Argument	Value	Description
psk	<i>String</i>	Pre-agreed key in the form of a 256-bit hexadecimal number, which consists of 64 hexadecimal digits, or in the form of ASCII string of 8 to 63 characters length.

Example

```
(config-if)> authentication wpa-psk Eethaich9z  
Network::Interface::Wifi: "WifiMaster1/AccessPoint0": WPA PSK set.
```

```
(config-if)> no authentication wpa-psk  
Network::Interface::Wifi: "WifiMaster1/AccessPoint0": WPA PSK ►  
removed.
```

History

Version	Description
2.00	The interface authentication wpa-psk command has been introduced.

3.29.15 interface auto-ssid

Description Generate a custom wireless network name (SSID) based on the router's MAC address.

Prefix no No

Change settings Yes

Multiple input No

Interface type WifiMaster

Synopsis

```
(config-if)> auto-ssid <template> <prefix>
```

Arguments

Argument	Value	Description
template	mac4	Template name — the last 4 or 6 digits of the MAC address to be added to the prefix.
	mac6	
prefix	<i>String</i>	Custom string at the user's choice.

Example

```
(config-if)> auto-ssid mac4 12313213
Network::Interface::AccessPoint: "WifiMaster0/AccessPoint0": ►
generated SSID "12313213207E".
```

```
(config-if)> auto-ssid mac6 12313213
Network::Interface::AccessPoint: "WifiMaster0/AccessPoint0": ►
generated SSID "1231321369207E".
```

History

Version	Description
3.08	The interface auto-ssid command has been introduced.

3.29.16 interface backhaul

Description

Enable support of [VLAN](#) for wireless connection between routers Keenetic in the trunk mode. By default, setting is disabled.

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

WiFiMaster

Synopsis

```
(config-if)> backhaul
```

```
(config-if)> no backhaul
```

Example

```
(config-if)> backhaul
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint1": ►
backhaul mode enabled.
```

```
(config-if)> no backhaul
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint1": ►
backhaul mode disabled.
```

History

Version	Description
3.02	The interface backhaul command has been introduced.

3.29.17 interface band-steering

Description Enable *Band Steering* for AP 5 GHz. By default, the setting is enabled.

For correct *Band Steering* operation it is necessary to fulfill the following conditions:

- access points 2,4 GHz and 5 GHz are enabled both
- they have the same SSID's
- they have the same security settings (encryption type, key value, etc.)

Command with **no** prefix disables the *Band Steering*.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFiMaster

Synopsis

```
(config-if)> band-steering
(config-if)> no band-steering
```

Example

```
(config-if)> band-steering
Network::Interface::Rtx::WifiMaster: "WifiMaster1": band steering ►
enabled.

(config-if)> no band-steering
Network::Interface::Rtx::WifiMaster: "WifiMaster1": band steering ►
disabled.
```

History

Version	Description
2.09	The interface band-steering command has been introduced.

3.29.18 interface band-steering preference

Description Set the band to give a preference in *Band Steering* technology. By default, the value is not defined.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFiMaster

Synopsis

```
(config-if)> band-steering preference <band>
(config-if)> no band-steering preference
```

Arguments

Argument	Value	Description
band	2	2,4 GHz band.
	5	5 GHz band.

Example

```
(config-if)> band-steering preference 5
Network::Interface::Rtx::WifiMaster: "WifiMaster1": band steering ►
preference is 5 GHz.
```

```
(config-if)> no band-steering preference
Network::Interface::Rtx::WifiMaster: "WifiMaster1": band steering ►
preference disabled.
```

History

Version	Description
2.09	The interface band-steering preference command has been introduced.

3.29.19 interface ccp

Description Enable [CCP](#) support during establishing connection.

Command with **no** prefix disables [CCP](#).

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> ccp
(config-if)> no ccp
```

Example

```
(config-if)> ccp
CCP enabled.
```

```
(config-if)> no ccp
CCP disabled.
```

History	Version	Description
	2.00	The interface ccp command has been introduced.

3.29.20 interface channel

Description Set the radio channel (broadcasting frequency band) for wireless interfaces. Wi-Fi interfaces take integers from 1 to 14 (frequency range from 2.412 GHz to 2.484 GHz) and from 36 to 165 (frequency range from 5.180 GHz to 5.825 GHz) as channel numbers. By default, auto value is used.

Command with **no** prefix resets to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Radio

Synopsis

```
(config-if)> channel <channel>
(config-if)> no channel
```

Arguments	Argument	Value	Description
	channel	number	Number of radio channel.
		auto	Radio channel number is detected automatically.

Example

```
(config-if)> channel 8
Network::Interface::Rtx::WifiMaster: "WifiMaster0": channel set ►
to 8.
```

```
(config-if)> channel 36
Network::Interface::Rtx::WifiMaster: "WifiMaster1": channel set ►
to 36.
```

```
(config-if)> no channel
Network::Interface::Rtx::WifiMaster: "WifiMaster0": auto channel ►
mode set.
```

History	Version	Description
	2.00	The interface channel command has been introduced.

3.29.21 interface channel auto-rescan

Description Set a schedule for radio channel automatic scanning. By default, the setting is disabled.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Radio

Synopsis

```
(config-if)> channel auto-rescan [ <hh>:<mm> ] interval <interval>
```

```
(config-if)> no channel auto-rescan
```

Arguments

Argument	Value	Description
interval	1	Rescan interval in hours.
	6	
	12	
	24	

Example

```
(config-if)> channel auto-rescan interval 1
Network::Interface::Rtx::WifiMaster: "WifiMaster0": scheduled ►
auto rescan, interval 1 hour.
```

```
(config-if)> no channel auto-rescan
Network::Interface::Rtx::WifiMaster: "WifiMaster0": auto rescan ►
disabled.
```

History

Version	Description
2.07	The interface channel auto-rescan command has been introduced.

3.29.22 interface channel width

Description Set the bandwidth for a specified channel. By default, 40-below value is used.

Command with **no** prefix resets to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Radio

Synopsis

```
(config-if)> channel width <width>
(config-if)> no channel width
```

Arguments

Argument	Value	Description
width	20	Set bandwidth equal to 20 MHz.
	40-above	Expand the bandwidth up to 40 MHz using next channel.
	40-below	Expand the bandwidth up to 40 MHz using previous channel.

Example

```
(config-if)> channel width 20
Network::Interface::Rtx::WifiMaster: "WifiMaster0": channel ►
bandwidth setting applied.
```

```
(config-if)> no channel width
Network::Interface::Rtx::WifiMaster: "WifiMaster0": channel ►
bandwidth settings reset to default.
```

History

Version	Description
2.04	The interface channel width command has been introduced.

3.29.23 interface chilli coaport

Description Set [UDP](#) port to which disconnect requests from the [RADIUS](#) client are sent.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli coaport <coaport>
(config-if)> no chilli coaport
```

Arguments

Argument	Value	Description
coaport	<i>Integer</i>	The CoA port number.

Example

```
(config-if)> chilli coaport 3940
Chilli::Interface: "Chilli0": coaport set to 3940.
```

```
(config-if)> no chilli coaport
Chilli::Interface: "Chilli0": coaport reset to default.
```

History

Version	Description
2.10	The interface chilli coaport command has been introduced.

3.29.24 interface chilli dhcpif

Description

Assign Chilli interface to the system network interface.

Command with **no** prefix cancels the association.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Chilli

Synopsis

```
(config-if)>  chilli dhcpif <dhcpif>
```

```
(config-if)> no chilli dhcpif
```

Arguments

Argument	Value	Description
dhcpif	<i>Interface</i>	Full interface name or an alias.

Example

```
(config-if)> chilli dhcpif Bridge1
Chilli::Interface: "Chilli0": bound to Bridge1.
```

```
(config-if)> no chilli dhcpif
Chilli::Interface: "Chilli0": unbound.
```

History

Version	Description
2.10	The interface chilli dhcpif command has been introduced.

3.29.25 interface chilli dns

Description

Set IP address of the DNS server.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli dns <dns1> [ <dns2> ]
```

```
(config-if)> no chilli dns
```

Arguments

Argument	Value	Description
dns1	<i>IP address</i>	Address of primary DNS server.
dns2	<i>IP address</i>	Address of secondary DNS server.

Example

```
(config-if)> chilli dns 8.8.8.8 1.1.1.1
Chilli::Interface: "Chilli0": DNS servers set to 8.8.8.8, 1.1.1.1.
```

```
(config-if)> no chilli dns
Chilli::Interface: "Chilli0": DNS servers reset to default.
```

History

Version	Description
2.10	The interface chilli dns command has been introduced.

3.29.26 interface chilli lease

Description Configure the lease time of the connected client IP addresses. By default, the value 3600 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli lease <lease>
```

```
(config-if)> no chilli lease
```

Arguments

Argument	Value	Description
lease	<i>Integer</i>	Lease time in seconds. The maximum value is 259200.

Example

```
(config-if)> chilli lease 1000
Chilli::Interface: "Chilli0": lease has been set 1000 seconds.
```

```
(config-if)> no chilli lease
Chilli::Interface: "Chilli0": lease has been reset to default ►
(3600 seconds).
```

History

Version	Description
2.11	The interface chilli lease command has been introduced.

3.29.27 interface chilli login

Description

Configure authorization to connect to the [RADIUS](#) server.

Prefix no

No

Change settings

No

Multiple input

No

Interface type

Chilli

Synopsis

```
(config-if)> chilli login <mac> [ username <username> password <password>
]
```

Arguments

Argument	Value	Description
mac	<i>MAC address</i>	MAC address for authentication.
username	<i>String</i>	Username for authentication.
password	<i>String</i>	The password for authentication.

Example

```
(config-if)> interface Chilli0 chilli login 00:01:02:03:04:05
Chilli::Interface: "Chilli0": sent login request for ►
00:01:02:03:04:05
```

```
(config-if)> interface Chilli0 chilli login 00:01:02:03:04:05 ►
username test password test
Chilli::Interface: "Chilli0": sent login request for ►
00:01:02:03:04:05
```

History

Version	Description
4.00	The interface chilli login command has been introduced.

3.29.28 interface chilli logout

Description

Force the MAC address of the specified client to be disabled.

Prefix no	No
Change settings	No
Multiple input	No
Interface type	Chilli

Synopsis `(config-if)> chilli logout (<mac> | all)`

Arguments

Argument	Value	Description
mac	MAC address	MAC address of the registered client.
all	Keyword	Disable all MAC addresses.

Example

```
(config-if)> chilli logout 64:a2:22:51:b4:11
```

```
(config-if)> chilli logout all
Chilli::Interface: "Chilli0": service restarted.
```

History

Version	Description
2.10	The interface chilli logout command has been introduced.

3.29.29 interface chilli macauth

Description Enable user authentication option based on MAC address detection only.
Command with **no** prefix disables the setting.

Prefix no	Yes
Change settings	Yes
Multiple input	No
Interface type	Chilli

Synopsis `(config-if)> chilli macauth`
`(config-if)> no chilli macauth`

Example

```
(config-if)> chilli macauth
Chilli::Interface: "Chilli0": macauth set to "".
```

```
(config-if)> no chilli macauth
Chilli::Interface: "Chilli0": macauth cleared.
```

History

Version	Description
2.10	The interface chilli macauth command has been introduced.

3.29.30 interface chilli macpasswd

Description

Set the password for MAC address authentication.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Chilli

Synopsis

```
(config-if)> chilli macpasswd <macpasswd>
```

```
(config-if)> no chilli macpasswd
```

Arguments

Argument	Value	Description
macpasswd	<i>String</i>	The user password.

Example

```
(config-if)> chilli macpasswd 1234567890  
Chilli::Interface: "Chilli0": macpasswd set to "1234567890".
```

```
(config-if)> no chilli macpasswd  
Chilli::Interface: "Chilli0": macpasswd cleared.
```

History

Version	Description
2.11	The interface chilli macpasswd command has been introduced.

3.29.31 interface chilli nasip

Description

Set [RADIUS](#) option NAS IP Address. Allows you to configure and use an arbitrary IP address.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type Chilli

Synopsis

```
(config-if)> chilli nasip (<address> | interface <wan> | auto)
```

```
(config-if)> no chilli nasip
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	Specific IP address of the server.
wan	<i>Interface</i>	IP address from the specified WAN interface.
auto	<i>Keyword</i>	IP address from the current WAN interface.

Example

```
(config-if)> chilli nasip 95.213.215.187  
Chilli::Interface: "Chilli0": NAS IP address set to ►  
"95.213.215.187".
```

```
(config-if)> chilli nasip interface ISP  
Chilli::Interface: "Chilli0": NAS IP interface set to ►  
"GigabitEthernet1".
```

```
(config-if)> chilli nasip auto  
Chilli::Interface: "Chilli0": NAS IP address set to auto.
```

```
(config-if)> no chilli nasip  
Chilli::Interface: "Chilli0": NAS IP address cleared.
```

History

Version	Description
2.10	The interface chilli nasip command has been introduced.

3.29.32 interface chilli nasmac

Description Set MAC address for [RADIUS](#) Called-Station-ID attribute. By default, MAC address of the guest network is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli nasmac <mac>
```

```
(config-if)> no chilli nasmac
```

Arguments

Argument	Value	Description
mac	<i>MAC address</i>	New MAC address for RADIUS Called-Station-ID.

Example

```
(config-if)> chilli nasmac 50:ff:20:00:1e:86
Chilli::Interface: "Chilli0": NAS MAC address set to ►
"50:ff:20:00:1e:86".
```

```
(config-if)> no chilli nasmac
Chilli::Interface: "Chilli0": NAS MAC address cleared.
```

History

Version	Description
2.11	The interface chilli nasmac command has been introduced.

3.29.33 interface chilli profile

Description

Assign Chilli profile to the Chilli interface.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Chilli

Synopsis

```
(config-if)> chilli profile <profile>
```

```
(config-if)> no chilli profile
```

Arguments

Argument	Value	Description
profile	<i>String</i>	<i>RADIUS</i> server profile name.

Example

```
(config-if)> chilli profile Wi-Fi_SYSTEM
Chilli::Interface: "Chilli0": assigned profile: Wi-Fi.
```

```
(config-if)> no chilli profile
Chilli::Interface: "Chilli0": profile cleared.
```

History

Version	Description
2.10	The interface chilli profile command has been introduced.

3.29.34 interface chilli radius

Description Add the [RADIUS](#) server addresses.

Command with **no** prefix removes the servers.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli radius <server1> [ <server2> ]
(config-if)> no chilli radius
```

Arguments

Argument	Value	Description
server1	<i>String</i>	Address of first RADIUS server.
server2	<i>String</i>	Address of second RADIUS server.

Example

```
(config-if)> chilli radius radius.example.net radius2.example.net
Chilli::Interface: "Chilli0": RADIUS servers set to ►
radius.example.net, radius2.example.net.
```

```
(config-if)> no chilli radius
Chilli::Interface: "Chilli0": RADIUS servers cleared.
```

History

Version	Description
2.10	The interface chilli radius command has been introduced.

3.29.35 interface chilli radiusacctport

Description Set accounting UDP-port of [RADIUS](#) server. By default, value 1813 is used.

Command with **no** prefix resets port to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli radiusacctport <radiusacctport>
```

```
(config-if)> no chilli radiusacctport
```

Arguments

Argument	Value	Description
radiusacctport	<i>String</i>	The port number.

Example

```
(config-if)> chilli radiusacctport 1819
Chilli::Interface: "Chilli0": radiusacctport set to 1819.
```

```
(config-if)> no chilli radiusacctport
Chilli::Interface: "Chilli0": radiusacctport reset to default.
```

History

Version	Description
3.06	The interface chilli radiusacctport command has been introduced.

3.29.36 interface chilli radiusauthport

Description Set authentication UDP-port of *RADIUS* server. By default, value 1812 is used.

Command with **no** prefix resets port to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli radiusauthport <radiusauthport>
```

```
(config-if)> no chilli radiusauthport
```

Arguments

Argument	Value	Description
radiusauthport	<i>String</i>	The port number.

Example

```
(config-if)> chilli radiusauthport 1820
Chilli::Interface: "Chilli0": radiusauthport set to 1820.
```

```
(config-if)> no chilli radiusauthport
Chilli::Interface: "Chilli0": radiusauthport reset to default.
```

History

Version	Description
3.06	The interface chilli radiusauthport command has been introduced.

3.29.37 interface chilli radiuslocationid

Description Set location identifier of *RADIUS* server. It should be in the format isocc=, cc=, ac=, network=.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli radiuslocationid <radiuslocationid>
(config-if)> no chilli radiuslocationid
```

Arguments

Argument	Value	Description
radiuslocationid	<i>String</i>	Location identifier value.

Example

```
(config-if)> chilli radiuslocationid ►
isocc=,cc=,ac=,network=WiFiSYSTEM,
Chilli::Interface: "Chilli0": radiuslocationid set to ►
"isocc=,cc=,ac=,network=WiFiSYSTEM,".
```

```
(config-if)> no chilli radiuslocationid
Chilli::Interface: "Chilli0": radiuslocationid cleared.
```

History

Version	Description
2.10	The interface chilli radiuslocationid command has been introduced.

3.29.38 interface chilli radiuslocationname

Description Set location name of *RADIUS* server.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli radiuslocationname <radiuslocationname>
```

```
(config-if)> no chilli radiuslocationname
```

Arguments

Argument	Value	Description
radiuslocationname	<i>String</i>	Location name.

Example

```
(config-if)> chilli radiuslocationname MyHotSpot
Chilli::Interface: "Chilli0": radiuslocationname set to ►
"MyHotSpot".
```

```
(config-if)> no chilli radiuslocationname
Chilli::Interface: "Chilli0": radiuslocationname cleared.
```

History

Version	Description
2.10	The interface chilli radiuslocationname command has been introduced.

3.29.39 interface chilli radiusnasid

Description

Set Network Access Server identifier.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Chilli

Synopsis

```
(config-if)>  chilli radiusnasid <radiusnasid>
```

```
(config-if)> no chilli radiusnasid
```

Arguments

Argument	Value	Description
radiusnasid	<i>String</i>	NAS identifier.

Example

```
(config-if)> chilli radiusnasid keeneticru_12
Chilli::Interface: "Chilli0": radiusnasid set to "keeneticru_12".
```

```
(config-if)> no chilli radiusnasid
Chilli::Interface: "Chilli0": radiusnasid cleared.
```

History

Version	Description
2.10	The interface chilli radiusnasid command has been introduced.

3.29.40 interface chilli radiussecret

Description Set shared secret for both [RADIUS](#) servers.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli radiussecret <radiussecret>
(config-if)> no chilli radiussecret
```

Argument	Value	Description
radiussecret	<i>String</i>	A secret value.

Example

```
(config-if)> chilli radiussecret 12df34fd
Chilli::Interface: "Chilli0": radiussecret set to "12df34fd".

(config-if)> no chilli radiussecret
Chilli::Interface: "Chilli0": radiussecret cleared.
```

Version	Description
2.10	The interface chilli radiussecret command has been introduced.

3.29.41 interface chilli uamallowed

Description Specify the resource to which the client has access without first authenticating.
Command with **no** prefix removes the resource from the list. If you use no argument, the entire list of resources will be cleared.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type Chilli

Synopsis

```
(config-if)> chilli uamallowed <uamallowed>
(config-if)> no chilli uamallowed [ <uamallowed> ]
```

Arguments

Argument	Value	Description
uamallowed	<i>String</i>	IP-address, URL or subnetwork.

Example

```
(config-if)> chilli uamallowed 188.166.114.0/24
Chilli::Interface: "Chilli0": "188.166.114.0/24" added to walled ►
garden.
```

```
(config-if)> chilli uamallowed www.example.link
Chilli::Interface: "Chilli0": "www.example.link" added to walled ►
garden.
```

```
(config-if)> no chilli uamallowed 188.166.114.0/24
Chilli::Interface: "Chilli0": "188.166.114.0/24" removed from ►
walled garden.
```

```
(config-if)> no chilli uamallowed www.example.link
Chilli::Interface: "Chilli0": "www.example.link" removed from ►
walled garden.
```

```
(config-if)> no chilli uamallowed
Chilli::Interface: "Chilli0": walled garden cleared.
```

History

Version	Description
2.10	The interface chilli uamallowed command has been introduced.

3.29.42 interface chilli uamdomain

Description

Specify the domain name to which the client has access without first authenticating.

Command with **no** prefix removes the domain name from the list. If you use no argument, the entire list of domain names will be cleared.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

Chilli

Synopsis

```
(config-if)> chilli uamdomain <uamdomain>
```

```
(config-if)> no chilli uamdomain [ <uamdomain> ]
```

Arguments

Argument	Value	Description
uamdomain	<i>String</i>	Domain name of remote host.

Example

```
(config-if)> chilli uamdomain example.net
Chilli::Interface: "Chilli0": "example.net" added to walled ►
garden.
```

```
(config-if)> no chilli uamdomain example.net
Chilli::Interface: "Chilli0": "example.net" removed from walled ►
garden.
```

```
(config-if)> no chilli uamdomain
Chilli::Interface: "Chilli0": walled garden cleared.
```

History

Version	Description
2.10	The interface chilli uamdomain command has been introduced.

3.29.43 interface chilli uamhomepage

Description

Set URL of homepage to redirect unauthenticated users to.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Chilli

Synopsis

```
(config-if)> chilli uamhomepage <uamhomepage>
```

```
(config-if)> no chilli uamhomepage
```

Arguments

Argument	Value	Description
uamhomepage	<i>String</i>	Custom URL.

Example

```
(config-if)> chilli uamhomepage http://192.168.2.1/welcome.html
Chilli::Interface: "Chilli0": uamhomepage set to ►
"http://192.168.2.1/welcome.html".
```

```
(config-if)> no chilli uamhomepage
Chilli::Interface: "Chilli0": uamhomepage cleared.
```

History

Version	Description
2.10	The interface chilli uamhomepage command has been introduced.

3.29.44 interface chilli uamport

Description Set [TCP](#) port to bind to for authenticating clients. By default, value 3990 is used.

Command with **no** prefix resets port to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli uamport <uamport>
(config-if)> no chilli uamport
```

Arguments

Argument	Value	Description
uamport	<i>Integer</i>	The port number.

Example

```
(config-if)> chilli uamport 3922
Chilli::Interface: "Chilli0": uamport set to 3922.
```

```
(config-if)> no chilli uamport
Chilli::Interface: "Chilli0": uamport reset to default.
```

History

Version	Description
2.10	The interface chilli uamport command has been introduced.

3.29.45 interface chilli uamsecret

Description Set shared secret between [UAM](#) server and Chilli. The [UAM](#) secret is used to hash the challenge before password computation.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Chilli

Synopsis

```
(config-if)> chilli uamsecret <uamsecret>
```



```
(config-if)> no chilli uamsecret
```

Arguments

Argument	Value	Description
uamsecret	<i>String</i>	A secret value.

Example

```
(config-if)> chilli uamsecret 12df34fd
Chilli::Interface: "Chilli0": uamsecret set to "12df34fd".
```

```
(config-if)> no chilli uamsecret
Chilli::Interface: "Chilli0": uamsecret set to "".
```

History

Version	Description
2.10	The interface chilli uamsecret command has been introduced.

3.29.46 interface chilli uamserver

Description

Set URL of web server to use for authenticating clients.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Chilli

Synopsis

```
(config-if)>  chilli uamserver <uamserver>
```

```
(config-if)> no chilli uamserver
```

Arguments

Argument	Value	Description
uamserver	<i>String</i>	Custom URL of web server.

Example

```
(config-if)> chilli uamserver ►
https://auth.example.net/hotspotlogin
Chilli::Interface: "Chilli0": uamserver set to ►
"https://auth.example.net/hotspotlogin".
```

```
(config-if)> no chilli uamserver
Chilli::Interface: "Chilli0": uamserver cleared.
```

History

Version	Description
2.10	The interface chilli uamserver command has been introduced.

3.29.47 interface compatibility

Description

Set the standard for wireless communications, with which a given wireless adapter (the interface) must be compatible. For Wi-Fi interfaces, the compatibility is set by string of Latin letters A, B, G, N, that denote extensions to the standard IEEE 802.11. For example, the presence 'N' in the compatibility line will imply that the given adapter will be able to deal with the 802.11n-compatible devices via radio channel. The set of admissible compatibility lines is defined by the hardware capabilities of a particular adapter and provisions of the relevant additions to the IEEE 802.11 standard.

By default, "BGN" value is used for 2.4 GHz, "AN" — for 5 GHz.

Prefix no

No

Change settings

Yes

Multiple input

No

Interface type

Radio

Synopsis

```
(config-if)> compatibility <annex>
```

Arguments

Argument	Value	Description
annex	B, G, N	For 2,4 GHz.
	A, N	For 5 GHz.
	A, N+AC	Additional IEEE standard.

Example

```
(config-if)> compatibility N
Network::Interface::Rtx::WifiMaster: "WifiMaster0": PHY mode set.
```

```
(config-if)> compatibility N+AC
Network::Interface::Rtx::WifiMaster: "WifiMaster1": PHY mode set.
```

History

Version	Description
2.00	The interface compatibility command has been introduced.
2.06	New standard AC was added.

3.29.48 interface connect

Description

Start the process of connecting to a remote node.

Command with **no** prefix terminates the connection.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP, IP

Synopsis

```
(config-if)> connect [ via <via> ]
(config-if)> no connect
```

Argument	Value	Description
via	<i>Interface</i>	Interface through which remote node is accessed. For PPPoE this option is mandatory.

Example

```
(config-if)> connect via ISP
(config-if)> no connect
```

Version	Description
2.00	The interface connect command has been introduced.

3.29.49 interface country-code

Description Assign to the interface a literal country code, which influences the set of radio channels. By default, RU value is used.

Prefix no No

Change settings Yes

Multiple input No

Interface type Radio

Synopsis

```
(config-if)> country-code <code>
```

Argument	Value	Description
code	<i>String</i>	The country code.

Example

```
(config-if)> country-code RU
Network::Interface::Rtx::WifiMaster: "WifiMaster0": country code ►
set.
```

History

Version	Description
2.00	The interface country-code command has been introduced.

3.29.50 interface debug

Description

Enable debug mode of *PPP* connection. Detailed info about connection progress is saved to the system log. By default, setting is disabled.

Command with **no** prefix disables the debug mode.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

PPP

Synopsis

```
(config-if)> debug
```

```
(config-if)> no debug
```

Example

```
(config-if)> debug
Network::Interface::Base: Debug enabled.
```

```
(config-if)> no debug
Network::Interface::Base: Debug disabled.
```

History

Version	Description
2.00	The interface debug command has been introduced.

3.29.51 interface description

Description

Assign arbitrary description to the specified network interface.

Command with **no** prefix deletes the description.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> description <description>
```

```
(config-if)> no description
```

Arguments

Argument	Value	Description
description	<i>String</i>	Arbitrary description of the interface.

Example

```
(config-if)> description MYHOME
Network::Interface::Base: "Bridge0": description saved.
```

```
(config-if)> no description
Network::Interface::Base: "Bridge0": description saved.
```

History

Version	Description
2.00	The interface description command has been introduced.

3.29.52 interface down

Description

Disable the network interface and persist the state “down” to the settings.

Command with **no** prefix enables the network interface and deletes “down” from settings.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> down
```

```
(config-if)> no down
```

Example

```
(config-if)> down
Network::Interface::Base: "GigabitEthernet0/2": interface is down.
```

```
(config-if)> up
Network::Interface::Base: "GigabitEthernet0/2": interface is up.
```

History

Version	Description
2.00	The interface down command has been introduced.

3.29.53 interface duplex

Description

Set the duplex mode of the Ethernet port. By default, auto value is set.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings Yes**Multiple input** No**Interface type** Ethernet

Synopsis

```
(config-if)> duplex (full | half | auto)
```

```
(config-if)> no duplex
```

Arguments

Argument	Value	Description
mode	full	Full duplex protocol.
	half	Half duplex protocol.
	auto	Auto duplex protocol.

Example

```
(config-if)> duplex full
Network::Interface::Ethernet: "GigabitEthernet0/1": duplex set ►
to "full".
```

```
(config-if)> no duplex
Network::Interface::Ethernet: "GigabitEthernet0/1": duplex reset ►
to default.
```

History

Version	Description
2.06.B.1	The interface duplex command has been introduced.

3.29.54 interface dyndns nobind

Description Disable binding of a request to the WAN-interface.Command with **no** prefix enables the binding.**Prefix no** Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config-if)> dyndns nobind
```

```
(config-if)> no dyndns nobind
```

Example

```
(config-if)> dyndns nobind
DynDns::Client: Disabled bind on interface GigabitEthernet1.
```

```
(config-if)> no dyndns nobind
DynDns::Client: Enabled bind on interface GigabitEthernet1.
```

History

Version	Description
4.02	The interface dyndns nobind command has been introduced.

3.29.55 interface dyndns profile

Description

Assign the DynDns profile to the interface. Profile must be created and customized with [dyndns profile](#) commands before execution.

Command with **no** prefix unbinds the profile.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> dyndns profile <profile>
```

```
(config-if)> no dyndns profile
```

Arguments

Argument	Value	Description
profile	<i>String</i>	The name of DynDns profile.

Example

```
(config-if)> dyndns profile TEST  
DynDns::Profile: Interface set.
```

```
(config-if)> no dyndns profile TEST  
DynDns::Profile: Interface removed.
```

History

Version	Description
2.02	The interface dyndns profile command has been introduced.

3.29.56 interface dyndns update

Description

Update IP address for DynDns manually. By default command works in accordance with the policy of the DynDns service provider, that is not allows to update too often. Using the keyword force allows you to update excluding policy of the service provider.

Prefix no

No

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> dyndns update [ force ]
```

Arguments

Argument	Value	Description
force	<i>Keyword</i>	Not take into account the update rate recommended by service provider.

Example

```
(config-if)> dyndns update
```

History

Version	Description
2.00	The interface dyndns update command has been introduced.

3.29.57 interface encryption anonymous-dh

Description

Enable Anonymous DH for SSTP servers without a certificate.

Command with **no** prefix disables Anonymous DH.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

SSTP

Synopsis

```
(config-if)> encryption anonymous-dh
```

```
(config-if)> no encryption anonymous-dh
```

Example

```
(config-if)> encryption anonymous-dh
```

```
Network::Interface::Sstp: "SSTP0": anonymous DH TLS is enabled.
```

```
(config-if)> no encryption anonymous-dh
```

```
Network::Interface::Sstp: "SSTP0": anonymous DH TLS is disabled.
```

History

Version	Description
2.13	The interface encryption anonymous-dh command has been introduced.

3.29.58 interface encryption enable

Description

Enable encryption on the wireless interface. By default, [WEP](#) encryption is used.

Command with **no** prefix disables wireless interface encryption.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFi

Synopsis

```
(config-if)> encryption enable
(config-if)> no encryption enable
```

Example

```
(config-if)> encryption enable
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
wireless encryption enabled.

(config-if)> no encryption enable
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
wireless encryption disabled.
```

History

Version	Description
2.00	The interface encryption enable command has been introduced.

3.29.59 interface encryption key

Description Specify the [WEP](#) encryption keys. Depending on the bit, the key can be standard 64-bit [WEP](#) uses a 40 bit key (also known as WEP-40), or 128-bit [WEP](#) uses a 26 hexadecimal characters (13 characters ASCII). Overall, there can be 1 to 4 encryption keys, with one of them default key must be assigned.

Command with **no** prefix removes key.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type WiFi

Synopsis

```
(config-if)> encryption key <id> (<value> [default] | default)
(config-if)> no encryption key <id>
```

Arguments

Argument	Value	Description
id	<i>Integer</i>	The key number. Overall, up to 4 keys could be specified.
value	<i>String</i>	The key value as a hexadecimal number, consisting of 10 or 26 digits.

Argument	Value	Description
default	<i>Keyword</i>	Indicates that this key will be used by default.

Example

```
(config-if)> encryption key 1 1231231234
Network::Interface::Wifi: "WifiMaster0/AccessPoint0": WEP key 1 ►
set.
```

```
(config-if)> no encryption key 1
Network::Interface::Wifi: "WifiMaster0/AccessPoint0": WEP key 1 ►
removed.
```

History

Version	Description
2.00	The interface encryption key command has been introduced.

3.29.60 interface encryption mppe

Description

Enable [MPPE](#) encryption support.

Command with **no** prefix disables [MPPE](#) encryption.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

PPTP

Synopsis

```
(config-if)> encryption mppe
```

```
(config-if)> no encryption mppe
```

Example

```
(config-if)> encryption mppe
MPPE enabled.
```

```
(config-if)> no encryption mppe
MPPE disabled.
```

History

Version	Description
2.00	The interface encryption mppe command has been introduced.

3.29.61 interface encryption owe

Description

Enable [OWE](#) security algorithms on the wireless interface. By default, the setting is disabled.

Command with **no** prefix disables [OWE](#) support.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WifiMaster

Synopsis

```
(config-if)> encryption owe
(config-if)> no encryption owe
```

Example

```
(config-if)> encryption owe
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
OWE algorithms enabled.

(config-if)> no encryption owe
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
OWE algorithms disabled.
```

History

Version	Description
3.00	The interface encryption owe command has been introduced.

3.29.62 interface encryption tkip hold-down

Description Set the "countermeasure" timer value for [TKIP](#) when the joint use [WPA](#) and [WPA2](#) security algorithms on the wireless interface. By default, the value 60 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFi

Synopsis

```
(config-if)> encryption tkip hold-down <hold-down>
(config-if)> no encryption tkip hold-down
```

Arguments

Argument	Value	Description
hold-down	<i>Integer</i>	Timer value in seconds. Can take values in the range from 0 to 60. If timer is set to 0, the setting is disabled.

Example

```
(config-if)> encryption tkip hold-down 10
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
hold-down interval is 10 sec.
```

```
(config-if)> no encryption tkip hold-down
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
hold-down interval is reset to default (60 sec.).
```

History

Version	Description
3.08	The interface encryption tkip hold-down command has been introduced.

3.29.63 interface encryption wpa

Description

Enable [WPA](#) security algorithms on the wireless interface. Wireless interface can support the joint use of [WPA](#) and [WPA2](#), but supporting [WEP](#) automatically disables when any of the [WPA](#) is enabled.

Command with **no** prefix disables [WPA](#) support.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

WiFi

Synopsis

```
(config-if)> encryption wpa
```

```
(config-if)> no encryption wpa
```

Example

```
(config-if)> encryption wpa
WPA algorithms enabled.
```

History

Version	Description
2.00	The interface encryption wpa command has been introduced.

3.29.64 interface encryption wpa2

Description

Enable [WPA2](#) (IEEE 802.11i, RSN) security algorithms on the wireless interface. Wireless interface can support the joint use of [WPA](#) and [WPA2](#), but supporting [WEP](#) automatically disables when any of the [WPA](#) is enabled.

Command with **no** prefix disables [WPA2](#) support.

Prefix no

Yes

Change settings Yes**Multiple input** No**Interface type** WiFi

Synopsis

```
(config-if)> encryption wpa2
(config-if)> no encryption wpa2
```

Example

```
(config-if)> encryption wpa2
WPA2 algorithms enabled.
```

History	Version	Description
	2.00	The interface encryption wpa2 command has been introduced.

3.29.65 interface encryption wpa3

Description Enable [WPA3](#) security algorithms on the wireless interface. Wireless interface can support the joint use of [WPA2](#) and [WPA3](#). By default, the setting is disabled.

Command with **no** prefix disables [WPA3](#) support.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** WiFi

Synopsis

```
(config-if)> encryption wpa3
(config-if)> no encryption wpa3
```

Example

```
(config-if)> encryption wpa3
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
WPA3 algorithms enabled.

(config-if)> no encryption wpa3
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
WPA3 algorithms disabled.
```

History	Version	Description
	3.00	The interface encryption wpa3 command has been introduced.

3.29.66 interface encryption wpa3 suite-b

Description Enable [WPA3](#) security algorithms to protect sensitive data Suite-B for [WPA Enterprise](#). By default, the feature is disabled.

Prefix no No

Change settings Yes

Multiple input No

Interface type WiFi

Synopsis `(config-if)> encryption wpa3 suite-b`

Example `(config-if)> encryption wpa3 suite-b`
 Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint1": ►
 WPA3 SuiteB enabled.

History

Version	Description
3.01	The interface encryption wpa3 suite-b command has been introduced.

3.29.67 interface flowcontrol

Description Configure Ethernet flow control Tx/Rx. By default, the feature is enabled.
 Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis `(config-if)> flowcontrol on`
`(config-if)> no flowcontrol [send]`

Arguments

Argument	Value	Description
send	<i>Keyword</i>	Flow control works asynchronously.

Example `(config-if)> flowcontrol on`
 Network::Interface::Ethernet: "GigabitEthernet0/0": flow control ►
 enabled.

```
(config-if)> no flowcontrol send
Network::Interface::Ethernet: "GigabitEthernet0/0": flow control ►
send disabled.
```

History

Version	Description
2.08	The interface flowcontrol command has been introduced.

3.29.68 interface follow

Description

Copy settings from AP on WifiMaster0 (2.4 GHz) to the AP on WifiMaster with an index greater than zero (5 GHz or above).

The follower automatically copies all changes applied to the master access point.

If you change the follower settings, the link with the master access point is terminated.

Warning: The WifiMaster0 access points are always used as a source of settings. They never follow. They can only be followed.

Prefix no

No

Change settings

Yes

Multiple input

No

Interface type

AccessPoint

Synopsis

```
(config-if)> follow <access-point>
```

Arguments

Argument	Value	Description
access-point	<i>Interface</i>	The name of an AccessPoint interface on the WifiMaster0 2.4 GHz. You can see the list of available interfaces with help of follow [Tab] command.

Example

```
(config-if)> follow WifiMaster0/AccessPoint0
Network::Interface::AccessPoint: "WifiMaster1/AccessPoint0": set ►
to follow WifiMaster0/AccessPoint0.
```

History

Version	Description
3.07	The interface follow command has been introduced.

3.29.69 interface ft enable

Description	Enable support of <i>FT</i> for Access Point (FT Over the Air, OTA) within the IEEE 802.11r standard. By default, the option is disabled. For correct <i>FT</i> operation between 2,4 and 5 GHz APs it is necessary to fulfill the following conditions: • access points 2,4 GHz and 5 GHz are enabled both • they have the same SSID's • they have the same security settings (encryption type — WPA2 or without password, password value, etc.) Command with no prefix removes the setting.				
Prefix no	Yes				
Change settings	Yes				
Multiple input	No				
Interface type	AccessPoint				
Synopsis	<pre>(config-if)> ft enable</pre> <pre>(config-if)> no ft enable</pre>				
Example	<pre>(config-if)> ft enable Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ► fast transition enabled.</pre> <pre>(config-if)> no ft enable Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ► fast transition disabled.</pre>				
History	<table border="1"> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>2.13</td><td>The interface ft enable command has been introduced.</td></tr> </tbody> </table>	Version	Description	2.13	The interface ft enable command has been introduced.
Version	Description				
2.13	The interface ft enable command has been introduced.				

3.29.70 interface ft mdid

Description	Set Mobility Domain ID for <i>FT</i>. By default, KN value is used. Command with no prefix resets setting to default.
Prefix no	Yes
Change settings	Yes
Multiple input	No

Interface type	AccessPoint						
Synopsis	(config-if)> ft mdid <mdid> (config-if)> no ft mdid						
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td>mdid</td><td>String</td><td>The value of Mobility Domain ID. Consists of 2 ASCII symbols.</td></tr></table>	Argument	Value	Description	mdid	String	The value of Mobility Domain ID. Consists of 2 ASCII symbols.
Argument	Value	Description					
mdid	String	The value of Mobility Domain ID. Consists of 2 ASCII symbols.					
Example	(config-if)> ft mdid 1F Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ► fast transition MDID set to "1F". (config-if)> no ft mdid Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ► fast transition MDID reset to default.						
History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>2.13</td><td>The interface ft mdid command has been introduced.</td></tr></table>	Version	Description	2.13	The interface ft mdid command has been introduced.		
Version	Description						
2.13	The interface ft mdid command has been introduced.						

3.29.71 interface ft otd

Description	Enable support of <i>FT</i> Over-the-DS (Distribution System) within the IEEE 802.11r standard. This type of <i>FT</i> is used for roaming in outdated subscriber devices, for example, in the iPhone 4s. By default, the setting is disabled. Command with no prefix removes the setting.
Prefix no	Yes
Change settings	Yes
Multiple input	No
Interface type	AccessPoint
Synopsis	<pre>(config-if)> ft otd</pre> <pre>(config-if)> no ft otd</pre>
Example	<pre>(config-if)> ft otd</pre> <pre>Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►</pre> <pre>fast transition OTD enabled.</pre> <pre>(config-if)> no ft otd</pre> <pre>Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►</pre> <pre>fast transition OTD disabled.</pre>

History

Version	Description
2.13	The interface ft otd command has been introduced.

3.29.72 interface hide-ssid

Description

Enable hidden [SSID](#) mode. When using this feature, Access Point will not be displayed in the list of available wireless networks. But if user informed of the existence of this network and know its [SSID](#), then he can connect to it. The mode is disabled by default.

Command with **no** prefix disables the mode.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Access Point

Synopsis

```
(config-if)> hide-ssid
```

```
(config-if)> no hide-ssid
```

Example

```
(config-if)> hide-ssid
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
SSID broadcasting disabled.
```

```
(config-if)> no hide-ssid
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
SSID broadcasting enabled.
```

History

Version	Description
2.00	The interface hide-ssid command has been introduced.

3.29.73 interface iapp auto

Description

Generate [IAPP](#) key in automatic mode. To assign the key manually, use [interface iapp key](#) command.

Prefix no

No

Change settings

Yes

Multiple input

No

Interface type

Bridge

Synopsis

```
(config-if)> iapp auto
```

Example (config-if)> **iapp auto**
Network::Interface::Rtx::Iapp: Bridge0 autoconfigured.

History	Version	Description
	3.03	The interface iapp auto command has been introduced.

3.29.74 interface iapp key

Description Assign the *IAPP* Mobile Domain key for successful synchronization between Access Points where *FT* works (**interface ft enable** command). Access Points must belong to the same IP-subnet. By default, the key is not assigned.

Command with **no** prefix removes key value.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Bridge

Synopsis

```
(config-if)> iapp key <key>
```

```
(config-if)> no iapp key
```

Arguments	Argument	Value	Description
	key	<i>String</i>	The value of <i>IAPP</i> key. Maximum key length is 64 characters.

Example (config-if)> **iapp key 11223344556677**
Network::Interface::Rtx::Iapp: Bridge0 key applied.

```
(config-if)> no iapp key
```

Network::Interface::Rtx::Iapp: Bridge0 key cleared.

History	Version	Description
	2.13	The interface iapp key command has been introduced.

3.29.75 interface idle-timeout

Description Set the interval for the STA client to disconnect from the Access Point by inactivity timeout. By default, 600 value is used.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes**Multiple input** No**Interface type** WiFiMaster

Synopsis

```
(config-if)> idle-timeout <idle-timeout>
(config-if)> no idle-timeout
```

Arguments

Argument	Value	Description
idle-timeout	Integer	Idle-timeout value in seconds. Can take values in the range from 60 to 2147483646.

Example

```
(config-if)> idle-timeout 500
Network::Interface::Rtx::WifiMaster: "WifiMaster1": idle timeout ►
value is 500 sec.
```

```
(config-if)> no idle-timeout
Network::Interface::Rtx::WifiMaster: "WifiMaster1": idle timeout ►
disabled.
```

History

Version	Description
3.06	The interface idle-timeout command has been introduced.

3.29.76 interface igmp downstream

Description Enable *IGMP* mode on the interface in the direction of the multicast recipients. *service igmp-proxy* must be enabled on the device. There can be several downstream interfaces.

Command with **no** prefix disables the mode.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config-if)> igmp downstream
(config-if)> no igmp downstream
```

Example

```
(config-if)> igmp downstream
```

```
(config-if)> no igmp downstream
```

History	Version	Description
	2.00	The interface igmp downstream command has been introduced.

3.29.77 interface igmp fork

Description Enable the duplication of outgoing packets *IGMP* upstream to the specified interface. There can be only one fork interface.

Command with **no** prefix disables the mode.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-if)> igmp fork
(config-if)> no igmp fork
```

Example

```
(config-if)> igmp fork
(config-if)> no igmp fork
```

History	Version	Description
	2.00	The interface igmp fork command has been introduced.

3.29.78 interface igmp upstream

Description Enable *IGMP* mode on the interface in the direction of the multicast source. **service igmp-proxy** must be enabled on the device. Only one upstream interface is allowed.

Command with **no** prefix disables the mode.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-if)> igmp upstream
```

```
(config-if)> no igmp upstream
```

Example

```
(config-if)> igmp upstream
```

```
(config-if)> no igmp upstream
```

History

Version	Description
2.00	The interface igmp upstream command has been introduced.

3.29.79 interface include

Description

Specify Ethernet-interface name which will be added to the software bridge as a port.

Command with **no** prefix removes the interface from the bridge.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

Bridge

Synopsis

```
(config-if)> include <interface>
```

```
(config-if)> no include <interface>
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Name or alias of the Ethernet-interface that should be plugged into the bridge.

Example

```
(config-if)> include ISP
```

```
Network::Interface::Bridge: "Bridge0": ISP included.
```

```
(config-if)> no include
```

```
Network::Interface::Bridge: "Bridge0": removed ISP.
```

History

Version	Description
2.00	The interface include command has been introduced.

3.29.80 interface inherit

Description

Specify the name of the Ethernet-interface which will be added to the program bridge as a port. In contrast with the **include** command, **inherit** command

transfers some settings of the interface being added to the bridge, such as IP address, mask and IP-aliases. On removing either the bridge itself or the bridge interface, these settings, even if they have been changed will be copied back to the vacant interface.

The command allows one to add the device control interface to the bridge so that control is not lost.

Command with **no** prefix removes the interface from the bridge, returns the settings that have earlier been inherited by the bridge back to the interface, and resets these settings on the bridge.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type Bridge

Synopsis

```
(config-if)> inherit <interface>
(config-if)> no inherit <interface>
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Name or alias of the Ethernet-interface that should be plugged into the bridge.

Example

```
(config-if)> inherit GigabitEthernet0/Vlan3
Network::Interface::Bridge: "Bridge1": GigabitEthernet0/Vlan3 ►
inherited in Bridge1.
```

```
(config-if)> no inherit
Network::Interface::Bridge: "Bridge1": inherit removed.
```

History

Version	Description
2.00	The interface inherit command has been introduced.

3.29.81 interface ip access-group

Description Assign a named list of filtering rules ([ACL](#), see [access-list](#)) to the interface. Parameter in or out indicates the traffic direction for which the [ACL](#) will be applied. Several ACLs can be assigned to a single interface.

Command with **no** prefix disables the [ACL](#) for the specified interface and traffic direction.

Prefix no Yes

Change settings Yes

Multiple input Yes**Interface type** IP

Synopsis

```
(config-if)> ip access-group <acl> <direction>
(config-if)> no ip access-group [ <acl> [ <direction> ] ]
```

Arguments

Argument	Value	Description
acl	<i>String</i>	List of filtering rules as previously created using access-list command.
direction	in	Apply filtering to incoming packets.
	out	Apply filtering to outgoing packets.

Example

```
(config-if)> ip access-group BLOCK in
Network::Acl: Input "BLOCK" access list added to "CdcEthernet1".
```

```
(config-if)> ip access-group BLOCK out
Network::Acl: Output "BLOCK" access list added to "CdcEthernet1".
```

```
(config-if)> no ip access-group BLOCK in
Network::Acl: "BLOCK" access group deleted from "CdcEthernet1".
```

```
(config-if)> no ip access-group
Network::Acl: All access groups deleted from "CdcEthernet1".
```

History

Version	Description
2.00	The interface ip access-group command has been introduced.

3.29.82 interface ip address

Description Change the IP address and the mask of the network interface. If the address automatic configuration service is running on the interface, for instance, DHCP client, (see [interface ip address dhcp](#)), then the manually set address can be overwritten.

Command with **no** prefix resets the address to 0.0.0.0.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config-if)> ip address <address> <mask>
```



```
(config-if)> no ip address
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	The network interface address.
mask	<i>IP-mask</i>	The network interface mask. There are two ways to specify the mask: the canonical form (for example, 255.255.255.0) and the prefix with bit length (for example, /24).

Example

The network address, defined by the IP address and mask, can be specified in either of the two ways: specify a mask in the canonical form, or set the prefix bit length.

```
(config)> ip address 192.168.9.1/24
Network::Interface::Ip: "Bridge3": IP address is 192.168.9.1/24.
```

```
(config)> no ip address
Network::Interface::Ip: "Bridge3": IP address cleared.
```

History

Version	Description
2.00	The interface ip address command has been introduced.

3.29.83 interface ip address dhcp

Description

Start the DHCP client to automatically configure the network parameters: IP address and mask of the interface, [DNS](#) servers and default gateway.

Command with **no** prefix stops the DHCP client, removes the dynamically configured settings and restores the previous settings of IP address and mask.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Ethernet

Synopsis

```
(config-if)> ip address dhcp
```

```
(config-if)> no ip address dhcp
```

Example

```
(config-if)> ip address dhcp
Dhcp::Client: Started DHCP client on ISP.
```

```
(config-if)> no ip address dhcp
Dhcp::Client: Stopped DHCP client on ISP.
```

History

Version	Description
2.00	The interface ip address dhcp command has been introduced.
4.02	The optional argument hostname has been removed.

3.29.84 interface ip adjust-ttl recv

Description

Modify the TTL for all inbound packets on the interface.

Command with **no** prefix cancels the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-if)> ip adjust-ttl recv <recv>
```

```
(config-if)> no ip adjust-ttl recv
```

Arguments

Argument	Value	Description
recv	<i>Integer</i>	The value of TTL changing. Can take values in the range from 1 to 255 inclusively.

Example

```
(config-if)> ip adjust-ttl recv 1
Network::Interface::Ip: "CdcEthernet0": incoming TTL set to 1.
```

```
(config-if)> no ip adjust-ttl recv
Network::Interface::Ip: "CdcEthernet0": incoming TTL settings ►
removed.
```

History

Version	Description
3.07	The interface ip adjust-ttl recv command has been introduced. Previous command name is interface ip adjust-ttl .

3.29.85 interface ip adjust-ttl send

Description

Modify the TTL for all outbound packets on the interface.

Command with **no** prefix cancels the setting.

Prefix no

Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-if)> ip adjust-ttl send <send>
(config-if)> no ip adjust-ttl send
```

Argument	Value	Description
send	<i>Integer</i>	The value of TTL changing. Can take values in the range from 1 to 255 inclusively.

Example

```
(config-if)> ip adjust-ttl send 65
Network::Interface::Ip: "CdcEthernet1": outgoing TTL set to 65.

(config-if)> no ip adjust-ttl send
Network::Interface::Ip: "CdcEthernet1": outgoing TTL settings ►
removed.
```

Version	Description
2.09	The interface ip adjust-ttl send command has been introduced.

3.29.86 interface ip alias

Description Assign an additional IP address and mask to the network interface (alias).
Command with **no** prefix resets the specified alias to 0.0.0.0. If you use no arguments, the entire list of aliases will be removed.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP, Ethernet

Synopsis

```
(config-if)> ip alias <address> <mask>
(config-if)> no ip alias [ <address> <mask> ]
```

Argument	Value	Description
address	<i>IP address</i>	Additional address of the network interface.
mask	<i>IP-mask</i>	Additional mask of the network interface. There are two ways to specify the mask: the

Argument	Value	Description
		canonical form (for example, 255.255.255.0) and the prefix with bit length (for example, /24).

Example

```
(config-if)> ip alias 192.168.1.88/24
Network::Interface::Ip: "WifiMaster1/WifiStation0": alias 0 is ►
192.168.1.88/24.
```

```
(config-if)> no ip alias 192.168.1.88/24
Network::Interface::Ip: "WifiMaster1/WifiStation0": alias 0 reset ►
to 0.0.0.0/0.
```

```
(config-if)> no ip alias
Network::Interface::Ip: "WifiMaster1/WifiStation0": all aliases ►
removed.
```

History

Version	Description
2.00	The interface ip alias command has been introduced.

3.29.87 interface ip dhcp client broadcast

Description

Set broadcast bit in the DHCP Discover messages, that indicate to a server how the reply should be sent back to the client. By default, the setting is disabled.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Ethernet

Synopsis

```
(config-if)> ip dhcp client broadcast
```

```
(config-if)> no ip dhcp client broadcast
```

Example

```
(config-if)> ip dhcp client broadcast
Dhcp::Client: ISP DHCP client request broadcast enabled.
```

```
(config-if)> no ip dhcp client broadcast
Dhcp::Client: ISP DHCP client request broadcast disabled.
```

History

Version	Description
2.15	The interface ip dhcp client broadcast command has been introduced.

3.29.88 interface ip dhcp client class-id

Description

Specify the device vendor name where *DHCP* client is running (dhcp option 60).

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Ethernet

Synopsis

```
(config-if)> ip dhcp client class-id <class>
```

```
(config-if)> no ip dhcp client class-id
```

Arguments

Argument	Value	Description
class	<i>String</i>	Vendor class name, enclosed in double quotes.

Example

```
(config-if)> ip dhcp client class-id "Carrier"
Dhcp::Client: ISP DHCP client vendor class is set to "Carrier".
```

```
(config-if)> no ip dhcp client class-id
Dhcp::Client: ISP DHCP client vendor class is cleared.
```

History

Version	Description
2.02	The interface ip dhcp client class-id command has been introduced.

3.29.89 interface ip dhcp client debug

Description

Enable debug mode for DHCP client. Detailed info about DHCP client working is saved to the system log.

Command with **no** prefix disables the debug mode.

Prefix no

Yes

Change settings

Yes

Multiple input No**Interface type** Ethernet

Synopsis

```
(config-if)> ip dhcp client debug
```

```
(config-if)> no ip dhcp client debug
```

Example

```
(config-if)> ip dhcp client debug
Dhcp::Client: ISP DHCP client debug enabled.
```

```
(config-if)> no ip dhcp client debug
Dhcp::Client: ISP DHCP client debug disabled.
```

History

Version	Description
2.01	The interface ip dhcp client debug command has been introduced.

3.29.90 interface ip dhcp client displace

Description Displace static address of *what* if it conflicts with an address from DHCP client of main interface.

This command is executed automatically when you connect the USB Ethernet adapter. After that the configuration will be saved and device will be restarted.

Command with **no** prefix cancels the displacement for the specified interface.

Prefix no Yes**Change settings** Yes**Multiple input** Yes**Interface type** Ethernet

Synopsis

```
(config-if)> ip dhcp client displace <what> [ check-session ]
```

```
(config-if)> no ip dhcp client displace <what> [ check-session ]
```

Arguments

Argument	Value	Description
what	<i>Interface</i>	Name or alias of the interface whose static address will be displaced.
check-session	<i>Keyword</i>	With active SCGI sessions, it does not allow rebooting and changing the router's network address. By default, command is added to default-config.

Example

```
(config-if)> ip dhcp client displace Home
Dhcp::Client: ISP added "Home" displacement.
```

```
(config-if)> ip dhcp client displace Home check-session
Dhcp::Client: ISP added "Home" displacement.
```

```
(config-if)> no ip dhcp client displace Home
Dhcp::Client: ISP deleted "Home" displacement.
```

```
(config-if)> no ip dhcp client displace Home check-session
Dhcp::Client: ISP deleted "Home" displacement.
```

History

Version	Description
2.03	The interface ip dhcp client displace command has been introduced.
2.15	Argument check-session was added.

3.29.91 interface ip dhcp client dns-routes

Description

Enable automatic addition of host routes to the DNS server received from the DHCP server. By default, the setting is enabled.

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Ethernet

Synopsis

```
(config-if)> ip dhcp client dns-routes
```

```
(config-if)> no ip dhcp client dns-routes
```

Example

```
(config-if)> ip dhcp client dns-routes
Dhcp::Client: ISP DHCP client DNS host routes are enabled.
```

```
(config-if)> no ip dhcp client dns-routes
Dhcp::Client: ISP DHCP client DNS host routes are disabled.
```

History

Version	Description
2.00	The interface ip dhcp client dns-routes command has been introduced.

3.29.92 interface ip dhcp client fallback

Description Set static IP address in case of DHCP errors.

Command with **no** prefix cancels setting and sets 0.0.0.0 address.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis

```
(config-if)> ip dhcp client fallback <type>
```

```
(config-if)> no ip dhcp client fallback
```

Arguments

Argument	Value	Description
type	<i>String</i>	The type of IP address. Currently implemented only one type — static.

Example

```
(config-if)> ip dhcp client fallback static
Dhcp::Client: A DHCP address fallback is static.
```

```
(config-if)> no ip dhcp client fallback
Dhcp::Client: A DHCP address fallback set to zero for "ISP".
```

History

Version	Description
2.05	The interface ip dhcp client fallback command has been introduced.

3.29.93 interface ip dhcp client hostname

Description Assign a host name which is sent in DHCP-request.

Command with **no** prefix resets the host name to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis

```
(config-if)> ip dhcp client hostname <hostname>
```

```
(config-if)> no ip dhcp client hostname
```


Arguments

Argument	Value	Description
hostname	<i>String</i>	The host name to assign.

Example

```
(config-if)> ip dhcp client hostname MYHOME
Dhcp::Client: ISP DHCP client hostname is set to MYHOME.
```

```
(config-if)> no ip dhcp client hostname
Dhcp::Client: ISP DHCP client hostname is reset to default (HOME).
```

History

Version	Description
2.00	The interface ip dhcp client hostname command has been introduced.

3.29.94 interface ip dhcp client name-servers

Description

Use [DNS](#) server addresses which are received via [DHCP](#). By default, the function is enabled.

Command with **no** prefix denies using of [DNS](#) server addresses which are received via [DHCP](#).

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Ethernet

Synopsis

```
(config-if)> ip dhcp client name-servers
```

```
(config-if)> no ip dhcp client name-servers
```

Example

```
(config-if)> ip dhcp client name-servers
Dhcp::Client: ISP DHCP name servers are enabled.
```

```
(config-if)> no ip dhcp client name-servers
Dhcp::Client: ISP DHCP name servers are disabled.
```

History

Version	Description
2.00	The interface ip dhcp client name-servers command has been introduced.

3.29.95 interface ip dhcp client release

Description DHCP client releases lease IP address and goes into sleep mode. Another execution of this command takes DHCP client to the mode of automatical obtaining of IP address.

Prefix no No

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis (config-if)> **ip dhcp client release**

Example (config-if)> **ip dhcp client release**
Dhcp::Client: IP address released.

History

Version	Description
2.03	The interface ip dhcp client release command has been introduced.

3.29.96 interface ip dhcp client renew

Description DHCP client releases lease IP address and passes in a mode of obtaining a new one.

Prefix no No

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis (config-if)> **ip dhcp client renew**

Example (config-if)> **ip dhcp client renew**
Dhcp::Client: IP address renewed.

History

Version	Description
2.03	The interface ip dhcp client renew command has been introduced.

3.29.97 interface ip dhcp client routes

Description Enable receiving routes from the provider (dhcp options 33, 121, 242). By default it is enabled. In the configuration it is displayed only with **no** prefix.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis

```
(config-if)> ip dhcp client routes
(config-if)> no ip dhcp client routes
```

Example

```
(config-if)> ip dhcp client routes
Dhcp::Client: ISP DHCP client static routes are enabled.
```

```
(config-if)> no ip dhcp client routes
Dhcp::Client: ISP DHCP client static routes are disabled.
```

History

Version	Description
2.05	The interface ip dhcp client routes command has been introduced.

3.29.98 interface ip flow

Description Enable [NetFlow](#) sensor on the specified interface. By default, the setting is disabled.

Command with **no** prefix disables [NetFlow](#) sensor.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-if)> ip flow <direction>
(config-if)> no ip flow
```

Arguments

Argument	Value	Description
direction	ingress	Collection of incoming traffic.

Argument	Value	Description
	egress	Collection of outgoing traffic.
	both	Collection of incoming and outgoing traffic both.

Example

```
(config-if)> ip flow ingress
Netflow::Manager: NetFlow collector is enabled on interface ►
"Home" in "ingress" direction.
```

```
(config-if)> ip flow egress
Netflow::Manager: NetFlow collector is enabled on interface ►
"Home" in "egress" direction.
```

```
(config-if)> ip flow both
Netflow::Manager: NetFlow collector is enabled on interface ►
"Home" in "both" direction.
```

History

Version	Description
2.11	The interface ip flow command has been introduced.

3.29.99 interface ip global

Description

Set property “global” with a parameter to the interface. This property is necessary to configure the default route, DynDNS client and NAT functioning. Can represent global-interfaces as leading to the global network (the Internet).

Property “global” affects the interface priority in setting the default route. The higher the priority the more desirable it is for the user to access the global network through the specified interface. Internet access backup (WAN backup) functionality is using priority “global”.

By default, setting is disabled.

Command with **no** prefix removes property.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-if)> ip global (<priority> | order <order> | auto)
```

```
(config-if)> no ip global
```

Arguments

Argument	Value	Description
priority	<i>Integer</i>	Interface priority to configure the default route. Can take values in the range from 1 to 65534.
order	<i>Integer</i>	Relative priority between interfaces. It can take values in the range from 0 to 65534, but not more than the number of global interfaces.
auto	<i>Keyword</i>	Automatic priority calculation of the interface. The interface is located near the end of the list, but above order X.

Example

```
(config-if)> ip global 10
Network::Interface::IP: "L2TP0": global priority is 10.
```

```
(config-if)> ip global order 0
Network::Interface::IP: "L2TP0": order is 1.
```

```
(config-if)> ip global auto
Network::Interface::IP: Global priority recalculated.
```

```
(config-if)> no ip global
Network::Interface::IP: "L2TP0": global priority cleared.
```

History

Version	Description
2.00	The interface ip global command has been introduced.
2.09	The order and auto arguments were added.

3.29.100 interface ip mru

Description

Set the value of *MRU* to be transmitted to a remote node during establishing the *PPP* (*IPCP*) connection. By default, 1460 value is used.

Command with **no** prefix resets the *MRU* value to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

PPP

Synopsis

```
(config-if)> ip mru <mru>
```

```
(config-if)> no ip mru
```

Arguments

Argument	Value	Description
mru	<i>Integer</i>	<i>MRU</i> value.

Example

```
(config-if)> ip mru 1492
Network::Interface::Ppp: "PPPoE0": MRU saved.
```

```
(config-if)> no ip mru
Network::Interface::Ppp: "PPPoE0": MRU reset to default.
```

History

Version	Description
2.00	The interface ip mru command has been introduced.

3.29.101 interface ip mtu

Description

Set the *MTU* value on the network interface. When establishing a connection via *PPP (IPCP)*, packets with defined *MTU* size will be sent to the remote host, even if the host requested a lower *MTU* value.

Command with **no** prefix resets the *MTU* value to that which was before the first use of the command.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-if)> ip mtu <mtu>
```

```
(config-if)> no ip mtu
```

Arguments

Argument	Value	Description
mtu	<i>Integer</i>	<i>MTU</i> value. Can take values in the range from 64 to 65535 inclusively.

Example

```
(config-if)> ip mtu 1500
Network::Interface::Base: "GigabitEthernet1": static MTU is 1500.
```

```
(config-if)> no ip mtu
Network::Interface::Base: "GigabitEthernet1": static MTU reset to default.
```

History

Version	Description
2.00	The interface ip mtu command has been introduced.

3.29.102 interface ip name-servers

Description Enable the use of [DNS](#) server addresses on the interface. By default, the function is enabled.

Command with **no** prefix denies using of [DNS](#) server addresses on the interface.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-if)> ip name-servers
(config-if)> no ip name-servers
```

Example

```
(config-if)> ip name-servers
Dns::InterfaceSpecific: "GigabitEthernet1": accept IPv4 name ►
servers.

(config-if)> no ip name-servers
Dns::InterfaceSpecific: "GigabitEthernet1": ignore IPv4 name ►
servers.
```

History

Version	Description
4.00	The interface ip name-servers command has been introduced.

3.29.103 interface ip nat loopback

Description Enable reverse translation to send local requests to the local server from the Internet. By default, the setting is enabled for the Home segment interfaces (private and protected security levels).

Command with **no** prefix disables NAT loopback.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-if)> ip nat loopback
```

```
(config-if)> no ip nat loopback
```

Example

```
(config-if)> ip nat loopback
Network::StaticNat: NAT loopback is explicitly enabled on "Home".
```

```
(config-if)> no ip nat loopback
Network::StaticNat: NAT loopback is explicitly disabled on "Home".
```

History

Version	Description
2.11	The ip nat loopback command has been introduced.

3.29.104 interface ip remote

Description Set a remote peer static address.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> ip remote <address>
```

```
(config-if)> no ip remote
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	A remote peer address.

Example

```
(config-if)> ip remote 192.168.2.19
Network::Interface::Ppp: "L2TP0": remote address saved.
```

```
(config-if)> no ip remote
Network::Interface::Ppp: "L2TP0": remote address erased.
```

History

Version	Description
2.00	The interface ip remote command has been introduced.

3.29.105 interface ip tcp adjust-mss

Description Set the limit on the segment size of outgoing [TCP](#) sessions. If the [MSS](#) value, which is transmitted in the header of SYN-packets, exceeds the specified limit, command changes it. The command is applied to the interface and affects all outgoing [TCP](#) SYN packets.

Command with **no** prefix removes all limits from *MSS*.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-if)> ip tcp adjust-mss (pmtu | <mss> )
(config-if)> no ip tcp adjust-mss
```

Arguments

Argument	Value	Description
pmtu	<i>Keyword</i>	Set the upper limit of <i>MSS</i> , equal to the minimum <i>MTU</i> along the path to the remote peer.
mss	<i>Integer</i>	<i>MSS</i> upper limit.

Example

```
(config-if)> ip tcp adjust-mss pmtu
Network::Interface::Ip: "L2TP0": TCP-MSS adjustment enabled.
```

```
(config-if)> ip tcp adjust-mss 1300
Network::Interface::Ip: "L2TP0": TCP-MSS adjustment enabled.
```

```
(config-if)> no ip tcp adjust-mss
Network::Interface::Ip: "L2TP0": TCP-MSS adjustment disabled.
```

History

Version	Description
2.00	The interface ip tcp adjust-mss command has been introduced.

3.29.106 interface ipcp address

Description Use address from the remote peer.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> ipcp address
```

```
(config-if)> no ipcp address
```

Example

```
(config-if)> ipcp address
using address from remote peer
```

```
(config-if)> no ipcp address
not using address from remote peer
```

History

Version	Description
3.09	The interface ipcp address command has been introduced.

3.29.107 interface ipcp default-route

Description

Use the remote peer address as default gateway. By default, the setting is enabled.

Command with **no** prefix denies default gateway changing.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

PPP

Synopsis

```
(config-if)> ipcp default-route
```

```
(config-if)> no ipcp default-route
```

Example

```
(config-if)> ipcp default-route
Using peer as a default gateway.
```

History

Version	Description
2.00	The interface ipcp default-route command has been introduced.

3.29.108 interface ipcp dns-routes

Description

Use routes which are received via *IPCP*. By default, the setting is enabled.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input No**Interface type** PPP

Synopsis

```
(config-if)> ipcp dns-routes
(config-if)> no ipcp dns-routes
```

Example

```
(config-if)> ipcp dns-routes
DNS routes enabled

(config-if)> no ipcp dns-routes
DNS routes disabled
```

History

Version	Description
2.02	The interface ipcp dns-routes command has been introduced.

3.29.109 interface ipcp name-servers

Description Use [DNS](#) servers addresses which are received via [IPCP](#). By default, the setting is enabled.

Command with **no** prefix removes the setting.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** PPP

Synopsis

```
(config-if)> ipcp name-servers
(config-if)> no ipcp name-servers
```

Example

```
(config-if)> ipcp name-servers
using remote name servers.

(config-if)> no ipcp name-servers
not using remote name servers.
```

History

Version	Description
2.00	The interface ipcp name-servers command has been introduced.

3.29.110 interface ipcp vj

Description Enable compression of TCP/IP headers by Van Jacobson's method. By default, the setting is disabled.

Command with **no** prefix disables compression.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> ipcp vj [cid]
(config-if)> no ipcp vj
```

Arguments

Argument	Value	Description
cid	<i>Keyword</i>	Enable compression of Connection ID into headers.

Example

```
(config-if)> ipcp vj cid
VJ compression enabled.
```

```
(config-if)> no ipcp vj
VJ compression disabled.
```

History

Version	Description
2.03	The interface ipcp vj command has been introduced.

3.29.111 interface ipsec aggressive

Description Enable aggressive IKEv1 mode for compatibility with FritzBox L2TP/IPsec server.

Command with **no** prefix disables the mode.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Secure

Synopsis

```
(config-if)> ipsec aggressive
```

```
(config-if)> no ipsec aggressive
```

Example

```
(config-if)> ipsec aggressive
Network::Interface::Secure: IKEv1 Aggressive Mode is enabled.
```

```
(config-if)> no ipsec aggressive
Network::Interface::Secure: IKEv1 Aggressive Mode is disabled.
```

History

Version	Description
4.02	The interface ipsec aggressive command has been introduced.

3.29.112 interface ipsec encryption-level

Description

Set encryption level for *IPSec* connection that is automatically associated with the tunnel. By default, the `normal` value is used.

A detailed description of each level is given in the [Appendix](#).

Command with **no** prefix resets encryption level to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> ipsec encryption-level <level>
```

```
(config-if)> no ipsec encryption-level
```

Arguments

Argument	Value	Description
level	weak	Weak level, DES and MD5 algorithms enabled.
	normal	Level is compatible with most systems, priority is given to AES128 and SHA1.
	normal-3des	Level is compatible with most systems, priority is given to 3DES and SHA1.
	strong	The strongest level, <i>PFS</i> is mandatory, priority is given to AES256 and SHA1.
	weak-pfs	The same as weak, but for the second phase <i>PFS</i> group 1 and 2 is enabled.
	normal-pfs	The same as normal, but for the second phase <i>PFS</i> group 2 and 5 is enabled.
	normal-3des-pfs	The same as normal-3des, but for the second phase <i>PFS</i> group 5 and 14 is enabled.

Argument	Value	Description
	high	A set of modern algorithms for external providers of VPN services.
	strong-aead	The strongest level, priority is given to AES256 and SHA1 with addition of AEAD algorithms.
	strong-aead-pfs	The strongest level, PFS is mandatory, priority is given to AES256 and SHA1 with addition of AEAD algorithms.

Example

```
(config-if)> ipsec encryption-level high
Network::Interface::Secure: "IKE0": security level is set to ►
"high".
```

```
(config-if)> no ipsec encryption-level
Network::Interface::Secure: "IKE0": security level was reset.
```

History

Version	Description
2.08	The interface ipsec encryption-level command has been introduced.
3.07	New levels of encryption has been added — high, strong-aead and strong-aead-pfs.

3.29.113 interface ipsec force-encaps

Description

Enable support of [ESP](#) forced encapsulation in [UDP](#) for client tunnels. By default, the feature is disabled.

Command with **no** prefix cancels the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> ipsec force-encaps
```

```
(config-if)> no ipsec force-encaps
```

Example

```
(config-if)> ipsec force-encaps
Network::Interface::Secure: Force ESP in UDP encapsulation ►
enabled.
```

```
(config-if)> no ipsec force-encaps
Network::Interface::Secure: Force ESP in UDP encapsulation ►
disabled.
```

History

Version	Description
2.12	The interface ipsec force-encaps command has been introduced.

3.29.114 interface ipsec ignore

Description

Disable processing incoming *IKE* packets for *IPSec* service on the interface. By default the command is disabled.

Command with **no** prefix cancels the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> ipsec ignore
```

```
(config-if)> no ipsec ignore
```

Example

```
(config-if)> ipsec ignore
IpSec::Manager: Interface "Gre0" added to IPsec ignore list.
```

```
(config-if)> no ipsec ignore
IpSec::Manager: Interface "Gre0" removed from IPsec ignore list.
```

History

Version	Description
2.10	The interface ipsec ignore command has been introduced.

3.29.115 interface ipsec ikev2

Description

Enable IKEv2 protocol for *IPSec* connection that is automatically associated with the tunnel. By default, IKEv1 is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> ipsec ikev2
```

```
(config-if)> no ipsec ikev2
```

Example

```
(config-if)> ipsec ikev2
Network::Interface::Secure: IKEv2 is enabled.
```

```
(config-if)> no ipsec ikev2
Network::Interface::Secure: IKEv2 is disabled, enable IKEv1.
```

History

Version	Description
2.10	The interface ipsec ikev2 command has been introduced.

3.29.116 interface ipsec nail-up

Description

Enable automatic changes of the secret keys for L2TP/IPsec, EoIP/IPsec, Gre/IPsec, IPIP/IPsec tunnels. By default, setting is enabled.

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> ipsec nail-up
```

```
(config-if)> no ipsec nail-up
```

Example

```
(config-if)> ipsec nail-up
Network::Interface::Secure: SA renegotiation enabled.
```

```
(config-if)> no ipsec nail-up
Network::Interface::Secure: SA renegotiation disabled.
```

History

Version	Description
2.12	The interface ipsec nail-up command has been introduced.

3.29.117 interface ipsec name-servers

Description

Use [DNS](#) server addresses which are received via IKEv1 or IKEv2 [IPSec](#) server. By default, the function is enabled.

Command with **no** prefix denies using of [DNS](#) server addresses which are received via IKEv1 and IKEv2 [IPSec](#) server.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** Secure

Synopsis

```
(config-if)> ipsec name-servers
```

```
(config-if)> no ipsec name-servers
```

Example

```
(config-if)> ipsec name-servers
IpSec::Interface::Ike: "IKE0": automatic name servers via IKE ►
Configuration Payload are enabled.
```

```
(config-if)> no ipsec name-servers
IpSec::Interface::Ike: "IKE0": automatic name servers via IKE ►
Configuration Payload are disabled.
```

History

Version	Description
3.06	The interface ipsec name-servers command has been introduced.

3.29.118 interface ipsec preshared-key

Description Set PSK key for *IPSec* connection that is automatically associated with the tunnel. Command also enables *IPSec* for this tunnel.

Command with **no** prefix resets the key.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** Secure

Synopsis

```
(config-if)> ipsec preshared-key <key>
```

```
(config-if)> no ipsec preshared-key
```

Arguments

Argument	Value	Description
key	<i>String</i>	Secret PSK key value. Latin letters, numbers and equal signs are acceptable. The key length should be between 3 and 72 characters long.

Example

```
(config-if)> ipsec preshared-key gbp1gW3pBQK.g=
Network::Interface::Secure: "L2TP0": preshared key was set.
```

```
(config-if)> no ipsec preshared-key
Network::Interface::Secure: "L2TP0": preshared key was reset.
```

History

Version	Description
2.08	The interface ipsec preshared-key command has been introduced.

3.29.119 interface ipsec proposal lifetime

Description

Set lifetime of *IPSec* transformation Phase1 on the interface. By default, the value 28800 is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> ipsec proposal lifetime <lifetime>
```

```
(config-if)> no ipsec proposal lifetime
```

Arguments

Argument	Value	Description
lifetime	<i>Integer</i>	Lifetime of <i>IPSec</i> transformation in seconds. Can take values in the range from 60 to 2147483647.

Example

```
(config-if)> ipsec proposal lifetime 222222
Network::Interface::Secure: IPsec IKE proposal lifetime set to ►
222222 s.
```

```
(config-if)> no ipsec proposal lifetime
Network::Interface::Secure: IPsec IKE proposal lifetime reset ►
to 28800 s.
```

History

Version	Description
2.11	The interface ipsec proposal lifetime command has been introduced.

3.29.120 interface ipsec proposal local-id

Description Set custom local identifier for [IKE](#).
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Secure

Synopsis

```
(config-if)> ipsec proposal local-id <local-id>
(config-if)> no ipsec proposal local-id
```

Arguments

Argument	Value	Description
local-id	<i>String</i>	IP address or domain name of local host.

Example

```
(config-if)> ipsec proposal local-id 192.168.8.4
Network::Interface::Secure: Set IKE local ID to "192.168.8.4".
```

```
(config-if)> no ipsec proposal local-id
Network::Interface::Secure: Reset IKE local ID.
```

History

Version	Description
3.08	The interface ipsec proposal local-id command has been introduced.

3.29.121 interface ipsec proposal remote-id

Description Set custom remote identifier for [IKE](#).
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Secure

Synopsis

```
(config-if)> ipsec proposal remote-id <remote-id>
(config-if)> no ipsec proposal remote-id
```

Arguments

Argument	Value	Description
remote-id	<i>String</i>	IP address or domain name of remote host.

Example

```
(config-if)> ipsec proposal remote-id my.domain.com
Network::Interface::Secure: Set IKE remote ID to "my.domain.com".
```

```
(config-if)> no ipsec proposal remote-id
Network::Interface::Secure: Reset IKE remote ID.
```

History

Version	Description
3.08	The interface ipsec proposal remote-id command has been introduced.

3.29.122 interface ipsec transform-set lifetime

Description

Set lifetime of *IPSec* transformation Phase2 on the interface. By default, the value 28800 is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Secure

Synopsis

```
(config-if)> ipsec transform-set lifetime <lifetime>
```

```
(config-if)> no ipsec transform-set lifetime
```

Arguments

Argument	Value	Description
lifetime	<i>Integer</i>	Lifetime of <i>IPSec</i> transformation in seconds. Can take values in the range from 60 to 2147483647.

Example

```
(config-if)> ipsec transform-set lifetime 222222
Network::Interface::Secure: IPsec ESP transform-set lifetime set ►
to 222222 s.
```

```
(config-if)> no ipsec transform-set lifetime
Network::Interface::Secure: IPsec ESP transform-set lifetime ►
reset to 28800 s.
```

History

Version	Description
2.11	The interface ipsec transform-set lifetime command has been introduced.

3.29.123 interface ipv6 address

Description

Configure an IPv6 address on the interface. If the argument is **auto**, address is autoconfigured. Passing a literal address as an argument will assign it statically.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-if)> ipv6 address ( <address> | <block> | auto )
```

```
(config-if)> no ipv6 address [ <address> | <block> | auto ]
```

Arguments

Argument	Value	Description
address	<i>IPv6 address</i>	The network interface address.
block	<i>IPv6 address</i>	The network interface address with mask.
auto	<i>Keyword</i>	Enable stateless autoconfiguration.

Example

```
(config-if)> ipv6 address 2a01:291:2:612:52ff:20ff:fe00:1e87
Network::Interface::Ip6: "GigabitEthernet1": added static address ►
2a01:291:2:612:52ff:20ff:fe00:1e87.
```

```
(config-if)> ipv6 address 2001:db8::1
Network::Interface::Ip6: "GigabitEthernet1": added static address ►
2001:db8::1.
```

```
(config-if)> ipv6 address fd08:a648:e303::3/64
Network::Interface::Ip6: "GigabitEthernet1": added static address ►
fd08:a648:e303::3/64.
```

```
(config-if)> no ipv6 address 2a01:291:2:612:52ff:20ff:fe00:1e87
Network::Interface::Ip6: "GigabitEthernet1": removed static ►
address 2a01:291:2:612:52ff:20ff:fe00:1e87.
```

```
(config-if)> no ipv6 address
Network::Interface::Ip6: "GigabitEthernet1": cleared addresses.
```

History

Version	Description
2.00	The interface ipv6 address command has been introduced.

3.29.124 interface ipv6 dhcp client pd hint**Description**

Configure DHCPv6 client prefix delegation hint.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> ipv6 dhcp client pd hint <prefix>
```

```
(config-if)> no ipv6 dhcp client pd hint
```

Arguments

Argument	Value	Description
prefix	<i>Prefix</i>	Requested IPv6 prefix or only its length if specified as <code>::/length</code> .

Example

```
(config-if)> ipv6 dhcp client pd hint fd08:a648:e303::/64  
Ip6::Dhcp::Client: "GigabitEthernet1": set a prefix delegation ►  
hint to "fd08:a648:e303::/64".
```

```
(config-if)> ipv6 dhcp client pd hint ::/64  
Ip6::Dhcp::Client: "GigabitEthernet1": set a prefix delegation ►  
hint to "::/64".
```

```
(config-if)> no ipv6 dhcp client pd hint  
Ip6::Dhcp::Client: "GigabitEthernet1": reset prefix delegation ►  
hint.
```

History

Version	Description
4.01	The interface ipv6 dhcp client pd hint command has been introduced.

3.29.125 interface ipv6 id**Description**

Set the way of IPv6 interface identifier generation. By default, the eui64 value is used.

Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-if)> ipv6 id ( <suffix> | eui64 | random )
```

```
(config-if)> no ipv6 id
```

Arguments

Argument	Value	Description
suffix	<i>Suffix</i>	The static suffix.
eui64	<i>Keyword</i>	The identifier is based on the interface MAC address.
random	<i>Keyword</i>	Random generation of the interface identifier.

Example

```
(config-if)> ipv6 id ::2  
Network::Interface::Ip6: "Bridge0": interface ID is set to ::2.
```

```
(config-if)> ipv6 id eui64  
Network::Interface::Ip6: "Bridge0": interface ID is set to eui64.
```

```
(config-if)> ipv6 id random  
Network::Interface::Ip6: "Bridge0": interface ID is set to random.
```

```
(config-if)> no ipv6 id  
Network::Interface::Ip6: "Bridge0": interface ID is reset to ►  
default value.
```

History

Version	Description
4.01	The interface ipv6 id command has been introduced.

3.29.126 interface ipv6 name-servers

Description Configure retrieval of [DNS](#) information. When **auto** is set, enables DHCPv6 name-server requests.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-if)> ipv6 name-servers (auto)
```

```
(config-if)> no ipv6 name-servers [auto]
```

Arguments

Argument	Value	Description
auto	<i>Keyword</i>	Enable name-server autoconfiguration.

Example

```
(config-if)> ipv6 name-servers auto
Name servers provided by the interface network are accepted.
```

History

Version	Description
2.00	The interface ipv6 name-servers command has been introduced.

3.29.127 interface ipv6 prefix

Description

Configure prefix delegation. When **auto** is set, prefix is requested via DHCPv6-PD.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> ipv6 prefix (<prefix> | auto)
```

```
(config-if)> no ipv6 prefix [<prefix> | auto]
```

Arguments

Argument	Value	Description
auto	<i>Keyword</i>	Enable prefix delegation.
prefix	<i>Prefix</i>	Manual input of prefix.

Example

```
(config-if)> ipv6 prefix 2001:db8:43:ab12::/64
Static IPv6 prefix added.
```

History

Version	Description
2.00	The interface ipv6 prefix command has been introduced.

3.29.128 interface ipv6cp

Description

Enable *IPv6CP* support during establishing connection.

Command with **no** prefix disables *IPv6CP*.

Prefix no

Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> ipv6cp
(config-if)> no ipv6cp
```

Example

```
(config-if)> ipv6cp
IPv6CP enabled.
```

History	Version	Description
	2.00	The interface ipv6cp command has been introduced.

3.29.129 interface lcp acfc

Description Enable compression negotiation of the [Data Link Layer Address and Control fields](#). By default, the feature is disabled.

Command with **no** prefix disables this option and all the remote peer requests for the [ACFC](#) negotiation will be rejected.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> lcp acfc [cid]
(config-if)> no lcp acfc
```

Arguments	Argument	Value	Description
	cid	<i>Keyword</i>	Enable compression of Connection ID into headers.

Example

```
(config-if)> lcp acfc cid
ACFC compression enabled

(config-if)> no lcp acfc cid
ACFC compression disabled
```

History	Version	Description
	2.03	The interface lcp acfc command has been introduced.

3.29.130 interface lcp echo

Description Specify the testing rules of the *PPP* connection with *LCP* echo tools.

By default, interval is set to 30, count is set to 3.

Command with **no** prefix disables *LCP* echo.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> lcp echo <interval> <count> [adaptive]
```

```
(config-if)> no lcp echo
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	Interval between sending <i>LCP</i> echo, in seconds. If within the specified time interval there is no <i>LCP</i> echo request from the remote location, the same request will be sent there asking for response <i>LCP</i> reply.
count	<i>Integer</i>	The number of consecutive requests <i>LCP</i> echo sent, for which no response <i>LCP</i> reply was received. If count of <i>LCP</i> echo requests goes unanswered, the connection is terminated.
adaptive	<i>Keyword</i>	Pppd will send LCP echo-request frames only if no traffic was received from the peer since the last echo-request was sent.

Example

```
(config-if)> lcp echo 20 2
Network::Interface::Ppp: "PPPoE0": LCP echo parameters updated.
```

```
(config-if)> no lcp echo
Network::Interface::Ppp: "PPPoE0": LCP echo disabled.
```

History

Version	Description
2.00	The interface lcp echo command has been introduced.
2.06	The adaptive keyword has been added.

3.29.131 interface lcp pfc

Description Enable compression negotiation of the *PPP Protocol field*. By default, the feature is disabled.

Command with **no** prefix disables this option and all the remote peer requests for the *PFC* negotiation will be rejected.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> lcp pfc [cid]
(config-if)> no lcp pfc
```

Arguments

Argument	Value	Description
cid	<i>Keyword</i>	Enable compression of Connection ID into headers.

Example

```
(config-if)> lcp pfc cid
PFC compression enabled
```

```
(config-if)> no lcp pfc cid
PFC compression disabled
```

History

Version	Description
2.03	The interface lcp pfc command has been introduced.

3.29.132 interface ldpc

Description Enable the *LDPC* code for AP 5 GHz. By default, the feature is disabled.

Command with **no** prefix disables this feature.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WifiMaster

Synopsis

```
(config-if)> ldpc
(config-if)> no ldpc
```

Example

```
(config-if)> ldpc
Network::Interface::Rtx::WifiMaster: "WifiMaster1": LDPC enabled.
```

```
(config-if)> no ldpc
Network::Interface::Rtx::WifiMaster: "WifiMaster1": LDPC disabled.
```

History

Version	Description
2.07	The interface ldpc command has been introduced.

3.29.133 interface led wan

Description

Display the interface status by means of LED. SelectedWan control should be chosen with **system led** command. By default, function is disabled.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> led wan
```

```
(config-if)> no led wan
```

Example

```
(config-if)> led wan
Network::Interface::Led: Selected WAN GigabitEthernet1.
```

```
(config-if)> no led wan
Network::Interface::Led: Selected no WAN.
```

History

Version	Description
2.08	The interface led wan command has been introduced.

3.29.134 interface lldp disable

Description

Disable **LLDP** agent on interface. By default, the feature is enabled.

Command with **no** prefix enables **LLDP** agent.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> lldp disable
```

```
(config-if)> no lldp disable
```

Example

```
(config-if)> lldp disable
Network::DiscoveryManager: LLDP agent is disabled on interface ►
"ISP".
```

```
(config-if)> no lldp disable
Network::DiscoveryManager: LLDP agent is enabled on interface ►
"ISP".
```

History

Version	Description
2.11	The interface lldp disable command has been introduced.

3.29.135 interface mac access-list address

Description

Add a MAC address to the permit/deny filtering list of the interface. Type of access list is set with **interface mac access-list type** command.

Command with **no** prefix removes the specified MAC address from the [ACL](#).

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

Access Point

Synopsis

```
(config-if)> mac access-list address <address>
```

```
(config-if)> no mac access-list address <address>
```

Arguments

Argument	Value	Description
address	<i>MAC address</i>	A MAC address to be added to the ACL .

Example

```
(config-if)> mac access-list address 64:a2:f9:53:b2:12
Network::Interface::Ethernet: "WifiMaster0/AccessPoint1": added ►
64:a2:f9:53:b2:12 to the ACL.
```

```
(config-if)> no mac access-list address 64:a2:f9:53:b2:12
Network::Interface::Ethernet: "WifiMaster0/AccessPoint1": removed ►
64:a2:f9:53:b2:12 from the ACL.
```

```
(config-if)> no mac access-list address
Network::Interface::Ethernet: "WifiMaster0/AccessPoint1": ACL ►
cleared.
```

History

Version	Description
2.00	The interface mac access-list address command has been introduced.

3.29.136 interface mac access-list type

Description Set the type for filtering list of the interface. Type is not defined by default (none value assigned).

Prefix no No

Change settings Yes

Multiple input No

Interface type Access Point

Synopsis (config-if)> **mac access-list type** <type>

Arguments

Argument	Value	Description
type	none	Type of filtering list is not defined.
	permit	Only approved MAC addresses will be added to the list.
	deny	Only restricted MAC addresses will be added to the list.

Example

```
(config-if)> mac access-list type permit
Network::Interface::Ethernet: "WifiMaster0/AccessPoint1": ACL ►
type changed to permit.
```

History

Version	Description
2.00	The interface mac access-list type command has been introduced.

3.29.137 interface mac address

Description Set the MAC address to the specified network interface. Address is specified in hexadecimal format 00:00:00:00:00:00. The command allows one to assign arbitrary address, but warns the user if the new address “multicast” bit is set or “OUI enforced” bit is cleared.

Command with **no** prefix resets the original MAC addresses on the interface.

Warning: Change MAC address on Wi-Fi interface is prohibited.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** MAC

Synopsis

```
(config-if)> mac address <mac>
```

```
(config-if)> no mac address
```

Arguments

Argument	Value	Description
mac	<i>MAC address</i>	New MAC address of the interface.

Example

```
(config-if)> mac address 3C:1F:6E:2A:1C:BA
```

```
(config-if)> no mac address
```

History

Version	Description
2.00	The interface mac address command has been introduced.

3.29.138 interface mac address factory

Description Set the factory MAC address to the interface.**Prefix no** No**Change settings** Yes**Multiple input** No**Interface type** MAC

Synopsis

```
(config-if)> mac address factory <name>
```

Arguments

Argument	Value	Description
name	lan	"LAN" MAC address will be assigned to the interface.
	wan	"WAN" MAC address will be assigned to the interface.
	wlan5	"WLAN5" MAC address will be assigned to the interface.

Example

```
(config-if)> mac address factory lan
```

```
Core::System::UConfig: done.
```

History

Version	Description
2.00	The interface mac address factory command has been introduced.

3.29.139 interface mac band

Description

Bind a registered host to a 2.4 GHz or 5 GHz frequency band.

Command with **no** prefix removes the binding. If you use no argument, the entire list of bindings will be cleared.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

Bridge

Synopsis

```
(config-if)> mac band mac band
```

```
(config-if)> no mac band [ mac ]
```

Arguments

Argument	Value	Description
mac	<i>MAC address</i>	MAC address of the registered client.
band	0	2,4 GHz band.
	1	5 GHz band.

Example

```
(config-if)> mac band c0:b8:83:c2:cb:11 0
Network::Interface::Rtx::MacBand: "Bridge0": bound ►
c0:b8:83:c2:cb:11 to 2.4 GHz.
```

```
(config-if)> mac band c0:b8:83:c2:cb:11 1
Network::Interface::Rtx::MacBand: "Bridge0": bound ►
c0:b8:83:c2:cb:11 to 5 GHz.
```

```
(config-if)> no mac band c0:b8:83:c2:cb:85
Network::Interface::Rtx::MacBand: "Bridge0": unbound ►
c0:b8:83:c2:cb:85 from 2.4 GHz.
```

```
(config-if)> no mac band
Network::Interface::Rtx::MacBand: Unbound all hosts.
```

History

Version	Description
3.05	The interface mac band command has been introduced.

3.29.140 interface mac bssid

Description Specify the Access Point's MAC address to connect to [WISP](#).

Command with **no** prefix removes the MAC address.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WifiStation

Synopsis

```
(config-if)> mac bssid <bssid>
(config-if)> no mac bssid
```

Arguments

Argument	Value	Description
bssid	MAC address	MAC address of WISP Access Point.

Example

```
(config-if)> mac bssid 56:ff:20:00:1e:11
Network::Interface::WifiStation: BSSID set to 56:ff:20:00:1e:11.
```

```
(config-if)> no mac bssid
Network::Interface::WifiStation: BSSID cleared.
```

History

Version	Description
2.13	The interface mac bssid command has been introduced.

3.29.141 interface mac clone

Description Clone the MAC address from the operator's PC to the interface.

Prefix no No

Change settings Yes

Multiple input No

Interface type MAC, IP

Synopsis

```
(config-if)> mac clone
```

Example

```
(config-if)> mac clone
```

History

Version	Description
2.00	The interface mac clone command has been introduced.

3.29.142 interface mobile lte disable-band

Description Disable specified LTE band.

Command with **no** prefix enables LTE band. If you use no argument, the entire list of LTE bands will be enabled.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type Usb

Synopsis

```
(config-if)> mobile lte disable-band <band>
(config-if)> no mobile lte disable-band [ <band> ]
```

Argument	Value	Description
band	<i>Integer</i>	LTE band in the range from 1 to 43 inclusively.

Example

```
(config-if)> mobile lte disable-band 22
UsbQmi::Interface: "UsbQmi0": LTE band 22 disabled.

(config-if)> no mobile lte disable-band 22
UsbQmi::Interface: "UsbQmi0": LTE band 22 enabled.

(config-if)> no mobile lte disable-band
UsbQmi::Interface: "UsbQmi0": all LTE bands are enabled.
```

Version	Description
3.04	The interface mobile lte disable-band command has been introduced.

3.29.143 interface mobile name-servers

Description Use [DNS](#) server addresses which are received via mobile operator. By default, the function is enabled.

Command with **no** prefix denies using of [DNS](#) server addresses which are received via mobile operator.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> mobile name-servers
```

```
(config-if)> no mobile name-servers
```

Example

```
(config-if)> mobile name-servers
UsbQmi::Interface: "UsbQmi0": automatic name servers via QMI are ►
enabled.
```

```
(config-if)> no mobile name-servers
UsbQmi::Interface: "UsbQmi0": automatic name servers via QMI are ►
disabled.
```

History

Version	Description
3.06	The interface mobile name-servers command has been introduced.

3.29.144 interface mobile operator

Description

Set network identifier for [PLMN](#).

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Usb

Synopsis

```
(config-if)> mobile operator <PLMN>
```

```
(config-if)> no mobile operator
```

Arguments

Argument	Value	Description
PLMN	<i>String</i>	Operator identifier.

Example

```
(config-if)> mobile operator 25011
UsbQmi::Interface: Operator PLMN is set to "25011".
```

```
(config-if)> no mobile operator
UsbQmi::Interface: Operator PLMN cleared.
```

History

Version	Description
3.04	The interface mobile operator command has been introduced.

3.29.145 interface mobile pdp

Description Choose IP protocol version for USB modem. IPv6 can be selected only if the corresponding system component is installed. By default, ipv4 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> mobile pdp (ipv4 | ipv6 | ipv4v6)
```

```
(config-if)> no mobile pdp
```

Arguments

Argument	Value	Description
ipv4	<i>String</i>	IPv4 only.
ipv6	<i>String</i>	IPv6 only.
ipv4v6	<i>String</i>	IPv4 and IPv6 dual stack.

Example

```
(config-if)> mobile pdp ipv4
UsbQmi::Interface: Packet data protocol is set to "ipv4".
```

```
(config-if)> mobile pdp ipv4v6
UsbQmi::Interface: Packet data protocol is set to "ipv4v6".
```

```
(config-if)> no mobile pdp
Mobile::Interface: "UsbLte0": packet data protocol is reset to ►
default.
```

History

Version	Description
3.04	The interface mobile pdp command has been introduced.
3.08	The ipv6 argument and NO prefix were added.

3.29.146 interface mobile roaming

Description Enable mobile roaming.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> mobile roaming
(config-if)> no mobile roaming
```

Example

```
(config-if)> mobile roaming
UsbQmi::Interface: "UsbQmi0": roaming is enabled.

(config-if)> no mobile roaming
UsbQmi::Interface: "UsbQmi0": roaming is disabled.
```

History	Version	Description
	3.03	The interface mobile roaming command has been introduced.

3.29.147 interface mobile scan

Description Run a mobile network scan. The scanning process takes 20-50 seconds. Command with **no** prefix stops scanning.

Prefix no Yes

Change settings No

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> mobile scan
(config-if)> no mobile scan
```

Example

```
(config-if)> mobile scan
UsbQmi::Interface: Network scanning started.

(config-if)> no mobile scan
UsbQmi::Interface: Network scanning stopped.
```

History	Version	Description
	3.05	The interface mobile scan command has been introduced.

3.29.148 interface mobile umts disable-band

Description	Disable specified UMTS band. Command with no prefix enables UMTS band. If you use no argument, the entire list of UMTS bands will be enabled.		
Prefix no	Yes		
Change settings	Yes		
Multiple input	Yes		
Interface type	Usb		
Synopsis	<pre>(config-if)> mobile umts disable-band <band></pre> <pre>(config-if)> no mobile umts disable-band [<band>]</pre>		
Arguments			
	Argument	Value	Description
	band	Integer	UMTS band. Can take values 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 26.
Example	<pre>(config-if)> mobile umts disable-band 6</pre>		
	UsbQmi::Interface: "UsbQmi0": WCDMA band 6 disabled.		
	<pre>(config-if)> no mobile lte disable-band 6</pre>		
	UsbQmi::Interface: "UsbQmi0": WCDMA band 6 enabled.		
	<pre>(config-if)> no mobile lte disable-band</pre>		
	UsbQmi::Interface: "UsbQmi0": all WCDMA bands are enabled.		
History			
	Version	Description	
	3.05	The interface mobile umts disable-band command has been introduced.	

3.29.149 interface modem connect

Description	Command to connect for USB-modem. Modem must be initialized with tty init command before execution. Command with no prefix terminates the connection.	
Prefix no	Yes	
Change settings	Yes	
Multiple input	No	
Interface type	UsbModem	

Synopsis

```
(config-if)> modem connect ( dial <phone> | <string> )
```

```
(config-if)> no modem connect
```

Arguments

Argument	Value	Description
phone	<i>String</i>	The phone number for dialing.
string	<i>String</i>	An arbitrary command.

Example

```
(config-if)> modem connect dial *99#  
Network::Interface::UsbModem: "UsbModem0": connect sequence saved.
```

```
(config-if)> modem connect dial *99#  
Network::Interface::UsbModem: "UsbModem0": connect sequence ►  
cleared.
```

History

Version	Description
2.00	The interface modem connect command has been introduced.

3.29.150 interface modem timeout

Description

Set modem connection timeout. Setting is used for slow modems/connections. By default, 30 value is used.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

UsbModem

Synopsis

```
(config-if)> modem timeout <timeout>
```

```
(config-if)> no modem timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	Value of timeout in seconds. Can take values in the range from 1 to 600 inclusively.

Example

```
(config-if)> modem timeout 300  
Network::Interface::UsbModem: "UsbModem0": connect timeout is ►  
300 seconds.
```

```
(config-if)> no modem timeout
Network::Interface::UsbModem: "UsbModem0": connect timeout is ►
unchanged, defaults to 30 seconds.
```

History

Version	Description
2.05	The interface modem timeout command has been introduced.

3.29.151 interface openconnect accept-addresses

Description Enable address accepting from the [OpenConnect](#) server.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type OpenConnect

Synopsis

```
(config-if)> openconnect accept-addresses
(config-if)> no openconnect accept-addresses
```

Example

```
(config-if)> openconnect accept-addresses
OpenConnect::Interface: "OpenConnect0": enabled addresses accept.

(config-if)> no openconnect accept-addresses
OpenConnect::Interface: "OpenConnect0": disabled addresses accept.
```

History

Version	Description
4.02	The interface openconnect accept-addresses command has been introduced.

3.29.152 interface openconnect accept-routes

Description Enable receiving routes from a remote side via [OpenConnect](#).

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type OpenConnect

Synopsis

```
(config-if)> openconnect accept-routes
```

```
(config-if)> no openconnect accept-routes
```

Example

```
(config-if)> openconnect accept-routes  
OpenConnect::Interface: "OpenConnect0": enabled routes accept.
```

```
(config-if)> no openconnect accept-routes  
OpenConnect::Interface: "OpenConnect0": disabled routes accept.
```

History

Version	Description
4.03	The interface openconnect accept-routes command has been introduced.

3.29.153 interface openconnect authgroup

Description

Configure authgroup setting for the [OpenConnect](#).

Note: The command implements a connection to the Cisco ASA.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

OpenConnect

Synopsis

```
(config-if)> openconnect authgroup <authgroup>
```

```
(config-if)> no openconnect authgroup
```

Arguments

Argument	Value	Description
authgroup	<i>String</i>	The group name.

Example

```
(config-if)> openconnect authgroup MYEXAMPLE  
OpenConnect::Interface: "OpenConnect0": set auth group ►  
"MYEXAMPLE".
```

```
(config-if)> no openconnect authgroup  
OpenConnect::Interface: "OpenConnect0": removed auth group.
```

History

Version	Description
4.02	The interface openconnect authgroup command has been introduced.

3.29.154 interface openconnect dtls

Description Configure the DTLS mode for the [OpenConnect](#). By default, the mode is enabled.

Note: OpenConnect prefers PPP-over-DTLS. It will fall over to PPP-over-TLS if PPP-over-DTLS fails, or if it is disabled.

Command with **no** prefix disables the DTLS mode.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type OpenConnect

Synopsis

```
(config-if)> openconnect dtls
```

```
(config-if)> no openconnect dtls
```

Example

```
(config-if)> openconnect dtls
OpenConnect::Interface: "OpenConnect0": enabled DTLS mode.
```

```
(config-if)> no openconnect dtls
OpenConnect::Interface: "OpenConnect0": disabled DTLS mode.
```

History

Version	Description
4.03	The interface openconnect dtls command has been introduced.

3.29.155 interface openconnect protocol fortinet

Description Enable support [Fortinet](#)¹³ protocol for the [OpenConnect](#).

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type OpenConnect

Synopsis

```
(config-if)> openconnect protocol fortinet
```

```
(config-if)> no openconnect protocol
```

¹³ <https://www.infradead.org/openconnect/fortinet.html>

Example

```
(config-if)> openconnect protocol fortinet
OpenConnect::Interface: "OpenConnect0": set protocol "fortinet".

(config-if)> no openconnect protocol
OpenConnect::Interface: "OpenConnect0": removed protocol.
```

History

Version	Description
4.03	The interface openconnect protocol fortinet command has been introduced.

3.29.156 interface openvpn accept-routes

Description

Enable receiving routes from a remote side via OpenVPN.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

OpenVPN

Synopsis

```
(config-if)> openvpn accept-routes

(config-if)> no openvpn accept-routes
```

Example

```
(config-if)> openvpn accept-routes
Network::Interface::OpenVpn: "OpenVPN0": enable automatic routes ►
accept via tunnel.

(config-if)> no openvpn accept-routes
Network::Interface::OpenVpn: "OpenVPN0": disable automatic routes ►
accept via tunnel.
```

History

Version	Description
2.10	The interface openvpn accept-routes command has been introduced.

3.29.157 interface openvpn connect

Description

Set interface for OpenVPN connection. If you use no argument, connection is set via any interface.

Prefix no

No

Change settings

Yes

Multiple input	No						
Interface type	OpenVPN						
Synopsis	(config-if)> openvpn connect [via <via>] (config-if)> openvpn connect						
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td>via</td><td>Interface</td><td>Full interface name or an alias.</td></tr></table>	Argument	Value	Description	via	Interface	Full interface name or an alias.
Argument	Value	Description					
via	Interface	Full interface name or an alias.					
Example	(config-if)> openvpn connect via ISP Network::Interface::OpenVpn: "OpenVPN0": set connection via ISP. (config-if)> openvpn connect Network::Interface::OpenVpn: "OpenVPN0": set connection via any ► interface.						
History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>2.10</td><td>The interface openvpn connect command has been introduced.</td></tr></table>	Version	Description	2.10	The interface openvpn connect command has been introduced.		
Version	Description						
2.10	The interface openvpn connect command has been introduced.						

3.29.158 interface openvpn name-servers

Description	Use DNS server addresses which are received via OpenVPN server. By default, the function is enabled. Command with no prefix denies using of DNS server addresses which are received via OpenVPN server.
Prefix no	Yes
Change settings	Yes
Multiple input	No
Interface type	OpenVPN
Synopsis	<pre>(config-if)> openvpn name-servers</pre> <pre>(config-if)> no openvpn name-servers</pre>
Example	<pre>(config-if)> openvpn name-servers</pre> <pre>Network::Interface::OpenVpn: "OpenVPN0": automatic name servers ► via tunnel are enabled.</pre> <pre>(config-if)> no openvpn name-servers</pre> <pre>Network::Interface::OpenVpn: "OpenVPN0": automatic name servers ► via tunnel are disabled.</pre>

History

Version	Description
3.06	The interface openvpn name-servers command has been introduced.

3.29.159 interface peer

Description

Specify ID of the remote peer to which the [PPP](#) connection will be used. A more precise meaning of configuration depends on interface type. For example, for PPPoE the **interface peer** command specifies the name of access hub, for PPTP — remote host name or IP address, and for SSTP — specifies a remote server with port 443 or another.

Command with **no** prefix cancels the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

PPP

Synopsis

```
(config-if)> peer <peer>
```

```
(config-if)> no peer
```

Arguments

Argument	Value	Description
peer	<i>String</i>	Remote connection point ID or remote server address <code>host.example.net:port</code> . By default, port number is 443.

Example

```
(config-if)> peer 111
```

```
(config-if)> peer host.example.net:5555
```

History

Version	Description
2.00	The interface peer command has been introduced.
2.12	Added the ability to change the port of a remote server.

3.29.160 interface peer-isolation

Description

Enable the isolation of wireless clients in the Home segment. The setting applies on the Bridge interface and has an effect for all access points included in it. Also, it blocks traffic from wireless clients inside the L2 network.

Command with **no** prefix cancels the setting.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** Bridge

Synopsis

```
(config-if)> peer-isolation
```

```
(config-if)> no peer-isolation
```

Example

```
(config-if)> peer-isolation
```

```
Network::Interface::Ethernet: "Bridge0": peer isolation enabled.
```

```
(config-if)> no peer-isolation
```

```
Network::Interface::Ethernet: "Bridge0": peer isolation disabled.
```

History

Version	Description
2.10	The interface peer-isolation command has been introduced.

3.29.161 interface ping-check profile

Description Assign [Ping Check](#) profile to the interface.

Command with **no** prefix cancels the setting.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config-if)> ping-check profile <profile>
```

```
(config-if)> no ping-check profile
```

Arguments

Argument	Value	Description
profile	<i>String</i>	Profile name to assign.

Example

```
(config-if)> ping-check profile test
```

```
PingCheck::Client: Set ping-check profile for interface "ISP".
```

```
(config-if)> no ping-check profile
```

```
PingCheck::Client: Reset ping-check profile for interface "ISP".
```

History

Version	Description
2.04	The interface ping-check profile command has been introduced.

3.29.162 interface ping-check restart

Description

Enable interface restart if *Ping Check* is triggered (Internet is not available on interface). By default the function is disabled.

Command with **no** prefix disables the function.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> ping-check restart [ <interface> ]
```

```
(config-if)> no ping-check restart
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full name or alias of the interface to be restarted when the <i>Ping Check</i> on the binded interface is triggered. If this argument is not specified, the interface binded with <i>Ping Check</i> profile will be restarted.

Example

```
(config-if)> ping-check restart
PingCheck::Client: Enabled "PPPoE0" interface restart.
```

```
(config-if)> ping-check restart ISP
PingCheck::Client: Enabled "ISP" interface restart for "PPPoE0".
```

```
(config-if)> no ping-check restart
PingCheck::Client: Remove restart settings for "PPPoE0".
```

History

Version	Description
3.04	The interface ping-check restart command has been introduced.

3.29.163 interface pmf

Description

Enable *PMF* functionality.

Note: With [WPA2](#) or [WPA2+WPA3](#) encryption selected, the `pmf` command enables PMF Capable (MFPC) for the clients connecting to the AP.

If the client supports [PMF](#) functionality, then it will be able to connect with [PMF](#), if not, then it will connect without [PMF](#) to the AP.

If WPA3 encryption is selected, the [PMF](#) function becomes mandatory for clients connecting to the AP.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFi

Synopsis

```
(config-if)> pmf [force]
(config-if)> no pmf
```

Arguments

Argument	Value	Description
force	<i>Keyword</i>	Enable the mandatory PMF function for WPA2 encryption.

Example

```
(config-if)> pmf
Network::Interface::Rtx::WifiStation: "WifiMaster0/WifiStation0": ►
PMF enabled.
```

```
(config-if)> pmf force
Network::Interface::Mtk::WifiStation: "WifiMaster0/WifiStation0": ►
PMF forced.
```

```
(config-if)> no pmf
Network::Interface::Rtx::WifiStation: "WifiMaster0/WifiStation0": ►
PMF disabled.
```

History

Version	Description
2.09	The interface pmf command has been introduced.
4.01	The force keyword was added.

3.29.164 interface pmksa-lifetime

Description Change the [PMK](#) cache lifetime. By default, the value 1440 is set.

Prefix no No

Change settings Yes

Multiple input No

Interface type WiFiMaster

Synopsis `(config-if)> pmksa-lifetime <pmksa-lifetime>`

Arguments

Argument	Value	Description
pmksa-lifetime	<i>Integer</i>	Lifetime value, in minutes.

Example

```
(config-if)> interface WifiMaster1 pmksa-lifetime 43200
Network::Interface::Mtk::WifiMaster: "WifiMaster1": PMKSA cache ►
lifetime updated.
```

History

Version	Description
4.01	The interface pmksa-lifetime command has been introduced.

3.29.165 interface power

Description Set the transmitter power for the radio interface. Transmitter power is limited by the hardware capabilities and state laws applicable to radio broadcast. This command allows one to only reduce the power of the transmitter relative to its maximum power, such as to decrease potential interference with other devices in this range/band. By default, the setting value of the power is set to 100.

Prefix no No

Change settings Yes

Multiple input No

Interface type Radio

Synopsis `(config-if)> power <power>`

Arguments

Argument	Value	Description
power	<i>Integer</i>	The transmitter power as the percentage of the maximum power (from 1 to 100).

Example

```
(config-if)> power 1
Network::Interface::Rtx::WifiMaster: "WifiMaster0": TX power ►
level set.
```

History

Version	Description
2.00	The interface power command has been introduced.

3.29.166 interface pppoe service

Description Specify PPPoE service. If service is not defined, then PPPoE client will be connected to an arbitrary service.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPPoE

Synopsis

```
(config-if)> pppoe service <service>
(config-if)> no pppoe service
```

Arguments

Argument	Value	Description
service	<i>String</i>	Name of PPPoE service.

Example

```
(config-if)> pppoe service TEST
Network::Interface::Pppoe: "PPPoE0": service set.
```

```
(config-if)> no pppoe service
Network::Interface::Pppoe: "PPPoE0": service removed.
```

History

Version	Description
2.05	The interface pppoe service command has been introduced.

3.29.167 interface pppoe session auto-cleanup

Description Enable sending a PADT packet for the unfinished PPPoE session. By default the option is enabled.

Command with **no** prefix disables sending a PADT packet.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPPoE

Synopsis

```
(config-if)> pppoe session auto-cleanup
(config-if)> no pppoe session auto-cleanup
```

Example

```
(config-if)> pppoe session auto-cleanup
Network::Interface::Ppp: "PPPoE0": enabled session auto cleanup.

(config-if)> no pppoe session auto-cleanup
Network::Interface::Ppp: "PPPoE0": disabled session auto cleanup.
```

History

Version	Description
3.03	The interface pppoe session auto-cleanup command has been introduced.

3.29.168 interface preamble-short

Description

Use short *preamble*. By default, the setting is disabled.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Radio

Synopsis

```
(config-if)> preamble-short
(config-if)> no preamble-short
```

Example

```
(config-if)> preamble-short
Network::Interface::Rtx::WifiMaster: "WifiMaster0": short ►
preamble enabled.

(config-if)> no preamble-short
Network::Interface::Rtx::WifiMaster: "WifiMaster0": short ►
preamble disabled.
```

History

Version	Description
2.00	The interface preamble-short command has been introduced.

3.29.169 interface proxy connect

Description

Start the process of connecting to the proxy server. By default, connection is set via any interface.

Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Proxy

Synopsis

```
(config-if)> proxy connect [ via <via> ]
(config-if)> no proxy connect
```

Arguments

Argument	Value	Description
via	<i>Interface</i>	Interface through which remote node is accessed.

Example

```
(config-if)> proxy connect via WifiMaster1/WifiStation0
Proxy::Interface: "Proxy0": set connection via ►
WifiMaster1/WifiStation0.
```

```
(config-if)> no proxy connect
Proxy::Interface: "Proxy0": set connection via any interface.
```

History

Version	Description
3.09	The interface proxy connect command has been introduced.

3.29.170 interface proxy protocol

Description Set the connection protocol. By default, the http protocol and [TCP](#) connection is used for proxy server.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Proxy

Synopsis

```
(config-if)> proxy protocol <protocol>
(config-if)> no proxy protocol
```

Arguments

Argument	Value	Description
protocol	socks5	Use SOCKS5 protocol for connection.
	http	Use HTTP or HTTPS protocol for connection.

Example

```
(config-if)> proxy protocol socks5
Proxy::Interface: "Proxy0": set proxy protocol to socks5.
```

```
(config-if)> no proxy protocol
Proxy::Interface: "Proxy0": reset proxy protocol.
```

History

Version	Description
3.09	The interface proxy protocol command has been introduced.

3.29.171 interface proxy socks5-udp

Description

Enable [UDP](#) mode for the [SOCKS5](#) protocol. By default, the [UDP](#) mode is disabled.

Command with **no** prefix disables the mode.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Proxy

Synopsis

```
(config-if)> proxy socks5-udp
```

```
(config-if)> no proxy socks5-udp
```

Example

```
(config-if)> proxy socks5-udp
Proxy::Interface: "Proxy0": enable SOCKS5 UDP mode.
```

```
(config-if)> no proxy socks5-udp
Proxy::Interface: "Proxy0": disable SOCKS5 UDP mode.
```

History

Version	Description
4.1	The interface proxy socks5-udp command has been introduced.

3.29.172 interface proxy upstream

Description

Set proxy server for connection.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Proxy

Synopsis

```
(config-if)> proxy upstream <host> [<port>]
(config-if)> no proxy upstream
```

Arguments

Argument	Value	Description
host	<i>String</i>	IP-address or domain name of proxy server.
port	<i>Integer</i>	The server port.

Example

```
(config-if)> proxy upstream 161.8.174.48 1080
Proxy::Interface: "Proxy0": set proxy upstream to ►
161.8.174.48:1080.
```

```
(config-if)> no proxy upstream
Proxy::Interface: "Proxy0": cleared proxy upstream.
```

History

Version	Description
3.09	The interface proxy upstream command has been introduced.

3.29.173 interface reconnect-delay

Description Set the period of time between reconnection attempts. By default, value 3 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type PPP

Synopsis

```
(config-if)> reconnect-delay <sec>
(config-if)> no reconnect-delay
```

Arguments

Argument	Value	Description
sec	<i>Integer</i>	Value of time in seconds. Can take values in the range from 3 to 600.

Example

```
(config-if)> reconnect-delay 3
Network::Interface::Ppp: "PPTP1": reconnect delay set to 3 ►
seconds.
```

```
(config-if)> no reconnect-delay
Network::Interface::Ppp: "PPTP0": reconnect delay reset to ►
default.
```

History

Version	Description
2.11	The interface reconnect-delay command has been introduced.

3.29.174 interface rekey-interval

Description

Set the period of time between automatic changes of the secret keys, which all devices on the network share. By default, 86400 value is used.

Command with **no** prefix disables keys changing.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

WiFi

Synopsis

```
(config-if)> rekey-interval <interval>
```

```
(config-if)> no rekey-interval
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	Value of rekey interval in seconds.

Example

```
(config-if)> rekey-interval 3000
Network::Interface::Rtx::WifiMaster: "WifiMaster0": rekey ►
interval is 3000 sec.
```

```
(config-if)> no rekey-interval
Network::Interface::Rtx::WifiMaster: "WifiMaster0": rekey ►
interval disabled.
```

History

Version	Description
2.06	The interface rekey-interval command has been introduced.
2.15	Added default value of rekey interval 3600 sec.
3.04	Default value of rekey interval is changed to 86400 sec.

3.29.175 interface rename

Description

Assign arbitrary name to the specified network interface. The interface can be referred to by the new name just like by ID.

Command with **no** prefix removes the setting.

Warning: Do not rename Home interface. This can cause unpredictable system errors.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> rename <rename>
```

```
(config-if)> no rename
```

Arguments

Argument	Value	Description
rename	<i>String</i>	New interface name.

Example

```
(config-if)> rename PPPoE1  
Network::Interface::Base: "PPPoE0": renamed to "PPPoE1".
```

```
(config-if)> no rename  
Network::Interface::Base: "PPPoE0": name cleared.
```

History

Version	Description
2.08	The interface rename command has been introduced.

3.29.176 interface rf e2p set

Description

Change the memory cell value of calibration data at *offset* by *value* for the specified interface.

Prefix no

No

Change settings

No

Multiple input No

Interface type Radio

Synopsis `(config-if) rf e2p set <offset> <value>`

Arguments

Argument	Value	Description
offset	<i>Hex</i>	Memory cell location. Can take values in the range from 1E0 to 1FE.
value	<i>Hex</i>	Value to be set. Can take values in the range from 0 to FFFF.

Example

```
(config-if)> rf e2p set 1f6 0
Network::Interface::Rtx::WifiMaster: EEPROM [0x01F6]:0000 set.
```

History

Version	Description
2.04	The interface rf e2p set command has been introduced.

3.29.177 interface role

Description Set a role for the interface. Multiple roles can be assigned to one interface. Command is used for correct view of VLAN connections in the web interface.

Command with **no** prefix removes the role. If you use no arguments, the entire list of roles will be removed.

Prefix no Yes

Change settings No

Multiple input Yes

Synopsis `(config-if)> role <role> [ for <ifor> ]`

`(config-if)> no role [ role ]`

Arguments

Argument	Value	Description
role	inet	Interface is used for Internet connection.
	iptv	Interface is used for IPTV service.
	voip	Interface is used for VoIP service.
	misc	Interface is used for IP Policy .
ifor	<i>Interface</i>	Full interface name or an alias.

Example

```
(config-if)> role iptv for GigabitEthernet1
Network::Interface::Base: "GigabitEthernet1": assigned role ▶
"iptv" for GigabitEthernet1.

(config-if)> no role iptv for GigabitEthernet1
Network::Interface::Base: "GigabitEthernet1": deleted role "iptv".

(config-if)> no role
Network::Interface::Base: "GigabitEthernet1": deleted all roles.
```

History

Version	Description
2.06	The interface role command has been introduced.
2.10	Argument misc was added.

3.29.178 interface rrm

Description

Enable [RRM](#) for search of nearby APs according to IEEE 802.11k standard in order to provide this AP list to the subscriber device by request. By default, the option is disabled.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

AccessPoint

Synopsis

```
(config-if)> rrm
(config-if)> no rrm
```

Example

```
(config-if)> rrm
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ▶
RRM enabled.

(config-if)> no rrm
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ▶
RRM disabled.
```

History

Version	Description
2.13	The interface rrm command has been introduced.

3.29.179 interface rssi-threshold

Description Set the RSSI signal strength threshold for the Access Point at which Wi-Fi clients will be disconnected and cannot connect to the Access Point. By default, the RSSI value 0 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type AccessPoint

Synopsis

```
(config-if)> rssi-threshold <rssi-threshold>
(config-if)> no rssi-threshold
```

Argument	Value	Description
rssi-threshold	<i>Integer</i>	RSSI values in the range from -100 to 0. If value is set to 0, the setting is disabled.

Example

```
(config-if)> rssi-threshold -30
Network::Interface::Mtk::AccessPoint: "WifiMaster0/AccessPoint0": ►
rssi threshold is set to -30.
```

```
(config-if)> no rssi-threshold
Network::Interface::Mtk::AccessPoint: "WifiMaster0/AccessPoint0": ►
rssi threshold reset to 0.
```

Version	Description
4.01	The interface rssi-threshold command has been introduced.

3.29.180 interface schedule

Description Assign a schedule to the interface. Schedule must be created and customized with [schedule action](#) command before execution.

Command with **no** prefix unbinds the schedule.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-if)> schedule <schedule>
```

```
(config-if)> no schedule
```

Arguments

Argument	Value	Description
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(config-if)> schedule WIFI  
Network::Interface::Base: "WifiMaster0": schedule is "WiFi".
```

```
(config-if)> no schedule  
Network::Interface::Base: "WifiMaster0": schedule cleared.
```

History

Version	Description
2.06	The interface schedule command has been introduced.

3.29.181 interface security-level

Description

Specify the interface security level. The security levels define the firewall logic:

- Allow establishing private → public connections.
- Prohibit establishing connections coming to the public interface, i. e. in the direction public → private and public → public.
- The device itself accepts network connections (allows control) only from private interfaces.
- Data transfer between private interfaces can be allowed or disallowed depending on the **isolate-private** global parameter.
- protected interfaces have no access to device and to other private/protected subnetworks, but they have access to public interfaces and to the internet. The device provides only DHCP and DNS services to the protected segments.
- Data transfer from private to protected interfaces is forbidden by default. To allow such connection use the **no isolate-private** command.

Note: By default, to all newly created interfaces public security level assigned.

Access lists **access-list** have higher priority than the security levels, so they can be used to set additional rules of packet filtering.

Prefix no

No

Change settings Yes

Multiple input No

Interface type IP

Synopsis `(config-if)> security-level (public | private | protected)`

Example Despite the fact that there is no functionality to disable the firewall completely, it is possible to disable it for particular directions. Suppose that it is necessary to allow data transfer between the “home” network Home and global network PPPoE0. To accomplish that, to both interfaces must be assigned private security level and function **isolate-private** must be disabled.

```
(config)> interface Home security-level private
Network::Interface::IP: "Bridge0": security level set to ►
"private".
```

```
(config)> interface PPPoE0 security-level private
Network::Interface::IP: "PPPoE0": security level set to "private".
```

```
(config)> no isolate-private
Netfilter::Manager: Private networks not isolated.
```

Note: The firewall and the address translation — are the functions designed to solve fundamentally different problems. Enabling NAT between Home and PPPoE0 interfaces in the configuration shown above, does not prohibit access to the network Home from the global network. Even as the address translation is enabled by command **ip nat Home**, the packets from PPPoE0 will get to Home network.

History

Version	Description
2.00	The interface security-level command has been introduced.
2.06	The protected parameter was added.

3.29.182 interface sim pin

Description Set PIN-code for SIM card.
Command with **no** prefix removes PIN-code.

Prefix no Yes

Change settings No

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> sim pin <pin>
```

```
(config-if)> no sim pin
```

Arguments

Argument	Value	Description
pin	String	4 to 8 digits PIN.

Example

```
(config-if)> sim pin 0000  
Mobile::Interface: "UsbLte0": PIN code has been set.
```

```
(config-if)> no sim pin  
Mobile::Interface: "UsbLte0": PIN code has been reset.
```

History

Version	Description
3.02	The interface sim pin command has been introduced.
4.00	Prefix no was added.

3.29.183 interface sim slot

Description

Switch SIM-slot for QMI modem. By default, the 1 slot is set.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Usb

Synopsis

```
(config-if)> sim slot <slot>
```

```
(config-if)> no sim slot
```

Arguments

Argument	Value	Description
slot	1	Set 1 or 2 slot.
	2	

Example

```
(config-if)> sim slot 2  
Mobile::Interface: "UsbQmi0": SIM slot is set to "2".
```

```
(config-if)> no sim slot  
Mobile::Interface: "UsbQmi0": SIM slot is reset to default.
```

History

Version	Description
3.08	The interface sim slot command has been introduced.

3.29.184 interface speed

Description

Configure the speed of the Ethernet interface. By default, auto value is set.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Ethernet

Synopsis

```
(config-if)> speed (10 | 100 | 1000 | auto)
```

```
(config-if)> no speed
```

Arguments

Argument	Value	Description
10	<i>Keyword</i>	Connection speed in Mbit/s.
100		
1000		
auto	<i>Keyword</i>	Automatical speed configuration.

Example

```
(config-if)> speed 1000
Network::Interface::Ethernet: "GigabitEthernet1/0": speed set ►
to 1000.
```

```
(config-if)> no speed
Network::Interface::Ethernet: "GigabitEthernet1/0": speed reset ►
to default (auto-negotiation).
```

History

Version	Description
2.06.B.1	The interface speed command has been introduced.

3.29.185 interface speed nonegotiate

Description

Disable autonegotiation. By default, autonegotiation is enabled.

Command with **no** prefix enables autonegotiation.

Prefix no

Yes

Change settings Yes**Multiple input** No**Interface type** Ethernet

Synopsis

```
(config-if)> speed nonegotiate
```

```
(config-if)> no speed nonegotiate
```

Example

```
(config-if)> speed nonegotiate
Network::Interface::Ethernet: "GigabitEthernet1/0": ►
autonegotiation will be disabled for fixed speed.
```

```
(config-if)> no speed nonegotiate
Network::Interface::Ethernet: "GigabitEthernet1/0": ►
autonegotiation enabled..
```

History

Version	Description
2.08	The interface speed nonegotiate command has been introduced.

3.29.186 interface ssid

Description Specify the wireless network name (SSID) for WiFiStation and AccessPoint interfaces. Depending on the interface type, the SSID value is processed differently.

- For AccessPoint, the SSID is a necessary setting, without which the connection will not be accepted.
- For the WiFiStation SSID determines which access point WiFiStation will connect to. Without a specified SSID, WiFiStation can connect to any available wireless network at its discretion.

Command with **no** prefix resets network name to default.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** WiFi

Synopsis

```
(config-if)> ssid <ssid>
```

```
(config-if)> no ssid
```


Arguments

Argument	Value	Description
ssid	<i>String</i>	Wireless Network Name (SSID).

Example

```
(config-if)> ssid MYNETWORK
Network::Interface::Wireless: "WifiMaster0/AccessPoint0": SSID ►
saved.
```

```
(config-if)> no ssid
Network::Interface::Rtx::AccessPoint: "WifiMaster0/AccessPoint0": ►
SSID reset.
```

History

Version	Description
2.00	The interface ssid command has been introduced.

3.29.187 interface standby enable

Description

Enable the standby mode. When the standby mode is enabled for an interface, it is automatically turned off when another WAN connection with a higher global priority is up and running.

The standby option is ignored in following cases:

- the global priority is not configured;
- the standby interface is included in a group, such as Bridge;
- the current WAN connection operates over the standby interface.

Command with **no** prefix disables the standby mode.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> standby enable
```

```
(config-if)> no standby enable
```

Example

```
(config-if)> standby enable
Network::Interface::Standby: "CdcEthernet0": enabled.
```

```
(config-if)> no standby enable
Network::Interface::Standby: "CdcEthernet0": disabled.
```

History

Version	Description
4.00	The interface standby enable command has been introduced.

3.29.188 interface storm-control disable

Description

Enable the broadcast storm control on the Bridge interface. By default, the setting is enabled.

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Bridge

Synopsis

```
(config-if)> storm-control disable
```

```
(config-if)> no storm-control disable
```

Example

```
(config-if)> storm-control disable
Network::Interface::Bridge: "Bridge0": disabled storm control and loop detector.
```

```
(config-if)> no storm-control disable
Network::Interface::Bridge: "Bridge0": enabled storm control and loop detector.
```

History

Version	Description
4.00	The interface storm-control disable command has been introduced.

3.29.189 interface switchport access

Description

Set the port [VLAN](#) ID for access mode. Allows to transfer frames of the specified [VLAN](#) to the port and remove [VLAN](#) marker from the transferred frames.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Port

Synopsis

```
(config-if)> switchport access vlan <vid>
```

```
(config-if)> no switchport access vlan
```

Arguments

Argument	Value	Description
vid	<i>Integer</i>	Access VLAN ID. Can take values in the range from 1 to 4094 inclusively.

Example

```
(config-if)> switchport access vlan 1
Network::Interface::Switch: "FastEthernet0/0": set access VLAN ►
ID: 1.
```

History

Version	Description
2.06	The interface switchport access command has been introduced.

3.29.190 interface switchport friend

Description

Configure unidirectional [VLAN](#) for multicast traffic in addition to access [VLAN](#). Port can be a member of one access [VLAN](#). This command enables forwarding of downstream traffic from a different [VLAN](#) (called "friend"). Friend packets are transmitted without a tag.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Port

Synopsis

```
(config-if)> switchport friend vlan <vid>
```

```
(config-if)> no switchport friend vlan
```

Arguments

Argument	Value	Description
vid	<i>Integer</i>	Friend VLAN ID. Can take values in the range from 1 to 4094 inclusively.

Example

```
(config-if)> switchport friend vlan 2
Network::Interface::Switch: "FastEthernet0/0": set friend VLAN ►
ID: 2.
```

History

Version	Description
2.06	The interface switchport friend command has been introduced.

3.29.191 interface switchport mode

Description

Set access or trunk mode for [VLAN](#). By default, access mode is set.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Port

Synopsis

```
(config-if)> switchport mode [ (access [q-in-q] ) | trunk]
```

```
(config-if)> no switchport mode
```

Arguments

Argument	Value	Description
mode	access	Enable the access mode to a VLAN , that is the mode when only the untagged frames pass through the port. The incoming frames get tagged with the PVID marker, which is set with switchport access command. The port is an output one only for VLAN with PVID ID. Once a frame is transferred to the port, the VLAN marker gets removed.
	trunk	Enable the VLAN trunk mode, that is the mode when frames belonging to several VLANs get transmitted through the port. In this case each frame gets tagged. The list of IDs of VLAN networks that include the port is set with switchport trunk command.
q-in-q	<i>Keyword</i>	Enable double tagging.

Example

```
(config-if)> switchport mode access
Network::Interface::Switch: "FastEthernet0/1": access mode ►
enabled.
```

History

Version	Description
2.06	The interface switchport mode command has been introduced.

3.29.192 interface switchport trunk

Description Add a port to the [VLAN](#). Allows receiving and transmitting of the given [VLAN](#) frames to the port, such that VLAN marker from the transmitted frames is not removed. In the trunk mode it is allowed to add a port to several VLANs.

Command with **no** prefix removes the port from the specified [VLAN](#). If you use no argument, the port will be removed from all the VLANs.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type Port

Synopsis

```
(config-if)> switchport trunk vlan <vid>
(config-if)> no switchport trunk vlan [ vid ]
```

Argument	Value	Description
vid	<i>Integer</i>	VLAN ID. Can take values in the range from 1 to 4094 inclusively.

Example

```
(config-if)> switchport trunk vlan 100
Network::Interface::Switch: "FastEthernet0/1": set trunk VLAN ►
ID: 100.
```

Version	Description
2.06	The interface switchport trunk command has been introduced.

3.29.193 interface traffic-counter action disconnect

Description Disconnect from the provider when the traffic limit is reached.

Prefix no No

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> traffic-counter action <trigger> disconnect
```

Arguments

Argument	Value	Description
trigger	limit	Disconnection trigger on a limit traffic.

Example

```
(config-if)> traffic-counter action limit disconnect
UsbQmi::TrafficCounter: "UsbQmi0": set disconnect action for ►
trigger "limit".
```

History

Version	Description
3.06	The interface traffic-counter action disconnect command has been introduced.

3.29.194 interface traffic-counter action sms-alert message

Description Set [SMS](#) alert message.

Prefix no No

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> traffic-counter action <trigger> sms-alert message
<message>
```

Arguments

Argument	Value	Description
trigger	threshold	SMS alerting trigger is a threshold.
	limit	SMS alerting trigger is a traffic limit.
message	<i>String</i>	SMS alerting message.

Example

```
(config-if)> traffic-counter action threshold sms-alert message ►
TEXT
UsbQmi::TrafficCounter: "UsbQmi0": set message for trigger ►
"threshold".
```

History

Version	Description
3.06	The interface traffic-counter action sms-alert message command has been introduced.

3.29.195 interface traffic-counter action sms-alert phone

Description Set phone numbers for [SMS](#) alerting.

Prefix no	No											
Change settings	Yes											
Multiple input	Yes											
Interface type	Usb											
Synopsis	(config-if)> traffic-counter action <trigger> sms-alert phone <phone>											
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td rowspan="2">trigger</td><td>threshold</td><td>SMS alerting trigger is a threshold.</td></tr><tr><td>limit</td><td>SMS alerting trigger is a traffic limit.</td></tr><tr><td>phone</td><td>String</td><td>Phone number for SMS alerting. Up to three phone numbers can be set.</td></tr></table>	Argument	Value	Description	trigger	threshold	SMS alerting trigger is a threshold.	limit	SMS alerting trigger is a traffic limit.	phone	String	Phone number for SMS alerting. Up to three phone numbers can be set.
Argument	Value	Description										
trigger	threshold	SMS alerting trigger is a threshold.										
	limit	SMS alerting trigger is a traffic limit.										
phone	String	Phone number for SMS alerting. Up to three phone numbers can be set.										
Example	(config-if)> traffic-counter action threshold sms-alert phone ► +71112223344 UsbQmi::TrafficCounter: "UsbQmi0": add phone number ► "+71112223344" for action "threshold".											
History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>3.06</td><td>The interface traffic-counter action sms-alert phone command has been introduced.</td></tr></table>	Version	Description	3.06	The interface traffic-counter action sms-alert phone command has been introduced.							
Version	Description											
3.06	The interface traffic-counter action sms-alert phone command has been introduced.											

3.29.196 interface traffic-counter enable

Description	Enable the mobile traffic counter. By default, setting is disabled. Command with no prefix disables the mobile traffic counter.
Prefix no	Yes
Change settings	Yes
Multiple input	No
Interface type	Usb
Synopsis	<pre>(config-if)> traffic-counter enable (config-if)> no traffic-counter enable</pre>
Example	<pre>(config-if)> traffic-counter enable UsbQmi::TrafficCounter: "UsbQmi0": enabled. (config-if)> no traffic-counter enable UsbQmi::TrafficCounter: "UsbQmi0": disabled.</pre>

History

Version	Description
3.06	The interface traffic-counter enable command has been introduced.

3.29.197 interface traffic-counter limit**Description**

Set the traffic counter limit in megabytes, gigabytes or terabytes.

Command with **no** prefix resets configuration.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Usb

Synopsis

```
(config-if)> traffic-counter limit <value> <unit>
```

```
(config-if)> no traffic-counter limit
```

Arguments

Argument	Value	Description
value	<i>Integer</i>	Limit traffic value.
unit	<i>String</i>	Limit value units: MB, GB, TB, MiB, GiB, TiB.

Example

```
(config-if)> traffic-counter limit 4 TB
UsbQmi::TrafficCounter: "UsbQmi0": set limit to 4 TB.
```

```
(config-if)> no traffic-counter limit
UsbQmi::TrafficCounter: "UsbQmi0": reset limit.
```

History

Version	Description
3.06	The interface traffic-counter limit command has been introduced.

3.29.198 interface traffic-counter monthly**Description**

Set the day of the month to restart the traffic counter.

Command with **no** prefix resets configuration.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type Usb

Synopsis

```
(config-if)> traffic-counter monthly <day-of-month>
```

```
(config-if)> no traffic-counter monthly
```

Arguments

Argument	Value	Description
day-of-month	<i>Integer</i>	The day of the month from 1 to 31 to restart the traffic counter.

Example

```
(config-if)> traffic-counter monthly 31  

UsbQmi::TrafficCounter: "UsbQmi0": set day of month to "31".
```

```
(config-if)> no traffic-counter monthly  

UsbQmi::TrafficCounter: "UsbQmi0": reset day of month.
```

History

Version	Description
3.06	The interface traffic-counter monthly command has been introduced.

3.29.199 interface traffic-counter set

Description Set the current value of the traffic counter.**Prefix no** No**Change settings** Yes**Multiple input** No**Interface type** Usb

Synopsis

```
(config-if)> traffic-counter set <value> <unit>
```

Arguments

Argument	Value	Description
value	<i>Integer</i>	Numeric counter value (either integer or floating point).
unit	<i>String</i>	Limit value units: MB, GB, TB, MiB, GiB, TiB.

Example

```
(config-if)> traffic-counter set 1.54 GB  

UsbQmi::TrafficCounter: "UsbQmi0": set value to 1.54 GB.
```

History

Version	Description
3.06	The interface traffic-counter set command has been introduced.

3.29.200 interface traffic-counter threshold

Description Set the traffic counter warning threshold.
Command with **no** prefix resets configuration.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> traffic-counter threshold <threshold>
(config-if)> no traffic-counter threshold
```

Argument	Value	Description
threshold	<i>Integer</i>	Threshold value as a percentage of the limit. Can take values from 1 to 99 percent.

Example

```
(config-if)> traffic-counter threshold 99
UsbQmi::TrafficCounter: "UsbQmi0": set treshold to 99 percent ►
of the limit.

(config-if)> no traffic-counter threshold
UsbQmi::TrafficCounter: "UsbQmi0": reset threshold.
```

Version	Description
3.06	The interface traffic-counter threshold command has been introduced.

3.29.201 interface traffic-shape

Description Set the limit of data rate on a specified interface in both directions. By default speed is not limited.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-if)> traffic-shape rate <rate> [ asymmetric <upstream-rate> ]
[ schedule <schedule> ]
```

```
(config-if)> no traffic-shape
```

Arguments

Argument	Value	Description
rate	<i>Integer</i>	Value of data download rate in Kbps. Limit could be in the range from 64 Kbps to 1 Gbps.
upstream-rate	<i>Integer</i>	Data upload rate in Kbps. Value can be in the range from 64 Kbps to 1 Gbps.
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(config-if)> traffic-shape rate 5000
TrafficControl::Manager: "Bridge0" interface rate limited to ►
5000 kbit/s.
```

```
(config-if)> traffic-shape rate 5000 asymmetric 500
TrafficControl::Manager: "Bridge0" interface rate limited to ►
5000/500 kbit/s.
```

```
(config-if)> no traffic-shape
TrafficControl::Manager: Rate limit removed for "Bridge0" ►
interface.
```

History

Version	Description
2.05	The interface traffic-shape command has been introduced.
3.04	The upstream-rate argument was added.

3.29.202 interface tty init

Description Add initialization string at specified position index for RAS (UsbModem), NDIS (UsbLte), QMI (UsbQmi) modems.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> tty init [ <index> ] <string> [ sleep <delay> ]
```

```
(config-if)> no tty init [ <index> ]
```

Arguments

Argument	Value	Description
index	<i>Integer</i>	Position, the line number where you want to insert a string.
string	<i>String</i>	Modem initialization string.
delay	<i>Integer</i>	Modem delay value in seconds.

Example

```
(config-if)> tty init AT^SYSCFG=14,2,3fffffff,0,1
Mobile::Interface: "UsbQmi0": initialization string inserted.
```

```
(config-if)> tty init AT^SYSCFG=14,2,3fffffff,0,1 sleep 1
Mobile::Interface: "UsbQmi0": initialization string inserted.
```

```
(config-if)> no tty init
Mobile::Interface: "UsbQmi0": initialization strings erased.
```

History

Version	Description
4.00	The interface tty init command has been introduced.

3.29.203 interface tty send

Description Send AT command to UsbLte, UsbQmi modems.

Prefix no No

Change settings Yes

Multiple input No

Interface type Usb

Synopsis `(config-if)> tty send <command> [ <expect> ] [ <timeout> ]`

Arguments

Argument	Value	Description
command	<i>String</i>	AT command.
expect	<i>String</i>	Expected response. Default response is OK ERROR.
timeout	<i>Integer</i>	Time to wait in seconds. Default value is 3.

Example

```
(config-if)> tty send ATI
".Built@Aug 23 2019:16:28:33"
OK
Mobile::Interface: "UsbLte0": got expected response.
```

```
(config-if)> tty send ATI OK|ERROR 2
".Built@Aug 23 2019:16:28:33"
```

```

OK
Mobile::Interface: "UsbLte0": got expected response.

(config-if)> tty send ATI OKEY 2
".Built@Aug 23 2019:16:28:33"
OK
Mobile::Interface error[73140786]: "UsbLte0": timeout waiting ►
for expected response.

```

History

Version	Description
3.09	The interface tty send command has been introduced.

3.29.204 interface tunnel destination

Description

Set the remote end of tunnel. If it is used in conjunction with an automatic [IPSec](#) connection associated with the tunnel, remote host becomes the initiator of an [IPSec](#) connection.

Command with **no** prefix resets the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Tunnel

Synopsis

```
(config-if)> tunnel destination <destination>
```

```
(config-if)> no tunnel destination
```

Arguments

Argument	Value	Description
destination	<i>String</i>	IP address or domain name of the remote host.

Example

```
(config-if)> tunnel destination example.net
Network::Interface::Tunnel: "Gre0": destination set to ►
example.net.
```

```
(config-if)> no tunnel destination
Network::Interface::Tunnel: "Gre0": destination was reset.
```

History

Version	Description
2.08	The interface tunnel destination command has been introduced.

3.29.205 interface tunnel eoip id

Description Set identifier of EoIP tunnel.

Command with **no** prefix resets the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Eoip

Synopsis

```
(config-if)> tunnel eoip id <id>
```

```
(config-if)> no tunnel eoip id
```

Arguments

Argument	Value	Description
id	<i>Integer</i>	Tunnel ID.

Example

```
(config-if)> tunnel eoip id 50
```

Network::Interface::Tunnel: "Gre0": eoip id interface set to auto.

```
(config-if)> no tunnel eoip id
```

Network::Interface::Tunnel: "Gre0": eoip id was reset.

History

Version	Description
2.08	The interface tunnel eoip id command has been introduced.

3.29.206 interface tunnel gre keepalive

Description Enable support of Cisco-like keepalive for GRE tunnel. By default, interval is set to 5, count is set to 3.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Tunnel

Synopsis

```
(config-if)> tunnel gre keepalive <interval> [count]
```

```
(config-if)> no tunnel gre keepalive
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	The interval of sending keepalive packets in seconds. Can take values in the range from 0 to 60. If 0 is set, then GRE keepalive replies is enabled only and the router will not react on the tunnel state change.
count	<i>Integer</i>	Number of attempts to send keepalive packets. Can take values in the range from 1 to 20.

Example

```
(config-if)> tunnel gre keepalive 10 7
Network::Interface::Gre: "Gre0": set GRE keepalive to 10 s (7 ►
retries).
```

```
(config-if)> no tunnel gre keepalive
Network::Interface::Gre: "Gre0": disable GRE keepalive.
```

```
(config-if)> tunnel gre keepalive 0
Network::Interface::Gre: "Gre0": enable only GRE keepalive ►
replies.
```

History

Version	Description
2.10	The interface tunnel gre keepalive command has been introduced.

3.29.207 interface tunnel source

Description

Set the local end of tunnel. If it is used in conjunction with an automatic [IPSec](#) connection associated with the tunnel, then the reception mode of IPsec IKE connections is activated to establish a secure tunnel.

Prefix no No

Change settings Yes

Multiple input No

Interface type Tunnel

Synopsis

```
(config-if)> tunnel source (auto | <interface> | <address>)
```

Arguments

Argument	Value	Description
auto	<i>Keyword</i>	Set the current working WAN interface.
interface	<i>Interface</i>	Full interface name or an alias.
address	<i>IP address</i>	Local IP-adress of the tunnel.

Example

```
(config-if)> tunnel source auto
Network::Interface::Tunnel: "Gre0": set source interface to auto.
```

History

Version	Description
2.08	The interface tunnel source command has been introduced.
2.09	The auto argument has been added.
3.08	The no prefix was removed as obsolete.

3.29.208 interface tx-burst

Description

Enable Wi-Fi packet aggregation (Tx Burst). By default, the setting is disabled.

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> tx-burst
```

```
(config-if)> no tx-burst
```

Example

```
(config-if)> tx-burst
Network::Interface::Rtx::WifiMaster: Tx Burst enabled.
```

History

Version	Description
2.07	The interface tx-burst command has been introduced.

3.29.209 interface tx-queue length

Description

Set the size of the queue of outgoing packets on the interface. By default, 1000 value is set.

Command with **no** prefix resets to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> tx-queue length <length>
```

```
(config-if)> no tx-queue length
```


Arguments

Argument	Value	Description
length	<i>Integer</i>	Queue length can take values in the range from 0 to 65536.

Example

```
(config-if)> tx-queue length 255
Network::Interface::Base: "L2TP0": TX queue length is 255.
```

```
(config-if)> no tx-queue length
Network::Interface::Base: "L2TP0": TX queue length reset to ►
default.
```

History

Version	Description
3.06	The interface tx-queue length command has been introduced.

3.29.210 interface tx-queue scheduler cake

Description

Set the [CAKE](#) package scheduler for the interface. By default, the value `cake` is used for DSL and USB-modem interfaces, `fq_codel` — for all others.

Command with **no** prefix resets the scheduler to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-if)> tx-queue scheduler cake
```

```
(config-if)> no tx-queue scheduler cake
```

Example

```
(config-if)> tx-queue scheduler cake
Network::Interface::Base: "L2TP0": set TX queue scheduler to ►
"cake".
```

```
(config-if)> no tx-queue scheduler cake
Network::Interface::Base: "L2TP0": set default TX queue scheduler.
```

History

Version	Description
3.06	The interface tx-queue scheduler cake command has been introduced.

3.29.211 interface tx-queue scheduler fq_codel

Description Set the [FQ_CODEL](#) package scheduler for the interface. By default, the value cake is used for DSL and USB-modem interfaces, fq_codel — for all others.

Command with **no** prefix resets the scheduler to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-if)> tx-queue scheduler fq_codel
(config-if)> no tx-queue scheduler fq_codel
```

Example

```
(config-if)> tx-queue scheduler fq_codel
Network::Interface::Base: "L2TP0": set TX queue scheduler to ►
"fq_codel".

(config-if)> no tx-queue scheduler fq_codel
Network::Interface::Base: "L2TP0": set default TX queue scheduler.
```

History

Version	Description
3.06	The interface tx-queue scheduler fq_codel command has been introduced.

3.29.212 interface up

Description Enable the network interface and persist the state “up” to the settings.

Command with **no** prefix disables the the network interface and deletes “up” from settings. Also **interface down** command can be used.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-if)> up
(config-if)> no up
```

Example

```
(config-if)> up
Interface enabled.
```

History

Version	Description
2.00	The interface up command has been introduced.

3.29.213 interface usb acq

Description Lock 3G/LTE/5G mode for NDIS (UsbLte) modems.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> usb acq {acq}
(config-if)> no usb acq
```

Arguments

Argument	Value	Description
acq	gsm	2G network.
	umts	3G network.
	lte	4G network.
	nr5g	5G network.

Example

```
(config-if)> usb acq nr5g
Mobile::Interface: "UsbLte0": ACQ saved.
```

```
(config-if)> no usb acq
Mobile::Interface: "UsbLte0": ACQ cleared.
```

History

Version	Description
2.09	The interface usb acq command has been introduced.
4.02	The nr5g argument was added.

3.29.214 interface usb apn

Description Set access point name (APN) for USB-modems in NDIS mode. Modem reboots after applying the command.

Command with **no** prefix resets the setting.

Prefix no Yes

Change settings Yes**Multiple input** No**Interface type** Usb

Synopsis

```
(config-if)> usb apn <apn>
```

```
(config-if)> no usb apn
```

Arguments

Argument	Value	Description
apn	<i>String</i>	Access point name.

Example

```
(config-if)> usb apn example.net
```

```
Network::Interface::Usb: "UsbModem0": APN saved.
```

```
(config-if)> no usb apn
```

```
Network::Interface::Usb: "UsbModem0": APN cleared.
```

History

Version	Description
2.05	The interface usb apn command has been introduced.

3.29.215 interface usb device-id

Description Assign vendor and model ID to the UsbModem interface. It is necessary for modem and interface binding.

If there is an interface UsbModem[N] with the appropriate DeviceID, then automatic binding is occur. If there is no such interface, it will be created automatically with the appropriate DeviceID.

Command with **no** prefix deletes the setting.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** Usb

Synopsis

```
(config-if)> usb device-id <vendor> <model>
```

```
(config-if)> no usb device-id
```

Arguments

Argument	Value	Description
vendor	<i>String</i>	Vendor info.
model	<i>String</i>	Model info.

Example (config-if)> **usb device-id 12d1 1001**
Device ID saved.

History

Version	Description
2.00	The interface usb device-id command has been introduced.

3.29.216 interface usb port-id

Description Bind of RAS (UsbModem), CdcEthernet, NDIS (UsbLte), QMI (UsbQmi) modems interface to USB port identifier.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> usb port-id ( <port> | auto )
```

```
(config-if)> no usb port-id
```

Arguments

Argument	Value	Description
port	<i>String</i>	USB port identifier.
auto	<i>Keyword</i>	Auto USB port selection.

Example

```
(config-if)> usb port-id 1  
Network::Interface::Usb: "CdcEthernet0": port ID is set to "1".
```

```
(config-if)> usb port-id auto  
Network::Interface::Usb: "CdcEthernet0": port ID is automatically  
set to "2/4".
```

```
(config-if)> no usb port-id  
Network::Interface::Usb: "CdcEthernet0": port ID removed.
```

History

Version	Description
4.01	The interface usb port-id command has been introduced.

3.29.217 interface usb power-cycle

Description Turn off power on the usb-modem for a specified period of time. This function is used to hardware reset usb-modem in case of freezing.

Prefix no No

Change settings No

Multiple input No

Interface type Usb

Synopsis (config-if)> **usb power-cycle** *⟨pause⟩*

Arguments

Argument	Value	Description
pause	<i>Integer</i>	Period of time in which usb-modem will be disabled, in milliseconds.

Example

```
(config-if)> usb power-cycle 3000
Network::Interface::Usb: "UsbLte0": started 3000 ms. power cycle.
```

History

Version	Description
2.03	The interface usb power-cycle command has been introduced.

3.29.218 interface usb power-fail

Description Specify further actions in case the usb-modem power-off did not help.

Prefix no No

Change settings Yes

Multiple input No

Interface type Usb

Synopsis (config-if)> **usb power-fail** *⟨interval⟩* (**retry** *⟨pause⟩* | **reboot**)

Arguments

Argument	Value	Description
interval	<i>Integer</i>	Time to wait for modem detection after its power reset, in seconds. Can take values in the range from 0 to 60 inclusively.
pause	<i>Integer</i>	Period of time in which usb-modem will be disabled, in seconds. Can take values in the range from 0 to 60 inclusively.

Argument	Value	Description
reboot	<i>Keyword</i>	Reboot of the entire system.

Example

```
(config-if)> usb power-fail 60 reboot
Network::Interface::Usb: "YotaOne1": enabled power fail action: ►
reboot.
```

History

Version	Description
2.10	The interface usb power-fail command has been introduced.

3.29.219 interface usb wwan-force-connected

Description Disable CDC-modem link polling via HTTP. By default, the feature is disabled.

Command with **no** prefix disables the function.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)>  usb wwan-force-connected
(config-if)> no usb wwan-force-connected
```

Example

```
(config-if)> usb wwan-force-connected
Network::Interface::Usb: "UsbLte0": force WWAN link status.
```

```
(config-if)> no usb wwan-force-connected
Network::Interface::Usb: "UsbLte0": unforce WWAN link status.
```

History

Version	Description
2.12	The interface wwan-force-connected command has been introduced.

3.29.220 interface vga-clamp

Description Enable [VGA](#) technology adjustment. By default, adjustment is disabled.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes**Multiple input** No**Interface type** WiFiMaster

Synopsis

```
(config-if)> vga-clamp <vga-clamp>
```

```
(config-if)> no vga-clamp
```

Arguments

Argument	Value	Description
vga-clamp	<i>Integer</i>	The value of correction. Can take values in the range from 1 to 8 inclusively.

Example

```
(config-if)> vga-clamp 1
Network::Interface::Rtx::WifiMaster: "WifiMaster0": VGA clamp ►
set to 1.
```

```
(config-if)> no vga-clamp
Network::Interface::Rtx::WifiMaster: "WifiMaster0": VGA clamp ►
disabled.
```

```
(config-if)> vga-clamp 2
Network::Interface::Rtx::WifiMaster: "WifiMaster1": VGA clamp ►
set to 2.
```

```
(config-if)> no vga-clamp
Network::Interface::Rtx::WifiMaster: "WifiMaster1": VGA clamp ►
disabled.
```

History

Version	Description
2.09	The interface vga-clamp command has been introduced.

3.29.221 interface vlan qos egress map

Description Configure *NTCE* priority mapping to [IEEE P802.1p](https://en.wikipedia.org/wiki/IEEE_P802.1p)¹⁴ PCP for outgoing packets. By default, value 0 is used.

Command with **no** prefix resets the [IEEE P802.1p](https://en.wikipedia.org/wiki/IEEE_P802.1p)¹⁵ PCP value to default.

Prefix no Yes**Change settings** Yes**Multiple input** Yes**Interface type** Ethernet

¹⁴ https://en.wikipedia.org/wiki/IEEE_P802.1p

¹⁵ https://en.wikipedia.org/wiki/IEEE_P802.1p

Synopsis

```
(config-if)> vlan qos egress map <priority> <pcp>
```

```
(config-if)> no vlan qos egress map [<priority>]
```

Arguments

Argument	Value	Description
priority	<i>Integer</i>	NTCE priority number. Can take values in the range from 0 to 7 inclusively. If the value is 0, all outgoing packets will receive this PCP.
pcp	<i>Integer</i>	The new value of the IEEE P802.1p ¹⁶ priority code point.

Example

```
(config-if)> vlan qos egress map 0 2
```

```
Network::Interface::Vlan: "GigabitEthernet0/Vlan1": enabled ►  
mapping priority 0 to PCP 2.
```

```
(config-if)> no vlan qos egress map 0
```

```
Network::Interface::Vlan: "GigabitEthernet0/Vlan1": reset PCP ►  
mapping for priority 0.
```

History

Version	Description
4.02	The interface vlan qos egress map command has been introduced.

3.29.222 interface web-api address

Description

Set the IP address to access the modem's web interface connected to the router.

Command with **no** prefix deletes the address.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Usb

Synopsis

```
(config-if)> web-api address <address>
```

```
(config-if)> no web-api address
```

Arguments

Argument	Value	Description
address	<i>IP-address</i>	The web interface address.

¹⁶ https://en.wikipedia.org/wiki/IEEE_P802.1p

Example

```
(config-if)> web-api address 192.168.8.1
Mobile::Interface: "CdcEthernet0": WEB address is set.
```

```
(config-if)> no web-api address
Mobile::Interface: "CdcEthernet0": WEB address cleared.
```

History

Version	Description
3.08	The interface web-api address command has been introduced.

3.29.223 interface web-api login

Description

Specify the user name to access the modem's web interface connected to the router.

Command with **no** prefix deletes the user name.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Usb

Synopsis

```
(config-if)> web-api login <login>
```

```
(config-if)> no web-api login
```

Arguments

Argument	Value	Description
login	<i>String</i>	User name for authentication. Maximum user name length is 64 characters.

Example

```
(config-if)> web-api login myadmin
Mobile::Interface: "CdcEthernet0": WEB login is set.
```

```
(config-if)> no web-api login
Mobile::Interface: "CdcEthernet0": WEB login cleared.
```

History

Version	Description
3.08	The interface web-api login command has been introduced.

3.29.224 interface web-api password

Description

Set a password to access the modem's web interface connected to the router.

Command with **no** prefix deletes the password.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Usb

Synopsis

```
(config-if)> web-api password <password>
(config-if)> no web-api password
```

Argument	Value	Description
password	<i>String</i>	The password for authentication. Maximum password length is 64 characters.

Example

```
(config-if)> web-api password 12345678910
Mobile::Interface: "CdcEthernet0": WEB password is set.

(config-if)> no web-api password
Mobile::Interface: "CdcEthernet0": WEB password cleared.
```

Version	Description
3.08	The interface web-api password command has been introduced.

3.29.225 interface wireguard asc

Description Configure the Advanced Security Configuration setting for [WireGuard](#).
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Wireguard

Synopsis

```
(config-if)> wireguard asc <jc> <jmin> <jmax> <s1> <s2> <h1> <h2> <h3> <h4>
(config-if)> no wireguard asc
```

Argument	Value	Description
jc	<i>String</i>	The number of packets with random data that are sent before the start of the session.

Argument	Value	Description
jmin	<i>String</i>	The minimum packet size for Junk packet. That is, all randomly generated packets will have a size no smaller than jmin.
jmax	<i>String</i>	The maximum size for Junk packets.
s1	<i>String</i>	The size of random data that will be added to the init packet.
s2	<i>String</i>	The size of random data that will be added to the response packet.
h1	<i>String</i>	The header of the first byte of the handshake.
h2	<i>String</i>	The header of the first byte of the handshake response.
h3	<i>String</i>	UnderLoad packet header.
h4	<i>String</i>	The header of the packet of the data packet. The interval of keepalive packet sending in seconds.

Example

```
(config-if)> wireguard asc 120 22 320 0 0 1 2 3 4
Wireguard::Interface: "Wireguard0": set ASC parameters.
```

```
(config-if)> no wireguard asc
Wireguard::Interface: "Wireguard0": reset ASC parameters.
```

History

Version	Description
4.02	The interface wireguard asc command has been introduced.

3.29.226 interface wireguard listen-port

Description Specify *UDP* port number to which incoming connections are accepted. By default, port number is not defined.

Command with **no** prefix resets the port.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Wireguard

Synopsis (config-if)> **wireguard listen-port** *<port>*

(config-if)> **no wireguard listen-port**

Arguments

Argument	Value	Description
port	<i>Integer</i>	Port number. Can take values in the range from 1 to 65535 inclusively.

Example

```
(config-if)> wireguard listen-port 11633
Wireguard::Interface: "Wireguard4": set listen port to "11633".
```

```
(config-if)> no wireguard listen-port
Wireguard::Interface: "Wireguard4": reset listen port.
```

History

Version	Description
3.03	The interface wireguard listen-port command has been introduced.

3.29.227 interface wireguard peer

Description

Add the remote peer public key to configure the secure connection using the [WireGuard](#) protocol.

Command with **no** prefix removes specified key.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

Wireguard

Group entry

(config-wg-peer)

Synopsis

```
(config-if)> wireguard peer <key>
```

```
(config-if)> no wireguard peer <key>
```

Arguments

Argument	Value	Description
key	<i>String</i>	Value of the key. Latin letters, numbers and equal signs are acceptable. The key length is 44 characters (Base64-encoded 32-byte string representation).

Example

```
(config-if)> wireguard peer ►
gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm0g=
(config-wg-peer)>
```

```
(config-if)> no wireguard peer ►
gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm0g=
```

```
Wireguard::Interface: "Wireguard4": removed peer ►
"gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmmg0=".
```

History

Version	Description
3.03	The interface wireguard peer command has been introduced.

3.29.227.1 interface wireguard peer allow-ips**Description**

Add the subnet of IP addresses to which the transmission of packets inside the tunnel is allowed.

Note: You can add 0.0.0.0/0 subnet to allow transmission to any addresses.

Command with **no** prefix removes the subnet. If you use no argument, the entire list of subnets will be removed.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

Wireguard

Synopsis

```
(config-wg-peer)> allow-ips <address> <mask>
```

```
(config-wg-peer)> no allow-ips [ <address> <mask> ]
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	Together with mask <i>mask</i> sets the subnet of IP addresses to be translated.
mask	<i>IP-mask</i>	Mask of subnet. There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).

Example

```
(config-wg-peer)> allow-ips 0.0.0.0/0
Wireguard::Interface: "Wireguard4": add allowed IPs ►
"0.0.0.0/0.0.0.0" from peer ►
"gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=".
```

```
(config-wg-peer)> allow-ips 192.168.11.0 255.255.255.0
Wireguard::Interface: "Wireguard4": add allowed IPs ►
"192.168.11.0/255.255.255.0" from peer ►
"gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=".
```

```
(config-wg-peer)> no allow-ips
Wireguard::Interface: "Wireguard4": clear allowed IPs of peer ►
"gbplgW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=".
```

History

Version	Description
3.03	The interface wireguard peer allow-ips command has been introduced.

3.29.227.2 interface wireguard peer client-id send

Description Configure the client ID for sending in message headers for [WireGuard](#).
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Wireguard

Synopsis

```
(config-wg-peer)> client-id send <client-id>
(config-wg-peer)> no client-id send
```

Arguments

Argument	Value	Description
client-id	<i>String</i>	Decimal number obtained by simple hexadecimal translation, for example: from 0x1620a6 you get simply 1450150. Client ID must be in the range from 1 to 16777215.

Example

```
(config-wg-peer)> client-id send 1450150
Wireguard::Interface: "Wireguard3": set peer ►
"4G0SzB1231234413PevDG4dy0Y/TCXG8fnKf20Ldjs=" send client ID to ►
"1450150".
```

```
(config-wg-peer)> no client-id send
Wireguard::Interface: "Wireguard3": reset send client ID for ►
peer "4G0SzB1231234413PevDG4dy0Y/TCXG8fnKf20Ldjs=".
```

History

Version	Description
4.02	The interface wireguard peer client-id send command has been introduced.

3.29.227.3 interface wireguard peer connect

Description Set interface for WireGuard peer connection. By default, connection is set via any interface.

Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WireGuard

Synopsis

```
(config-wg-peer)> connect via <via>
(config-wg-peer)> no connect
```

Arguments

Argument	Value	Description
via	<i>Interface</i>	Full interface name or an alias.

Example

```
(config-wg-peer)> connect via ISP
Wireguard::Interface: "Wireguard0": set peer ►
"IrtvFcVtI5wcqxn4cCmuWc+p8s8byP0zK/MAI67VmXs=" connect via "ISP"

(config-wg-peer)> no connect
Wireguard::Interface: "Wireguard0": disabled peer ►
"IrtvFcVtI5wcqxn4cCmuWc+p8s8byP0zK/MAI67VmXs=".
```

History

Version	Description
4.01	The interface wireguard peer connect command has been introduced.

3.29.227.4 interface wireguard peer endpoint

Description Set the remote peer address to which the *WireGuard* connection will be established.

Command with **no** prefix removes the endpoint.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Wireguard

Synopsis

```
(config-wg-peer)> endpoint <address> [:<port>]
```



```
(config-wg-peer)> no endpoint
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	IP address or domain name of the server.
port	<i>Integer</i>	The <i>UDP</i> server port.

Example

```
(config-wg-peer)> endpoint 10.0.1.10:11635
Wireguard::Interface: "Wireguard4": set peer ►
"gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=" endpoint to ►
"10.0.1.10:11635".
```

```
(config-wg-peer)> no endpoint
Wireguard::Interface: "Wireguard4": reset endpoint for peer ►
"gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=".
```

History

Version	Description
3.03	The interface wireguard peer endpoint command has been introduced.

3.29.227.5 interface wireguard peer keepalive-interval**Description**

Set the interval of keepalive packet sending for *WireGuard* connection monitoring. By default, the interval is not set.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Wireguard

Synopsis

```
(config-wg-peer)> keepalive-interval <interval>
```

```
(config-wg-peer)> no keepalive-interval
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	The interval of keepalive packet sending in seconds. Can take values in the range from 3 to 3600 inclusively.

Example

```
(config-wg-peer)> keepalive-interval 3
Wireguard::Interface: "Wireguard4": set peer ►
"gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=" keepalive interval ►
to "3".
```

```
(config-wg-peer)> no keepalive-interval
Wireguard::Interface: "Wireguard4": reset persistent keepalive ►
interval for peer "gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=".
```

History

Version	Description
3.03	The interface wireguard peer keepalive-interval command has been introduced.

3.29.227.6 interface wireguard peer preshared-key**Description**

Set preshared key for [WireGuard](#) connection to remote peer. The preshared key (PSK) is an optional security improvement as per the [WireGuard](#) protocol and should be a unique PSK per client for highest security. By default, PSK is not used.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Wireguard

Synopsis

```
(config-wg-peer)> preshared-key <preshared-key>
```

```
(config-wg-peer)> no preshared-key
```

Arguments

Argument	Value	Description
preshared-key	<i>String</i>	Secret PSK key value. Latin letters, numbers and equal signs are acceptable. The key length is 44 characters.

Example

```
(config-wg-peer)> preshared-key ►
WY2fkhJZuDcbYew7L8whBMzkReVf8KKzWJrmaR79F8z=
Wireguard::Interface: "Wireguard4": set preshared key for peer ►
"gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=".
```

```
(config-wg-peer)> no preshared-key
Wireguard::Interface: "Wireguard4": reset preshared key for peer ►
"gbp1gW3pBQKssrAdah1hiib13Jl123ZM8dBIjjPmm2g=".
```

History

Version	Description
3.03	The interface wireguard peer preshared-key command has been introduced.

3.29.228 interface wireguard private-key

Description Set or generate the private key to connect to the remote peers via [WireGuard](#) protocol. By default, private key is not configured.

Prefix no No

Change settings No

Multiple input No

Interface type Wireguard

Synopsis `(config-if)> wireguard private-key [ <private-key> ]`

Argument	Value	Description
private-key	<i>String</i>	A new private key value. Latin letters, numbers and equal signs are acceptable. The key length is 44 characters.

Example `(config-if)> wireguard private-key`
Wireguard::Interface: "Wireguard4": generated new private key.

`(config-if)> wireguard private-key ▶`
`UshaeghezaiJ7reo8iK6ear0eomujohkeen8jahX5uo=`
Wireguard::Interface: "Wireguard4": set private key.

Version	Description
3.03	The interface wireguard private-key command has been introduced.

3.29.229 interface wmm

Description Enable [WMM](#) on the interface.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Access Point

Synopsis `(config-if)> wmm`
`(config-if)> no wmm`

Example `(config-if)> wmm`
WMM extensions enabled.

History

Version	Description
2.00	The interface wmm command has been introduced.

3.29.230 interface wpa-eap radius secret

Description

Specify the shared secret for secure communication between a [RADIUS](#) server and a [RADIUS](#) client.

Command with **no** prefix deletes the shared secret.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Bridge

Synopsis

```
(config-if)> wpa-eap radius secret <secret>
```

```
(config-if)> no wpa-eap radius secret
```

Arguments

Argument	Value	Description
secret	<i>String</i>	The value of RADIUS shared secret. Maximum key length is 64 characters.

Example

```
(config-if)> wpa-eap radius secret ►
(+>R#G` }-JNxru'i8i|lK}wBN9E^X0Xa{xFOG-N^%FaTnr|S(e(q$/lP2/tbX/#Q
Network::Interface::Rtx::WpaEap: Bridge0 RADIUS secret applied.
```

```
(config-if)> no wpa-eap radius secret
Network::Interface::Rtx::WpaEap: Bridge0 RADIUS secret cleared.
```

History

Version	Description
3.01	The interface wpa-eap radius secret command has been introduced.

3.29.231 interface wpa-eap radius server

Description

Specify [RADIUS](#) server address.

Command with **no** prefix deletes the address.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type Bridge

Synopsis

```
(config-if)> wpa-eap radius server <address> [: <port> ]
(config-if)> no wpa-eap radius server
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	<i>RADIUS</i> server IP address.
port	<i>Integer</i>	<i>RADIUS</i> server port.

Example

```
(config-if)> wpa-eap radius server 192.168.10.10
Network::Interface::Rtx::WpaEap: Bridge0 RADIUS server set to ►
192.168.10.10.
```

```
(config-if)> wpa-eap radius server 192.168.10.10:1111
Network::Interface::Rtx::WpaEap: Bridge0 RADIUS server set to ►
192.168.10.10:1111.
```

```
(config-if)> no wpa-eap radius server
Network::Interface::Rtx::WpaEap: Bridge0 RADIUS server cleared.
```

History

Version	Description
3.01	The interface wpa-eap radius server command has been introduced.

3.29.232 interface wps

Description Enable *WPS* functionality.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFi

Synopsis

```
(config-if)> wps
(config-if)> no wps
```

Example

```
(config-if)> wps
WPS functionality enabled.
```

History

Version	Description
2.00	The interface wps command has been introduced.

3.29.233 interface wps auto-self-pin

Description Enable [WPS](#) auto-self-pin mode. By default auto-self-pin mode is enabled.
Command with **no** prefix disables this mode.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type WiFi

Synopsis

```
(config-if)> wps auto-self-pin
(config-if)> no wps auto-self-pin
```

Example

```
(config-if)> wps auto-self-pin
Network::Interface::Rtx::Wps: an auto self PIN mode enabled.
```

History	Version	Description
	2.04	The interface wps auto-self-pin command has been introduced.

3.29.234 interface wps button

Description Start WPS process using a software button. Process takes 2 minutes or until the first connection occurred.

Prefix no No

Change settings No

Multiple input No

Interface type WiFi

Synopsis

```
(config-if)> wps button <direction>
```

Arguments	Argument	Value	Description
	direction	send	Send WiFi configuration.
		receive	Receive WiFi configuration from Carrier.

Example

```
(config-if)> wps button send
Sending WiFi configuration process started (software button mode).
```

History

Version	Description
2.00	The interface wps button command has been introduced.

3.29.235 interface wps peer

Description Start WPS process using remote peer's PIN. Process takes 2 minutes or until the first connection occurred. By default, WPS PIN is disabled.

Prefix no No

Change settings No

Multiple input No

Interface type WiFi

Synopsis `(config-if)> wps peer <direction> <pin>`

Arguments

Argument	Value	Description
direction	send	Send WiFi configuration.
	receive	Receive WiFi configuration from the remote peer.
pin	<i>String</i>	PIN code of the remote peer.

Example

```
(config-if)> wps peer send 53794141
Network::Interface::Rtx::Wps: "WifiMaster0/AccessPoint0": peer ►
PIN WPS session started.
```

History

Version	Description
2.04	The interface wps peer command has been introduced.

3.29.236 interface wps self-pin

Description Start WPS process using self PIN. Process takes 2 minutes or until the first connection occur.

Prefix no No

Change settings No

Multiple input No

Interface type WiFi

Synopsis `(config-if)> wps self-pin <direction>`

Arguments

Argument	Value	Description
direction	send	Send WiFi configuration.
	receive	Receive WiFi configuration from Carrier.

Example

```
(config-if)> wps self-pin receive
Receiving WiFi configuration process started (self PIN mode).
```

History

Version	Description
2.00	The interface wps self-pin command has been introduced.

3.29.237 interface zerotier accept-addresses

Description

Enable address accepting from the [ZeroTier](#) server.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

ZeroTier

Synopsis

```
(config-if)> zerotier accept-addresses
```

```
(config-if)> no zerotier accept-addresses
```

Example

```
(config-if)> zerotier accept-addresses
ZeroTier::Interface: "ZeroTier0": enabled addresses accept.
```

```
(config-if)> no zerotier accept-addresses
ZeroTier::Interface: "ZeroTier0": disabled addresses accept.
```

History

Version	Description
4.01	The interface zerotier accept-addresses command has been introduced.

3.29.238 interface zerotier accept-routes

Description

Enable receiving routes from a remote side via [ZeroTier](#).

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings Yes

Multiple input No

Interface type ZeroTier

Synopsis

```
(config-if)> zerotier accept-routes
(config-if)> no zerotier accept-routes
```

Example

```
(config-if)> zerotier accept-routes
ZeroTier::Interface: "ZeroTier0": enabled routes accept.

(config-if)> no zerotier accept-routes
ZeroTier::Interface: "ZeroTier0": disabled routes accept.
```

History

Version	Description
4.01	The interface zerotier accept-routes command has been introduced.

3.29.239 interface zerotier connect

Description Set interface for [ZeroTier](#) connection. If you use no argument, connection is set via any interface.

Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type ZeroTier

Synopsis

```
(config-if)> zerotier connect [ via <via> ]
(config-if)> no zerotier connect
```

Arguments

Argument	Value	Description
via	<i>Interface</i>	Full interface name or an alias.

Example

```
(config-if)> zerotier connect via ISP
ZeroTier::Interface: "ZeroTier0": set connection via ISP.

(config-if)> no zerotier connect
ZeroTier::Interface: "ZeroTier0": set connection via any ►
interface.
```

History

Version	Description
4.01	The interface zerotier connect command has been introduced.

3.29.240 interface zerotier network-id

Description

Set identifier of *ZeroTier* tunnel.

Command with **no** prefix resets the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

ZeroTier

Synopsis

```
(config-if)> zerotier network-id <network-id>
```

```
(config-if)> no zerotier network-id
```

Arguments

Argument	Value	Description
network-id	<i>String</i>	Tunnel ID.

Example

```
(config-if)> zerotier network-id 816227940c13c37e
ZeroTier::Interface: "ZeroTier0": set network ID to ►
"816227940c13c37e".
```

```
(config-if)> no zerotier network-id
ZeroTier::Interface: "ZeroTier0": reset network ID.
```

History

Version	Description
4.01	The interface zerotier network-id command has been introduced.

3.30 ip arp

Description

Set static mapping between an IP address and a MAC address for hosts that do not support dynamic *ARP*.

Command with **no** prefix removes entry from ARP table. If you use no arguments, the whole list of ARP entries will be removed.

Prefix no

Yes

Change settings

Yes

Multiple input Yes

Synopsis

```
(config)> ip arp <ip> <mac>
```

```
(config)> no ip arp [ <ip> ]
```

Argument	Value	Description
ip	<i>IP address</i>	IP address in four-part dotted decimal format corresponding to the local data-link address.
mac	<i>MAC address</i>	MAC address as six groups of two hexadecimal digits separated by colons.

Example

```
(config)> ip arp 192.168.2.50 a1:2e:84:85:f4:21  
Network::ArpTable: Static ARP entry saved.
```

```
(config)> no ip arp 192.168.2.50  
Network::ArpTable: Static ARP entry deleted for 192.168.2.50.
```

```
(config)> no ip arp  
Network::ArpTable: Static ARP table cleared.
```

Version	Description
2.00	The ip arp command has been introduced.

3.31 ip dhcp class

Description Access to a group of commands to configure *DHCP* vendor class (option 60). If specified class name is not found, the command tries to create it.

Command with **no** prefix removes selected class.

Prefix no Yes

Change settings No

Multiple input Yes

Group entry (config-dhcp-class)

Synopsis

```
(config)> ip dhcp class <class>
```

```
(config)> no ip dhcp class <class>
```

Argument	Value	Description
class	<i>String</i>	The vendor-class name.

Example

```
(config)> ip dhcp class STB-One
Dhcp::Server: Vendor class "STB-One" has been created.
```

History

Version	Description
2.00	The ip dhcp class command has been introduced.

3.31.1 ip dhcp class option

Description

Set an option 60 to match the vendor-class.

Command with **no** prefix removes selected option.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-dhcp-class)> option <number> hex <data>
```

```
(config-dhcp-class)> no option <number>
```

Arguments

Argument	Value	Description
number	<i>Integer</i>	Option number. Now the only 60 value is used.
data	<i>String</i>	Value of an option.

Example

```
(config-dhcp-class)> option 60 hex FF
Dhcp::Server: Option 60 is set to FF.
```

History

Version	Description
2.00	The ip dhcp class option command has been introduced.

3.32 ip dhcp host

Description

Configure static linking of IP address to MAC address of the host. If the host with the specified name is not found, the command tries to create it. If the specified IP address is not in range of any pool, the command will remain in the settings, but will not affect the *DHCP server* functioning.

The command allows one to change the MAC address, leaving the old value IP address and vice versa — to change the IP address, leaving the old MAC address value intact.

Command with **no** prefix removes the host.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config)> ip dhcp host <host> [ mac ] [ ip ]
```

```
(config)> no ip dhcp host <host>
```

Arguments

Argument	Value	Description
host	<i>String</i>	Arbitrary host name, used to identify a MAC-IP pair in the settings.
mac	<i>MAC address</i>	MAC address of the host for static linking of IP address. If not specified, the value is taken from the previous configuration.
ip	<i>IP address</i>	IP address of the host. If not specified, the value is taken from the previous configuration.

Example

```
(config)> ip dhcp host HOST 192.168.1.44  
new host "HOST" has been created.
```

History

Version	Description
2.00	The ip dhcp host command has been introduced.

3.33 ip dhcp pool

Description

Access to a group of commands to configure DHCP-pool. If the pool is not found, the command tries to create it. For a pool one sets a list of DNS servers ([dns-server](#) command), default gateway ([default-router](#) command) and the lease time ([lease](#) command), as well as a range of dynamic IP addresses ([range](#) command).

Having configured the pool, it is necessary to enable the [DHCP](#) service using the [service dhcp](#) command.

You can enter up to 32 pools. Maximum pool name length is 32 characters.

Note: In the current version of the system no more than one pool per interface is supported. For [DHCP server](#) to function correctly it is required that the range of IP addresses set by [range](#) command belong to the network that is configured on one of the device's Ethernet-interfaces.

Command with **no** prefix removes the pool.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry (config-dhcp-pool)

Synopsis

```
(config)> ip dhcp pool <name>
```

```
(config)> no ip dhcp pool <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	DHCP pool name.

Example

```
(config)> ip dhcp pool test_pool  
pool "test_pool" has been created.
```

History

Version	Description
2.00	The ip dhcp pool command has been introduced.

3.33.1 ip dhcp pool bind

Description Bind the pool to specified interface.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis

```
(config-dhcp-pool)> bind <interface>
```

```
(config-dhcp-pool)> no bind <interface>
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias.

Example

```
(config-dhcp-pool)> bind FastEthernet0/Vlan2  
pool "test_pool" bound to interface FastEthernet0/Vlan2.
```

History

Version	Description
2.00	The ip dhcp pool bind command has been introduced.

3.33.2 ip dhcp pool bootfile

Description Set boot file path on TFTP server for DHCP client (option 67).

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis

```
(config-dhcp-pool)> bootfile <bootfile>
(config-dhcp-pool)> no bootfile
```

Arguments

Argument	Value	Description
bootfile	<i>Filename</i>	The boot file path.

Example

```
(config-dhcp-pool)> bootfile test.cnf
Dhcp::Pool: "_WEBADMIN": set bootfile option to "test.cnf".
```

```
(config-dhcp-pool)> no bootfile
Dhcp::Pool: "_WEBADMIN": cleared bootfile option.
```

History

Version	Description
2.11	The ip dhcp pool bootfile command has been introduced.

3.33.3 ip dhcp pool class

Description Access to a group of commands to configure [DHCP](#) vendor class for selected pool. If specified class name is not found, the command tries to create it.

To work correctly class name should be the same as for [ip dhcp class](#) command.

Command with **no** prefix removes selected class.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry (config-dhcp-pool-class)

Synopsis

```
(config-dhcp-pool)> class <class>
```

```
(config-dhcp-pool)> no class <class>
```

Arguments

Argument	Value	Description
class	<i>String</i>	The vendor-class name.

Example

```
(config-dhcp-pool)> class STB-One
Dhcp::Server: Vendor class "STB-One" has been created.
```

History

Version	Description
2.00	The ip dhcp pool class command has been introduced.

3.33.3.1 ip dhcp pool class option**Description**

Set additional options for *DHCP* client in case of vendor-class matching.

Command with **no** prefix removes selected option.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-dhcp-pool-class)> option <number> <type> <data>
```

```
(config-dhcp-pool-class)> no option <number>
```

Arguments

Argument	Value	Description
number	6	6 option, DNS server.
	42	42 option, NTP server.
	43	43 option, vendor specific information.
type	ip	Type of data is IP address. This type is not used for 43 option.
	hex	Type of data is hexadecimal number.
data	<i>String</i>	Value of an option.

Example

```
(config-dhcp-pool-class)> option 6 ip 192.168.1.1
Dhcp::Server: Option 6 is set to 192.168.1.1.
```


History	Version	Description
	2.00	The ip dhcp pool class option command has been introduced.

3.33.4 ip dhcp pool debug

Description Add debug messages to the system log. By default, the setting is disabled.
Command with **no** prefix disables debugging.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dhcp-pool)> debug
(config-dhcp-pool)> no debug
```

History	Version	Description
	2.01	The ip dhcp pool debug command has been introduced.

3.33.5 ip dhcp pool default-router

Description Configure default gateway IP address. If not specified, the address of the Ethernet-interface determined automatically for a given range **range** will be used.

Command with **no** prefix cancels the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dhcp-pool)> default-router <address>
(config-dhcp-pool)> no default-router
```

Arguments	Argument	Value	Description
	address	<i>IP address</i>	Default gateway address.

Example

```
(config-dhcp-pool)> default-router 192.168.1.88
pool "test_pool" router address has been saved.
```

History

Version	Description
2.00	The ip dhcp pool default-router command has been introduced.

3.33.6 ip dhcp pool dns-server

Description

Configure IP addresses of the DNS servers (DHCP option 6). If not specified, the address of the Ethernet-interface determined automatically for a given range **range** will be used.

Command with **no** prefix cancels the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-dhcp-pool)> dns-server ( <address1> [ address2 ] | disable)
```

```
(config-dhcp-pool)> no dns-server
```

Arguments

Argument	Value	Description
address1	<i>IP address</i>	Address of primary DNS server.
address2	<i>IP address</i>	Address of secondary DNS server.
disable	<i>Keyword</i>	Disable DHCP option 6.

Example

```
(config-dhcp-pool)> dns-server 192.168.1.88  
pool "test_pool" name server list has been saved.
```

History

Version	Description
2.00	The ip dhcp pool dns-server command has been introduced.
2.11	Disable argument has been added.

3.33.7 ip dhcp pool domain

Description

Specify the domain name that client should use when resolving hostnames via DNS (option 15).

Command with **no** prefix cancels the setting.

Prefix no

Yes

Change settings

Yes

Multiple input No

Synopsis

```
(config-dhcp-pool)> domain <domain>
(config-dhcp-pool)> no domain
```

Arguments	Argument	Value	Description
	domain	<i>String</i>	Local domain name.

Example

```
(config-dhcp-pool)> domain example.net
Dhcp::Pool: Domain option has been saved.
```

History	Version	Description
	2.05	The ip dhcp pool domain command has been introduced.

3.33.8 ip dhcp pool enable

Description Start to use the pool in the system.
Command with **no** prefix disables pool using.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dhcp-pool)> enable
(config-dhcp-pool)> no enable
```

Example

```
(config-dhcp-pool)> enable
Dhcp::Server: pool "111" is enabled.
```

History	Version	Description
	2.03	The ip dhcp pool enable command has been introduced.

3.33.9 ip dhcp pool lease

Description Set the lease time of DHCP pool IP address. By default, 25200 value is used (7 hours).

Command with **no** prefix resets lease time to default.

Prefix no Yes

Change settings Yes**Multiple input** No

Synopsis

```
(config-dhcp-pool)> lease <lease>
```

```
(config-dhcp-pool)> no lease
```

Argument	Value	Description
lease	<i>Integer</i>	Lease time in seconds. Can take values in the range from 1 to 259200 seconds (3 days).

Example

```
(config-dhcp-pool)> lease 259200
```

```
Dhcp::Pool: "_WEBADMIN": set lease time: 259200 seconds.
```

```
(config-dhcp-pool)> no lease
```

```
Dhcp::Pool: "_WEBADMIN": lease time reset to default (25200 ► seconds).
```

Version	Description
2.00	The ip dhcp pool lease command has been introduced.

3.33.10 ip dhcp pool next-server

Description Set TFTP server address for DHCP client (option 66).Command with **no** prefix removes the setting.**Prefix no** Yes**Change settings** Yes**Multiple input** No**Interface type** Ethernet

Synopsis

```
(config-dhcp-pool)> next-server <address>
```

```
(config-dhcp-pool)> no next-server
```

Argument	Value	Description
address	<i>IP address</i>	TFTP server address.

Example

```
(config-dhcp-pool)> next-server 10.1.1.11
```

```
Dhcp::Pool: "_WEBADMIN": set next server address: 10.1.1.11.
```

```
(config-dhcp-pool)> no next-server
```

```
Dhcp::Pool: "_WEBADMIN": cleared next server address.
```

History

Version	Description
2.11	The ip dhcp pool next-server command has been introduced.

3.33.11 ip dhcp pool option

Description

Set additional options for DHCP server.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

Ethernet

Synopsis

```
(config-dhcp-pool)> option <number> [ type ] <data>
```

```
(config-dhcp-pool)> no option <number>
```

Arguments

Argument	Value	Description
number	4	4 option, Time server. Type is IP address.
	6	6 option, DNS server. Type is IP address.
	42	42 option, NTP server. Type is IP address.
	44	44 option, NetBIOS server. Type is IP address.
	26	26 option, MTU. Can take values in the range from 0 to 65535 inclusively.
	121	121 option, Classless Static Routes. Type is IP address of the destination network and mask of the destination network the form of prefix bit length (for example, /24).
	249	249 option, Microsoft Classless Static Routes. Type is IP address of the destination network and mask of the destination network the form of prefix bit length (for example, /24).
type	hex	Hexadecimal number.
	ascii	ASCII number.
	ip	IP address. It is not applicable to 26 option. It is not specified as a keyword in the command.
data	<i>String</i>	Value of an option.

Example

```
(config-dhcp-pool)> option 4 192.168.2.1  
Dhcp::Pool: "_WEBADMIN_BRIDGE2": set option 4.
```

```
(config-dhcp-pool)> option 60 ascii "MSFT 5.0"
Dhcp::Pool: "_WEBADMIN_BRIDGE2": set option 60.
```

```
(config-dhcp-pool)> option 150 ip 41.57.50.46,42.54.50.46
Dhcp::Pool: "_WEBADMIN_BRIDGE2": set option 150.
```

```
(config-dhcp-pool)> no option 4
Dhcp::Pool: "_WEBADMIN_BRIDGE2": cleared option 4.
```

History

Version	Description
2.09	The ip dhcp pool option command has been introduced.

3.33.12 ip dhcp pool range

Description

Configure the range of dynamic addresses issued to DHCP clients of a subnet. The range is set by start and end IP addresses or the start address and size. The network interface to which the settings are applied is chosen automatically. Address of the chosen interface is used as the default gateway and DNS server, if other addresses are not specified using commands **ip dhcp pool default-router** and **ip dhcp pool dns-server**.

Command with **no** prefix removes the range.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-dhcp-pool)> range <begin> ( <end> | <size> )
```

```
(config-dhcp-pool)> no range
```

Arguments

Argument	Value	Description
begin	<i>IP address</i>	Pool's start address.
end	<i>IP address</i>	Pool's end address.
size	<i>Integer</i>	Pool size.

Example

```
(config-dhcp-pool)> range 192.168.15.43 3
pool "_WEBADMIN" range has been saved.
```

History

Version	Description
2.00	The ip dhcp pool range command has been introduced.

3.33.13 ip dhcp pool update-dns

Description Add static records into DNS-proxy when DHCP-address is assigned. The name of record is the hostname of the DHCP-request. By default, the feature is disabled.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dhcp-pool)> update-dns
(config-dhcp-pool)> no update-dns
```

Example

```
(config-dhcp-pool)> update-dns
Dhcp::Pool: DNS update has been enabled.
```

History

Version	Description
2.06	The ip dhcp pool update-dns command has been introduced.

3.33.14 ip dhcp pool wpad

Description Configure DHCP option 252 — [WPAD](#) protocol. By default, the option is disabled.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-dhcp-pool)> wpad <wpad>
(config-dhcp-pool)> no wpad
```

Arguments

Argument	Value	Description
wpad	<i>String</i>	URL of proxy.

Example

```
(config-dhcp-pool)> wpad http://wpad/wpad.dat
Dhcp::Pool: WPAD option has been saved.
```

History

Version	Description
2.05	The ip dhcp pool wpad command has been introduced.

3.34 ip dhcp relay enable

Description

Enable DHCP relay on an interface. DHCP relay takes priority over the router's DHCP server.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

Ethernet

Synopsis

```
(config-if)> ip dhcp relay enable
```

```
(config-if)> no ip dhcp relay enable
```

Example

```
(config-if)> ip dhcp relay enable
Dhcp::Relay: Service enabled on ISP.
```

```
(config-if)> no ip dhcp relay enable
Dhcp::Relay: Service disabled on ISP.
```

History

Version	Description
4.03	The ip dhcp relay enable command has been introduced.

3.35 ip dhcp relay lan

Description

Specify which network interface the DHCP relay will use to handle client's requests. Several "lan" interfaces can be specified, to which end the command should be entered several times, enumerating all desired interfaces one by one.

Command with **no** prefix disables the DHCP relay on the specified interface. If you use no argument, the DHCP relay will be removed from all interfaces.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config)> ip dhcp relay lan <interface>
```



```
(config)> no ip dhcp relay lan [ interface ]
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full name or an alias of Ethernet interface, through which DHCP relay will accept requests from clients.

Example

```
(config)> ip dhcp relay lan Home
added LAN interface Home.
```

History

Version	Description
2.00	The ip dhcp relay lan command has been introduced.

3.36 ip dhcp relay server

Description

Specify the IP address of the [DHCP server](#), to which the relay will forward client requests from the LAN.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> ip dhcp relay server <address>
```

```
(config)> no ip dhcp relay server [ address ]
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	IP address of the DHCP server .

Example

```
(config)> ip dhcp relay server 192.168.1.11
using DHCP server 192.168.1.11.
```

History

Version	Description
2.00	The ip dhcp relay server command has been introduced.

3.37 ip dhcp relay upstream interface

Description

Bind DHCP upstream to a specific interface.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis

```
(config-if)> ip dhcp relay upstream interface <interface>
(config-if)> no ip dhcp relay upstream interface
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(config-if)> ip dhcp relay upstream interface Home
Dhcp::Relay: Using WAN interface Home.
```

```
(config-if)> no ip dhcp relay upstream interface
Dhcp::Relay: WAN interface setting cleared.
```

History

Version	Description
4.03	The ip dhcp relay upstream interface command has been introduced.

3.38 ip dhcp relay upstream server

Description Specify an upstream IP address of the [DHCP server](#), to which the relay will forward client requests.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis

```
(config-if)> ip dhcp relay upstream server <server>
(config-if)> no ip dhcp relay upstream server
```

Arguments

Argument	Value	Description
server	<i>IP address</i>	IP address of the DHCP server .

Example

```
(config-if)> ip dhcp relay upstream server 192.168.17.1
Dhcp::Relay: Using DHCP server 192.168.17.1.
```

```
(config-if)> no ip dhcp relay upstream server
Dhcp::Relay: Server address setting cleared.
```

History

Version	Description
4.03	The ip dhcp relay upstream server command has been introduced.

3.39 ip dhcp relay wan

Description

Specify the network interface through which DHCP relay will interact with higher level [DHCP server](#). There can be only one interface of such type in the system. If exact address of the server is not specified (see [ip dhcp relay server](#)), the requests will be broadcasted. It is recommended to specify server address.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> ip dhcp relay wan <interface>
```

```
(config)> no ip dhcp relay wan [ interface ]
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full name or an alias of Ethernet interface, on which requests from the DHCP clients will be sent.

Example

```
(config)> ip dhcp relay wan FastEthernet0/Vlan2
using WAN interface FastEthernet0/Vlan2.
```

History

Version	Description
2.00	The ip dhcp relay wan command has been introduced.

3.40 ip esp alg enable

Description Enable *IPSec Passthrough* mode for *IPsec ESP* tunnel. By default, the setting is disabled.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> ip esp alg enable
(config)> no ip esp alg enable
```

Example

```
(config)> ip esp alg enable
Esp::Alg: Enabled.

(config)> no ip esp alg enable
Esp::Alg: Disabled.
```

History

Version	Description
3.05	The ip esp alg enable command has been introduced.

3.41 ip flow-cache timeout active

Description Set timeout of active sessions in cache. By default, the value 10 is used.

Command with **no** prefix resets the setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> ip flow-cache timeout active <timeout>
(config)> no ip flow-cache timeout active
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	The timeout value, in minutes. Can take values in the range from 1 to 30.

Example

```
(config)> ip flow-cache timeout active 1
Netflow::Manager: Active timeout set to "1" min.
```

```
(config)> no ip flow-cache timeout active
Netflow::Manager: Active timeout reset to "10" min.
```

History

Version	Description
2.11	The ip flow-cache timeout active command has been introduced.

3.42 ip flow-cache timeout inactive

Description Set timeout of inactive sessions in cache. By default, the value 20 is used.

Command with **no** prefix resets the setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> ip flow-cache timeout inactive <timeout>
```

```
(config)> no ip flow-cache timeout inactive
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	The timeout value, in seconds. Can take values in the range from 1 to 600.

Example

```
(config)> ip flow-cache timeout inactive 1
Netflow::Manager: Inactive timeout set to "1" s.
```

```
(config)> no ip flow-cache timeout inactive
Netflow::Manager: Inactive timeout reset to "20" s.
```

History

Version	Description
2.11	The ip flow-cache timeout inactive command has been introduced.

3.43 ip flow-export destination

Description Set parameters of *NetFlow* collector.

Command with **no** prefix removes collector's parameters.

Prefix no Yes

Change settings Yes

Multiple input

No

Synopsis

```
(config)> ip flow-export destination <address> <port>
```

```
(config)> no ip flow-export destination
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	IP address of the data collector.
port	<i>Integer</i>	Collector's UDP port number. Can take values 2055, 2056, 4432, 4739, 9025, 9026, 9995, 9996, 6343.

Example

```
(config)> ip flow-export destination 192.168.101.31 4739
Netflow::Manager: Export destination is set to ►
192.168.101.31:4739.
```

```
(config)> no ip flow-export destination
Netflow::Manager: Export destination is unset.
```

History

Version	Description
2.11	The ip flow-export destination command has been introduced.

3.44 ip flow-export version

DescriptionSet version of *NetFlow* collector. By default, 5 value is used.Command with **no** prefix resets version to default.**Prefix no**

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> ip flow-export version <version>
```

```
(config)> no ip flow-export version
```

Arguments

Argument	Value	Description
version	<i>String</i>	Version of protocol.

Example

```
(config)> ip flow-export version 9
Netflow::Manager: Set export protocol version to 9.
```

```
(config)> no ip flow-export version
Netflow::Manager: Reset export version to 5.
```

History

Version	Description
3.05	The ip flow-export version command has been introduced.

3.45 ip ftp

Description Access to a group of commands to configure access to **ftp**.

Prefix no No

Change settings No

Multiple input No

Interface type IP

Group entry (config-ftp)

Synopsis (config)> **ip ftp**

Example (config)> **ip ftp**
(config-ftp)>

History

Version	Description
2.08	The ip ftp command has been introduced.

3.45.1 ip ftp client-charset

Description Set default encoding on FTP server. By default, the UTF-8 is used.

Command with **no** prefix resets encoding to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis (config-ftp)> **client-charset** *<charset>*
(config-ftp)> **no client-charset**

Arguments

Argument	Value	Description
charset	utf-8	Encoding type.
	utf-16	
	utf-16le	
	utf-16be	
	utf-32	
	utf-32le	
	utf-32be	
	iso-8859-1	
	iso-8859-2	
	iso-8859-3	
	iso-8859-4	
	iso-8859-5	
	iso-8859-6	
	iso-8859-7	
	iso-8859-8	
	iso-8859-9	
	iso-8859-10	
	iso-8859-11	
	iso-8859-12	
	iso-8859-13	
	iso-8859-14	
	iso-8859-15	
	iso-8859-16	
	cp-037	
	cp-424	
	cp-437	
	cp-500	
	cp-737	
	cp-775	
	cp-850	
	cp-852	
	cp-852	
	cp-855	
	cp-856	
	cp-857	

Argument	Value	Description
	cp-860	
	cp-861	
	cp-862	
	cp-863	
	cp-864	
	cp-865	
	cp-866	
	cp-869	
	cp-874	
	cp-1026	
	cp-1250	
	cp-1251	
	cp-1252	
	cp-1253	
	cp-1254	
	cp-1255	
	cp-1256	
	cp-1257	
	cp-1258	
	koi8-r	
	koi8-u	
	kz-1048	
	nextstep	
	mac-celtic	
	mac-centeuro	
	mac-croatian	
	mac-cyrillic	
	mac-gaelic	
	mac-greek	
	mac-icelandic	
	mac-inuit	
	mac-roman	
	mac-romanian	
	mac-turkish	
	mac-ukrainian	

Example

```
(config-ftp)> client-charset utf-16
Ftp::Server: Set client charset to "utf-16".
```

```
(config-ftp)> no client-charset
Ftp::Server: Reset client charset to default.
```

History

Version	Description
2.11	The ip ftp client-charset command has been introduced.

3.45.2 ip ftp lockout-policy

Description

Set FTP server bruteforce detection parameters for public interfaces. By default, feature is enabled. If you use 0 as an argument, all bruteforce detection parameters will be reset to default.

Command with **no** prefix disables bruteforce detection.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-ftp)> lockout-policy <threshold> [<duration>] [<observation-window>]
```

```
(config-ftp)> no lockout-policy
```

Arguments

Argument	Value	Description
threshold	<i>Integer</i>	The number of failed attempts to log in. By default, 5 value is used. Can take values in the range from 3 to 20.
duration	<i>Integer</i>	An authorization ban duration for the specified IP in minutes. By default, 15 value is used. Can take values in the range from 1 to 60.
observation-window	<i>Integer</i>	Duration of suspicious activity observation in minutes. By default, 3 value is used. Can take values in the range from 1 to 10.

Example

```
(config-ftp)> lockout-policy 10 30 2
Ftp::Server: Bruteforce detection is enabled.
```

```
(config-ftp)> no lockout-policy
Ftp::Server: Bruteforce detection is disabled.
```

```
(config-ftp)> lockout-policy 0
Ftp::Server: Brute force detection reset to default.
```

History

Version	Description
2.12	The ip ftp lockout-policy command has been introduced.

3.45.3 ip ftp permissive

Description Access to the FTP server for all users without authentication.

Command with **no** prefix denies access.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis (config-ftp)> **permissive**

(config-ftp)> **no permissive**

Example (config-ftp)> **permissive**

(config-ftp)> **no permissive**

History

Version	Description
2.08	The ip ftp permissive command has been introduced.

3.45.4 ip ftp security-level

Description Set FTP security level. By default, private value is set.

Prefix no No

Change settings Yes

Multiple input No

Interface type IP

Synopsis (config-ftp)> **security-level (public | private | protected)**

Arguments

Argument	Value	Description
public	<i>Keyword</i>	Access to the FTP server is allowed for public, private and protected interfaces.
private	<i>Keyword</i>	Access to the FTP server is allowed for private interfaces.
protected	<i>Keyword</i>	Access to the FTP server is allowed for private and protected interfaces.

Example

```
(config-ftp)> security-level protected
Ftp::Manager: Security level changed to protected.
```

History

Version	Description
2.08	The ip ftp security-level command has been introduced.

3.46 ip host

Description Add a domain name and address as a DNS-record.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config)> ip host <domain> <address>
```

```
(config)> no ip host [ <domain> <address> ]
```

Arguments

Argument	Value	Description
domain	<i>String</i>	A domain name of a host.
address	<i>IP address</i>	An IP address of a host.

Example

```
(config)> ip host keenetic.local 192.168.1.22
Dns::Manager: Added static record for "keenetic.local", address ►
192.168.1.22.
```

```
(config)> no ip host keenetic.local 192.168.1.22
Dns::Manager: Record "keenetic.local", address 192.168.1.22 ►
deleted.
```

History

Version	Description
2.00	The ip host command has been introduced.

3.47 ip hotspot

Description Access to a group of commands for Hotspot configuration.

Prefix no No

Change settings No

Multiple input No

Interface type IP

Group entry (config-hotspot)

Synopsis (config)> **ip hotspot**

Example (config)> **ip hotspot**
(config-hotspot)>

History	Version	Description
	2.06	The ip hotspot command has been introduced.

3.47.1 ip hotspot auto-register disable

Description Forcibly disable automatic host registration in the Home segment. By default, the auto-registration is enabled.

Command with **no** prefix enables the auto-registration.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis (config-hotspot)> **auto-register disable**

(config-hotspot)> **no auto-register disable**

Example (config-hotspot)> **auto-register disable**
Hotspot::AutoRegister: Disabled host auto-registration.

(config-hotspot)> **no auto-register disable**
Hotspot::AutoRegister: Enabled host auto-registration.

History

Version	Description
4.02	The ip hotspot auto-register disable command has been introduced.

3.47.2 ip hotspot auto-scan interface

Description

Enable subnetwork passive scanning on interface. By default is enabled.

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

IP

Synopsis

```
(config-hotspot)> auto-scan interface <interface>
```

```
(config-hotspot)> no auto-scan interface <interface>
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias.

Example

```
(config-hotspot)> auto-scan interface WifiMaster0/AccessPoint1
Hotspot::Discovery::Manager: Subnetwork scanning on interface ►
"WifiMaster0/AccessPoint1" is unchanged.
```

```
(config-hotspot)> auto-scan interface WifiMaster0/AccessPoint1
Hotspot::Discovery::Manager: Subnetwork scanning on interface ►
"WifiMaster0/AccessPoint1" is disabled.
```

History

Version	Description
2.08	The ip hotspot auto-scan interface command has been introduced.

3.47.3 ip hotspot auto-scan interval

Description

Set interval for probes of online hosts. By default, the value 30 is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type	IP						
Synopsis	(config-hotspot)> auto-scan interval <i><interval></i> (config-hotspot)> no auto-scan interval						
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td>interval</td><td><i>Integer</i></td><td>Auto-scan probe interval in seconds.</td></tr></table>	Argument	Value	Description	interval	<i>Integer</i>	Auto-scan probe interval in seconds.
Argument	Value	Description					
interval	<i>Integer</i>	Auto-scan probe interval in seconds.					
Example	(config-hotspot)> auto-scan interval 10 Hotspot::Discovery::Manager: Auto-scan probe interval is set to ► 10 s. (config-hotspot)> no auto-scan interval Hotspot::Discovery::Manager: Auto-scan probe interval reset to ► default.						
History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>2.08</td><td>The ip hotspot auto-scan interval command has been introduced.</td></tr></table>	Version	Description	2.08	The ip hotspot auto-scan interval command has been introduced.		
Version	Description						
2.08	The ip hotspot auto-scan interval command has been introduced.						

3.47.4 ip hotspot auto-scan passive

Description	Set passive autoscan rate in hosts per seconds. By default, the value 3 is used. Command with no prefix resets setting to default.						
Prefix no	Yes						
Change settings	Yes						
Multiple input	No						
Interface type	IP						
Synopsis	<pre>(config-hotspot)> auto-scan passive <rate> hps</pre> <pre>(config-hotspot)> no auto-scan passive</pre>						
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td>rate</td><td><i>Integer</i></td><td>Passive autoscan rate.</td></tr></table>	Argument	Value	Description	rate	<i>Integer</i>	Passive autoscan rate.
Argument	Value	Description					
rate	<i>Integer</i>	Passive autoscan rate.					
Example	<pre>(config-hotspot)> auto-scan passive 5 hps</pre> <pre>Hotspot::Discovery::Manager: Auto-scan rate is set to 5 hps.</pre> <pre>(config-hotspot)> no auto-scan passive</pre> <pre>Hotspot::Discovery::Manager: Auto-scan rate reset to default.</pre>						

History

Version	Description
2.08	The ip hotspot auto-scan passive command has been introduced.

3.47.5 ip hotspot auto-scan timeout

Description

Set offline timeout for hosts. After the specified time, the missing host is removed from the online host list. By default, the value 35 is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-hotspot)> auto-scan timeout <timeout>
```

```
(config-hotspot)> no auto-scan timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	Offline timeout in seconds.

Example

```
(config-hotspot)> auto-scan timeout 31
Hotspot::Discovery::Manager: Auto-scan host offline timeout is ►
set to 31 s.
```

```
(config-hotspot)> no auto-scan timeout
Hotspot::Discovery::Manager: Auto-scan host offline timeout reset ►
to default.
```

History

Version	Description
2.08	The ip hotspot auto-scan timeout command has been introduced.

3.47.6 ip hotspot default-policy

Description

Define the Hotspot policy for all interfaces or assign IP Policy. Policy applies to all hosts that have no explicitly configured access rule, [ip hotspot policy](#).

Default policy: permit.

Command with **no** prefix resets policy to default.

Prefix no Yes**Change settings** Yes**Multiple input** Yes**Interface type** IP

Synopsis

```
(config-hotspot)> default-policy (<access> | <policy>)
```

```
(config-hotspot)> no default-policy
```

Arguments

Argument	Value	Description
access	permit	Permit access to the internet.
	deny	Deny access to the internet.
policy	<i>Policy</i>	Name of IP Policy profile.

Example

```
(config-hotspot)> default-policy permit
FHotspot::Manager: Default policy "permit" applied.
```

```
(config-hotspot)> default-policy deny
Hotspot::Manager: Default policy "deny" applied.
```

```
(config-hotspot)> default-policy Policy0
Hotspot::Manager: Default policy "Policy0" applied.
```

```
(config-hotspot)> no default-policy
Hotspot::Manager: Default policy cleared.
```

History

Version	Description
2.09	The ip hotspot default-policy command has been introduced.
2.12	Argument policy was added.

3.47.7 ip hotspot host

Description Setup bypass or block rules for specific Hotspot clients. Host rules override interface based policy (see [ip hotspot policy](#) command).

Command with **no** prefix removes the setting.

Prefix no Yes**Change settings** Yes**Multiple input** Yes**Interface type** IP

Synopsis

```
(config-hotspot)> host <mac> (<access> | schedule <schedule> | policy <policy>)
```

```
(config-hotspot)> no host <mac> (<access> | schedule | policy)
```

Arguments

Argument	Value	Description
mac	MAC address	Host MAC address. Host must be registered via known host in advance.
access	permit	Permit access to the internet.
	deny	Deny access to the internet.
schedule	Schedule	The name of the schedule that was created with schedule group of commands.
policy	Policy	Name of IP Policy profile.

Example

```
(config)> known host MYTEST 54:e4:3a:8a:f3:a7
Hotspot::Manager: Policy "permit" applied to interface "Home".
```

```
(config-hotspot)> host 54:e4:3a:8a:f3:a7 permit
Hotspot::Manager: Rule "permit" applied to host ►
"54:e4:3a:8a:f3:a7".
```

```
(config-hotspot)> host 54:e4:3a:8a:f3:a7 deny
Hotspot::Manager: Rule "deny" applied to host "54:e4:3a:8a:f3:a7".
```

```
(config-hotspot)> host 54:e4:3a:8a:f3:a7 schedule MYSCHEDULE
Hotspot::Manager: Schedule "MYSCHEDULE" applied to host ►
"54:e4:3a:8a:f3:a7".
```

```
(config-hotspot)> no host 54:e4:3a:8a:f3:a7 schedule
Hotspot::Manager: Host "54:e4:3a:8a:f3:a7" schedule disabled.
```

```
(config-hotspot)> host 54:e4:3a:8a:f3:a7 policy Policy0
Hotspot::Manager: Policy "Policy0" applied to host ►
"54:e4:3a:8a:f3:a7".
```

```
(config-hotspot)> no host 54:e4:3a:8a:f3:a7 policy
Hotspot::Manager: Policy removed from host "54:e4:3a:8a:f3:a7".
```

History

Version	Description
2.06	The ip hotspot host command has been introduced.
2.12	Arguments permit, deny, schedule, policy were added.

3.47.8 ip hotspot host conform

Description

Assign a segment-default policy for the registered hosts. Registration of a host is performed in advance by the [known host](#) command. By default, the setting is enabled.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-hotspot)> host <mac> conform
(config-hotspot)> no host <mac> conform
```

Argument	Value	Description
mac	MAC address	MAC address of host.

Example

```
(config-hotspot)> host 04:14:24:54:bc:52 conform
Hotspot::Manager: Conform applied to host "04:14:24:54:bc:52".

(config-hotspot)> no host 04:14:24:54:bc:52 conform
Hotspot::Manager: Conform removed from host "04:14:24:54:bc:52".
```

Version	Description
4.02	The ip hotspot host conform command has been introduced.

3.47.9 ip hotspot host priority

Description Assign a specific priority to all traffic bound to a registered host. Registration of a host is performed in advance by the **known host** command.

Command with **no** prefix removes the priority.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-hotspot)> host <mac> priority <priority>
(config-hotspot)> no host <mac> priority
```

Argument	Value	Description
mac	MAC address	Host MAC address.

Argument	Value	Description
priority	1	Top.
	2	Critical.
	3	High.
	4	Medium-high.
	5	Medium.
	6	Normal (Default).
	7	Low.

Example

```
(config-hotspot)> host 04:d2:c1:14:bc:59 priority 7
```

```
Hotspot::Manager: Applied priority "7" to host ►  
"04:d2:c1:14:bc:59".
```

```
(config-hotspot)> no host 04:d2:c1:14:bc:59 priority
```

```
Hotspot::Manager: Removed priority from host "04:d2:c1:14:bc:59".
```

History

Version	Description
3.08	The ip hotspot host priority command has been introduced.

3.47.10 ip hotspot policy

Description

Define the Hotspot policy for a specific interface. Policy applies to all hosts that have no explicitly configured access rule, **ip hotspot host**.

Default policy: permit.

Command with **no** prefix resets policy to default.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

IP

Synopsis

```
(config-hotspot)> policy <interface> (<access> | <policy>)
```

```
(config-hotspot)> no policy <interface>
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Ethernet interface full name or an alias.
access	permit	Permit access to the internet.
	deny	Deny access to the internet.

Argument	Value	Description
policy	<i>Policy</i>	Name of IP Policy profile.

Example

```
(config-hotspot)> policy Home permit
Hotspot::Manager: Policy "permit" applied to interface "Home".
```

```
(config-hotspot)> policy Home deny
Hotspot::Manager: Policy "deny" applied to interface "Home".
```

```
(config-hotspot)> policy Home Policy0
Hotspot::Manager: Policy "Policy0" applied to interface "Home".
```

```
(config-hotspot)> no policy Home
Hotspot::Manager: Interface "Home" policy cleared.
```

History

Version	Description
2.06	The ip hotspot policy command has been introduced.
2.12	Argument policy was added.

3.47.11 ip hotspot priority

Description

Assign a specific priority to all traffic bound to the interface.

Command with **no** prefix removes the priority.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

IP

Synopsis

```
(config-hotspot)> priority <interface> <priority>
```

```
(config-hotspot)> no priority <interface>
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias.
priority	1	Top.
	2	Critical.
	3	High.
	4	Medium-high.
	5	Medium.
	6	Normal (Default).

Argument	Value	Description
	7	Low.

Example

```
(config-hotspot)> priority Home 7
Hotspot::Manager: Applied priority "7" to interface "Home".
```

```
(config-hotspot)> no priority Home
Hotspot::Manager: Removed priority from interface "Home".
```

History

Version	Description
3.08	The ip hotspot priority command has been introduced.

3.47.12 ip hotspot wake

Description Send Wake-on-LAN packet to private and protected interfaces of the host.

Prefix no No

Change settings No

Multiple input No

Interface type IP

Synopsis `(config-hotspot)> wake <mac>`

Arguments

Argument	Value	Description
mac	<i>MAC address</i>	Host MAC address.

Example

```
(config-hotspot)> wake a8:1e:84:11:f1:22
Hotspot::Manager: WoL sent to host: a8:1e:84:11:f1:22.
```

History

Version	Description
2.08	The ip hotspot wake command has been introduced.

3.48 ip http lockout-policy

Description Set HTTP bruteforce detection parameters for public interfaces. By default, feature is enabled. If you use 0 as an argument, all bruteforce detection parameters will be reset to default.

Command with **no** prefix disables bruteforce detection.

Prefix no Yes

Change settings Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config)> ip http lockout-policy <threshold> [ <duration> [
<observation-window> ]]

(config)> no ip http lockout-policy
```

Arguments

Argument	Value	Description
threshold	<i>Integer</i>	The number of failed attempts to log in. By default, 5 value is used. Can take values in the range from 4 to 20.
duration	<i>Integer</i>	An authorization ban duration for the specified IP in minutes. By default, 15 value is used. Can take values in the range from 1 to 60.
observation-window	<i>Integer</i>	Duration of suspicious activity observation in minutes. By default, 3 value is used. Can take values in the range from 1 to 10.

Example

```
(config)> ip http lockout-policy 10 30 2
Http::Manager: Bruteforce detection is enabled.
```

```
(config)> no ip http lockout-policy
Http::Manager: Bruteforce detection is disabled.
```

```
(config)> ip http lockout-policy 0
Http::Manager: Bruteforce detection reset to default.
```

History

Version	Description
2.08	The ip http lockout-policy command has been introduced.

3.49 ip http log access

Description Enable debug mode for web server (nginx). By default, feature is disabled. Command with **no** prefix disables the debug mode.

Prefix no Yes**Change settings** Yes**Multiple input** No

Interface type IP

Synopsis

```
(config)> ip http log access
```

```
(config)> no ip http log access
```

Example

```
(config)> ip http log access
Http::Manager: Enabled access logging.
```

```
(config)> no ip http log access
Http::Manager: Disabled access logging.
```

History

Version	Description
3.00	The ip http log access command has been introduced.

3.50 ip http log auth

Description Enable logging of failed authorization attempts to the system. By default, feature is disabled.

Command with **no** prefix disables logging.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config)> ip http log auth
```

```
(config)> no ip http log auth
```

Example

```
(config)> ip http log auth
Http::Manager: Auth logging enabled.
```

```
(config)> no ip http log auth
Http::Manager: Auth logging disabled.
```

History

Version	Description
2.08	The ip http log auth command has been introduced.

3.51 ip http log webdav

Description Enable logging of failed connection attempts to the [WebDAV](#) server. By default, feature is disabled.

Command with **no** prefix disables logging.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config)> ip http log webdav
(config)> no ip http log webdav
```

Example

```
(config)> ip http log webdav
WebDav::Server: Enabled request tracing.

(config)> no ip http log webdav
WebDav::Server: Disabled request tracing.
```

History

Version	Description
3.04	The ip http log webdav command has been introduced.

3.52 ip http port

Description Assign HTTP port for Web interface of Carrier. By default, 80 value is used.

Command with **no** prefix resets HTTP port to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config)> ip http port <port>
(config)> no ip http port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	New HTTP port.

Example

```
(config)> ip http port 8080
Http::Manager: Port changed to 8080.
```

```
(config)> no ip http port
Http::Manager: Port reset to 80.
```

History

Version	Description
2.08	The ip http port command has been introduced.

3.53 ip http proxy

Description

Access to a group of commands to configure HTTP proxy. If the proxy is not found, the command tries to create it.

Command with **no** prefix removes the proxy.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

IP

Group entry

(config-http-proxy)

Synopsis

```
(config)> ip http proxy <name>
```

```
(config)> no ip http proxy <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	HTTP proxy name.

Example

```
(config)> ip http proxy TEST
Http::Manager: Proxy "TEST" successfully created.
```

History

Version	Description
2.08	The ip http proxy command has been introduced.

3.53.1 ip http proxy auth

Description

Enable authorization for HTTP proxy. By default, the setting is disabled.

Command with **no** prefix disables HTTP proxy authorization.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-http-proxy)> auth
```

```
(config-http-proxy)> no auth
```

Example

```
(config-http-proxy)> auth  
Http::Manager: Proxy password auth is enabled.
```

```
(config-http-proxy)> no auth  
Http::Manager: Proxy password auth is disabled.
```

History

Version	Description
2.10	The ip http proxy auth command has been introduced.

3.53.2 ip http proxy dns-override

Description

Enable local DNS overrides for fourth level domains KeenDNS. By default, the setting is enabled.

Note:

For the fourth level domain KeenDNS, a static DNS A-record with the address 78.47.125.180 (this is the IP we purchased for the name my.keenetic.net) is added for access in the router's local network.

After disabling this feature, the static DNS A-record with the address 78.47.125.180 is removed from the router's system for the fourth level domain KeenDNS.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-http-proxy)> dns-override
```

```
(config-http-proxy)> no dns-override
```

Example

```
(config-http-proxy)> dns-override  
Http::Proxy: "test": enabled DNS override.
```

```
(config-http-proxy)> no dns-override  
Http::Proxy: "test": disabled DNS override.
```

History

Version	Description
4.03	The ip http proxy dns-override command has been introduced.

3.53.3 ip http proxy domain

Description

Set domain name that specifies the [FQDN](#) of the virtual host.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-http-proxy)> domain static <domain>
```

```
(config-http-proxy)> no domain
```

Arguments

Argument	Value	Description
domain	<i>String</i>	A domain name.

Example

```
(config-http-proxy)> domain static example.net  
Http::Manager: Configured base domain for proxy: test.
```

```
(config-http-proxy)> no domain  
Http::Manager: Removed ndns domain for proxy: test.
```

History

Version	Description
2.08	The ip http proxy domain command has been introduced.

3.53.4 ip http proxy domain ndns

Description

Set HTTP proxy domain through NDNS. If enabled, setting [ip http proxy domain](#) is deleted.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type IP

Synopsis

```
(config-http-proxy)> domain ndns
(config-http-proxy)> no domain ndns
```

Example

```
(config-http-proxy)> domain ndns
Http::Manager: Configured ndns domain for proxy: test.

(config-http-proxy)> no domain
Http::Manager: Removed ndns domain for proxy: test.
```

History

Version	Description
2.08	The ip http proxy domain ndns command has been introduced.

3.53.5 ip http proxy force-host

Description Enable the Host header rewriting for the upstream.
Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-http-proxy)> force-host <force-host>
(config-http-proxy)> no force-host
```

Arguments

Argument	Value	Description
force-host	<i>String</i>	IP address or domain name.

Example

```
(config-http-proxy)> force-host 192.168.8.1
Http::Proxy: "modem": enabled Host header enforcing to ►
"192.168.8.1".

(config-http-proxy)> force-host modem.keenetic.pro
Http::Proxy: "modem": enabled Host header enforcing to ►
"modem.keenetic.pro".

(config-http-proxy)> no force-host
Http::Proxy: "modem": disabled Host header enforcing.
```

History

Version	Description
3.06	The ip http proxy force-host command has been introduced.

3.53.6 ip http proxy preserve-host

Description

Set option to save the original header for the host when passing through a proxy.

Command with **no** prefix disable option.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-http-proxy)> preserve-host
```

```
(config-http-proxy)> no preserve-host
```

Example

```
(config-http-proxy)> preserve-host  
Http::Manager: Proxy HTTP Host header preservation is enabled.
```

```
(config-http-proxy)> no preserve-host  
Http::Manager: Proxy HTTP Host header preservation is disabled.
```

History

Version	Description
2.13	The ip http proxy preserve-host command has been introduced.

3.53.7 ip http proxy preserve-origin

Description

Enable the option to save the Origin header for the host when passing through a proxy.

Command with **no** prefix disable option.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-http-proxy)> preserve-origin
```

```
(config-http-proxy)> no preserve-origin
```

Example

```
(config-http-proxy)> preserve-origin
Http::Proxy: "test": enabled Origin header preservation.
```

```
(config-http-proxy)> no preserve-origin
Http::Proxy: "test": disabled Origin header preservation.
```

History

Version	Description
4.02	The ip http proxy preserve-origin command has been introduced.

3.53.8 ip http proxy preserve-referer

Description

Enable the option to save the Referer header for the host when passing through a proxy.

Command with **no** prefix disable option.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-http-proxy)> preserve-referer
```

```
(config-http-proxy)> no preserve-referer
```

Example

```
(config-http-proxy)> preserve-referer
Http::Proxy: "test": enabled Referer header preservation.
```

```
(config-http-proxy)> no preserve-referer
Http::Proxy: "test": disabled Referer header preservation.
```

History

Version	Description
4.02	The ip http proxy preserve-referer command has been introduced.

3.53.9 ip http proxy security-level

Description

Set the security level for HTTP proxy service. By default, private value is set.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config-http-proxy)> security-level (public | private)
```

```
(config-http-proxy)> no security-level
```

Arguments

Argument	Value	Description
public	<i>Keyword</i>	Access to the HTTP proxy is allowed for public, private and protected interfaces.
private	<i>Keyword</i>	Access to the HTTP proxy is allowed for private interfaces only.

Example

```
(config-http-proxy)> security-level public
```

```
Http::Proxy: "test1": set public security level.
```

```
(config-http-proxy)> no security-level
```

```
Http::Proxy: "test1": unset public security level.
```

History

Version	Description
3.05	The ip http proxy security-level command has been introduced.

3.53.10 ip http proxy ssl redirect

Description Enable automatic redirection on domains with SSL certificate for HTTP proxy service. By default, the redirection is enabled.

Command with **no** prefix disables redirection.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config-http-proxy)> ssl redirect
```

```
(config-http-proxy)> no ssl redirect
```

Example

```
(config)> ip http ssl redirect
```

```
Http::Proxy: "mytest": enabled SSL redirect.
```



```
(config)> no ip http ssl redirect
Http::Proxy: "mytest": disabled SSL redirect.
```

History

Version	Description
4.00	The ip http proxy ssl redirect command has been introduced.

3.53.11 ip http proxy timeout

Description Configure connection timeout for HTTP proxies. By default, the value 60 is used.

Command with **no** prefix resets timeout to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-http-proxy)> timeout <timeout>
```

```
(config-http-proxy)> no timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	Timeout value in the range from 5 to 86400 seconds.

Example

```
(config-http-proxy)> timeout 5
Http::Proxy: "test": set upstream timeout to "5" s.
```

```
(config-http-proxy)> no timeout
Http::Proxy: "test": reset upstream timeout.
```

History

Version	Description
4.02	The ip http proxy timeout command has been introduced.

3.53.12 ip http proxy upstream

Description Set HTTP or HTTPS server address for request redirecting.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-http-proxy)> upstream (http | https | connect) ( mac | ip | fqdn ) [ port ]
```

```
(config-http-proxy)> no upstream
```

Arguments

Argument	Value	Description
http	<i>Keyword</i>	HTTP server.
https	<i>Keyword</i>	HTTPS server.
connect	<i>Keyword</i>	IP address and the port number of OpenVPN server.
mac	<i>MAC address</i>	MAC address of server.
ip	<i>IP address</i>	IP address of server.
fqdn	<i>FQDN</i>	Full domain name of server.
port	<i>Integer</i>	The port number.

Example

```
(config-http-proxy)> upstream http 192.168.1.1 8080  
Http::Proxy: "test": set http upstream 192.168.1.1, port 8080.
```

```
(config-http-proxy)> upstream https google.com 443  
Http::Proxy: "test": set https upstream google.com, port 443.
```

```
(config-http-proxy)> upstream connect 127.0.0.1 8000  
Http::Proxy: "test": set connect upstream 127.0.0.1, port 8000.
```

```
(config-http-proxy)> no upstream  
Http::Proxy: "test": reset upstream.
```

History

Version	Description
2.08	The ip http proxy upstream command has been introduced.
3.05	https keyword was added.
4.03	connect keyword was added.

3.53.13 ip http proxy x-real-ip

Description Enable X-Real-IP and X-Forwarded-For header support for HTTP proxy.
Command with **no** prefix disables headers.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-http-proxy)> x-real-ip
(config-http-proxy)> no x-real-ip
```

Example

```
(config-http-proxy)> x-real-ip
Http::Proxy: "test1": enabled X-Real-IP and X-Forwarded-For ►
headers.
```

```
(config-http-proxy)> no x-real-ip
Http::Proxy: "test1": disabled X-Real-IP and X-Forwarded-For ►
headers.
```

History

Version	Description
3.05	The ip http proxy x-real-ip command has been introduced.

3.54 ip http security-level

Description Set the security level for remote access to the Keenetic web interface. By default, private value is set.

Prefix no No

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config)> ip http security-level (public [ssl] | private | protected)
```

Arguments

Argument	Value	Description
public	<i>Keyword</i>	Access to the web interface is allowed for public, private and protected interfaces via HTTP and HTTPS.
private	<i>Keyword</i>	Access to the web interface is allowed for private interfaces.
protected	<i>Keyword</i>	Access to the web interface is allowed for private and protected interfaces.
ssl	<i>Keyword</i>	Access to the web interface is allowed for public interfaces via HTTPS only.

Example

```
(config)> ip http security-level protected
Http::Manager: Security level changed to protected.
```

```
(config)> ip http security-level public ssl
Http::Manager: Security level set to public SSL.
```

History

Version	Description
2.08	The ip http security-level command has been introduced.
3.00	Parameter ssl was added.

3.55 ip http ssl acme debug

Description

Enable debug for the [ACME](#) service. By default, setting is disabled.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> ip http ssl acme debug
```

```
(config)> no ip http ssl acme debug
```

Example

```
(config)> ip http ssl acme debug
Acme::Client: Enabled debug.
```

```
(config)> no ip http ssl acme debug
Acme::Client: Disabled debug.
```

History

Version	Description
4.03	The ip http ssl acme debug command has been introduced.

3.56 ip http ssl acme ecdsa

Description

Enable support for certificates based on ECDSA cryptography.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input No

Synopsis

```
(config)> ip http ssl acme ecdsa
```

```
(config)> no ip http ssl acme ecdsa
```

Example

```
(config)> ip http ssl acme ecdsa
Acme::Client: Enabled ECDSA chain.
```

```
(config)> no ip http ssl acme ecdsa
Acme::Client: Disabled ECDSA chain.
```

History	Version	Description
	3.09	The ip http ssl acme ecdsa command has been introduced.

3.57 ip http ssl acme get

Description Generate and sign SSL certificate for the specified domain name (by default, KeenDNS). Access from the Internet should be granted.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(config)> ip http ssl acme get [ <domain> ]
```

Arguments	Argument	Value	Description
	domain	<i>String</i>	KeenDNS domain name.

Example

```
(config)> ip http ssl acme get mytest.keenetic.pro
Acme::Client: Obtaining certificate for domain ►
"mytest.keenetic.pro" is started.
```

History	Version	Description
	2.11	The ip http ssl acme get command has been introduced.

3.58 ip http ssl acme revoke

Description Revoke and remove SSL certificate for the specified domain name (KeenDNS, by default).

Prefix no No

Change settings No

Multiple input No

Synopsis `(config)> ip http ssl acme revoke <domain>`

Arguments

Argument	Value	Description
domain	<i>String</i>	KeenDNS domain name.

Example

```
(config)> ip http ssl acme revoke mytest.keenetic.pro
Acme::Client: Revoking certificate for domain ►
"mytest.keenetic.pro" is started.
```

History

Version	Description
2.11	The ip http ssl acme revoke command has been introduced.

3.59 ip http ssl acme list

Description Show a list of free Let`s Encrypt certificates in the system.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config)> ip http ssl acme list`

Example

```
(config)> ip http ssl acme list
certificate:
    domain: cc6b5a71a7644903b51a5454.keenetic.io
    should-be-renewed: no
    is-expired: no
    issue-time: 2018-06-20T09:16:30.000Z
    expiration-time: 2018-09-17T09:16:30.000Z

certificate:
    domain: mytest.keenetic.pro
    should-be-renewed: no
    is-expired: no
    issue-time: 2018-06-28T16:36:56.000Z
    expiration-time: 2018-09-25T16:36:56.000Z
```

History

Version	Description
2.11	The ip http ssl acme list command has been introduced.

3.60 ip http ssl enable

Description Enable HTTP SSL server. By default, the server is disabled.

Command with **no** prefix disables SSL server.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config)> ip http ssl enable
(config)> no ip http ssl enable
```

Example

```
(config)> ip http ssl enable
Http::Manager: Enabled SSL service.

(config)> no ip http ssl enable
Http::Manager: Disabled SSL service.
```

History

Version	Description
2.07	The ip http ssl enable command has been introduced.

3.61 ip http ssl port

Description Assign HTTPS port for Web interface of Carrier. By default, 443 value is used.

Command with **no** prefix resets HTTPS port to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config)> ip http ssl port <port>
(config)> no ip http ssl port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	New HTTPS port.

Example

```
(config)> ip http ssl port 4343
Http::Manager: SSL port changed to 4343.
```

```
(config)> no ip http ssl port
Http::Manager: SSL port reset to 443.
```

History

Version	Description
4.00	The ip http ssl port command has been introduced.

3.62 ip http ssl redirect

Description

Enable automatic redirection on domains with SSL certificate. By default, the redirection is enabled.

Command with **no** prefix disables redirection.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config)> ip http ssl redirect
```

```
(config)> no ip http ssl redirect
```

Example

```
(config)> ip http ssl redirect
Http::Manager: Redirect to SSL is enabled.
```

```
(config)> no ip http ssl redirect
Http::Manager: Redirect to SSL is disabled.
```

History

Version	Description
2.11	The ip http ssl redirect command has been introduced.

3.63 ip http webdav

Description

Access to a group of commands to configure [WebDAV](#) server.

Prefix no

No

Change settings

No

Multiple input

No

Interface type

IP

Group entry (config-webdav)

Synopsis (config)> **ip http webdav**

Example (config)> **ip http webdav**
Core::Configurator: Done.
(config-webdav)>

History	Version	Description
	3.04	The ip http webdav command has been introduced.

3.63.1 ip http webdav enable

Description Enable [WebDAV](#) server. By default, the server is disabled.
Command with **no** prefix disables [WebDAV](#) server.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis (config-webdav)> **enable**
(config-webdav)> **no enable**

Example (config-webdav)> **enable**
WebDav::Server: Enabled.
(config-webdav)> **no enable**
WebDav::Server: Disabled.

History	Version	Description
	3.04	The ip http webdav enable command has been introduced.

3.63.2 ip http webdav permissive

Description Access to the [WebDAV](#) server for all users without authentication.
Command with **no** prefix denies anonymous access.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-webdav)> permissive
(config-webdav)> no permissive
```

Example

```
(config-webdav)> permissive
WebDav::Server: Enabled permissive mode.

(config-webdav)> no permissive
WebDav::Server: Disabled permissive mode.
```

History

Version	Description
3.04	The ip http webdav permissive command has been introduced.

3.63.3 ip http webdav security-level

Description Set the security level for remote access to the [WebDAV](#) server. By default, private value is set.

Prefix no No

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-webdav)> security-level (public | private)
```

Arguments

Argument	Value	Description
public	<i>Keyword</i>	Access to the WebDAV server is allowed for public, private and protected interfaces.
private	<i>Keyword</i>	Access to the WebDAV server is allowed for private interfaces.

Example

```
(config-webdav)> security-level public
Http::Manager: WebDAV security level set to public.
```

History

Version	Description
3.04	The ip http webdav security-level command has been introduced.

3.64 ip http x-frame-options

Description Set X-Frame-Options header value for web server (nginx) in Home network segment.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config)> ip http x-frame-options <x-frame-options>
(config)> no ip http x-frame-options <x-frame-options>
```

Arguments

Argument	Value	Description
x-frame-options	<i>String</i>	The X-Frame-Option value.

Example

```
(config)> ip http x-frame-options DENY
Http::Manager: Set X-Frame-Options to "DENY".
```

```
(config)> no ip http x-frame-options DENY
Http::Manager: Disabled X-Frame-Options header.
```

History

Version	Description
3.05	The ip http x-frame-options command has been introduced.

3.65 ip name-server

Description Configure DNS server IP addresses. Addresses saved in this fashion are called static as opposite to dynamic — as registered by *PPP* or *DHCP* services.

Active, that addressed being used are the ones that have been registered most recently as compared to the others. Usually, the system uses the addresses which were obtained by several recent successfully connected *PPP* or *DHCP* services. If none of the services registers *DNS* addresses, static settings will be active. However, if after registering dynamic addresses the static settings are changed by the user, they become active until the new dynamic addresses are registered.

ip name-server command can be entered multiple times if several DNS-server addresses need to be setup. Moreover, each entered address can be associated with one or more domain names for working with specific areas, such as local names in the corporate network.

Command with **no** prefix removes the specified DNS server address from the static and the active lists if the command is furnished with arguments. If you use no arguments, the entire list of static addresses will be removed.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP

Synopsis

```
(config)> ip name-server <address> [ : <port> ] [ <domain> ] [ on <interface> ] ]
```

```
(config)> no ip name-server [ <address> [ : <port> ] ] [ <domain> ] [ on <interface> ] ]
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	Name server address.
port	<i>Integer</i>	Name server port.
domain	<i>String</i>	Domain for which the server will be used. In resolving names the DNS-proxy first selects the address of the server with name best matching the requested domain. If the domain is not specified, the server will be used for all requests. Use "" as default domain. The maximum number of domains per one DNS entry is 16.
interface	<i>Interface</i>	Interface name to configure.

Example

```
(config)> ip name-server 8.8.8.8 "" on ISP
Dns::InterfaceSpecific: Name server 8.8.8.8 added, domain ►
(default), interface ISP.
```

```
(config)> no ip name-server
Dns::Manager: Static name server list cleared.
```

History

Version	Description
2.00	The ip name-server command has been introduced.
2.14	Argument port was added.

3.66 ip nat

Description Enable translation of “local” addresses of network *network* or network behind the interface *interface*. For example, command `ip nat Home` means that

all packets from the network Home, passing through the router will undergo IP spoofing.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP

Synopsis

```
(config)> ip nat ( <interface> | <address> <mask> )
```

```
(config)> no ip nat ( <interface> | <address> <mask> )
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Source interface name (full name or an alias).
address	<i>IP address</i>	Together with mask <i>mask</i> sets the range of source IP addresses to be translated.
mask	<i>IP-mask</i>	Mask of a translation range. There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).

Example

```
(config)> ip nat Home  
Network::Nat: A NAT rule added.
```

```
(config)> no ip nat Home  
Network::Nat: A NAT rule removed.
```

History

Version	Description
2.00	The ip nat command has been introduced.

3.67 ip nat full-cone

Description Enable mode *Full Cone NAT*. By default, the mode is disabled.

Command with **no** prefix disables the mode.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config)> ip nat full-cone
```

```
(config)> no ip nat full-cone
```

Example

```
(config)> ip nat full-cone
Network::Nat: Full cone mode enabled.
```

```
(config)> no ip nat full-cone
Network::Nat: Full cone mode disabled.
```

History

Version	Description
3.01	The ip nat full-cone command has been introduced.

3.68 ip nat oc

Description

Enable translation for [OpenConnect](#) clients.

Note: Command is available if the [OpenConnect](#) VPN server component is installed.

Command with **no** prefix removes the rule.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config)> ip nat oc
```

```
(config)> no ip nat oc
```

Example

```
(config)> ip nat oc
OcServer::Nat: OpenConnect VPN NAT enabled.
```

```
(config)> no ip nat oc
OcServer::Nat: OpenConnect VPN NAT disabled.
```

History

Version	Description
4.02	The ip nat oc command has been introduced.

3.69 ip nat restricted-cone

Description

Enable mode [Restricted NAT](#). By default, the mode is disabled.

Command with **no** prefix disables the mode.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config)> ip nat restricted-cone
```

```
(config)> no ip nat restricted-cone
```

Example

```
(config)> ip nat restricted-cone
Network::Nat: Restricted cone mode enabled.
```

```
(config)> no ip nat restricted-cone
Network::Nat: Restricted cone mode disabled.
```

History

Version	Description
3.01	The ip nat restricted-cone command has been introduced.

3.70 ip nat sstp

Description Enable translation for [SSTP](#) clients.

Note: Command is available if the [SSTP](#) VPN server component is installed.

Command with **no** prefix removes the rule.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config)> ip nat sstp
```

```
(config)> no ip nat sstp
```

Example

```
(config)> ip nat sstp
SstpServer::Nat: SSTP VPN NAT enabled.
```

```
(config)> no ip nat sstp
SstpServer::Nat: SSTP VPN NAT disabled.
```

History

Version	Description
2.12	The ip nat sstp command has been introduced.

3.71 ip nat vpn

Description

Enable translation for PPTP clients.

Note: Command is available if the PPTP VPN server component is installed.

Command with **no** prefix removes the rule.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config)> ip nat vpn
```

```
(config)> no ip nat vpn
```

Example

```
(config)> ip nat vpn
VpnServer::Nat: PPTP VPN NAT enabled.
```

```
(config)> no ip nat vpn
VpnServer::Nat: PPTP VPN NAT disabled.
```

History

Version	Description
2.04	The ip nat vpn command has been introduced.

3.72 ip policy

Description

Access to a group of commands to configure IP Policy — a default route selection rules for hosts and home network segments. If the IP Policy profile is not found, the command tries to create it. You can enter up to 64 profiles.

Command with **no** prefix removes the defined IP Policy profile from the list.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Group entry

(config-policy)

Synopsis

```
(config)> ip policy <name>
```

```
(config)> no ip policy <name>
```

Arguments

Argument	Value	Description
name	<i>Policy</i>	IP Policy name. Latin letters, numbers, hyphens and underscores are acceptable. Not more than 32 characters.

Example

```
(config)> ip policy Policy0  
Network::PolicyTable: Created policy "Policy0".
```

```
(config)> no ip policy Policy0  
Network::PolicyTable: Removed policy "Policy0".
```

History

Version	Description
2.12	The ip policy command has been introduced.

3.72.1 ip policy description

Description

Assign an arbitrary description to the specified IP Policy profile.

Command with **no** prefix removes description.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-policy)> description <description>
```

```
(config-policy)> no description
```

Arguments

Argument	Value	Description
description	<i>String</i>	An arbitrary description of the IP Policy. Latin letters, numbers, hyphens and underscores are acceptable. Not more than 256 characters.

Example

```
(config-policy)> description PolicyOne  
Network::PolicyTable: "Policy0": updated description.
```

```
(config-policy)> no description  
Network::PolicyTable: "Policy0": updated description.
```

History

Version	Description
2.12	The ip policy description command has been introduced.

3.72.2 ip policy ipv6 route

Description

Add a static route to the routing table to describe a rule of IPv6-packets transmission through a particular gateway or network interface for IP Policy specific.

Command with **no** prefix removes the IPv6 route with the specified parameters.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

IP

Synopsis

```
(config-policy)> ipv6 route <prefix> (<interface> [<gateway>] | <gateway>
) [auto] [ <metric> ] [reject]
```

```
(config-policy)> no ipv6 route <prefix> (<interface> [<gateway>] | <gateway>
)
```

Arguments

Argument	Value	Description
prefix	<i>Prefix</i>	IPv6 prefix.
interface	<i>Interface</i>	Full interface name or an alias.
gateway	<i>IP address</i>	IP address of the router in a directly connected network.
auto	<i>Keyword</i>	Allows you to apply the route when specified gateway becomes available.
metric	<i>Integer</i>	Route metrics. Ignored in the current implementation.
reject	<i>Keyword</i>	Enable route to use only the selected interface for routing the traffic to the specified destination. If the specified interface is not active, the traffic is not sent via other possible routes. This option works only when using the auto option and cannot be applied to the default route.

Example

```
(config-policy)> ipv6 route 2002:c100:aeb5::/48 ISP auto reject
Network::Ip6::RoutingTable: Added static route: ►
2002:c100:aeb5:100::/56 via ISP.
```

```
(config-policy)> ipv6 route 2002:c100:aeb5::/48 ISP
Network::Ip6::RoutingTable: Added static route: ►
2002:c100:aeb5::/48 via ISP.
```

```
(config-policy)> no ipv6 route 2002:c100:aeb5::/48 ISP
Network::Ip6::RoutingTable: Deleted static route: ►
2002:c100:aeb5::/48 via ISP.
```

History

Version	Description
4.03	The ip policy ipv6 route command has been introduced.

3.72.3 ip policy multipath

Description Enable the function of simultaneous use of WAN connections in the balancing mode.

Command with **no** prefix disables the function.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-policy)> multipath
(config-policy)> no multipath
```

Example

```
(config-policy)> multipath
Network::PolicyTable: "Policy0": enable multipath.
```

```
(config-policy)> no multipath
Network::PolicyTable: "Policy0": disable multipath.
```

History

Version	Description
2.14	The ip policy multipath command has been introduced.

3.72.4 ip policy permit

Description Permit IP Policy for the global interface. If single IP Policy is permitted for multiple interfaces, you can specify a priority for each of them.

Command with **no** prefix denies the IP Policy for specified interface. If you use no arguments, IP Policy will be denied for the entire list of interfaces.

Prefix no Yes

Change settings Yes**Multiple input** Yes**Interface type** IP

Synopsis

```
(config-policy)> permit global <interface> [ order <order> ]
```

```
(config-policy)> no permit [ global <interface> ]
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias.
order	<i>Integer</i>	The priority of global interface to which the IP Policy is permitted. Can take values in the range from 1 to 65534, but not more than the number of global interfaces.

Example

```
(config-policy)> permit global L2TP0 order 0
Network::PolicyTable: "Policy0": set permission to use L2TP0.
```

```
(config-policy)> no permit global L2TP0
Network::PolicyTable: "Policy0": set no permission to use L2TP0.
```

History

Version	Description
2.12	The ip policy permit command has been introduced.

3.72.5 ip policy permit auto

Description Permit new connections for the IP Policy automatically. By default, the feature is disabled.

Command with **no** prefix removes auto permission.

Prefix no Yes**Change settings** Yes**Multiple input** No**Interface type** IP

Synopsis

```
(config-policy)> permit auto
```

```
(config-policy)> no permit auto
```

Example

```
(config-policy)> permit auto
Network::PolicyTable: "Policy0": set auto permission.
```

```
(config-policy)> no permit auto
Network::PolicyTable: "Policy0": set auto permission.
```

History

Version	Description
2.12	The ip policy permit auto command has been introduced.

3.72.6 ip policy rate-limit input

Description Add the input rate-limiting parameters to global interfaces of the IP Policy.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-policy)> rate-limit <interface> input (<rate> | auto)
(config-policy)> no rate-limit <interface> input
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	The name of a global IP interface to rate-limit its traffic for a group of policy assignees.
rate	<i>Integer</i>	The ingress rate limit in kbps. Can take values in the range from 64 to 1000000.
auto	<i>Keyword</i>	Auto-ingress mode.

Example

```
(config-policy)> rate-limit WifiMaster1/WifiStation0 input auto
Network::PolicyTable: "Policy0": set input rate limit to "auto".
```

```
(config-policy)> rate-limit WifiMaster1/WifiStation0 input 100000
Network::PolicyTable: "Policy0": set input rate limit to "100000" ► kbps.
```

```
(config-policy)> rate-limit WifiMaster1/WifiStation0 no input
Network::PolicyTable: "Policy0": reset input rate limit.
```

History

Version	Description
3.05	The ip policy rate-limit input command has been introduced.

3.72.7 ip policy rate-limit output

Description Add output rate-limiting parameters to global interfaces of the IP Policy.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-policy)> rate-limit <interface> output ( <rate> | auto)
```

```
(config-policy)> no rate-limit <interface> output
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	The name of a global IP interface to rate-limit its traffic for a group of policy assignees.
rate	<i>Integer</i>	The ingress rate limit in kbps. Can take values in the range from 64 to 1000000.
auto	<i>Keyword</i>	Auto-ingress mode.

Example

```
(config-policy)> rate-limit ISP output auto  
Network::PolicyTable: "Policy0": set output rate limit to "auto".
```

```
(config-policy)> rate-limit ISP output 1000  
Network::PolicyTable: "Policy0": set output rate limit to "1000" ►  
kbps.
```

```
(config-policy)> rate-limit ISP no output  
Network::PolicyTable: "Policy0": reset ouput rate limit.
```

History

Version	Description
3.05	The ip policy rate-limit output command has been introduced.
3.08	The auto argument has been added.

3.72.8 ip policy route

Description Add a static route to the routing table to describe a rule of IP-packets transmission through a particular gateway or network interface for IP Policy specific.

Command with **no** prefix removes the route with the specified parameters.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP

Synopsis

```
(config-policy)> route ( <network> <mask> | <host> ) ( <gateway> [ <network>
] | <interface> ) [ auto ] [ <metric> ] [ reject ]

(config-policy)> no route ( <network> <mask> | <host> ) [ <interface> | <gateway>
] [ <metric> ]
```

Arguments

Argument	Value	Description
network	<i>IP address</i>	IP address of the destination network.
mask	<i>IP-mask</i>	Mask of the destination network. There are two ways to enter the mask: in the canonical form (for example, 255.255.255.0) and in the form of prefix bit length (for example, /24).
host	<i>IP address</i>	IP address of the destination node.
interface	<i>Interface</i>	Interface full name or an alias. Specified as the direction of the packet transferring, if the interface has a point-to-point channel connected that requires no additional addressing within the channel. If priority interface ip global is set on the interface, the route is added to the system table only if there is no other higher priority route with the same address.
gateway	<i>IP address</i>	IP address of the router in a directly connected network. Can be specified along with the interface name, if it is required to specify interface ip global priority. If no interface is specified, the systemd determines it automatically based on the current IP settings.
auto	<i>Keyword</i>	Allows you to apply the route when specified gateway becomes available.
metric	<i>Integer</i>	Route metrics. Ignored in the current implementation.
reject	<i>Keyword</i>	Enable route to use only the selected interface for routing the traffic to the specified destination. If the specified interface is not active, the traffic is not sent via other possible routes. This option works only when using the auto option and cannot be applied to the default route.

Example

```
(config-policy)> route 123.123.123.123 Wireguard1 auto reject
Network::RoutingTable: Added static route: 123.123.123.123/32 ►
via Wireguard1.
```

```
(config-policy)> no route 123.123.123.123 Wireguard1
Network::RoutingTable: Deleted static route: 123.123.123.123/32 ►
via Wireguard1.
```

```
(config-policy)> no route 123.123.123.123
Network::RoutingTable: Deleted static route: 123.123.123.123/32 ►
via Wireguard1.
```

History

Version	Description
4.03	The ip policy route command has been introduced.

3.72.9 ip policy standalone

Description

Enable "standalone" mode, which static routes through interfaces with the "global" property are not automatically copied from the main settings to the selected IP policy profile.

Description

Command with **no** prefix disables the function.

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-policy)> standalone
```

```
(config-policy)> no standalone
```

Example

```
(config-policy)> standalone
Network::PolicyTable: "Policy0": enable standalone mode.
```

```
(config-policy)> no standalone
Network::PolicyTable: "Policy0": disable standalone mode.
```

History

Version	Description
4.02	The ip policy standalone command has been introduced.

3.73 ip route

Description

Add a static route to the routing table to describe a rule of IP-packets transmission through a particular gateway or network interface.

As the destination network, one can specify default keyword. In this case, a default route will be created.

Command with **no** prefix removes the route with the specified parameters.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP

Synopsis

```
(config)> ip route ( <network> <mask> | <host> | default ) ( <gateway>
[ <interface> | <interface> ] [auto] [metric] [reject]
```

```
(config)> no ip route ( <network> <mask> | <host> | default ) [ <gateway> |
<interface> ] [metric]
```

Arguments

Argument	Value	Description
network	<i>IP address</i>	IP address of the destination network.
mask	<i>IP-mask</i>	Mask of the destination network. There are two ways to enter the mask: in the canonical form (for example, 255.255.255.0) and in the form of prefix bit length (for example, /24).
host	<i>IP address</i>	IP address of the destination node.
default	<i>Keyword</i>	Helps specify default routes.
interface	<i>Interface</i>	Interface full name or an alias. Specified as the direction of the packet transferring, if the interface has a point-to-point channel connected that requires no additional addressing within the channel. If priority interface ip global is set on the interface, the route is added to the system table only if there is no other higher priority route with the same address.
gateway	<i>IP address</i>	IP address of the router in a directly connected network. Can be specified along with the interface name, if it is required to specify interface ip global priority. If no interface is specified, the systemd determines it automatically based on the current IP settings.
auto	<i>Keyword</i>	Allows you to apply the route when specified gateway becomes available.
metric	<i>Integer</i>	Route metrics. Ignored in the current implementation.
reject	<i>Keyword</i>	Enable route to use only the selected interface for routing the traffic to the specified

Argument	Value	Description
		destination. If the specified interface is not active, the traffic is not sent via other possible routes. This option works only when using the auto option and cannot be applied to the default route.

Example

```
(config)> ip route default Home
Network::RoutingTable: Added static route: 0.0.0.0/0 via Home.
```

```
(config)> ip route 123.123.123.123 Wireguard1 auto reject
Network::RoutingTable: Added static route: 123.123.123.123/32 ►
via Wireguard1.
```

```
(config)> no ip route 123.123.123.123 Wireguard1
Network::RoutingTable: Deleted static route: 123.123.123.123/32 ►
via Wireguard1.
```

```
(config)> no ip route default
Network::RoutingTable: No such route: 0.0.0.0/0.
```

History

Version	Description
2.00	The ip route command has been introduced.
3.08	The reject option was added.

3.74 ip search-domain

Description Assign search domain to resolve hostnames that are not fully qualified.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> ip search-domain <domain>
```

```
(config)> no ip search-domain
```

Arguments

Argument	Value	Description
domain	<i>String</i>	The domain name to assign.

Example

```
(config)> ip search-domain my.example
```

```
(config)> no ip search-domain my.example
```

History

Version	Description
2.00	The ip search-domain command has been introduced.

3.75 ip sip alg direct-media

Description

Replace IP address in Owner field of SDP. This feature is used to not configure port forwarding separately for VoIP traffic. By default, the setting is disabled.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> ip sip alg direct-media
```

```
(config)> no ip sip alg direct-media
```

Example

```
(config)> ip sip alg direct-media
Sip::Alg: Direct media enabled.
```

```
(config)> no ip sip alg direct-media
Sip::Alg: Direct media disabled.
```

History

Version	Description
2.11	The ip sip alg direct-media command has been introduced.

3.76 ip sip alg port

Description

Specify a port number for SIP messages other than the default port. By default, port number is 5060.

Command with **no** prefix resets port to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> ip sip alg port <port>
```

```
(config)> no ip sip alg port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	The port number.

Example

```
(config)> ip sip alg port 7090
Sip::Alg: Port set to 7090.
```

```
(config)> no ip sip alg port
Sip::Alg: Port reset to default.
```

History

Version	Description
2.12	The ip sip alg port command has been introduced.

3.77 ip ssh

Description

Access to a group of commands to manage SSH-server.

Prefix no

No

Change settings

No

Multiple input

No

Interface type

IP

Group entry

(config-ssh)

Synopsis

```
(config)> ip ssh
```

Example

```
(config)> ip ssh
(config-ssh)>
```

History

Version	Description
2.12	The ip ssh command has been introduced.

3.77.1 ip ssh cipher

Description

Set a symmetric key cipher for SSH session.

Command with **no** prefix removes the specified cipher.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

IP

Synopsis**(config-ssh)> cipher <cipher>****(config-ssh)> no cipher <cipher>****Arguments**

Argument	Value	Description
cipher	chacha20-poly1305@openssh.com	An encryption algorithm ChaCha20-Poly1305.
	aes128-ctr	An encryption algorithm AES128-CTR.
	aes256-ctr	An encryption algorithm AES1256-CTR.
	aes128-gcm@openssh.com	An encryption algorithm AES128-GCM.
	aes256-gcm@openssh.com	An encryption algorithm AES256-GCM.

Example

```
(config-ssh)> cipher chacha20-poly1305@openssh.com
Ssh::Manager: Added cipher "chacha20-poly1305@openssh.com".
```

```
(config-ssh)> no cipher chacha20-poly1305@openssh.com
Ssh::Manager: Use default ciphers.
```

History

Version	Description
3.04	The ip ssh cipher command has been introduced.

Version	Description
3.05	New encryption algorithms aes128-gcm@openssh.com, aes256-gcm@openssh.com were added.

3.77.2 ip ssh keygen

Description

Regeneration of a given type key.

Prefix no

No

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis**(config-ssh)> keygen <keygen>****Arguments**

Argument	Value	Description
keygen	default	Automatic generation of a new open key RSA2048 + ECDSA-NISTP521.

Argument	Value	Description
	rsa-1024	Automatic generation of a new open RSA-key with a length of 1024 bits.
	rsa-2048	Automatic generation of a new open RSA-key with a length of 2048 bits.
	rsa-4096	Automatic generation of a new open RSA-key with a length of 4096 bits.
	ecdsa-nistp256	Automatic generation of a new open ECDSA-key with a length of 256 bits.
	ecdsa-nistp384	Automatic generation of a new open ECDSA-key with a length of 384 bits.
	ecdsa-nistp521	Automatic generation of a new open ECDSA-key with a length of 521 bits.
	ed25519	Automatic generation of a new open ED25519 key with a length of 256 bits.

Example

```
(config-ssh)> keygen default
Ssh::Manager: Key generation is in progress...
```

History

Version	Description
2.12	The ip ssh keygen command has been introduced.

3.77.3 ip ssh lockout-policy

Description

Set SSH bruteforce detection parameters for public interfaces. By default, feature is enabled. If you use 0 as an argument, all bruteforce detection parameters will be reset to default.

Command with **no** prefix disables bruteforce detection.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-ssh)> lockout-policy <threshold> [ <duration> [
<observation-window> ] ]
```

```
(config-ssh)> no lockout-policy
```

Arguments

Argument	Value	Description
threshold	<i>Integer</i>	The number of failed attempts to log in. By default, 5 value is used. Can take values in the range from 4 to 20.
duration	<i>Integer</i>	An authorization ban duration for the specified IP in minutes. By default, 15 value is used. Can take values in the range from 1 to 60.
observation-window	<i>Integer</i>	Duration of suspicious activity observation in minutes. By default, 3 value is used. Can take values in the range from 1 to 10.

Example

```
(config-ssh)> lockout-policy 10 30 2
Ssh::Manager: Bruteforce detection is reconfigured.
```

```
(config-ssh)> no lockout-policy
Ssh::Manager: Bruteforce detection is disabled.
```

```
(config-ssh)> lockout-policy 0
Ssh::Manager: Bruteforce detection reset to default.
```

History

Version	Description
2.12	The ip ssh lockout-policy command has been introduced.

3.77.4 ip ssh port

Description Specify port number for SSH connection. By default, 22 port number is used.

Command with **no** prefix resets port number to default.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-ssh)> port <number>
```

```
(config-ssh)> no port
```

Arguments

Argument	Value	Description
number	<i>Integer</i>	Port number. Can take values in the range from 1 to 65535 inclusively.

Example

```
(config-ssh)> port 2626
Ssh::Manager: Port changed to 2626.
```

```
(config-ssh)> no port
Ssh::Manager: Port reset to 22.
```

History

Version	Description
2.12	The ip ssh port command has been introduced.

3.77.5 ip ssh security-level

Description

Set SSH security level. By default, private value is set.

Prefix no

No

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-ssh)> security-level (public | private | protected)
```

Arguments

Argument	Value	Description
public	<i>Keyword</i>	Access to the SSH server is allowed for public, private and protected interfaces.
private	<i>Keyword</i>	Access to the SSH server is allowed for private interfaces.
protected	<i>Keyword</i>	Access to the SSH server is allowed for private and protected interfaces.

Example

```
(config-ssh)> security-level protected
Ssh::Manager: Security level changed to protected.
```

History

Version	Description
2.12	The ip ssh security-level command has been introduced.

3.77.6 ip ssh session timeout

Description

Set the lifetime of inactive session for SSH connection. By default, 300 value is used, i.e. the function of activity tracking within a session is disabled.

Command with **no** prefix resets timeout to default.

Prefix no

Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-ssh)> session timeout <timeout>
(config-ssh)> no session timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	The lifetime of inactive session. Can take values in the range from 5 to $2^{32}-1$ seconds inclusively.

Example

```
(config-ssh)> session timeout 123456
Ssh::Manager: A session timeout value set to 123456 seconds.
```

```
(config-ssh)> no session timeout
Ssh::Manager: A session timeout reset.
```

History

Version	Description
3.03	The ip ssh session timeout command has been introduced.

3.77.7 ip ssh sftp

Description Access to a group of commands to manage [SFTP](#) server.

Prefix no No

Change settings No

Multiple input No

Interface type IP

Group entry (config-sftp)

Synopsis

```
(config)> ip ssh sftp
```

Example

```
(config)> ip ssh sftp
(config-sftp)>
```

History

Version	Description
3.04	The ip ssh sftp command has been introduced.

3.77.7.1 ip ssh sftp enable

Description Enable *SFTP* server.
Command with **no** prefix disables the server.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-sftp)> enable
(config-sftp)> no enable
```

Example

```
(config-sftp)> enable
Ssh::Manager: Enabled SFTP server.

(config-sftp)> no enable
Ssh::Manager: Disabled SFTP server.
```

History

Version	Description
3.04	The ip ssh sftp enable command has been introduced.

3.77.7.2 ip ssh sftp permissive

Description Access to the *SFTP* server for all users without authentication.
Command with **no** prefix denies access.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-sftp)> permissive
(config-sftp)> no permissive
```

Example

```
(config-sftp)> permissive
(config-sftp)> no permissive
```

History	Version	Description
	3.04	The ip ssh sftp permissive command has been introduced.

3.77.7.3 ip ssh sftp root

Description Set root directory on *SFTP* server by default.
Command with **no** prefix resets root directory.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-sftp)> root (<directory> | <directory> )
(config-sftp)> no root
```

Arguments	Argument	Value	Description
	directory	<i>String</i>	Path to default root directory.

Example

```
(config-sftp)> root files_ssd:/
Sftp::Server: A default root directory set to "files_ssd:/".
```

```
(config-sftp)> no root files_ssd:/
Sftp::Server: A default root directory reset.
```

History	Version	Description
	3.04	The ip ssh sftp root command has been introduced.

3.78 ip static

Description Define translation rule for global and local IP addresses. If *interface* or *network* corresponds to the interface with *security level* public, then the destination address translation (DNAT) will occur. If *to-address* corresponds to the interface with *security level* public, then source address translation (SNAT) will occur. TCP/UDP port number is always treated as the destination port.

If *network* corresponds to a single address and this address is equal to *to-address*, then this rule will prohibit the translation of the specified address, which could have been done based on the specified rules **ip nat**.

ip static rules have higher priority than the **ip nat** rules.

When using the translation rule, the router opens access to the specified port, so there is no need to make additional configuration of the firewall.

Command with **no** prefix enables the rule or removes the rule.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP

Synopsis

```
(config)> ip static [ <protocol> ] ( <interface> | ( <address> <mask> ) )
    ( <port> through <end-port> ( <to-address> | <to-host> |
    <to-interface> ) |
    <port> ( <to-address> | <to-host> | <to-interface> ) [ <to-port> ] |
    <to-address> | <to-host> | <to-interface> )
```

```
(config)> no ip static [ <protocol> ] ( <interface> | ( <address> <mask> ) )
    ( <port> through <end-port> ( <to-address> | <to-host> |
    <to-interface> ) |
    <port> ( <to-address> | <to-host> | <to-interface> ) [ <to-port> ] |
    <to-address> | <to-host> | <to-interface> )]
```

Arguments

Argument	Value	Description
protocol	tcp	TCP protocol.
	udp	UDP protocol.
	icmp	ICMP protocol.
	tcpudp	TCP and UDP protocols.
	gre	GRE protocol.
	ipip	IP in IP protocol.
interface	<i>Interface</i>	Input interface name (full name or alias).
comment	<i>String</i>	User's notes with symbol ! before them.
address	<i>IP address</i>	Along with mask <i>mask</i> sets the range of destination IP addresses that are to be translated.
mask	<i>IP-mask</i>	Translation range mask. There are two ways to enter the mask: the canonical form (for example, 255 . 255 . 255 . 0) and the form of prefix bit length (for example, /24).
port	<i>Integer</i>	TCP/UDP port number for which a translation request comes. If not specified, all incoming requests will be translated.
end-port	<i>Integer</i>	The end of the range of ports.

Argument	Value	Description
to-address	<i>IP address</i>	The destination address after translation.
to-host	<i>MAC address</i>	The destination MAC address after translation. Only MAC address from known hosts are accepted. If the known host is deleted, then the associated rules will be deleted too.
to-port	<i>Integer</i>	TCP/UDP port number after translation. If not specified, the destination port remains the same.
to-interface	<i>Interface</i>	Interface name after translation.

Example

Let there be a router between the “local” network 172.16.1.0/24 ([security level](#) private) and “global” network 10.0.0.0/16 ([security level](#) public). It is required that all requests coming to the “global” interface of this router on port 80 to be broadcast to the “local” server with the address 172.16.1.33. The sequence of commands to implement the required schema might look like this:

```
(config)> interface Home ip address 192.168.1.1/24
Network::Interface::Ip: "Bridge0": IP address is 192.168.1.1/24.
```

```
(config)> ip static tcp ISP 80 172.16.1.33 80
Network::StaticNat: Static NAT rule has been added.
```

```
(config)> ip static tcp ISP 21 00:0e:c6:a1:22:11 !test
Network::StaticNat: Static NAT rule is already there.
```

```
(config)> ip static disable
Network::StaticNat: Static NAT disable unchanged.
```

```
(config)> no ip static disable
Network::StaticNat: Static NAT rule enabled.
```

```
(config)> no ip static
Network::StaticNat: Static NAT rules have been removed.
```

History

Version	Description
2.00	The ip static command has been introduced.
2.06	The to-host argument has been added.

3.79 ip static rule

Description

Disable IP address translation rule or set rule operation time by schedule.

Command with **no** prefix enables the rule or removes the rule schedule.

Prefix no

Yes

Change settings Yes**Multiple input** Yes**Interface type** IP

Synopsis

```
(config)> ip static rule <index> (disable | schedule <schedule>)
```

```
(config)> no ip static rule <index> (disable | schedule)
```

Arguments

Argument	Value	Description
index	<i>Integer</i>	The translation rule number.
disable	<i>Keyword</i>	Disable the translation rule.
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(config)> ip static rule 0 schedule test_schedule
Network::StaticNat: Static NAT rule schedule applied.
```

```
(config)> ip static rule 0 disable
Network::StaticNat: Static NAT rule disabled.
```

```
(config)> no ip static rule 0 disable
Network::StaticNat: Static NAT rule enabled.
```

```
(config)> no ip static rule 0 schedule
Network::StaticNat: Static NAT rule schedule removed.
```

History

Version	Description
2.08	The ip static rule command has been introduced.

3.80 ip telnet

Description Access to a group of commands to manage Telnet server.**Prefix no** No**Change settings** No**Multiple input** No**Interface type** IP**Group entry** (config-telnet)

Synopsis

```
(config)> ip telnet
```

Example

```
(config)> ip telnet
(config-telnet)>
```

History

Version	Description
2.08	The ip telnet command has been introduced.

3.80.1 ip telnet lockout-policy

Description Set Telnet bruteforce detection parameters for public interfaces. By default, feature is enabled. If you use 0 as an argument, all bruteforce detection parameters will be reset to default.

Command with **no** prefix disables bruteforce detection.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config-telnet)> lockout-policy <threshold> [ <duration> [
<observation-window> ]]
```

```
(cconfig-telnet)> no lockout-policy
```

Arguments

Argument	Value	Description
threshold	<i>Integer</i>	The number of failed attempts to log in. By default, 5 value is used. Can take values in the range from 4 to 20.
duration	<i>Integer</i>	An authorization ban duration for the specified IP in minutes. By default, 15 value is used. Can take values in the range from 1 to 60.
observation-window	<i>Integer</i>	Duration of suspicious activity observation in minutes. By default, 3 value is used. Can take values in the range from 1 to 10.

Example

```
(config-telnet)> lockout-policy 10 30 2
Telnet::Server: Bruteforce detection is reconfigured.
```

```
(config-telnet)> no lockout-policy
Telnet::Server: Bruteforce detection is disabled.
```

```
(config-telnet)> lockout-policy 0
Telnet::Server: Bruteforce detection is enabled.
```

History

Version	Description
2.08	The ip telnet lockout-policy command has been introduced.

3.80.2 ip telnet port

Description

Specify port number for telnet connection. By default, 23 port number is used.

Command with **no** prefix resets port number to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-telnet)> port <number>
```

```
(config-telnet)> no port
```

Arguments

Argument	Value	Description
number	<i>Integer</i>	Port number. Can take values in the range from 1 to 65535 inclusively.

Example

```
(config-telnet)> port 2525  
Telnet::Server: Port unchanged.
```

```
(config-telnet)> no port  
Telnet::Server: Port unchanged.
```

History

Version	Description
2.08	The ip telnet port command has been introduced.

3.80.3 ip telnet security-level

Description

Set Telnet security level. By default, private value is set.

Prefix no

No

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-telnet)> security-level (public | private | protected)
```

Arguments

Argument	Value	Description
public	<i>Keyword</i>	Access to the Telnet server is allowed for public, private and protected interfaces.
private	<i>Keyword</i>	Access to the Telnet server is allowed for private interfaces.
protected	<i>Keyword</i>	Access to the Telnet server is allowed for private and protected interfaces.

Example

```
(config-telnet)> security-level protected  
Telnet::Manager: Security level changed to protected.
```

History

Version	Description
2.08	The ip telnet security-level command has been introduced.

3.80.4 ip telnet session max-count

Description

Set the maximal number of simultaneous sessions for telnet connection. By default, 4 value is used.

Command with **no** prefix resets count to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-telnet)> session max-count <count>
```

```
(config-telnet)> no session max-count
```

Arguments

Argument	Value	Description
count	<i>Integer</i>	The maximal number of simultaneous sessions. Can take values in the range from 1 to 4 inclusively.

Example

```
(config-telnet)> session max-count 4  
Telnet::Server: The maximum session count set to 4.
```

```
(config-telnet)> no session max-count  
Telnet::Server: The maximum session count reset to 4.
```

History

Version	Description
2.08	The ip telnet session max-count command has been introduced.

3.80.5 ip telnet session timeout

Description

Set the lifetime of inactive session for telnet connection. By default, 300 value is used which means that the function of activity tracking within a session is disabled.

Command with **no** prefix resets timeout to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config-telnet)> session timeout <timeout>
```

```
(config-telnet)> no session timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	The lifetime of inactive session. Can take values in the range from 5 to $2^{32}-1$ seconds inclusively.

Example

```
(config-telnet)> session timeout 600
Telnet::Server: A session timeout value set to 600 seconds.
```

```
(config-telnet)> no session timeout
Telnet::Server: A session timeout reset.
```

History

Version	Description
2.08	The ip telnet session timeout command has been introduced.

3.81 ip traffic-shape host

Description

Set the limit of data rate on a specified known host in both directions. By default speed is not limited.

Command with **no** prefix removes the setting for specified host. If you use no arguments, the entire list of rate limits for all hosts will be removed.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP

Synopsis

```
(config)> ip traffic-shape host <mac> rate <rate> [asymmetric
<upstream-rate>] [schedule <schedule>]
```

```
(config)> no ip traffic-shape host [<mac>]
```

Arguments

Argument	Value	Description
mac	<i>MAC address</i>	MAC address of the known host.
rate	<i>Integer</i>	Value of data download rate in Kbps. Limit could be in the range from 64 Kbps to 1 Gbps.
upstream-rate	<i>Integer</i>	Data upload rate in Kbps. Value can be in the range from 64 Kbps to 1 Gbps.
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(config)> ip traffic-shape host a8:1e:82:81:f1:21 rate 80
TrafficControl::Manager: "a8:1e:82:81:f1:21" host rate limited ►
to DL 80 / UL 80 Kbits/sec.
```

```
(config)> ip traffic-shape host a8:1e:82:81:f1:21 rate 80 ►
asymmetric 64
TrafficControl::Manager: "a8:1e:82:81:f1:21" host rate limited ►
to DL 80 / UL 64 Kbits/sec..
```

```
(config)> ip traffic-shape host a8:1e:82:81:f1:21 rate 80 ►
asymmetric 64 schedule Update
TrafficControl::Manager: "a8:1e:82:81:f1:21" host rate limited ►
to DL 80 / UL 64 Kbits/sec (controlled by schedule Update).
```

```
(config)> no ip traffic-shape host a8:1e:82:81:f1:21
TrafficControl::Manager: Rate limit removed for host ►
"a8:1e:82:81:f1:21".
```

```
(config)> no ip traffic-shape host a8:1e:82:81:f1:21
TrafficControl::Manager: Rate limit removed for host ►
"a8:1e:82:81:f1:21".
```

```
(config)> no ip traffic-shape host
TrafficControl::Manager: Rate limits for all hosts removed.
```

History

Version	Description
2.05	The ip traffic-shape host command has been introduced.

2.08	The schedule argument was added.
3.04	The upstream-rate argument was added.

3.82 ip traffic-shape unknown-host

Description Set the data rate limitation for unregistered devices in both directions. By default, speed is unlimited.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type IP

Synopsis

```
(config)> ip traffic-shape unknown-host rate <rate> [ asymmetric
<upstream-rate> ]
(config)> no ip traffic-shape unknown-host rate
```

Arguments

Argument	Value	Description
rate	<i>Integer</i>	The data download rate in Kbps. Value could be in the range from 64 Kbps to 1 Gbps.
upstream-rate	<i>Integer</i>	Data upload rate in Kbps. Value can be in the range from 64 Kbps to 1 Gbps.

Example

```
(config)> ip traffic-shape unknown-host rate 80
TrafficControl::Manager: Rate limit for unknown hosts set to 80 ►
Kbits/sec.
```

```
(config)> ip traffic-shape unknown-host rate 80 asymmetric 64
TrafficControl::Manager: Rate limit for unknown hosts set to ►
80/64 Kbits/sec.
```

```
(config)> no ip traffic-shape unknown-host rate
TrafficControl::Manager: Rate limit for unknown hosts removed.
```

History

Version	Description
2.09	The ip traffic-shape unknown-host command has been introduced.
3.04	The upstream-rate argument was added.

3.83 ipv6 local-prefix

Description Configure a local (ULA) prefix. Argument can be a literal prefix or **default**, which generates a persistent unique prefix automatically.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> ipv6 local-prefix (default | <prefix>)
```

```
(config)> no ipv6 local-prefix [default | <prefix>]
```

Arguments

Argument	Value	Description
default	<i>Keyword</i>	Generate persistent unique prefix.
prefix	<i>Prefix</i>	Local ULA prefix. Must be a valid prefix in the block fd00::/8 with a prefix length no longer than 48.

Example

```
(config)> ipv6 local-prefix default  
Ip6::Prefixes: Default ULA prefix enabled.
```

```
(config)> ipv6 local-prefix fd01:db8:43::/48  
Ip6::Prefixes: Added static prefix: fd01:db8:43::/48.
```

```
(config)> no ipv6 local-prefix default  
Ip6::Prefixes: Default ULA prefix disabled.
```

```
(config)> no ipv6 local-prefix fd01:db8:43::/48  
Ip6::Prefixes: Deleted static prefix: fd01:db8:43::/48.
```

History

Version	Description
2.00	The ipv6 local-prefix command has been introduced.

3.84 ipv6 name-server

Description Configure DNS server IPv6-addresses. Addresses saved in this fashion are called static as opposite to dynamic — as registered by *PPP* or *DHCP* services.

ipv6 name-server command can be entered multiple times if several DNS server addresses need to be setup.

Command with **no** prefix removes the specified DNS server address from the static and the active lists if the command is furnished with arguments, or clears the list of static addresses if the command has no arguments.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config)> ipv6 name-server <address> [ <domain> [ on <interface> ] ]
```

```
(config)> no ipv6 name-server [ <address> [ <domain> [ on <interface> ] ] ]
```

Arguments

Argument	Value	Description
address	<i>IPv6-address</i>	Name server address.
domain	<i>String</i>	Domain for which the server will be used. In resolving names the DNS-proxy first selects the address of the server with name best matching the requested domain. If the domain is not specified, the server will be used for all requests. Use "" as default domain.
interface	<i>Interface</i>	Interface name to configure.

Example

```
(config)> ipv6 name-server 2001:4860:4860::8888  
Dns::Manager: Name server 2001:4860:4860::8888 added, domain ►  
(default).
```

```
(config)> ipv6 name-server 123::456 "" on ISP  
Dns::InterfaceSpecific: "GigabitEthernet1": name server 123::456 ►  
added, domain (default).
```

```
(config)> ipv6 name-server 2001:4860:4860::8888 google.com  
Dns::Manager: Name server 2001:4860:4860::8888 added, domain ►  
google.com.
```

```
(config)> no ipv6 name-server 2001:4860:4860::8888  
Dns::Manager: Name server 2001:4860:4860::8888, domain (default) ►  
deleted.
```

```
(config)> no ipv6 name-server 123::456 "" on ISP  
Dns::InterfaceSpecific: Name server 123::456 deleted, domain ►  
(default).
```

```
(config)> no ipv6 name-server 2001:4860:4860::8888 google.com  
Dns::Manager: Name server 2001:4860:4860::8888, domain google.com ►  
deleted.
```

```
(config)> no ipv6 name-server  
Dns::Manager: Static name server list cleared.
```

History

Version	Description
2.00	The ipv6 name-server command has been introduced.
4.00	The interface argument was added.

3.85 ipv6 pass

Description

Enable Pass Through mode on the router for IPv6-packets. By default, the feature is disabled.

Command with **no** prefix disables the function.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> ipv6 pass through <wan-iface> <lan-iface>
```

```
(config)> no ipv6 pass
```

Arguments

Argument	Value	Description
wan-iface	<i>Interface</i>	Full WAN-interface name or an alias.
lan-iface	<i>Interface</i>	Full LAN-interface name or an alias.

Example

```
(config)> ipv6 pass through ISP Home  
Ip6::Pass: Configured pass from "GigabitEthernet1" to "Bridge0".
```

```
(config)> no ipv6 pass  
Ip6::Pass: Disabled.
```

History

Version	Description
2.06	The ipv6 pass command has been introduced.

3.86 ipv6 route

Description

Add a static route to the routing table to describe a rule of IPv6-packets transmission through a particular gateway or network interface.

As the destination network keyword `default` can be specified. In this case, a default route will be created.

Command with **no** prefix removes the route with the specified parameters.

Prefix no

Yes

Change settings Yes**Multiple input** Yes

Synopsis

```
(config)> ipv6 route ( <prefix> | default ) ( <interface> [<gateway>] | <gateway> )
```

```
(config)> no ipv6 route ( <prefix> | default ) ( <interface> [<gateway>] | <gateway> )
```

Arguments

Argument	Value	Description
prefix	<i>Prefix</i>	IPv6 prefix.
default	<i>Keyword</i>	Default prefix.
interface	<i>Interface</i>	Full interface name or an alias.
gateway	<i>IP address</i>	IP address of the router in a directly connected network.

Example

```
(config)> ipv6 route 2002:c100:aeb5::/48 ISP  
route added
```

```
(config)> no ipv6 route 2002:c100:aeb5::/48 ISP  
route erased
```

```
(config)> ipv6 route 2002:c100:aeb5:100::/56 2002:c100:aeb5::33  
route added
```

```
(config)> no ipv6 route 2002:c100:aeb5:100::/56 2002:c100:aeb5::33  
route erased
```

History

Version	Description
2.00	The ipv6 route command has been introduced.
2.11	gateway argument has been added.

3.87 ipv6 static

Description Define the rule to allow incoming connection to a specified port of a registered home network device.

Command with **no** prefix removes the rule.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config)> ipv6 static <protocol> ( <interface> <mac> | <mac> ) [ <port> [
through <end-port> ] ]
```

```
(config)> no ipv6 static [ <protocol> ( <interface> <mac> | <mac> ) [ <port> [
through <end-port> ] ] ]
```

Arguments

Argument	Value	Description
protocol	tcp	TCP protocol.
	udp	UDP protocol.
	tcpudp	TCP and UDP protocol.
	icmp6	ICMPv6 protocol.
interface	<i>Interface</i>	Input interface name (full name or an alias).
mac	<i>MAC address</i>	MAC address of host.
port	<i>Integer</i>	TCP/UDP port number for which incoming request comes.
end-port	<i>Integer</i>	The end of the range of ports.

Example

```
(config)> ipv6 static tcp ISP 04:d1:c3:24:bc:19 81
Ip6::Firewall: Static rule added.
```

```
(config)> ipv6 static tcp 04:d1:c3:24:bc:19 8080
Ip6::Firewall: Static rule added.
```

```
(config)> ipv6 static tcp ISP 04:d1:c3:24:bc:19 8080 through 8081
Ip6::Firewall: Static rule added.
```

```
(config)> ipv6 static icmpv6 ISP 04:d1:c3:24:bc:19
Ip6::Firewall: Static rule added.
```

```
(config)> no ipv6 static icmpv6 ISP 04:d1:c3:24:bc:19
Ip6::Firewall: Static rule removed.
```

```
(config)> no ipv6 static
Ip6::Firewall: Static rules cleared.
```

History

Version	Description
2.12	The ipv6 static command has been introduced.
4.00	The icmpv6 argument was added.

3.88 ipv6 subnet

Description

Access to a group of commands to configure a LAN IPv6 segment. If the segment is not found, the command tries to create it.

Prefix no

Yes

Change settings Yes**Multiple input** Yes**Group entry** (config-subnet)

Synopsis

```
(config)> ipv6 subnet <name>
```

```
(config)> no ipv6 subnet [ <name> ]
```

Arguments

Argument	Value	Description
name	<i>String</i>	Subnet name or an alias.

Example

```
(config)> ipv6 subnet Default
(config-subnet)>
```

History

Version	Description
2.00	The ipv6 subnet command has been introduced.

3.88.1 ipv6 subnet bind

Description Bind the subnet to an interface.Command with **no** prefix cancels binding.**Prefix no** Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config-subnet)> bind <bind>
```

```
(config-subnet)> no bind
```

Arguments

Argument	Value	Description
bind	<i>Interface</i>	Full interface name or an alias.

Example

```
(config-subnet)> bind WifiMaster0/AccessPoint1
Ip6::Subnets: Interface "WifiMaster0/AccessPoint1" bound to ►
subnet "Default".
```

```
(config-subnet)> no bind
Ip6::Subnets: Interface unbound from subnet "Default".
```

History	Version	Description
	2.00	The ipv6 subnet bind command has been introduced.

3.88.2 ipv6 subnet dns-server

Description Configure DNS server for subnets.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-subnet)> dns-server ( <address1> [ <address2> ] | disable )
(config-subnet)> no dns-server
```

Arguments	Argument	Value	Description
	address1	<i>IPv6-address</i>	Address of primary name DNS server.
	address2	<i>IPv6-address</i>	Address of secondary name DNS server.
	disable	<i>Keyword</i>	Disable DNS server.

Example

```
(config-subnet)> dns-server 2606:4700:4700::1111
Network::Ip6::Subnets: Set name server 2606:4700:4700::1111 for ►
subnet "Default".

(config-subnet)> dns-server 2606:4700:4700::1111 ►
2606:4700:4700::1001
Network::Ip6::Subnets: Set name servers 2606:4700:4700::1111 ►
2606:4700:4700::1001 for subnet "Default".

(config-subnet)> dns-server disable
Network::Ip6::Subnets: Disable name servers for subnet "Default".

(config-subnet)> no dns-server
Network::Ip6::Subnets: Cleared name servers for subnet "Default".
```

History	Version	Description
	4.03	The ipv6 subnet dns-server command has been introduced.

3.88.3 ipv6 subnet mode

Description Select the address configuration mode for hosts in the subnet. Exclusive options are **dhcp** and **slaac**. The former will enable a local DHCPv6 server for the purposes of address assignment, and the latter will enable SLAAC (Stateless Address Autoconfiguration).

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-subnet)> mode <mode>
(config-subnet)> no mode
```

Arguments

Argument	Value	Description
mode	slaac	Enable SLAAC (stateless autoconfiguration).
	dhcp	Enable DHCPv6 server (stateful autoconfiguration).

Example

```
(config-subnet)> mode dhcp
Ip6::Subnets: Subnet "Default" enabled as DHCP.
```

```
(config-subnet)> no mode
Ip6::Subnets: Subnet "Default" disabled.
```

History

Version	Description
2.00	The ipv6 subnet mode command has been introduced.

3.88.4 ipv6 subnet number

Description Assign the subnet ID, which will determine the advertised prefix for the segment. Must be unique across subnets.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(config-subnet)> number <number>
```

Arguments

Argument	Value	Description
number	<i>Integer</i>	Unique subnet ID.

Example (config-subnet)> **number 2**
Ip6::Subnets: Number 2 assigned to subnet "Default".

History	Version	Description
	2.00	The ipv6 subnet number command has been introduced.

3.88.5 ipv6 subnet prefix delegate

Description Set delegated prefix length.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis (config-subnet)> **prefix delegate** *<delegate>*
(config-subnet)> **no prefix delegate**

Arguments	Argument	Value	Description
	delegate	<i>Integer</i>	The value must be less than prefix length.

Example (config-subnet)> **prefix delegate 63**
Network::Ip6::Subnets: Delegate length is /63 assigned to subnet ► "Default".
(config-subnet)> **no prefix delegate**
Network::Ip6::Subnets: Prefix delegation disabled for subnet ► "Default".

History	Version	Description
	4.00	The ipv6 subnet prefix delegate command has been introduced.

3.88.6 ipv6 subnet prefix length

Description Set subnet prefix length. By default, /64 prefix length is set.
Command with **no** prefix resets to default.

Prefix no Yes

Change settings Yes

Multiple input No**Synopsis**`(config-subnet)> prefix length <length>``(config-subnet)> no prefix length`**Arguments**

Argument	Value	Description
length	<i>Integer</i>	Prefix length can take values in the range from /32 to /64.

Example

```
(config-subnet)> prefix length 62
Network::Ip6::Subnets: Length is /62 assigned to subnet "Default".
```

```
(config-subnet)> no prefix length
Network::Ip6::Subnets: Length reset to default for subnet ►
"Default".
```

History

Version	Description
4.00	The ipv6 subnet prefix length command has been introduced.

3.89 isolate-private

Description

Prohibit data transfer between any interfaces with [security level](#) private. Enabled by default.

Command with **no** prefix cancels the command, allowing data transfer between private interfaces.

Prefix no Yes**Change settings** Yes**Multiple input** No**Synopsis**`(config)> isolate-private``(config)> no isolate-private`**Example**

```
(config)> isolate-private
Netfilter::Manager: Private networks isolated.
```

```
(config)> no isolate-private
Netfilter::Manager: Private networks not isolated.
```

History

Version	Description
2.00	The isolate-private command has been introduced.

3.90 kabinet

Description Access to a group of commands to configure KAbiNET authenticator parameters.

Command with **no** prefix resets all parameters to default.

Prefix no Yes

Change settings Yes

Multiple input No

Group entry (kabinet)

Synopsis

```
(config)> kabinet
(config)> no kabinet
```

Example

```
(config)> kabinet
(kabinet)>

(config)> no kabinet
Kabinet::Authenticator: A configuration reset.
```

History

Version	Description
2.02	The kabinet command has been introduced.

3.90.1 kabinet access-level

Description Set an access level for KAbiNET authenticator. By default, access level internet is used.

Command with **no** prefix resets level to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(kabinet)> access-level <level>
(kabinet)> no access-level
```

Arguments

Argument	Value	Description
level	lan	Access level value.
	internet	

Example

```
(kabinet)> access-level lan
Kabinet::Authenticator: An access level set to "lan".
```

```
(kabinet)> access-level internet
Kabinet::Authenticator: An access level set to "internet".
```

```
(kabinet)> no access-level
Kabinet::Authenticator: An access level reset to "internet".
```

History

Version	Description
2.02	The kabinet access-level command has been introduced.

3.90.2 kabinet interface

Description

Bind KABINET authenticator to the specified interface.

Command with **no** prefix unbinds interface.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(kabinet)> interface <interface>
```

```
(kabinet)> no interface
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(kabinet)> interface [Tab]
```

```
Usage template:
  interface {interface}
```

Choose:

```
    GigabitEthernet1
    ISP
    WifiMaster0/AccessPoint2
    WifiMaster1/AccessPoint1
    WifiMaster0/AccessPoint3
    WifiMaster0/AccessPoint0
    AccessPoint
```

```
(kabinet)> interface ISP
Kabinet::Authenticator: Bound to GigabitEthernet1.
```



```
(kabinet)> no interface
Kabinet::Authenticator: Interface binding cleared.
```

History

Version	Description
2.02	The kabinet interface command has been introduced.

3.90.3 kabinet password

Description Set a password for KABINET authenticator. By default, password is not set.

Command with **no** prefix clears the password.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(kabinet)> password <password>
(kabinet)> no password
```

Arguments

Argument	Value	Description
password	<i>String</i>	The password for authentication.

Example

```
(kabinet)> password 123456789
Kabinet::Authenticator: A password set.
```

```
(kabinet)> no password
Kabinet::Authenticator: A password cleared.
```

History

Version	Description
2.02	The kabinet password command has been introduced.

3.90.4 kabinet port

Description Set the server port for KABINET authenticator. By default, values 8314 or 8899 are used.

Command with **no** prefix resets port to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(kabinet)> port <port>
```

```
(kabinet)> no port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	The port number.

Example

```
(kabinet)> port 12345
Kabinet::Authenticator: A server port set.
```

```
(kabinet)> no port
Kabinet::Authenticator: A server port reset.
```

History

Version	Description
2.14	The kabinet port command has been introduced.

3.90.5 kabinet protocol-version

Description

Set version of KABINET authenticator protocol. By default, protocol version 2 is used.

Command with **no** prefix resets protocol to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(kabinet)> protocol-version <version>
```

```
(kabinet)> no protocol-version
```

Arguments

Argument	Value	Description
version	<i>String</i>	Version of protocol.

Example

```
(kabinet)> protocol-version 1
Kabinet::Authenticator: A protocol version set to "1".
```

```
(kabinet)> no protocol-version
Kabinet::Authenticator: A protocol version reset to "2".
```

History

Version	Description
2.02	The kabinet protocol-version command has been introduced.

3.90.6 kabinet server

Description Set an IP address of KABiNET authentication server. By default, IP 10.0.0.1 is used.

Command with **no** prefix resets the address.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(kabinet)> server <address>
```

```
(kabinet)> no server
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	Authentication server address.

Example

```
(kabinet)> server 77.222.111.1
Kabinet::Authenticator: A server address set.
```

```
(kabinet)> no server
Kabinet::Authenticator: A server address reset.
```

History

Version	Description
2.02	The kabinet server command has been introduced.

3.91 known host

Description Set known host.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config)> known host <name> <mac>
```

```
(config)> no known host [ mac ]
```

Arguments

Argument	Value	Description
name	<i>String</i>	Arbitrary host name.
mac	<i>MAC address</i>	MAC address.

Example

```
(config)> known host MY 00:0e:c6:a2:22:a1
Core::KnownHosts: New host "MY" has been created.
```

```
(config)> no known host 00:0e:c6:a2:22:a1
Core::KnownHosts: Host 00:0e:c6:a1:26:a8 has been removed.
```

History

Version	Description
2.00	The known host command has been introduced.

3.92 mdns

Description

Access to a group of commands to manage *mDNS* service.

Prefix no

No

Change settings

No

Multiple input

No

Group entry

(config-mdns)

Synopsis

```
(config)> mdns
```

Example

```
(config)> mdns
Core::Configurator: Done.
(config-mdns)>
```

History

Version	Description
3.07	The mdns command has been introduced.

3.92.1 mdns reflector disable

Description

Forcibly disable transparency mode between home network segments, irrespective of segment isolation (see the [interface security-level](#) command).

Command with **no** prefix disables the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-mdns)> reflector disable
```

```
(config-mdns)> no reflector disable
```

Example

```
(config-mdns)>reflector disable
Mdns::Manager: Reflector disabled.

(config-mdns)>no reflector disable
Mdns::Manager: Reflector enabled.
```

History	Version	Description
	3.07	The mdns reflector disable command has been introduced.

3.92.2 mdns reflector enforce

Description Forcibly enable transparency mode between home network segments, irrespective of segment isolation (see the [interface security-level](#) command).

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-mdns)> reflector enforce
(config-mdns)> no reflector enforce
```

Example

```
(config-mdns)>reflector enforce
Mdns::Manager: Reflector enforced.

(config-mdns)>no reflector enforce
Mdns::Manager: Reflector unenforced.
```

History	Version	Description
	3.07	The mdns reflector enforce command has been introduced.

3.93 mws acquire

Description Attach new device to [MWS](#).

Command with **no** prefix stops the acquisition.

Prefix no Yes

Change settings No

Multiple input No

Synopsis

```
(config)> mws acquire <candidate> [eula-accept] [dpn-accept]
[no-update]
```

```
(config)> no mws acquire <candidate>
```

Arguments

Argument	Value	Description
candidate	<i>String</i>	Device ID — MAC address or CID.
eula-accept	<i>Keyword</i>	Send eula accept command.
dpn-accept	<i>Keyword</i>	Send Device Privacy Notice accept.
no-update	<i>Keyword</i>	Acquisition without firmware update confirmation.

Example

```
(config)> mws acquire ab1409a2-0f87-11e8-8f23-3d5f5921b253 ►
eula-accept
Mws::Controller: Candidate "ab1409a2-0f87-11e8-8f23-3d5f5921b253" ►
acquire started.
```

```
(config)> mws acquire 7207838e-af7d-11e6-8029-25463bd03811 ►
eula-accept dpn-accept no-update
Mws::Controller: Candidate "7207838e-af7d-11e6-8029-25463bd03811" ►
acquire started.
```

```
(config)> no mws acquire 60:31:97:3f:36:00
Mws::Controller: Candidate "60:31:97:3f:36:00" acquire stopped.
```

History

Version	Description
2.15	The mws acquire command has been introduced.

3.94 mws auto-ap-shutdown

Description

Enable automatic shutdown of the Wi-Fi System Extenders when communication with the Controller is inaccessible. By default, the setting is disabled.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> mws auto-ap-shutdown
```

```
(config)> no mws auto-ap-shutdown
```

Example

```
(config)> mws auto-ap-shutdown
Mws::Controller: Automatic access points shutdown enabled.
```

```
(config)> no mws auto-ap-shutdown
Mws::Controller: Automatic access points shutdown disabled.
```

History

Version	Description
3.08	The mws auto-ap-shutdown command has been introduced.

3.95 mws backhaul shutdown

Description

Disable hidden wireless backhaul access points for [MWS](#) service. By default, the setting is enabled.

Command with **no** prefix enables hidden wireless backhaul access points.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> mws backhaul shutdown
```

```
(config)> no mws backhaul shutdown
```

Example

```
(config)> mws backhaul shutdown
Mws::Controller: Backhaul disabled.
```

```
(config)> no mws backhaul shutdown
Mws::Controller: Backhaul enabled.
```

History

Version	Description
3.04	The mws backhaul shutdown command has been introduced.

3.96 mws log stp

Description

Enable STP logging for the interface. Allows you to track sent and received BPDU packets.

Command with **no** prefix disables logging for specified interface. If you use no argument, the entire list of STP logging will be removed.

Prefix no

Yes

Change settings

No

Multiple input Yes**Synopsis**

```
(config)> mws log stp <interface>
(config)> no mws log stp [ <interface> ]
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(config)> mws log stp Bridge0
Network::Interface::Rtx::WifiController: Enabled STP logging for ►
"Bridge0".
```

```
(config)> no mws log stp Bridge0
Network::Interface::Rtx::WifiController: Disabled STP logging ►
for "Bridge0".
```

```
(config)> no mws log stp
Network::Interface::Rtx::WifiController: Disabled all STP logging.
```

History

Version	Description
3.06	The mws log stp command has been introduced.

3.97 mws member

Description Command with **no** prefix removes [MWS](#) member. If you use no argument, the entire list of members will be cleared.

Prefix no Yes**Change settings** No**Multiple input** No**Synopsis**

```
(config)> no mws member [ member ]
```

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.

Example

```
(config)> mws no member 2937a388-0d00-11e7-8029-7119319f930e
Mws::MemberList: Member 2937a388-0d00-11e7-8029-7119319f930e ►
pending factory reset.
```


History

Version	Description
2.15	The mws member command has been introduced.

3.98 mws member debug

Description

Enable [MWS](#) member debug. By default, setting is disabled.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> mws member <member> debug
```

```
(config)> no mws member <member> debug
```

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.

Example

```
(config)> mws member 60:31:97:3c:11:12 debug
Mws::MemberList: Member "60:31:97:3c:11:12" ►
(7207838e-af7d-11e6-8011-25463bd03812) RCI debug enabled.
```

```
(config)> no mws member 60:31:97:3c:11:12 debug
Mws::MemberList: Member "60:31:97:3c:11:12" ►
(7207838e-af7d-11e6-8011-25463bd03812) RCI debug disabled.
```

History

Version	Description
3.05	The mws member debug command has been introduced.

3.99 mws member dpn-accept

Description

Accept [DPN](#) for [MWS](#) member.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(config)> mws member <member> dpn-accept
```

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.

Example

```
(config)> mws member 7207838e-af7d-11e6-8029-25463bd03828 ▶
dpn-accept
Mws::Controller: Candidate "ab1409a2-0f87-11e8-8f23-3d5f5921b253" ▶
acquire started.
```

History

Version	Description
3.05	The mws member dpn-accept command has been introduced.

3.100 mws member port access

Description

Assign the LAN port of the Extender to the specified network segment.

By default, the LAN port is assigned to Home segment (Bridge0).

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> mws member <member> port <port> access <interface>
```

```
(config)> mws member <member> port <port> no access [ <interface> ]
```

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.
port	<i>Integer</i>	The LAN port number.
interface	<i>Interface</i>	Full name of the network segment (Bridge interface).

Example

```
(config)> mws member cb7038f8-c49b-11ea-8f23-e123fd1a0e3e port ▶
3 access Bridge2
Mws::Controller::Manager: "cb7038f8-c49b-11ea-8f23-e123fd1a0e3e": ▶
port "3" has been attached to "Bridge2".
```

```
(config)> mws member 11:ff:22:43:5c:bf port 1 access Bridge2
Mws::Controller::Manager: "11:ff:22:43:5c:bf": port "1" has been ▶
attached to "Bridge2".
```

```
(config)> mws member 11:ff:22:43:5c:bf port 1 no access Bridge2
Mws::Controller::Manager: "11:ff:22:43:5c:bf": port "1" has been ►
attached to "Bridge0".
```

History

Version	Description
4.02	The mws member port access command has been introduced.

3.101 mws member port disable

Description

Disable the LAN port of the Extender.

Command with **no** prefix enables the LAN port.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> mws member <member> port <port> disable
```

```
(config)> mws member <member> port <port> no disable
```

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.
port	<i>Integer</i>	The LAN port number.

Example

```
(config)> mws member 21:f3:20:43:5c:bf port 3 disable
Mws::Controller::Manager: "21:f3:20:43:5c:bf": port "3" has been ►
set to "down".
```

```
(config)> mws member 21:f3:20:43:5c:bf port 3 no disable
Mws::Controller::Manager: "21:f3:20:43:5c:bf": port "3" has been ►
set to "up".
```

History

Version	Description
4.02	The mws member port disable command has been introduced.

3.102 mws member reboot

Description

Reboot the [MWS](#) member. The process of rebooting extenders should be displayed in the [show mws member](#) command output.

Prefix no No**Change settings** No**Multiple input** No**Synopsis** `(config)> mws member <member> reboot [ <interval> ]`**Arguments**

Argument	Value	Description
member	<i>String</i>	Device ID — MAC-address or CID.
interval	<i>Integer</i>	Timeout for reboot in seconds. Can take values in the range from 0 to 60 inclusively). If not specified, the reboot will be executed immediately.

Example

```
(config)> mws member 7207838e-af7d-11e6-8029-25463bd03828 reboot ►
10
Mws::MemberList: Member "50:ff:21:1a:b1:f2" ►
(7207838e-af7d-11e6-8029-25463bd03828) pending reboot.
```

History

Version	Description
3.08	The mws member reboot command has been introduced.

3.103 mws member update channel

Description Configure the update channel for the Extenders. By default, value `stable` is used.Command with **no** prefix resets setting to default.**Prefix no** Yes**Change settings** Yes**Multiple input** No**Synopsis** `(config)> mws member <member> update channel <channel>``(config)> no mws member <member> update channel`**Arguments**

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.
channel	<i>String</i>	Update channel name. The list of channels is available in the command components auto-update channel .

Example

```
(config)> mws member 8a33ff16-2c3c-11ef-9111-7bd989541127 update ►
channel preview
Mws::Controller::MemberList: "50:11:20:22:33:1b" update channel ►
is "preview".
```

```
(config)> no mws member 8a33ff16-2c3c-11ef-9396-7bd989541127 ►
update channel
Mws::Controller::MemberList: "50:ff:20:c5:97:1b" reset an update ►
channel to default.
```

History

Version	Description
4.02	The mws member update channel command has been introduced.

3.104 mws member update check

Description Check for an update for the [MWS](#) member.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(config)> mws member <member> update check
```

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.

Example

```
(config)> mws member 21:ff:22:32:18:af update check
Mws::Controller::Updater: "21:ff:22:32:18:af": checking for an ►
update.
```

History

Version	Description
4.00	The mws member update check command has been introduced.

3.105 mws member update start

Description Start the [MWS](#) member update.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(config)> mws member <member> update start
```

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.

Example

```
(config)> mws member 21:ff:22:32:18:af update start
Mws::Controller::Updater: "21:ff:22:32:18:af": pending update, ►
"(auto)" sandbox.
```

History

Version	Description
4.00	The mws member update start command has been introduced.

3.106 mws member update stop

Description

Stop the [MWS](#) member update.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(config)> mws member <member> update stop
```

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.

Example

```
(config)> mws member 21:ff:22:32:18:af update stop
Mws::Controller::Updater: "21:ff:22:32:18:af": update stopped.
```

History

Version	Description
4.00	The mws member update stop command has been introduced.

3.107 mws reboot

Description

Reboot the whole [MWS](#).

Prefix no

No

Change settings

No

Multiple input No

Synopsis (config)> **mws reboot**

Example (config)> **mws reboot**
Mws::Controller: Pending reboot Modular Wi-Fi System in 10 ► seconds.

History	Version	Description
	3.08	The mws reboot command has been introduced.

3.108 mws revisit

Description Re-read status of potential *MWS* member.

Prefix no Yes

Change settings No

Multiple input No

Synopsis (config)> **mws revisit** <candidate>
(config)> **no mws revisit** <candidate>

Arguments	Argument	Value	Description
	candidate	String	Device ID — MAC address or CID.

Example (config)> **mws revisit 50:ff:20:08:71:62**
Mws::Controller: Candidate "50:ff:20:08:71:62" revisit started.
(config)> **mws no revisit 50:ff:20:08:71:62**
Mws::Controller: Candidate "50:ff:20:08:71:62" revisit stopped.

History	Version	Description
	2.15	The mws revisit command has been introduced.

3.109 mws stp priority

Description Set the STP Bridge Priority. By default, the value 32768 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings No

Multiple input Yes

Synopsis

```
(config)> mws stp priority <priority>
(config)> no mws stp priority
```

Arguments

Argument	Value	Description
priority	0	The STP Bridge Priority value.
	4096	
	8192	
	12288	
	16384	
	20480	
	24576	
	28672	
	32768	
	36864	
	40960	
	45056	
	49152	
	53248	

Example

```
(config)> mws stp priority 4096
Mws::Controller::Manager: Applied STP priority 4096.

(config)> no mws stp priority
Mws::Controller::Manager: STP priority reset to default (32768).
```

History

Version	Description
4.01	The mws stp priority command has been introduced.

3.110 mws update start

Description Start the *MWS* update.

If there are updates for members, then the members are updated sequentially. Then, if there is an update for the controller, then the controller update is started. If there are no updates, then nothing happens.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config)> mws update start [controller | members]`

Arguments

Argument	Value	Description
controller	<i>Keyword</i>	Update the controller, don't try to update members. If members update is running, the controller will be updated after them.
members	<i>Keyword</i>	Update a members, don't try to update the controller.

Example

```
(config)> mws update start
Mws::Controller::Manager: Updating MWS.
```

```
(config)> mws update start controller
Mws::Controller::Manager: Updating controller.
```

```
(config)> mws update stop
Mws::Controller::Manager: Updating members.
```

History

Version	Description
4.00	The mws update start command has been introduced.

3.111 mws update stop

Description Stop the [MWS](#) update.

Prefix no No

Change settings No

Multiple input No

Synopsis `(config)> mws update stop`

Example

```
(config)> mws update stop
Mws::Controller::Manager: Update stopped.
```

History

Version	Description
4.00	The mws update stop command has been introduced.

3.112 mws zone

Description Limit the connection area of the client device within the specified [MWS](#) members.

Command with **no** prefix removes the specified setting. If you use no arguments, the entire list of restrictions will be removed.

Prefix no Yes

Change settings No

Multiple input Yes

Synopsis

```
(config)> mws zone <mac> <cid>
```

```
(config)> no mws zone [ <mac> <cid> ]
```

Arguments

Argument	Value	Description
mac	MAC address	MAC address of client device. It must be listed as a known host.
cid	CID	Identifier of MWS member.

Example

```
(config)> mws zone 11:22:33:ec:58:e2 ►
12298f60-d886-11e7-9396-176971eeb8d6
Mws::Controller: Added zone 11:22:33:ec:58:e2 ►
12298f60-d886-11e7-9396-176971eeb8d6.
```

```
(config)> no mws zone 11:22:33:ec:58:e2 ►
12298f60-d886-11e7-9396-176971eeb8d6
Mws::Controller: Deleted zone 11:22:33:ec:58:e2 ►
12298f60-d886-11e7-9396-176971eeb8d6.
```

```
(config)> no mws zone
Mws::Controller: Cleared all zones.
```

History

Version	Description
3.06	The mws zone command has been introduced.

3.113 nextdns

Description Access to a group of commands to configure [NextDNS](#) profiles.

Prefix no No

Change settings No

Multiple input No

Group entry (nextdns)

Synopsis (config)> **nextdns**

Example (config)> **nextdns**
Core::Configurator: Done.
(nextdns)>

History

Version	Description
3.08	The netxdns command has been introduced.

3.113.1 nextdns assign

Description Assign profile of protection to the host. By default System profile is used for all hosts and local network segments.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis (nextdns)> **assign** <host> <token> | **interface** <iface> <token>
(nextdns)> **no assign** [<host> | **interface** <iface>]

Arguments

Argument	Value	Description
host	<i>MAC address</i>	MAC address to assign.
token	<i>Integer</i>	Authentication token (ID).
iface	<i>Interface</i>	Full interface name or an alias.

Example (nextdns)> **assign 11:24:c4:54:bc:59 1f2a36**
NextDns::Client: Reassociated host "11:24:c4:54:bc:59" with ►
profile "1f2a36".

(nextdns)> **assign interface Home 1f2a36**
NextDns::Client: Associated interface "Home" with profile ►
"1f2a36".

(nextdns)> **no assign 11:24:c4:54:bc:59**
NextDns::Client: Removed profile for host "11:24:c4:54:bc:59".

(nextdns)> **no assign Bridge0**
NextDns::Client: Removed profile for interface "Bridge0".

History

Version	Description
3.08	The nextdns assign command has been introduced.

3.113.2 nextdns authenticate

Description Specify login for *NextDNS* account.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(nextdns)> authenticate <login> <password> [ <pin> ]
```

```
(nextdns)> no authenticate
```

Arguments

Argument	Value	Description
login	<i>String</i>	Login to <i>NextDNS</i> account.
password	<i>String</i>	Password to <i>NextDNS</i> account.
pin	<i>String</i>	Pin to <i>NextDNS</i> account.

Example

```
(nextdns)> authenticate account@gmail.com 123456789 1234
NextDns::Client: Authenticated successfully.
```

History

Version	Description
3.08	The nextdns authenticate command has been introduced.

3.113.3 nextdns authtoken

Description Specify authentication token for *NextDNS* account.

Command with **no** prefix removes the token.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nextdns)> authtoken <authtoken>
```

```
(nextdns)> no authtoken
```

Arguments

Argument	Value	Description
authtoken	<i>String</i>	Authentication token (ID) for <i>NextDNS</i> account.

Example

```
(nextdns)> authtoken 1f2a36
NextDns::Client: Set authentication token.
```

```
(nextdns)> no authtoken
NextDns::Client: Cleared authentication token.
```

History

Version	Description
3.08	The nextdns authtoken command has been introduced.

3.113.4 nextdns check-availability

Description Check availability of *NextDNS* service.

Prefix no No

Change settings No

Multiple input No

Synopsis `(nextdns)> check-availability`

Example

```
(nextdns)> check-availability
NextDns::Client: NextDNS DNS-over-HTTPS is available.
```

History

Version	Description
3.08	The nextdns check-availability command has been introduced.

3.114 ndns

Description Access to a group of commands to manage KeenDNS service.

Prefix no No

Change settings No

Multiple input No

Group entry `(ndns)`

Synopsis `(config)> ndns`

Example

```
(config)> ndns
Core::Configurator: Done.
```

History

Version	Description
2.07	The ndns command has been introduced.

3.114.1 ndns book-name

Description

Reserve Public DNS device hostname allocation.

For hostname transmission to another Keenetic device transfer-code parameter is used.

To transfer hostname it is necessary:

1. Execute command with transfer-code on the transmitting side.
2. Execute the same command with the same parameters on the receiving side.

Lifetime of transfer-code is 1 week.

Prefix no

No

Change settings

Yes

Multiple input

No

Synopsis

```
(ndns)> book-name <name> <domain> [ <access> [ ipv6 <access6> ] |
<transfer-code> ]
```

Arguments

Argument	Value	Description
name	<i>String</i>	The hostname for allocation.
domain	<i>String</i>	Second-level domain.
access	auto	Automatic access type.
	cloud	Hostname is registered on the cloud server IP address, HTTP traffic is tunneled to the Carrier.
	direct	Hostname is registered on the Carrier WAN-address.
access6	cloud	Enable cloud mode for IPv6 address.
transfer-code	<i>Hex</i>	Code for domain transmission to another Keenetic device. The length is 32 symbols.

Example

```
(ndns)> book-name test keenetic.pro
done, layout = view, title = NDSS::ndns/bookName ►
```

```
(Public DNS Hostname Booking):
  client, geo = *, ip = 193.0.174.200, format = ►
clean, date = 2025-06-04T09:59:12.072Z, standalone = false:

  fields:
    field, name = name, title = Public Name:
    field, name = domain, title = Domain Name:
    field, name = updated, title = Updated, type ►
= date, variant = date:
    field, name = address, title = IP Address:
    field, name = access, title = Access Mode ►
IP4, default = unknown:
    field, name = address6, title = IPv6 Address:
    field, name = access6, title = Access Mode ►
IPv6, default = unknown:
    field, name = transfer, title = Transfer:

    name: test
    domain: keenetic.pro
    acme: LE
    updated: 2025-06-04T09:59:12.059Z
    address: 0.0.0.0
    access: cloud
    address6: ::
    access6: cloud
    transfer: false

Ndns::Client: Booked "test.keenetic.pro".
```

```
(ndns)> book-name test keenetic.pro ►
121d567f901a345b289c121b567c903c

done, layout = view, title = NDSS::ndns/bookName ►
(Public DNS Hostname Booking), sub-title =
The name booking was successful.: client, geo = *, ip = ►
193.0.174.137, format =
clean, date = 2018-12-13T09:04:41.939Z, standalone = false:

  fields:
    field, name = name, title = Public Name:
    field, name = domain, title = Domain Name:
    field, name = updated, title = Updated, type ►
= date, variant = date:
    field, name = address, title = IP Address:
    field, name = access, title = Access Mode ►
IP4, default = unknown:
    field, name = address6, title = IPv6 Address:
    field, name = access6, title = Access Mode ►
IPv6, default = unknown:
    field, name = transfer, title = Transfer:

    name: test
    domain: keenetic.pro
    acme: LE
```

```

updated: 2018-12-13T08:47:11.014Z
address: 0.0.0.0
access: cloud
access6: none
transfer: true

```

```
Ndns::Client: Booked "test.keenetic.pro".
```

```
(ndns)> book-name test keenetic.pro cloud ipv6 cloud
```

```

done, layout = view, title = NDSS::ndns/bookName ▶
(Public DNS Hostname Booking), sub-title = The name booking was ▶
successful.:

```

```

client, geo = *, ip = 193.0.174.200, format = ▶
clean, date = 2019-05-23T09:12:29.145Z, standalone = false:

```

```

fields:
  field, name = name, title = Public Name:
  field, name = domain, title = Domain Name:
  field, name = updated, title = Updated, type ▶
= date, variant = date:
  field, name = address, title = IP Address:
  field, name = access, title = Access Mode ▶
IP4, default = unknown:
  field, name = address6, title = IPv6 Address:
  field, name = access6, title = Access Mode ▶
IPv6, default = unknown:
  field, name = transfer, title = Transfer:

```

```

name: test
domain: keenetic.pro
acme: LE
updated: 2019-05-23T09:12:16.197Z
address: 0.0.0.0
access: cloud
address6: ::
access6: cloud
transfer: false

```

```
Ndns::Client: Booked "test.keenetic.pro".
```

History

Version	Description
2.07	The ndns book-name command has been introduced.
2.14	Parameter ipv6 was added.

3.114.2 ndns check-name

Description Check the availability of hostname for allocation.

Prefix no No

Change settings No

Multiple input No

Synopsis `(ndns)> check-name <name>`

Arguments

Argument	Value	Description
name	<i>String</i>	The hostname for allocation.

Example

```
(ndns)> check-name testname

list:
  item:
    domain: keenetic.link
    name: testname
    available: yes
    acme: yes

  item:
    domain: keenetic.name
    name: testname
    available: yes
    acme: yes

  item:
    domain: keenetic.pro
    name: testname
    available: no
    acme: yes

Ndns::Client: Check completed.
```

History

Version	Description
2.07	The ndns check-name command has been introduced.

3.114.3 ndns drop-name

Description Drop Public DNS device hostname allocation.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(ndns)> drop-name <name> <domain>`

Arguments

Argument	Value	Description
name	<i>String</i>	The hostname for dropping.
domain	<i>String</i>	Second-level domain.

Example

```
(ndns)> drop-name test keenetic.pro

done, title = The name is un-booked., x-xml-debug ▶
= message-basic, hl = true, code = 200, icon = tick, layout = ▶
message, delay = false, x-ui-debug = UiBasic-object, rootName = ▶
done:
    client, geo = *, ip = 193.0.174.200, format = ▶
clean, date = 2025-06-04T10:04:36.236Z, standalone = false:
    reason: Success
    message, debug = x-string, class = code ▶
style--block: The name is un-booked.

    detail, layout = list:
        columns:
            column, id = type, title = Type:
            column, id = peer, title = Peer:
            column, id = detail, title = Detail:
            column, id = elapsed, title = Time, ▶
variant = period, scale = 1:

Ndns::Client: Dropped "test keenetic.pro".
```

History

Version	Description
2.07	The ndns drop-name command has been introduced.

3.114.4 ndns get-booked

Description Get actual info from the server about current booked Public DNS hostname.

Prefix no No

Change settings No

Multiple input No

Synopsis `(ndns)> get-booked`

Example

```
(ndns)> get-booked

done, layout = view, title = ▶
NDSS::ndns/updateBooking (Update Name Booking Address and ▶
Expiration):
    client, geo = *, ip = 193.0.174.200, format = ▶
clean, date = 2025-06-10T11:35:27.933Z, standalone = false:
```

```

        fields:
            field, name = name, title = Public Name:
            field, name = domain, title = Domain Name:
            field, name = updated, title = Updated, type ▶
= date, variant = date:
            field, name = address, title = IP Address:
            field, name = access, title = Access Mode ▶
(ip4), default = unknown:
            field, name = address6, title = IPv6 Address:
            field, name = access6, title = Access Mode ▶
(ipv6), default = unknown:
            field, name = transfer, title = Transfer:

        name: test
        domain: keenetic.pro
        acme: LE
        address: 0.0.0.0
        access: cloud
        address6: ::
        access6: cloud
        updated: 2025-06-10T07:19:49.113Z
        transfer: false

Ndns::Client: Got a booked name description.

```

History

Version	Description
2.08	The ndns get-booked command has been introduced.

3.114.5 ndns get-update

Description Update Public DNS device hostname allocation on the server.

Prefix no No

Change settings No

Multiple input No

Synopsis (ndns)> **get-update** [<access> [**ipv6** <access6>]]

Arguments

Argument	Value	Description
access	auto	Automatic access type.
	cloud	Hostname is registered on the cloud server IP address, HTTP traffic is tunneled to the Carrier.
	direct	Hostname is registered on the Carrier WAN-address. This command allows to enable support for the Static NAT (NAT 1-1) on the

Argument	Value	Description
		server side in the KeenDNS account parameters.
access6	cloud	Enable cloud mode for IPv6 address.

Example

```
(ndns)> get-update auto

done, layout = view, title = ►
NDSS::ndns/updateBooking (Update Name Booking Address and ►
Expiration):
    client, geo = *, ip = 193.0.174.200, format = ►
clean, date = 2025-06-04T10:13:22.594Z, standalone = false:

    fields:
        field, name = name, title = Public Name:
        field, name = domain, title = Domain Name:
        field, name = updated, title = Updated, type ►
= date, variant = date:
            field, name = address, title = IP Address:
            field, name = access, title = Access Mode ►
(ip4), default = unknown:
                field, name = address6, title = IPv6 Address:
                field, name = access6, title = Access Mode ►
(ipv6), default = unknown:
                    field, name = transfer, title = Transfer:

    name: test
    domain: keenetic.pro
    acme: LE
    address: 0.0.0.0
    access: cloud
    access6: none
    updated: 2025-06-04T10:08:29.866Z
    transfer: false

Ndns::Client: Updated a booked name.
```

```
(ndns)> get-update cloud ipv6 cloud

done, layout = view, title = ►
NDSS::ndns/updateBooking (Update Name Booking Address and ►
Expiration):
    client, geo = *, ip = 193.0.174.200, format = ►
clean, date = 2025-06-04T10:15:08.638Z, standalone = false:

    fields:
        field, name = name, title = Public Name:
        field, name = domain, title = Domain Name:
        field, name = updated, title = Updated, type ►
= date, variant = date:
            field, name = address, title = IP Address:
            field, name = access, title = Access Mode ►
```

```
(ip4), default = unknown:
    field, name = address6, title = IPv6 Address:
    field, name = access6, title = Access Mode ▶
(ipv6), default = unknown:
    field, name = transfer, title = Transfer:

    name: test
    domain: keenetic.pro
    acme: LE
    address: 0.0.0.0
    access: cloud
    address6: ::
    access6: cloud
    updated: 2025-06-04T10:15:08.633Z
    transfer: false

Ndns::Client: Updated a booked name.
```

```
(ndns)> get-update direct

    done, layout = view, title = ▶
NDSS::ndns/updateBooking (Update Name Booking Address and ▶
Expiration):
    client, geo = *, ip = 193.0.174.200, format = ▶
clean, date = 2025-06-04T10:16:04.151Z, standalone = false:

    fields:
        field, name = name, title = Public Name:
        field, name = domain, title = Domain Name:
        field, name = updated, title = Updated, type ▶
= date, variant = date:
        field, name = address, title = IP Address:
        field, name = access, title = Access Mode ▶
(ip4), default = unknown:
        field, name = address6, title = IPv6 Address:
        field, name = access6, title = Access Mode ▶
(ipv6), default = unknown:
        field, name = transfer, title = Transfer:

        name: test
        domain: keenetic.pro
        acme: LE
        address: 193.0.174.200
        access: direct
        access6: none
        updated: 2025-06-04T10:16:04.149Z
        transfer: false

Ndns::Client: Updated a booked name.
```

History

Version	Description
2.07	The ndns get-update command has been introduced.

2.14	Parameter ipv6 was added.
------	---------------------------

3.115 ntce

Description Access to a group of commands to configure the [NTCE](#) service.

Prefix no No

Change settings No

Multiple input No

Group entry (config-ntce)

Synopsis (config)> **ntce**

Example (config)> **ntce**
(config-ntce)>

History

Version	Description
3.07	The ntce command has been introduced.

3.115.1 ntce debug

Description Enable debug for the [NTCE](#) service. By default, setting is disabled.
Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis (config-ntce)> **debug**
(config-ntce)> **no debug**

Example (config-ntce)> **debug**
Ntce::Manager: Enabled debug.
(config-ntce)> **no debug**
Ntce::Manager: Disabled debug.

History

Version	Description
3.07	The ntce debug command has been introduced.

3.115.2 ntce filter assign host

Description Assign *NTCE* filter profile to a registered host.

The new profile can be added with **ntce filter profile** command.

The list of profiles in the system can be displayed with **show ntce filter profile** command.

Command with **no** prefix removes the defined profile for host. If you use no argument, the entire list of profiles will be cleared for hosts.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ntce)> filter assign host <host> <profile>
```

```
(config-ntce)> no filter assign host [ <host> ]
```

Argument	Value	Description
host	<i>MAC address</i>	MAC address of registered host.
profile	<i>String</i>	NTCE filter profile name.

Example

```
(config-ntce)> filter assign host 04:12:c4:54:bc:59 test
Ntce::Profiles: Associated host "04:d4:12:54:bc:59" with profile ►
"test".
```

```
(config-ntce)> no filter assign host 04:d4:12:54:bc:59
Ntce::Profiles: Removed profile for host "04:d4:12:54:bc:59".
```

```
(config-ntce)> no filter assign host
Ntce::Profiles: Removed profiles for hosts.
```

Version	Description
4.02	The ntce filter assign host command has been introduced.

3.115.3 ntce filter assign interface

Description Assign *NTCE* filter profile to an interface.

The new profile can be added with **ntce filter profile** command.

The list of profiles in the system can be displayed with **show ntce filter profile** command.

Command with **no** prefix removes the defined profile for interface. If you use no argument, the entire list of profiles for interfaces will be cleared.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ntce)> filter assign interface <interface> <profile>
(config-ntce)> no filter assign interface [ <interface> ]
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Network interface name.
profile	<i>String</i>	NTCE filter profile name.

Example

```
(config-ntce)> filter assign interface Bridge0 test
Ntce::Profiles: "test": associated interface "Bridge0" with ►
profile "test".
```

```
(config-ntce)> no filter assign interface Bridge0
Ntce::Profiles: Removed profile for interface "Bridge0".
```

```
(config-ntce)> no filter assign interface
Ntce::Profiles: Removed profiles for interfaces.
```

History

Version	Description
4.02	The ntce filter assign interface command has been introduced.

3.115.4 ntce filter profile

Description Create a custom *NTCE* filtering profile.

Command with **no** prefix removes the profile.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP

Synopsis

```
(config-ntce)> filter profile <name>
(config-ntce)> no filter profile <name>
```


Arguments

Argument	Value	Description
name	<i>String</i>	NTCE filter profile name.

Example

```
(config-ntce)> filter profile test
Ntce::Profiles: Created profile "test".
```

```
(config-ntce)> no filter profile test
Ntce::Profiles: "test": removed profile.
```

History

Version	Description
4.02	The ntce filter profile command has been introduced.

3.115.5 ntce filter profile application

Description

Add application to the [NTCE](#) filter profile.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ntce)> filter profile <name> application <application>
```

```
(config-ntce)> no filter profile <name> application <application>
```

Arguments

Argument	Value	Description
name	<i>String</i>	NTCE filter profile name.
application	<i>String</i>	Application name.

Example

```
(config-ntce)> filter profile test application youtube-kids
Ntce::Profiles: "test": added application "youtube-kids".
```

```
(config-ntce)> no filter profile test application youtube-kids
Ntce::Profiles: "test": removed application "youtube-kids".
```

History

Version	Description
4.02	The ntce filter profile application command has been introduced.

3.115.6 ntce filter profile description

Description Assign description for the *NTCE* filter profile.
Command with **no** prefix deletes the profile description.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ntce)> filter profile <name> description <description>
(config-ntce)> no filter profile <name> description
```

Arguments

Argument	Value	Description
name	<i>String</i>	NTCE filter profile name.
description	<i>String</i>	Arbitrary description of the profile.

Example

```
(config-ntce)> filter profile test description myprofile
Ntce::Profiles: "test": set description "myprofile".
```

```
(config-ntce)> no filter profile test description
Ntce::Profiles: "test": set description "".
```

History

Version	Description
4.02	The ntce filter profile description command has been introduced.

3.115.7 ntce filter profile group

Description Add application group to the *NTCE* filter profile.
Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ntce)> filter profile <name> group <group>
(config-ntce)> no filter profile <name> group <group>
```

Arguments

Argument	Value	Description
name	<i>String</i>	NTCE filter profile name.

Argument	Value	Description
group	<i>String</i>	Application group name.

Example

```
(config-ntce)> filter profile test group gaming
Ntce::Profiles: "test": added group "gaming".
```

```
(config-ntce)> no filter profile test group gaming
Ntce::Profiles: "test": removed group "gaming".
```

History

Version	Description
4.02	The ntce filter profile group command has been introduced.

3.115.8 ntce filter profile schedule

Description

Assign a schedule work to the [NTCE](#) filter profile.

Command with **no** prefix unbinds the schedule.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ntce)> filter profile <name> schedule <schedule>
```

```
(config-ntce)> no filter profile <name> schedule
```

Arguments

Argument	Value	Description
name	<i>String</i>	NTCE filter profile name.
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(config-ntce)> filter profile test schedule schedule1
Ntce::Profiles: "test": set schedule "schedule1".
```

```
(config-ntce)> no filter profile test schedule
Ntce::Profiles: "test": removed schedule.
```

History

Version	Description
4.02	The ntce filter profile schedule command has been introduced.

3.115.9 ntce filter profile type

Description Set the permission type of the *NTCE* filter profile.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(config-ntce)> filter profile <name> type <type>`

Arguments

Argument	Value	Description
name	<i>String</i>	NTCE filter profile name.
type	permit	Permit type profile.
	deny	Deny type profile.

Example

```
(config-ntce)> filter profile test type permit
Ntce::Profiles: "test": set type "permit".
```

```
(config-ntce)> filter profile test type deny
Ntce::Profiles: "test": set type "deny".
```

History

Version	Description
4.02	The ntce filter profile type command has been introduced.

3.115.10 ntce memory-watcher

Description Enable the memory pressure watcher mechanism for the *NTCE* service. By default, setting is enabled.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(config-ntce)> memory-watcher`
`(config-ntce)> no memory-watcher`

Example

```
(config-ntce)> memory-watcher
Ntce::Manager: Enabled automatic memory pressure handler.
```

```
(config-ntce)> no memory-watcher
Ntce::Manager: Disabled automatic memory pressure handler.
```

History

Version	Description
3.08	The ntce memory-watcher command has been introduced.

3.115.11 ntce qos category priority

Description

Set priorities for traffic categories.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ntce)> qos category <category>priority <priority>
```

```
(config-ntce)> qos category <category>no priority
```

Arguments

Argument	Value	Description
category	calling	① Top.
	gaming	② Critical.
	streaming	③ High.
	work	④ Medium-high.
	surfing	⑤ Medium.
	other	⑥ Normal (Default).
	filetransferring	⑦ Low.
priority	Integer	Priority value. Can take values in the range from 1 to 7.

Example

```
(config-ntce)> qos category work priority 7
Ntce::Manager: Set category "work" priority to "7".
```

```
(config-ntce)> qos category other no priority
Ntce::Manager: Reset QoS priority for category "work".
```

History

Version	Description
3.08	The ntce qos category priority command has been introduced.

3.115.12 ntce qos enable

Description Enable IntelliQoS, which ensures inbound, and outbound bandwidth for prioritized applications and tasks via pre-defined category groups presets. By default the service is disabled.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ntce)> qos enable
(config-ntce)> no qos enable
```

Example

```
(config-ntce)> qos enable
Ntce::Manager: Enabled QoS.
```

```
(config-ntce)> no qos enable
Ntce::Manager: Disabled QoS.
```

History

Version	Description
3.07	The ntce qos enable command has been introduced.

3.115.13 ntce upstream rate-limit input

Description Add limitation on the inbound traffic for specified interface.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-ntce)> upstream rate-limit <interface> input (<rate> | auto)
(config-ntce)> no upstream rate-limit <interface> input
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	The name of a global interface to rate-limit.
rate	<i>Integer</i>	The ingress rate limit in kbps. Can take values in the range from 64 to 1000000.
auto	<i>Keyword</i>	Auto-ingress mode.

Example

```
(config-ntce)> upstream rate-limit ISP input auto
Ntce::Upstreams: Set ISP input rate limit to "auto".
```

```
(config-ntce)> upstream rate-limit ISP input 1000000
Ntce::Upstreams: Set ISP input rate limit to "1000000" kbps.
```

```
(config-ntce)> no upstream rate-limit ISP input
Ntce::Upstreams: Reset ISP input rate limit.
```

History

Version	Description
4.01	The ntce upstream rate-limit input command has been introduced.

3.115.14 ntce upstream rate-limit output

Description

Add limitation on the outbound traffic for specified interface.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-ntce)> upstream rate-limit <interface> output (<rate> | auto)
```

```
(config-ntce)> no upstream rate-limit <interface> output
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	The name of a global interface to rate-limit.
rate	<i>Integer</i>	The ingress rate limit in kbps. Can take values in the range from 64 to 1000000.
auto	<i>Keyword</i>	Auto-ingress mode.

Example

```
(config-ntce)> upstream rate-limit ISP output auto
Ntce::Upstreams: Set ISP output rate limit to "auto".
```

```
(config-ntce)> upstream rate-limit ISP output 1000000
Ntce::Upstreams: Set ISP output rate limit to "1000000" kbps.
```

```
(config-ntce)> no upstream rate-limit ISP output
Ntce::Upstreams: Reset ISP output rate limit.
```

History

Version	Description
4.01	The ntce upstream rate-limit output command has been introduced.

3.116 ntp

Description Access to configure [NTP](#) client.

Command with **no** prefix resets [NTP](#) client configuration to default.

Prefix no Yes

Change settings No

Multiple input No

Synopsis (config)> **no ntp**

Example (config)> **no ntp**
Ntp::Client: Configuration reset.

History

Version	Description
2.00	The ntp command has been introduced.

3.117 ntp master

Description Enable [SNTP](#) server in private and protected network segments.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis (config)> **ntp master**

(config)> **no ntp master**

Example (config)> **ntp mater**
Ntp::Server: Enabled master mode.

(config)> **no ntp master**
Ntp::Server: Disabled master mode.

History

Version	Description
3.09	The ntp master command has been introduced.

3.118 ntp server

Description Add a new *NTP* server to the list. You can enter up to 8 *NTP* servers.

Command with **no** prefix deletes *NTP* server from the list. If you use no argument, the entire list of *NTP* servers will be removed.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config)> ntp server <server>
```

```
(config)> no ntp server [ <server> ]
```

Arguments

Argument	Value	Description
server	<i>String</i>	Host of <i>NTP</i> server.

Example

```
(config)> ntp server pool.ntp.org
Ntp::Client: Server "pool.ntp.org" has been added.
```

```
(config)> no ntp server
Ntp::Client: All NTP servers removed.
```

History

Version	Description
2.00	The ntp server command has been introduced.

3.119 ntp source

Description Set a specific source IP address for *NTP* service.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config)> ntp source <address>
```

```
(config)> no ntp source
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	The source IP address for all NTP packets.

Example

```
(config)> ntp source 192.168.2.2
Ntp::Client: Source has been set.
```

```
(config)> no ntp source
Ntp::Client: Source has been reset.
```

History

Version	Description
4.01	The ntp source command has been introduced.

3.120 ntp sync-period

Description

Set a period for time synchronization. By default, 1 week is used.

Command with **no** prefix resets time synchronization to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> ntp sync-period <period>
```

```
(config)> no ntp sync-period
```

Arguments

Argument	Value	Description
period	<i>Integer</i>	Time synchronization, in minutes. Can take values in the range from 60 minutes to 1 month.

Example

```
(config)> ntp sync-period 60
Ntp::Client: A synchronization period set to 60 minutes.
```

```
(config)> no ntp sync-period
Ntp::Client: Synchronization period value reset.
```

History

Version	Description
2.00	The ntp sync-period command has been introduced.

3.121 object-group fqdn

Description

Create an object group with automatic FQDN name resolution.

Command with **no** prefix removes the group.

Prefix no

Yes

Change settings Yes**Multiple input** Yes**Interface type** IP**Group entry** (config-ogrp-fqdn)

Synopsis

```
(config)> object-group fqdn <name>
```

```
(config)> no object-group fqdn <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Name of the FQDN object group.

Example

```
(config)> object-group fqdn TEST  
Network::ObjectGroup: "TEST": group created.
```

```
(config)> no object-group fqdn TEST  
Network::ObjectGroup: "TEST": group removed.
```

History

Version	Description
4.03	The object-group fqdn command has been introduced.

3.121.1 object-group fqdn exclude

Description Add or remove non-matching element of the object group.Command with **no** prefix removes the setting.**Prefix no** Yes**Change settings** Yes**Multiple input** Yes**Synopsis**

```
(config-ogrp-fqdn)> exclude <address>
```

```
(config-ogrp-fqdn)> no exclude <address>
```

Arguments

Argument	Value	Description
address	<i>FQDN</i>	IP address or domain name.

Example

```
(config-ogrp-ip)> exclude 8.8.8.8
Network::ObjectGroup: "test": added exclude tcpudp 1.2.3.0/24 ►
70-80.
```

```
(config-ogrp-ip)> no exclude 8.8.8.8
Network::ObjectGroup: "TEST": removed excluded FQDN "8.8.8.8".
```

History

Version	Description
4.03	The object-group fqdn exclude command has been introduced.

3.121.2 object-group fqdn include

Description

Add or remove matching element of the object group.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(config-ogrp-fqdn)> include <address>
```

```
(config-ogrp-fqdn)> no include <address>
```

Arguments

Argument	Value	Description
address	<i>FQDN</i>	IP address or domain name.

Example

```
(config-ogrp-fqdn)> include google.com
Network::ObjectGroup: "TEST": added included FQDN "google.com".
```

```
(config-ogrp-fqdn)> no include google.com
Network::ObjectGroup: "TEST": removed included FQDN "google.com".
```

History

Version	Description
4.03	The object-group fqdn include command has been introduced.

3.122 object-group ip

Description Create an object group of IP type, which can store IPv4 subnets with optional L4 protocol and port range info.

Command with **no** prefix removes the group.

Prefix no Yes

Change settings Yes

Multiple input Yes

Interface type IP

Group entry (config-ogrp-ip)

Synopsis

```
(config)> object-group ip <name>
(config)> no object-group ip <name>
```

Argument	Value	Description
name	<i>String</i>	Name of the IPv4 object group.

Example

```
(config)> object-group ip test
Network::ObjectGroup: "test": group created.
```

```
(config)> no object-group ip test
Network::ObjectGroup: "test": group removed.
```

Version	Description
4.00	The object-group ip command has been introduced.

3.122.1 object-group ip exclude

Description Add or remove non-matching element of the object group.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ogrp-ip)> exclude <proto> <address> [ <port> [ <end-port> ] ]
```

```
(config-ogrp-ip)> no exclude <proto> <address> [ <port> [<end-port>]]
```

Arguments

Argument	Value	Description
proto	ip	<i>IP</i> protocol (include <i>TCP</i> , <i>UDP</i> , <i>ICMP</i> and other).
	tcp	<i>TCP</i> protocol.
	udp	<i>UDP</i> protocol.
	tcpudp	<i>TCP</i> and <i>UDP</i> protocols.
	icmp	<i>ICMP</i> protocol.
	esp	<i>ESP</i> protocol.
	gre	<i>GRE</i> protocol.
	ipip	<i>IP in IP</i> protocol.
address	<i>String</i>	IP address or subnet (in the form of prefix bit length (e.g. 1.2.3.0/24)).
port	<i>Integer</i>	TCP/UDP port number for which a translation request comes. If not specified, all incoming requests will be translated.
end-port	<i>Integer</i>	The end of the range of ports.

Example

```
(config-ogrp-ip)> exclude tcpudp 1.2.3.0/24 70 80
Network::ObjectGroup: "test": added exclude tcpudp 1.2.3.0/24 ►
70-80.
```

```
(config-ogrp-ip)> no exclude tcpudp 1.2.3.0/24 70 80
Network::ObjectGroup: "test": removed exclude tcpudp 1.2.3.0/24 ►
70-80.
```

History

Version	Description
4.00	The object-group ip exclude command has been introduced.

3.122.2 object-group ip include

Description Add or remove matching element of the object group.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-ogrp-ip)> include <proto> <address> [ <port> [<end-port>]]
```

```
(config-ogrp-ip)> no include <proto> <address> [ <port> [<end-port>]]
```

Arguments

Argument	Value	Description
proto	ip	IP protocol (include TCP , UDP , ICMP and other).
	tcp	TCP protocol.
	udp	UDP protocol.
	tcpudp	TCP and UDP protocols.
	icmp	ICMP protocol.
	esp	ESP protocol.
	gre	GRE protocol.
	ipip	IP in IP protocol.
address	<i>String</i>	IP address or subnet (in the form of prefix bit length (e.g. 1.2.3.0/24)).
port	<i>Integer</i>	TCP/UDP port number for which a translation request comes. If not specified, all incoming requests will be translated.
end-port	<i>Integer</i>	The end of the range of ports.

Example

```
(config-ogrp-ip)> include tcpudp 1.2.3.0/24 75 80  
Network::ObjectGroup: "test": added include tcpudp 1.2.3.0/24 ►  
75-80.
```

```
(config-ogrp-ip)> no include tcpudp 1.2.3.0/24 75 80  
Network::ObjectGroup: "test": removed include tcpudp 1.2.3.0/24 ►  
75-80.
```

History

Version	Description
4.00	The object-group ip include command has been introduced.

3.123 oc-server

Description	Access to a group of commands to configure OpenConnect server parameters.
Prefix no	No
Change settings	No
Multiple input	No
Group entry	(oc-server)

Synopsis

```
(config)> oc-server
```

Example

```
(config)> oc-server
(oc-server)>
```

History

Version	Description
4.02	The oc-server command has been introduced.

3.123.1 oc-server camouflage

Description

Enable the camouflage mode for the [OpenConnect](#) server, which provides greater security from remote service scanning. By default, the mode is disabled.

Command with **no** prefix disables the camouflage mode.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(oc-server)> camouflage
```

```
(oc-server)> no camouflage
```

Example

```
(oc-server)> camouflage
OcServer::Manager: Enabled camouflage mode.
```

```
(oc-server)> no camouflage
OcServer::Manager: Disabled camouflage mode.
```

History

Version	Description
4.02	The oc-server camouflage command has been introduced.

3.123.2 oc-server debug

Description

Enable debug mode for [OpenConnect](#) server. Detailed information about the progress of the [OpenConnect](#) client connection to the [OpenConnect](#) server is saved to the system log. By default, setting is disabled.

Command with **no** prefix disables the debug mode.

Prefix no

Yes

Change settings

Yes

Multiple input No

Synopsis

```
(oc-server)> debug
(oc-server)> no debug
```

Example

```
(oc-server)> debug
OcServer::Manager: Enabled debug.

(oc-server)> no debug
OcServer::Manager: Disabled debug.
```

History	Version	Description
	4.03	The oc-server debug command has been introduced.

3.123.3 oc-server interface

Description Bind [OpenConnect](#) server to the specified interface.
Command with **no** prefix unbinds the interface.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(oc-server)> interface <interface>
(oc-server)> no interface
```

Arguments	Argument	Value	Description
	interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(oc-server)> interface Bridge0
OcServer::Manager: Bound to Bridge0.

(oc-server)> no interface
OcServer::Manager: Reset interface binding.
```

History	Version	Description
	4.02	The oc-server interface command has been introduced.

3.123.4 oc-server mtu

Description Set *MTU* value to be transmitted to *OpenConnect* server. By default, 1350 value is used.

Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(oc-server)> mtu <value>
(oc-server)> no mtu
```

Arguments

Argument	Value	Description
value	<i>Integer</i>	<i>MTU</i> value. Can take values in the range from 128 to 1500 inclusively.

Example

```
(oc-server)> mtu 1350
OcServer::Manager: MTU set to 1350.
```

```
(oc-server)> no mtu
OcServer::Manager: MTU reset.
```

History

Version	Description
4.02	The oc-server mtu command has been introduced.

3.123.5 oc-server multi-login

Description Allow connection to *OpenConnect* server for multiple users from one account.

Command with **no** prefix disables this feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(oc-server)> multi-login
(oc-server)> no multi-login
```

Example

```
(oc-server)> multi-login
OcServer::Manager: Enabled multiple login.
```

```
(oc-server)> no multi-login
OcServer::Manager: Disabled multiple login.
```

History

Version	Description
4.02	The oc-server multi-login command has been introduced.

3.123.6 oc-server pool-range

Description Assign a pool of addresses for the clients that connect to the [OpenConnect](#) server.

Command with **no** prefix removes a pool.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(oc-server)> oc-server <begin> [ <size> ]
(oc-server)> no oc-server
```

Arguments

Argument	Value	Description
begin	<i>IP address</i>	Start address of pool.
size	<i>Integer</i>	Pool size.

Example

```
(oc-server)> pool-range 192.168.1.30 7
OcServer::Manager: Configured pool range 192.168.1.30 to ►
192.168.1.36.
```

```
(oc-server)> no pool-range
OcServer::Manager: Reset pool range.
```

History

Version	Description
4.02	The oc-server pool-range command has been introduced.

3.123.7 oc-server route

Description Assign a route which is transmitted in DHCP INFORM messages to the [OpenConnect](#) server clients.

Command with **no** prefix cancels the specified route. If you use no arguments, the entire list of routes will be cleared.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(oc-server)> route <address> <mask>
(oc-server)> no route [ <address> <mask> ]
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	Network client address.
mask	<i>IP-mask</i>	Network client mask. There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).

Example

```
(oc-server)> route 192.168.2.0/24
Vpn::DhcpInform: "OCSRVPN": added DHCP INFORM route to ►
192.168.2.0/24.
```

```
(oc-server)> no route 192.168.2.0/24
Vpn::DhcpInform: "OCSRVPN": removed DHCP INFORM route to ►
192.168.2.0/24.
```

```
(oc-server)> no route
Vpn::DhcpInform: "OCSRVPN": cleared DHCP INFORM routes.
```

History

Version	Description
4.03	The oc-server route command has been introduced.

3.123.8 oc-server session-logout

Description Terminate an active or stalled session on the [OpenConnect](#) server.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(oc-server)> session-logout <session>
```

Arguments

Argument	Value	Description
session	<i>Integer</i>	Identifier of the OpenConnect session (can be viewed using the show oc-server command).

Example

```
(oc-server)> session-logout 6
OcServer::Manager: Session "6" is terminated.
```

History	Version	Description
	4.03	The oc-server session-logout command has been introduced.

3.123.9 oc-server session-preempt

Description Enable to preempt VPN sessions when **oc-server multi-login** option is disabled for the *OpenConnect* server.

Command with **no** prefix disables the preempt.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(oc-server)> session-preempt
(oc-server)> no session-preempt
```

Example

```
(oc-server)> session-preempt
OcServer::Manager: Enabled session preemption.
```

```
(oc-server)> no session-preempt
OcServer::Manager: Disabled session preemption.
```

History	Version	Description
	4.03	The oc-server session-preempt command has been introduced.

3.123.10 oc-server static-ip

Description Bind IP address to the user. User account must have vpn-oc tag.

Command with **no** prefix removes binding.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(oc-server)> static-ip <name> <address>
```

```
(oc-server)> no static-ip <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Username.
address	<i>IP address</i>	IP address to bind.

Example

```
(oc-server)> static-ip admin 192.168.1.30
OcServer::Manager: Static IP 192.168.1.30 assigned to user ►
"admin".
```

```
(oc-server)> no static-ip admin
OcServer::Manager: Static IP address removed for user "admin".
```

History

Version	Description
4.02	The oc-server static-ip command has been introduced.

3.124 opkg chroot

Description

Enable chroot for *opkg*. If enabled, root directory is changed to /opt before executing any opkg script. By default, the setting is disabled.

Command with **no** prefix disables chroot mode.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> opkg chroot
```

```
(config)> no opkg chroot
```

Example

```
(config)> opkg chroot
Opkg::Manager: Chroot enabled.
```

```
(config)> no opkg chroot
Opkg::Manager: Chroot disabled.
```

History

Version	Description
2.05	The opkg chroot command has been introduced.

3.125 opkg disk

Description Configure partition for *opkg* software. This setting is required to install and run *opkg*.

Once configured, the partition will be mounted to /opt using **mount --bind**, and the **initrc** script executed immediately, see also [Section 3.127 on page 480](#).

If /opt/install directory is not empty, all contained *.ipk and *.tgz archives are unpacked to /opt before running initrc. Archives are deleted after installation.

Command with **no** prefix disables the opkg feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> opkg disk <disk> [ <url> ]
(config)> no opkg disk
```

Arguments

Argument	Value	Description
disk	String	Partition label or UUID.
url	String	URL of installer package.

Example

```
(config)> opkg disk ext4_opkg:/
Opkg::Manager: Disk is set to: ext4_opkg:/.
```

```
(config)> opkg disk storage:/ ►
https://bin.entware.net/aarch64-k3.10/installer/aarch64-installer.tar.gz
Opkg::Manager: Disk is set to: storage:/.
```

```
(config)> no opkg disk
Opkg::Manager: Disk is unset.
```

History

Version	Description
2.05	The opkg disk command has been introduced.
4.02	The url argument was added.

3.126 opkg dns-override

Description Disable *TCP* and *UDP* 53 port for DNS proxy.

Disables port allows to replace embedded DNS proxy with a custom service, such as BIND or Dnsmasq of *opkg*.

Command with **no** prefix returns port work for DNS proxy.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> opkg dns-override
(config)> no opkg dns-override
```

Example

```
(config)> opkg dns-override
Opkg::Manager: DNS override enabled.

(config)> no opkg dns-override
Opkg::Manager: DNS override disabled.
```

History

Version	Description
2.05	The opkg dns-override command has been introduced.

3.127 opkg initrc

Description Set initial script. Default value — /opt/etc/initrc.

When the *opkg disk* is mounted, and the packages are installed, the system will execute the initial script. If *path* is a directory, the system will execute all contained scripts in alphabetic order.

Command with **no** prefix resets initrc to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> opkg initrc <path>
(config)> no opkg initrc
```

Arguments

Argument	Value	Description
path	<i>Filename</i>	Initial script file or directory.

Example

```
(config)> opkg initrc /opt/etc/init.d/rc.unslung
Opkg::Manager: Configured init script: ►
```



```
"/opt/etc/init.d/rc.unslung".
(config)> no opkg initrc
Opkg::Manager: Init script reset to default: /opt/etc/initrc.
```

History

Version	Description
2.05.C.3	The opkg initrc command has been introduced.

3.128 opkg timezone

Description Configure TZ environment variable and /opt/var/TZ file for *opkg* software. Default — timezone is undefined.

It depends on the *opkg* C library, how timezone is interpreted. The value of TZ can be either a POSIX timezone specification in the form `stdoffset[dst[offset]][,start[/time],end[/time]]`, or the name of a zoneinfo-binary-format timezone file (the form used by glibc and almost all GNU systems).

Command with **no** prefix resets timezone to undefined.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> opkg timezone(auto | <timezone>)
(config)> no opkg timezone
```

Arguments

Argument	Value	Description
timezone	String	Timezone specification to be assigned to the TZ environment variable and written to /opt/var/TZ.
auto	Keyword	Automatic timezone assignment. Specification is generated from system wide settings, see Section 3.168.4 on page 680 .

Example

```
(config)> opkg timezone auto
Opkg::Manager: Enabled automatic timezone.
(config)> opkg timezone UTC
Opkg::Manager: Enabled timezone "UTC".
(config)> no opkg timezone
Opkg::Manager: Timezone reset to undefined.
```

History

Version	Description
2.05.C.3	The opkg timezone command has been introduced.

3.129 ping-check profile

Description Access to a group of commands to configure *Ping Check* profile. If the profile is not found, the command tries to create it.

Command with **no** prefix removes *Ping Check* profile.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry (config-pchk)

Synopsis

```
(config)> ping-check profile <name>
(config)> no ping-check profile <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	<i>Ping Check</i> profile name. You can see the list of available profiles with help of ping-check profile [Tab] command.

Example

```
(config)> ping-check profile [Tab]
```

```
Usage template:
    profile {name}
```

```
Choose:
    TEST
    MYMY
```

```
(config)> ping-check profile new_prof
PingCheck::Client: Profile "new_prof" has been created.
(config-pchk)>
```

```
(config)> no ping-check profile new_prof
PingCheck::Client: Profile "new_prof" has been deleted.
```

History

Version	Description
2.04	The ping-check profile command has been introduced.

3.129.1 ping-check profile host

Description Assign hostname for testing. By default, hostname is assigned according to country code.

Command with **no** prefix removes the hostname.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-pchk)> host <host>
(config-pchk)> no host [ <host> ]
```

Arguments

Argument	Value	Description
host	<i>Hostname</i>	Name or address of remote host.

Example

```
(config-pchk)> host 8.8.8.8
PingCheck::Profile: "test": add host "8.8.8.8" for testing.
```

```
(config-pchk)> host google.com
PingCheck::Profile: "test": add host "google.com" for testing.
```

```
(config-pchk)> no host
PingCheck::Profile: "test": hosts cleared.
```

History

Version	Description
2.04	The ping-check profile host command has been introduced.

3.129.2 ping-check profile max-fails

Description Specify the number of consecutive failed requests to a remote host by obtaining of which the Internet at the interface considered absent. By default, value 5 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-pchk)> max-fails <count>
(config-pchk)> no max-fails
```

Arguments

Argument	Value	Description
count	<i>Integer</i>	Amount of failed requests. Can take values in the range from 1 to 10 inclusively.

Example

```
(config-pchk)> max-fails 7
PingCheck::Profile: "test": uses 7 fail count for disabling ►
interface.
```

```
(config-pchk)> no max-fails
PingCheck::Profile: "test": fail count is reset to 5.
```

History

Version	Description
2.04	The ping-check profile max-fails command has been introduced.

3.129.3 ping-check profile min-success

Description

Specify the number of consecutive success requests to a remote host by obtaining of which the Internet at the interface considered present. By default, value 5 is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-pchk)> min-success <count>
```

```
(config-pchk)> no min-success
```

Arguments

Argument	Value	Description
count	<i>Integer</i>	Amount of success requests. Can take values in the range from 1 to 10 inclusively.

Example

```
(config-pchk)> min-success 3
PingCheck::Profile: "test": uses 3 success count for enabling ►
interface.
```

```
(config-pchk)> no min-success
PingCheck::Profile: "test": success count is reset to 5.
```

History

Version	Description
2.04	The ping-check profile min-success command has been introduced.

3.129.4 ping-check profile mode

Description Set [Ping Check](#) mode. By default, icmp value is used.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(config-pchk)> mode <mode>`

Arguments

Argument	Value	Description
mode	icmp	The availability testing of remote host will be done by ICMP-echo request (ping) sending.
	connect	The availability testing of remote host will be done by TCP-connection establishing to specified port.
	tls	The availability testing of remote host will be done by TLS-connection.
	uri	The availability testing of remote host will be done by URI checking.

Example

```
(config-pchk)> mode tls
PingCheck::Profile: "test": uses tls mode.
```

History

Version	Description
2.04	The ping-check profile mode command has been introduced.
3.09	The tls argument was added.
4.00	The uri argument was added.

3.129.5 ping-check profile port

Description Specify port for connection to the remote host. Setting has a meaning for connect mode of [Ping Check](#) (see [ping-check profile mode](#) command).

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(config-pchk)> port <port>`

```
(config-pchk)> no port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	Port number. Can take values in the range from 1 to 65534 inclusively.

Example

```
(config-pchk)> port 80
PingCheck::Profile: "test": uses port 80 for testing.
```

```
(config-pchk)> no port
PingCheck::Profile: "test": port is cleared.
```

History

Version	Description
2.04	The ping-check profile port command has been introduced.

3.129.6 ping-check profile power-cycle

Description

Enable power-cycle for USB network interface. Enabled by default.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-pchk)> power-cycle
```

```
(config-pchk)> no power-cycle
```

Example

```
(config-pchk)> power-cycle
PingCheck::Profile: "test": enabled USB power cycle.
```

```
(config-pchk)> power-cycle
PingCheck::Profile: "test": disabled USB power cycle.
```

History

Version	Description
2.04	The ping-check profile power-cycle command has been introduced.

3.129.7 ping-check profile timeout

Description

Set the maximum response time of the remote host for a single request in seconds. By default, 2 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-pchk)> timeout <timeout>
(config-pchk)> no timeout
```

Argument	Value	Description
timeout	<i>Integer</i>	Response time in seconds. Can take values in the range from 1 to 10 inclusively.

Example

```
(config-pchk)> timeout 4
PingCheck::Profile: "test": timeout is changed to 4 seconds.
```

```
(config-pchk)> no timeout
PingCheck::Profile: "test": timeout is reset to 2.
```

Version	Description
2.04	The ping-check profile timeout command has been introduced.

3.129.8 ping-check profile update-interval

Description Set periodicity of *Ping Check* performing.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(config-pchk)> update-interval <seconds>
```

Argument	Value	Description
seconds	<i>Integer</i>	Refresh period in seconds. Can take values in the range from 3 to 3600 inclusively.

Example

```
(config-pchk)> update-interval 60
PingCheck::Profile: "test": update interval is changed to 60 ► seconds.
```

History

Version	Description
2.04	The ping-check profile update-interval command has been introduced.

3.129.9 ping-check profile uri

Description Assign URI ([Uniform Resource Identifier](https://en.wikipedia.org/wiki/Uniform_Resource_Identifier)¹⁷) host for testing.

Command with **no** prefix removes the host.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-pchk)> uri <uri>
(config-pchk)> no uri [ <uri> ]
```

Arguments

Argument	Value	Description
uri	<i>Hostname</i>	Name or address of remote HTTP or HTTPS host.

Example

```
(config-pchk)> uri http://localhost:8888/
PingCheck::Profile: "TEST": add URI "http://localhost:8888/" for ►
testing.
```

```
(config-pchk)> uri https://localhost:4343/
PingCheck::Profile: "TEST": add URI "https://localhost:4343/" ►
for testing.
```

```
(config-pchk)> no uri http://localhost:8888/
PingCheck::Profile: "TEST": URIs cleared.
```

```
(config-pchk)> no uri
PingCheck::Profile: "TEST": URIs cleared.
```

History

Version	Description
4.00	The ping-check profile uri command has been introduced.

3.130 ppe

Description Enable Packet Processing Engine. By default, the setting is turned on.

¹⁷ https://en.wikipedia.org/wiki/Uniform_Resource_Identifier

Command with **no** prefix disables specified accelerator.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> ppe <engine>
(config)> no ppe [<engine>]
```

Arguments	Argument	Value	Description
	engine	software	Software accelerator.

Example

```
(config)> ppe software
Network::Interface::Rtx::Ppe: Software PPE enabled.
```

```
(config)> no ppe
Network::Interface::Rtx::Ppe: All PPE disabled.
```

History	Version	Description
	2.00	The ppe command has been introduced.
	2.05	Argument engine was implemented.

3.131 pppoe pass

Description Enable PPPoE Pass Through function. You can enter up to 10 network nodes.
Command with **no** prefix disables the function.

Prefix no Yes

Change settings Yes

Multiple input No

Interface type Ethernet

Synopsis

```
(config)> pppoe pass through <wan-iface> <lan-iface>
(config)> no pppoe pass through
```

Arguments	Argument	Value	Description
	wan-iface	Interface	The starting interface — full WAN-interface name or an alias.

Argument	Value	Description
lan-iface	<i>Interface</i>	The finishing interface — full LAN-interface name or an alias.

Example

```
(config)> pppoe pass through Home ISP
Pppoe::Pass: Configured pass from "Bridge0" to "GigabitEthernet1".
```

```
(config)> no pppoe pass
Pppoe::Pass: Disabled.
```

History

Version	Description
2.00	The pppoe pass command has been introduced.

3.132 printer

Description

Access to a group of commands to configure the printer. If the printer is not found, the command tries to create it.

Command with **no** prefix deletes the printer.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Group entry

(config-printer)

Synopsis

```
(config)> printer <id>
```

```
(config)> no printer <id>
```

Arguments

Argument	Value	Description
id	<i>String</i>	Printer ID.

Example

```
(config)> printer 0924:3cf4
(config-printer)>
```

History

Version	Description
2.00	The printer command has been introduced.

3.132.1 printer bidirectional

Description

Enable bidirectional mode for printer.

Command with **no** prefix disables bidirectional mode.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-printer)> bidirectional
(config-printer)> no bidirectional
```

Example

```
(config-printer)> bidirectional
Printer::Manager: A bidirectional mode enabled.

(config-printer)> no bidirectional
Printer::Manager: A bidirectional mode disabled.
```

History

Version	Description
2.04	The printer bidirectional command has been introduced.

3.132.2 printer debug

Description Enable debug mode for printer. If you use no argument, debug level 1 will be set.

Command with **no** prefix disables debug mode.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-printer)> debug [ level <level> ]
(config-printer)> no debug
```

Arguments

Argument	Value	Description
level	<i>Integer</i>	The debug level. Can take values in the range from 1 to 3 inclusively.

Example

```
(config-printer)> debug level 3
Printer::Manager: a debug level set to 3.

(config-printer)> no debug
Printer::Manager: A debug mode disabled.
```

History

Version	Description
2.04	The printer debug command has been introduced.

3.132.3 printer firmware

Description Set printer firmware file.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-printer)> firmware <firmware>
```

```
(config-printer)> no firmware
```

Arguments

Argument	Value	Description
firmware	<i>String</i>	Path to firmware file.

Example

```
(config-printer)> firmware storage:sihp1018.dl  
Printer::Manager: A printer firmware set.
```

```
(config-printer)> no firmware  
Printer::Manager: A printer firmware set.
```

History

Version	Description
2.00	The printer firmware command has been introduced.

3.132.4 printer name

Description Assign an arbitrary name to the printer.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(config-printer)> name <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Arbitrary printer name.

Example (config-printer)> **name Canon**
Printer::Manager: A printer name set.

History	Version	Description
	2.00	The printer name command has been introduced.

3.132.5 printer port

Description Set printer port if printer type is direct. By default, TCP-port is 9100.

Prefix no No

Change settings Yes

Multiple input No

Synopsis (config-printer)> **port** *port*

Arguments	Argument	Value	Description
	port	<i>Integer</i>	Printer port.

Example (config-printer)> **port 2012**
Printer::Manager: A port set.

History	Version	Description
	2.00	The printer port command has been introduced.

3.132.6 printer status-polling

Description Enable printer status polling. By default, status polling is enabled.

Command with **no** prefix disables printer status polling.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis (config-printer)> **status-polling**
(config-printer)> **no status-polling**

Example (config-printer)> **status-polling**
Printer::Manager: Status polling enabled.

```
(config-printer)> no status-polling
Printer::Manager: Status polling disabled.
```

History

Version	Description
3.04	The printer status-polling command has been introduced.

3.132.7 printer type

Description Set printer type.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(config-printer)> type <type>`

Arguments

Argument	Value	Description
type	cifs	Printer connected via CIFS .
	direct	Printer connected directly to device.

Example

```
(config-printer)> type direct
Printer::Manager: A printer type set.
```

History

Version	Description
2.00	The printer type command has been introduced.

3.133 schedule

Description Access to a group of commands to configure the schedule. If the schedule is not found, the command tries to create it.

Command with **no** prefix deletes the schedule.

Prefix no Yes

Change settings Yes

Multiple input Yes

Group entry `(config-sched)`

Synopsis `(config)> schedule <name>`

```
(config)> no schedule <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	A schedule name.

History

Version	Description
2.06	The schedule command has been introduced.

3.133.1 schedule action

Description Specify the actions to be performed according to the selected schedule.

Command with **no** prefix cancels the action.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-sched)> action <action> <min> <hour> <dow>
```

```
(config-sched)> no action [ <action> <min> <hour> <dow> ]
```

Arguments

Argument	Value	Description
action	start	Action of the beginning.
	stop	Action of the end.
min	<i>Integer</i>	The minutes.
hour	<i>Integer</i>	The hours.
dow	<i>Integer</i>	Days of the week, separated by commas. 0 and 7 mean Sunday. * means daily.

Example

```
(config-sched)> action start 0 9 1,2,3,4,5
Core::Schedule::Manager: Updated schedule "WIFI".
```

History

Version	Description
2.06	The schedule action command has been introduced.

3.133.2 schedule description

Description Set description for the selected schedule.

Command with **no** prefix deletes the description.

Prefix no Yes**Change settings** No**Multiple input** No

Synopsis

```
(config-sched)> description <description>
```

```
(config-sched)> no description
```

Arguments

Argument	Value	Description
description	<i>String</i>	Text of the description.

Example

```
(config-sched)> description "Schedule for on/off Access Point"
Core::Schedule::Manager: Updated description of schedule "WIFI".
```

History

Version	Description
2.06	The schedule description command has been introduced.

3.133.3 schedule led

Description Set LED indication for the scheduled events. SelectedSchedule control should be chosen with **system led** command.

Command with **no** prefix removes LED indication.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(config-sched)> led <action>
```

```
(config-sched)> no led
```

Arguments

Argument	Value	Description
action	start	LED shows the beginning of the scheduled event.
	stop	LED shows the end of the scheduled event.

Example

```
(config-sched)> led start
Core::Schedule::Led: Selected schedule "111".
```


History

Version	Description
2.08	The schedule led command has been introduced.

3.134 service afp

Description Enable [AFP](#) service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service afp
```

```
(config)> no service afp
```

Example

```
(config)> service afp
Afp::Server: Enabled.
```

History

Version	Description
2.06	The service afp command has been introduced.

3.135 service cifs

Description Enable [CIFS](#) service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service cifs
```

```
(config)> no service cifs
```

Example

```
(config)> service cifs
Cifs::ServerTsmB: Enabled.
```

```
(config)> no service cifs
Cifs::ServerTsmB: Disabled.
```

History

Version	Description
2.00	The service cifs command has been introduced.

3.136 service dhcp

Description Enable [DHCP server](#). If there is not enough settings to start the service (see [ip dhcp pool](#)), the service will not respond to the network. As soon as there are enough settings, the service will be enabled automatically.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service dhcp
(config)> no service dhcp
```

Example

```
(config)> service dhcp
service enabled.
```

History	Version	Description
	2.00	The service dhcp command has been introduced.

3.137 service dhcp-relay

Description Enable DHCP-relay. If there are not enough settings to start the service (see [ip dhcp relay lan](#), [ip dhcp relay server](#), [ip dhcp relay wan](#)), it will not respond within the network. As soon as there are enough settings, the service will be enabled automatically.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service dhcp-relay
(config)> no service dhcp-relay
```

Example

```
(config)> service dhcp-relay
service enabled.
```

History	Version	Description
	2.00	The service dhcp-relay command has been introduced.

3.138 service dlna

Description Enable [DLNA](#) service. If there are not enough settings to start the service (see [dlna](#)), it will not respond within the network. As soon as there are enough settings, the service will be enabled automatically.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service dlna
(config)> no service dlna
```

Example

```
(config)> service dlna
DLNA server enabled.
```

History	Version	Description
	2.00	The service dlna command has been introduced.

3.139 service dns-proxy

Description Enable DNS-proxy. To configure the parameters of the service, use [Section 3.21 on page 126](#) group of commands.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(config)> service dns-proxy
```

Example

```
(config)> service dns-proxy
Dns::Manager: DNS proxy enabled.
```

History	Version	Description
	2.00	The service dns-proxy command has been introduced.

3.140 service ftp

Description Enable FTP server that provides the user with access to connected USB-drives, configuration files and a file with firmware update.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service ftp
(config)> no service ftp
```

Example

```
(config)> service ftp
FTP server enabled.
```

History	Version	Description
	2.00	The service ftp command has been introduced.

3.141 service http

Description Enable HTTP server that provides the user with Web-interface to configure Carrier.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service http
(config)> no service http
```

Example

```
(config)> service http
HTTP server enabled.
```

History	Version	Description
	2.00	The service http command has been introduced.

3.142 service igmp-proxy

Description Enable IGMP-proxy. For the service functioning it is necessary to have one upstream interface and at least one downstream interface. If there are not enough settings to run the service, the service will not function. As soon as there are enough settings, the service will start automatically.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service igmp-proxy
(config)> no service igmp-proxy
```

Example

```
(config)> service igmp-proxy
IGMP proxy enabled.
```

History

Version	Description
2.00	The service igmp-proxy command has been introduced.

3.143 service internet-checker

Description Enable the Internet-checker to monitor the state of Internet connection on the device. By default, service is enabled.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service internet-checker
(config)> no service internet-checker
```

Example

```
(config)> service internet-checker
Network::InternetChecker: Hosts check enabled.
```

```
(config)> no service internet-checker
Network::InternetChecker: Hosts check disabled.
```

History

Version	Description
2.13	The service internet-checker command has been introduced.

3.144 service ipsec

Description

Enable *IPsec* service. By default, service is disabled.

Command with **no** prefix stops the service.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> service ipsec
```

```
(config)> no service ipsec
```

Example

```
(config)>service ipsec  
IpSec::Manager: Service enabled.
```

History

Version	Description
2.06	The service ipsec command has been introduced.

3.145 service kabinet

Description

Enable KAbINET authenticator service. By default it is disabled.

Command with **no** prefix stops the service.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> service kabinet
```

```
(config)> no service kabinet
```

Example

```
(config)> service kabinet  
Kabinet::Authenticator: Authenticator enabled.
```

```
(config)> service kabinet  
Kabinet::Authenticator: Authenticator disabled.
```

History	Version	Description
	2.02	The service kabinet command has been introduced.

3.146 service mdns

Description Enable *mDNS* service. By default, service is enabled.
Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service mdns
(config)> no service mdns
```

Example

```
(config)>service mdns
(config)>no service mdns
```

History	Version	Description
	2.15	The service mdns command has been introduced.

3.147 service mws

Description Enable *MWS* service. By default, service is disabled.
Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service mws
(config)> no service mws
```

Example

```
(config)> service mws
Mws::Controller: Enabled.

(config)> no service mws
Mws::Controller: Disabled.
```

History

Version	Description
2.15	The service mws command has been introduced.

3.148 service ntce

Description Enable *NTCE* service. By default it is disabled.
Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service ntce
(config)> no service ntce
```

Example

```
(config)> service ntce
Ntce::Manager: Enabled.
```

History

Version	Description
2.09	The service ntce command has been introduced. Previous command name is service dpi .

3.149 service ntp

Description Enable *NTP* service. By default it is enabled.
Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service ntp
(config)> no service ntp
```

Example

```
(config)> service ntp
Ntp::Client: NTP service enabled.

(config)> no service ntp
Ntp::Client: NTP service disabled.
```


History	Version	Description
	3.09	The service ntp command has been introduced. Previous command name is service ntp-client .

3.150 service oc-server

Description Enable [OpenConnect](#) server.
Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service oc-server
(config)> no service oc-server
```

Example

```
(config)> service oc-server
OcServer::Manager: Service enabled.
```

```
(config)> no service oc-server
OcServer::Manager: Service disabled.
```

History	Version	Description
	4.02	The service oc-server command has been introduced.

3.151 service snmp

Description Enable [SNMP](#) service. By default, the service is disabled.
Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service snmp
(config)> no service snmp
```

Example

```
(config)> service snmp
Snmp::Manager: SNMP service was enabled.
```

```
(config)> no service snmp
Snmplib::Manager: SNMP service was disabled.
```

History

Version	Description
2.08	The service snmp command has been introduced.

3.152 service ssh

Description

Enable the SSH server that provides the user with command line interface to configure the device.

Command with **no** prefix stops the service.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> service ssh
```

```
(config)> no service ssh
```

Example

```
(config)> service ssh
Ssh::Manager: SSH server enabled.
```

```
(config)> no service ssh
Ssh::Manager: SSH server disabled.
```

History

Version	Description
2.12	The service ssh command has been introduced.

3.153 service sstp-server

Description

Enable [SSTP](#) server.

Command with **no** prefix stops the service.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> service sstp-server
```

```
(config)> no service sstp-server
```

Example

```
(config)> service sstp-server
SstpServer::Manager: Service enabled.
```

```
(config)> no service sstp-server
SstpServer::Manager: Service disabled.
```

History	Version	Description
	2.12	The service sstp-server command has been introduced.

3.154 service telnet

Description Enable the telnet server that provides the user with command line interface to configure the device.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service telnet
```

```
(config)> no service telnet
```

Example

```
(config)> service tel
Telnet server enabled.
```

History	Version	Description
	2.00	The service telnet command has been introduced.

3.155 service torrent

Description Enable BitTorrent client that provides the user with peer-to-peer sharing of very large files, such as entire movies and TV shows.

Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service torrent
```

```
(config)> no service torrent
```

Example

```
(config)> service torrent
server enabled.
```

History

Version	Description
2.00	The service torrent command has been introduced.

3.156 service udpxy

Description

Enable *udpxy* service.

Command with **no** prefix stops the service.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> service udpxy
```

```
(config)> no service udpxy
```

Example

```
(config)> service udpxy
Udpxy::Manager: a service enabled.
```

History

Version	Description
2.03	The service udpxy command has been introduced.

3.157 service upnp

Description

Enable *UPnP* service.

Command with **no** prefix stops the service.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> service upnp
```

```
(config)> no service upnp
```

History	Version	Description
	2.00	The service upnp command has been introduced.

3.158 service vpn-server

Description Enable VPN server.
Command with **no** prefix stops the service.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> service vpn-server
(config)> no service vpn-server
```

Example

```
(config)> service vpn-server
VpnServer::Manager: Service enabled.

(config)> no service vpn-server
VpnServer::Manager: Service disabled.
```

History	Version	Description
	2.04	The service vpn-server command has been introduced.

3.159 show

Description Access to a group of commands to display various diagnostic information about system. All commands of this group do not change system settings.

Prefix no No

Change settings No

Multiple input No

Group entry (show)

Synopsis

```
(config)> show
```

History	Version	Description
	2.00	The show command has been introduced.

3.159.1 show access

Description Show user access for directory on USB drive.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> access <directory>`

Arguments

Argument	Value	Description
directory	<i>String</i>	Path to the folder on USB drive.

Example

```
(show)> access PENDRIVE:doc

      user:
        name: admin
        assigned: write
        effective: write
        exists: yes
      user:
        name: test
        assigned: read
        effective: read
        exists: yes
```

History

Version	Description
2.00	The show access command has been introduced.

3.159.2 show acme

Description Show *ACME* client status.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> acme`

Example

```
(show)> acme
acme:
  real-time: yes
  ndns-domain: mytest.keenetic.pro
  ndns-domain-acme: yes
```

```

ndns-domain-error: no
default-domain: cc6b5a71a7644903b51a5454.keenetic.io
account-pending: no
account-running: no
get-pending: no
get-running: no
revoke-pending: no
revoke-running: no
reissue-queue-size: 0
revoke-queue-size: 0
retries: 0
checker-timer: 82499
apply-timer: 0
acme-account: 36902346

```

History

Version	Description
2.11	The show acme command has been introduced.

3.159.3 show afp

Description Show [AFP](#) server status.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **afp**

Example

```

(show)> afp
    enabled: yes
    automount: yes
    permissive: yes

    share:
        mount: C253-062D:
        label: FLASH
    timemachine: yes
    description:
        active: yes

    share:
        mount: C253-062D:/FOR_AFP
        label: AFP
    timemachine: yes
    description:
        active: yes

```

History

Version	Description
2.06	The show afp command has been introduced.

3.159.4 show associations

Description

Show list of wireless stations associated with an access point. If you use no argument, the entire list of wireless stations will be displayed.

Prefix no

No

Change settings

No

Multiple input

No

Interface type

Access Point

Synopsis

```
(show)> associations [ <name> ]
```

Arguments

Argument	Value	Description
name	<i>String</i>	An access point name. You can see the list of available access points with help of associations [Tab] command.

Example

```
(show)> associations [Tab]
```

```
Usage template:
  associations [{name}]
```

```
Choose:
```

```
WifiMaster0/AccessPoint2
WifiMaster1/AccessPoint1
WifiMaster0/AccessPoint3
WifiMaster0/AccessPoint0
      AccessPoint
WifiMaster1/AccessPoint2
WifiMaster0/AccessPoint1
      GuestWiFi
WifiMaster1/AccessPoint3
WifiMaster1/AccessPoint0
      AccessPoint_5G
```

```
(show)> associations WifiMaster0/AccessPoint0
```

```
station:
    mac: ec:1f:72:d3:6d:3f
    ap: WifiMaster0/AccessPoint0
authenticated: 1
txrate: 130
```



```
        uptime: 3804
        txbytes: 2058837
        rxbytes: 25023483
        ht: 20
        mode: 11n
        gi: 800
        rssi: -26
        mcs: 15

    station:
        mac: 20:aa:4b:5c:09:0e
        ap: WifiMaster0/AccessPoint0
    authenticated: 1
        txrate: 270
        uptime: 19662
        txbytes: 19450396
        rxbytes: 70800065
        ht: 40
        mode: 11n
        gi: 800
        rssi: -41
        mcs: 15
```

History

Version	Description
2.00	The show associations command has been introduced.

3.159.5 show button

Description Show information about specified system button. If you use no argument, the entire list of all buttons on the device will be displayed. Available buttons depend on hardware configuration.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **button** [*<name>*]

Arguments

Argument	Value	Description
name	String	The button name.

Example

```
(show)> button FN1

    buttons:
        button, name = FN1:
            is_switch: no
            position: 2
```

```
position_count: 2
clicks: 0
elapsed: 0
hold_delay: 3000
```

History

Version	Description
2.00	The show button command has been introduced.

3.159.6 show button bindings

Description Show a list of actions associated with device buttons.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **button bindings**

Example

```
(show)> button bindings

bindings:

    binding, index = 0:
        button: RESET
        action: click
        active_handler: Reboot
        default_handler: Reboot
        protected: yes

    binding, index = 1:
        button: RESET
        action: hold
        active_handler: FactoryReset
        default_handler: FactoryReset
        protected: yes

    binding, index = 2:
        button: WLAN
        action: click
        active_handler: WpsStartMainAp
        default_handler: WpsStartMainAp
        protected: no

    binding, index = 3:
        button: WLAN
        action: double-click
        active_handler: WpsStartMainAp5
        default_handler: WpsStartMainAp5
```

```
protected: no

binding, index = 4:
    button: WLAN
    action: hold
active_handler: WifiToggle
default_handler: WifiToggle
protected: no

binding, index = 5:
    button: FN1
    action: click
active_handler: UnmountUsb1
default_handler: UnmountUsb1
protected: no

binding, index = 6:
    button: FN1
    action: double-click
active_handler:
default_handler:
protected: no

binding, index = 7:
    button: FN1
    action: hold
active_handler:
default_handler:
protected: no

binding, index = 8:
    button: FN2
    action: click
active_handler: UnmountUsb2
default_handler: UnmountUsb2
protected: no

binding, index = 9:
    button: FN2
    action: double-click
active_handler:
default_handler:
protected: no

binding, index = 10:
    button: FN2
    action: hold
active_handler:
default_handler:
protected: no
```

History

Version	Description
2.03	The show button bindings command has been introduced.

3.159.7 show button handlers

Description Show a list of available button handlers in the system.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **button handlers**

Example

```
(show)> button handlers

handlers:
  handler, name = LedToggle:
short_description: toggle system LED states
  protected: no
  switch_related: no

  handler, name = FactoryReset:
short_description: reset a configuration to factory ►
defaults
  protected: yes
  switch_related: no

  handler, name = UnmountUsb1:
short_description: unmount USB 1 port storages
  protected: no
  switch_related: no

  handler, name = UnmountUsb2:
short_description: unmount USB 2 port storages
  protected: no
  switch_related: no

  handler, name = Reboot:
short_description: reboot the system
  protected: yes
  switch_related: no

  handler, name = DlnaDirectoryRescan:
short_description: rescan DLNA directory for newer media ►
files
  protected: no
  switch_related: no
```

```

        handler, name = DlnaDirectoryFullRescan:
        short_description: remove a DLNA database and rescan a ►
DLNA directory
        protected: no
        switch_related: no

        handler, name = DectHandsetRegistrationToggle:
        short_description: toggle a DECT handset registration
        protected: no
        switch_related: no

        handler, name = DectHandsetPagingToggle:
        short_description: toggle a DECT handset paging
        protected: no
        switch_related: no

        handler, name = OpkgRunScript:
        short_description: run Opkg script
        protected: no
        switch_related: no

        handler, name = TorrentAltSpeedToggle:
        short_description: toggle a Torrent alternative speed ►
mode
        protected: no
        switch_related: no

        handler, name = TorrentClientStateToggle:
        short_description: toggle a Torrent client state
        protected: no
        switch_related: no

        handler, name = WifiToggle:
        short_description: on/off all Wi-Fi interfaces
        protected: no
        switch_related: no

        handler, name = WpsStartMainAp:
        short_description: start WPS (2.4 GHz main access point)
        protected: no
        switch_related: no

        handler, name = WpsStartMainAp5:
        short_description: start WPS (5 GHz main access point)
        protected: no
        switch_related: no

        handler, name = WifiGuestApToggle:
        short_description: toggle a guest access point state ►
(2.4 GHz)
        protected: no
        switch_related: no

        handler, name = WpsStartStation:

```

```

short_description: start WPS (2.4 GHz Wi-Fi station)
  protected: no
  switch_related: no

  handler, name = WpsStartStation5:
short_description: start WPS (5 GHz Wi-Fi station)
  protected: no
  switch_related: no

```

History

Version	Description
2.03	The show button handlers command has been introduced.

3.159.8 show chilli profiles

Description Show the list of available [RADIUS](#) server profiles.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **chilli profiles**

Example (show)> **chilli profiles**

```

profile:
  name: Iron Wi-Fi
  url: https://www.ironwifi.com/
  description: Hosted RADIUS and Captive Portal

  preset:
    uamserver: ►
https://europe-west3.ironwifi.com/api/pages/uam/

    radius:
      server1: 35.198.88.176

  radiuslocationid:

    dns:
      dns1: 8.8.8.8
      dns2: 8.8.4.4

  custom: uamsecret

  custom: radiussecret

  custom: radiusnasid

```

History	Version	Description
	2.10	The show chilli profiles command has been introduced.

3.159.9 show cifs

Description Show *CIFS* server status.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **cifs**

Example (show)> **cifs**

```

    enabled: yes

    master: no

    automount: yes

    permissive: yes

    share:
        mount: 9430B54530B52EDC:
        label: 9430B54530B52EDC
    description:
        active: no

```

History	Version	Description
	2.00	The show cifs command has been introduced.

3.159.10 show clock date

Description Show the current system date.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **clock date**

Example (show)> **clock date**

```

weekday: 4
  day: 18
  month: 1
  year: 2018
  hour: 8
  min: 46
  sec: 2
  msec: 660
  dst: inactive

  tz:
    locality: GMT
    stdoffset: 0
    dstoffset: 0
    usesdst: no
    rule: GMT0
    custom: no

```

History

Version	Description
2.00	The show clock date command has been introduced.

3.159.11 show clock timezone-list

Description Show the list of available timezones.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **clock timezone-list**

Example (show)> **clock timezone-list**

```

timezones:
  tz:
    locality: Adak
    stdoffset: -36000
    dstoffset: -32400
  tz:
    locality: Aden
    stdoffset: 10800
    dstoffset: -1
  tz:
    locality: Almaty
    stdoffset: 21600
    dstoffset: -1
  tz:
    locality: Amsterdam

```



```

stdoffset: 3600
dstoffset: 7200
  tz:
    locality: Anadyr
stdoffset: 43200
dstoffset: -1
...
...
...

```

History

Version	Description
2.00	The show clock timezone-list command has been introduced.

3.159.12 show components status

Description Display components updates status.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **component status**

Example

```

(show)> components status

      update:
        state: idle

(show)> components status

      update:
        state: running
        progress: 41

```

History

Version	Description
4.00	The show components status command has been introduced.

3.159.13 show configurator status

Description Show information about system configurator.

Prefix no No

Change settings No

Multiple input

No

Synopsis`(show)> configurator status`**Example**

```
(show)> configurator status

touch: Thu, 18 Oct 2018 14:37:25 GMT

    header, name = Model: Keenetic Giga

    header, name = Version: 2.06.1

    header, name = Agent: http/rci

    header, name = Last change: Thu, 18 Oct 2018 14:37:25 GMT

    serving:
        name: Session /var/run/ndm.core.socket
        time: 0.000397

    request, host = 192.168.1.42, name = admin:
        parse: show configurator status
```

History

Version	Description
2.06	The show configurator status command has been introduced.

3.159.14 show credits

Description

Show the license information about specified installed package in KeeneticOS. If you use no argument, the entire list of all installed packages on the device will be displayed.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis`(show)> credits [ <package> ]`**Arguments**

Argument	Value	Description
package	<i>String</i>	Package name.

Example

```
(show)> credits

package:
```

```

        name: accel-ppp
        title: High performance accel-ppp VPN server
        homepage: https://accel-ppp.org/

package:
    name: accel-ppp-l2tp
    title: L2TP plugin for accel-ppp
    homepage: https://accel-ppp.org/

package:
    name: accel-ppp-pptp
    title: PPTP plugin for accel-ppp
    homepage: https://accel-ppp.org/

package:
    name: accel-ppp-sstp
    title: SSTP plugin for accel-ppp
    homepage: https://accel-ppp.org/

package:
    name: avahi-daemon
    title: An mDNS/DNS-SD implementation (daemon)
    homepage: http://www.avahi.org/

package:
    name: coova-chilli
    title: Wireless LAN HotSpot controller (Coova ►
Chilli Version)
    homepage: http://www.coova.org/CoovaChilli

package:
    name: crconf
    title: Netlink-based CryptoAPI userspace ►
management utility
    homepage:

package:
    name: dhcpv6
    title: DHCPv6 client + server
    homepage: http://wide-dhcpv6.sourceforge.net/

package:
    name: dropbear
    title: Small SSH2 client/server
    homepage: http://matt.ucc.asn.au/dropbear/

package:
    name: iperf3-ssl
    title: Internet Protocol bandwidth measuring ►
tool with iperf_auth support
    homepage: https://github.com/esnet/iperf

package:
    name: kernel

```

```
    title: Linux kernel
    homepage: http://www.kernel.org/

package:
    name: kmod-ipt-account
    title: ACCOUNT netfilter module
    homepage:

package:
    name: kmod-ipt-chaos
    title: CHAOS netfilter module
    homepage:

package:
    name: kmod-ipt-compat-xtables
    title: API compatibilty layer netfilter module
    homepage:

package:
    name: kmod-ipt-condition
    title: Condition netfilter module
    homepage:

package:
    name: kmod-ipt-delude
    title: DELUDE netfilter module
    homepage:

package:
    name: kmod-ipt-dhcpmac
    title: DHCPMAC netfilter module
    homepage:

package:
    name: kmod-ipt-dnetmap
    title: DNETMAP netfilter module
    homepage:

package:
    name: kmod-ipt-fuzzy
    title: fuzzy netfilter module
    homepage:

package:
    name: kmod-ipt-geoip
    title: geoip netfilter module
    homepage:

package:
    name: kmod-ipt-iface
    title: iface netfilter module
    homepage:

package:
```

```
        name: kmod-ipt-ipmark
        title: IPMARK netfilter module
homepage:

package:
    name: kmod-ipt-ipp2p
    title: IPP2P netfilter module
homepage:

package:
    name: kmod-ipt-ipv4options
    title: ipv4options netfilter module
homepage:

package:
    name: kmod-ipt-length2
    title: length2 netfilter module
homepage:

package:
    name: kmod-ipt-logmark
    title: LOGMARK netfilter module
homepage:

package:
    name: kmod-ipt-lscan
    title: lscan netfilter module
homepage:

package:
    name: kmod-ipt-netflow
    title: Netflow netfilter module for Linux kernel
homepage: http://ipt-netflow.sourceforge.net/

package:
    name: kmod-ipt-psd
    title: psd netfilter module
homepage:

package:
    name: kmod-ipt-quota2
    title: quota2 netfilter module
homepage:

package:
    name: kmod-ipt-sysrq
    title: SYSRQ netfilter module
homepage:

package:
    name: kmod-ipt-tarpit
    title: TARPIT netfilter module
homepage:
```

```

package:
  name: kmod-nf-nathelper-rtsp
  title: RTSP Conntrack and NAT helpers
  homepage: https://github.com/maru-sama/rtsp-linux

package:
  name: kmod-wireguard
  title: WireGuard kernel module
  homepage:

package:
  name: libattr
  title: Extended attributes (xattr) manipulation ►
library
  homepage: http://savannah.nongnu.org/projects/attr

package:
  name: libav
  title: This package contains Libav library
  homepage: https://libav.org/

package:
  name: libavahi
  title: An mDNS/DNS-SD implementation (No D-Bus)
  homepage: http://www.avahi.org/

package:
  name: libcurl
  title: A client-side URL transfer library
  homepage: http://curl.haxx.se/

package:
  name: libdaemon
  title: A lightweight C library that eases the ►
writing of UNIX daemons
  homepage: ►
http://0pointer.de/lennart/projects/libdaemon/

package:
  name: libdb47
  title: Berkeley DB library (4.7)
  homepage: http://www.sleepycat.com/products/db.shtml

package:
  name: libevent
  title: Event notification library
  homepage: http://www.monkey.org/~provos/libevent/

package:
  name: libexif
  title: Library for JPEG files with EXIF tags
  homepage: https://libexif.github.io

package:

```

```

        name: libexpat
        title: An XML parsing library
        homepage: https://libexpat.github.io/

    package:
        name: libgcrypt
        title: GNU crypto library
        homepage: ►
http://directory.fsf.org/security/libgcrypt.html

    package:
        name: libgpg-error
        title: GnuPG error handling helper library
        homepage: ►
http://www.gnupg.org/related_software/libgpg-error/

    package:
        name: libid3tag
        title: An ID3 tag manipulation library
        homepage: https://www.underbit.com/products/mad/

    package:
        name: libjpeg
        title: The Independent JPEG Group's JPEG runtime ►
library
        homepage: http://www.ijg.org/

    package:
        name: liblzo
        title: A real-time data compression library
        homepage: http://www.oberhumer.com/opensource/lzo/

    package:
        name: libnghttp2
        title: Library implementing the framing layer ►
of HTTP/2
        homepage: https://nghttp2.org/

    package:
        name: libopenssl
        title: Open source SSL toolkit (libraries ►
(libcrypto.so, libssl.so))
        homepage: http://www.openssl.org/

    package:
        name: libpcap
        title: Low-level packet capture library
        homepage: http://www.tcpdump.org/

    package:
        name: libtommath
        title: A free number theoretic multiple-precision ►
integer library
        homepage: https://www.libtom.net/

```

```
package:
  name: libusb
  title: A library for accessing Linux USB devices
  homepage: http://libusb.info/

package:
  name: mini_snmpd
  title: Lightweight SNMP daemon
  homepage: http://troglobit.github.io/mini-snmpd.html

package:
  name: minidlna
  title: UPnP A/V & DLNA Media Server
  homepage: http://minidlna.sourceforge.net/

package:
  name: miniupnpd
  title: Lightweight UPnP daemon
  homepage: http://miniupnp.tuxfamily.org/

package:
  name: netatalk
  title: netatalk
  homepage: http://netatalk.sourceforge.net

package:
  name: nginx
  title: Nginx web server
  homepage: http://nginx.org/

package:
  name: nginx-stream-module
  title: Nginx stream module
  homepage:

package:
  name: openvpn
  title: Open source VPN solution using OpenSSL
  homepage: http://openvpn.net

package:
  name: pjproject
  title: PJSIP
  homepage: http://www.pjsip.org/

package:
  name: pureftpd
  title: FTP server
  homepage: http://www.pureftpd.org

package:
  name: radvd
  title: Router advertisement daemon
```



```

    homepage: http://www.litech.org/radvd/

    package:
      name: sstp-client
      title: SSTP client for Linux
      homepage: http://sstp-client.sourceforge.net/

    package:
      name: strongswan
      title: Strongswan IKEv1/IKEv2 ISAKMP and IPsec
suite      homepage: https://www.strongswan.org/

    package:
      name: transmission-daemon
      title: A free, lightweight BitTorrent client
      homepage: http://www.transmissionbt.com

    package:
      name: tspc
      title: TSP client
      homepage: http://www.broker.ipv6.ac.uk

    package:
      name: tzdata
      title: Timezone data files
      homepage: https://www.iana.org/time-zones

    package:
      name: udpxy
      title: Convert UDP IPTV streams into HTTP stream
      homepage: http://sourceforge.net/projects/udpxy

    package:
      name: zlib
      title: Library implementing the deflate
compression method      homepage: http://www.zlib.net/

```

```
(show)> credits nginx
```

```

    copying: /*
      * Copyright (C) 2002-2019 Igor Sysoev
      * Copyright (C) 2011-2019 Nginx, Inc.
      * All rights reserved.
      *
      * Redistribution and use in source and binary
forms, with or without      * modification, are permitted provided that
the following conditions    * are met:
      * 1. Redistributions of source code must
retain the above copyright  * notice, this list of conditions and the

```

```

following disclaimer.
    * 2. Redistributions in binary form must ►
reproduce the above copyright
    * notice, this list of conditions and the ►
following disclaimer in the
    * documentation and/or other materials ►
provided with the distribution.
    *
    * THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND ►
CONTRIBUTORS ``AS IS'' AND
    * ANY EXPRESS OR IMPLIED WARRANTIES, ►
INCLUDING, BUT NOT LIMITED TO, THE
    * IMPLIED WARRANTIES OF MERCHANTABILITY AND ►
FITNESS FOR A PARTICULAR PURPOSE
    * ARE DISCLAIMED. IN NO EVENT SHALL THE ►
AUTHOR OR CONTRIBUTORS BE LIABLE
    * FOR ANY DIRECT, INDIRECT, INCIDENTAL, ►
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
    * DAMAGES (INCLUDING, BUT NOT LIMITED TO, ►
PROCUREMENT OF SUBSTITUTE GOODS
    * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; ►
OR BUSINESS INTERRUPTION)
    * HOWEVER CAUSED AND ON ANY THEORY OF ►
LIABILITY, WHETHER IN CONTRACT, STRICT
    * LIABILITY, OR TORT (INCLUDING NEGLIGENCE ►
OR OTHERWISE) ARISING IN ANY WAY
    * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ►
ADVISED OF THE POSSIBILITY OF
    * SUCH DAMAGE.
    */

```

History

Version	Description
3.01	The show credits command has been introduced.

3.159.15 show crypto ike key

Description Show info about selected *IKE* key. If you use no argument, the entire list of *IKE* keys will be displayed.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **crypto ike key** [*name*]

Arguments

Argument	Value	Description
name	<i>String</i>	Name of selected <i>IKE</i> key.

Example

```
(show)> crypto ike key

IpSec:
  ike_key, name = test:
    type: address
    id: 10.10.10.10

    ike_key, name = test2:
      type: any
      id: ►
```

History

Version	Description
2.06	The show crypto ike key command has been introduced.

3.159.16 show crypto map

Description

Show info about selected *IPsec* crypto map. If you use no argument, the entire list of *IPsec* crypto maps will be displayed.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(show)> crypto map [map-name]
```

Arguments

Argument	Value	Description
map-name	<i>String</i>	Name of selected crypto map.

Example

```
(show)> crypto map test

IpSec:
  crypto_map, name = test:
    config:
      remote_peer: ipsec.example.com
      crypto_ipsec_profile_name: prof1
      mode: tunnel

      local_network:
        net: 172.16.200.0
        mask: 24
        protocol: IPv4

      remote_network:
        net: 172.16.201.0
        mask: 24
        protocol: IPv4
```

```

status:
primary_peer: true

phase1:
    name: test
    unique_id: 572
    ike_state: ESTABLISHED
establish_time: 1451301596
rekey_time: 0
reauth_time: 1451304277
local_addr: 10.10.10.15
remote_addr: 10.10.10.20
ike_version: 2
    local_spi: 00a6ebfc9d90f1c2
    remote_spi: 3cd201ef496df75c
    local_init: yes
    ike_cypher: aes-cbc-256
    ike_hmac: sha1
    ike_dh_group: 2

phase2_sa_list:
    phase2_sa, index = 0:
        unique_id: 304
        request_id: 185
        sa_state: INSTALLED
        mode: TUNNEL
        protocol: ESP
    encapsulation: yes
        local_spi: ca59bfcf
        remote_spi: cde23d83
    ipsec_cypher: esp-aes-256
    ipsec_hmac: esp-sha1-hmac
    ipsec_dh_group:
        in_bytes: 7152
        in_packets: 115
        in_time: 1451302507
        out_bytes: 6008
        out_packets: 98
        out_time: 1451302507
        rekey_time: 1451305159
        local_ts: 172.16.200.0/24
        remote_ts: 172.16.201.0/24

state: PHASE2_ESTABLISHED

```

History

Version	Description
2.06	The show crypto map command has been introduced.

3.159.17 show defaults**Description**

Show the general default wireless and system parameters.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **defaults**

Example

```
(show)> defaults

servicetag: *****92181
servicehost: ndss.*.*
servicepass: *****
wlanssid: Keenetic-0000
wlankey: *****
wlanwps: *****
country: EA
ndmhwid: KN-1012
product: Giga
ctrlsum: a*****a4096b06a0f178abab3f2647d
serial: S****WF*****
signature: valid
integrity: ok
locked: yes
```

History	Version	Description
	2.00	The show defaults command has been introduced.

3.159.18 show dlna

Description Show DLNA server status.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **dlna**

Example

```
(show)> dlna

running: yes
```

History	Version	Description
	2.00	The show dlna command has been introduced.

3.159.19 show dns-proxy

Description Show a list of current *DNS over TLS* and *DNS over HTTPS* servers.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **dns-proxy**

Example (show)> **dns-proxy**

```

    proxy-status:
        proxy-name: System

    proxy-config:

rpc_port = 54321
rpc_ttl = 10000
rpc_wait = 10000
timeout = 7000
proceed = 500
stat_file = /var/ndnproxymain.stat
stat_time = 10000
dns_server = 127.0.0.1:40500 .
dns_server = 127.0.0.1:40501 .
dns_server = 127.0.0.1:40508 .
dns_server = 127.0.0.1:40509 .
static_a = my.keenetic.net 78.47.125.180
static_a = cc6b5a71a7644903b51a5454.keenetic.io 78.47.125.180
static_a = myhome23.keenetic.pro 78.47.125.180
set-profile-ip 127.0.0.1 0
set-profile-ip ::1 0
dns_tcp_port = 53
dns_udp_port = 53

    proxy-stat:

# ndnproxy statistics file

Total incoming requests: 809
Proxy requests sent:      659
Cache hits ratio:        0.192 (155)
Memory usage:            44.41K

DNS Servers

      Ip      Port  R.Sent  A.Rcvd  NX.Rcvd  ►
Med.Resp Avg.Resp Rank
      127.0.0.1 40500      2      2      0      ►
40ms      40ms    10

```

```
17ms      127.0.0.1 40501    652    651    0    ►
17ms      10
17ms      127.0.0.1 40508    2      0      0    ►
0ms       4
0ms       127.0.0.1 40509    3      1      0    ►
326ms     326ms    3

    proxy-safe:

    proxy-tls:
    server-tls:
        address: 1.1.1.1
        port: 853
        sni: cloudflare-dns.com
        spki:
        interface:

    server-tls:
        address: 8.8.8.8
        port: 853
        sni: dns.google.com
        spki:
        interface:

    proxy-tls-filters:

    proxy-https:
    server-https:
        uri: https://dns.adguard.com/dns-query
        format: dns
        spki:
        interface:

    server-https:
        uri: ►
https://cloudflare-dns.com/dns-query?ct=application/dns-json
        format: json
        spki:
        interface:

    proxy-https-filters:
```

History

Version	Description
3.01	The show dns-proxy command has been introduced.

3.159.20 show dns-proxy filter presets

Description Show the list of filtering presets. There is always at least 1 preset, but can be many more.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> dns-proxy filter presets [ <lang> ]`

Arguments

Argument	Value	Description
lang	<i>String</i>	Language to show in “description” and “short-description” fields. If requested lang is absent English version will be returned.

Output

Element	Description
description	Long readable profile description. Has translation map.
id	Short name to be used in dns-proxy commands.
short-description	Short description to be used in combo-boxes and titles. Has translation map.
stale	Set to true when preset is obsolete and no longer works.

Example

```
(show)> dns-proxy filter presets en

version: 4

presets:
  id: opendns-family
  url: ▶
https://www.opendns.com/home-internet-security/
  stale: no
  short-description: OpenDNS - FamilyShield
  description: Blocks domains that are categorized as ▶
Tasteless, Proxy/Anonymizer, Sexuality and Pornography.

presets:
  id: quad9-security
  url: https://quad9.net/home/individuals/
  stale: no
  short-description: Quad9 - Security Protection
  description: Blocks malicious hostnames to protect ▶
against a wide range of threats such as malware, phishing, ▶
spyware, and botnets. Improves performance in addition to ▶
guaranteeing
privacy.

presets:
  id: cleanbrowsing-security
  url: https://cleanbrowsing.org/filters
  stale: no
```



```

short-description: CleanBrowsing - Security Filter
description: Blocks access to phishing, spam, malware ▶
and malicious domains. Our database of malicious domains is ▶
updated hourly and considered to be one of the best in the ▶
industry.

Note that it does not block adult content.

presets:
  id: cleanbrowsing-adult
  url: https://cleanbrowsing.org/filters
  stale: no
short-description: CleanBrowsing - Adult Filter
description: Blocks access to all adult, pornographic ▶
and explicit sites. It does not block proxy or VPNs, nor ▶
mixed-content sites. Sites like Reddit are allowed. Google and ▶
Bing are set
to the Safe Mode. Malicious and Phishing ▶
domains are blocked.

```

History

Version	Description
3.08	The show dns-proxy filter presets command has been introduced.

3.159.21 show dns-proxy filter profiles

Description Show the list of filtering profiles.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **dns-proxy filter profiles**

Example (show)> **dns-proxy filter profiles**

```

profiles:
  id: DnsProfile0
  description: test

```

History

Version	Description
3.08	The show dns-proxy filter profiles command has been introduced.

3.159.22 show dpn document

Description Show *DPN* agreement text.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> dpn document [ <version> ] [ <language> ]`

Arguments

Argument	Value	Description
version	<i>String</i>	Version of <i>DPN</i> . If not specified, the latest version is shown.
language	<i>String</i>	The language of <i>DPN</i> . If not specified, the English version is shown.

Example

```
(show)> dpn document
20200330

DEVICE PRIVACY NOTICE

Last update 2020-30-03

This End User License Agreement (this "Agreement") constitutes a valid and binding agreement between Keenetic Limited, including all affiliates and subsidiaries ("Keenetic", "us", "our" or "we") and You (as defined below) of the Software (as defined below), including the Software installed onto any one of our Keenetic products (the "Product") and/or the Software legally obtained from or provided by an App Platform (as defined below) authorised by Keenetic. Keenetic and You shall be collectively referred to as the "Parties", and individually as a "Party".
```

```
(show)> dpn document 20200330 es
20200330

CONTRATO DE LICENCIA DEL USUARIO FINAL

Última actualización 30/03/2020

El presente contrato de licencia del usuario final (el presente Contrato) constituye un acuerdo válido y vinculante celebrado entre Keenetic
```

Limited, incluidas todas las filiales y sucursales ("Keenetic", "nosotros", "nuestro/a" o "nos") y Usted (tal y como se define a continuación) del Software (tal y como se define a continuación), ► incluido el Software instalado en cualquiera de nuestros productos de ► Keenetic (el "Producto") y/o el Software obtenido o proporcionado legalmente ► por la Plataforma de la aplicación (tal y como se define a continuación) autorizado por Keenetic. Se referirá a Keenetic y Usted, en ► conjunto, como las "Partes" y, de forma individual, como una "Parte".

History

Version	Description
3.05	The show dpn document command has been introduced.

3.159.23 show dpn list

Description Show the list of [DPN](#) available in the system.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **dpn list**

Example

```
(show)> dpn list
      dpn:
        version: 20200330

      document:
        lang: de
        format: txt
        format: md

      document:
        lang: en
        format: txt
        format: md

      document:
        lang: es
        format: txt
```

```
format: md
document:
  lang: fr
format: txt
format: md
document:
  lang: it
format: txt
format: md
document:
  lang: pl
format: txt
format: md
document:
  lang: pt
format: txt
format: md
document:
  lang: ru
format: txt
format: md
document:
  lang: sv
format: txt
format: md
document:
  lang: tr
format: txt
format: md
document:
  lang: uk
```

```
format: txt

format: md
```

History

Version	Description
3.05	The show dpn list command has been introduced.

3.159.24 show dot1x

Description Show 802.1x client status on the interface. To manage 802.1x client status on the interface authentication must be configured with [interface authentication](#) group of commands.

Prefix no No

Change settings No

Interface type Ethernet

Multiple input No

Synopsis (show)> **dot1x** [*interface*]

Argument	Value	Description
interface	<i>Interface</i>	An Ethernet interface name. You can see the list of available Ethernet interfaces with help of dot1x [Tab] command.

Example

```
(show)> dot1x [Tab]

Usage template:
    dot1x [{name}]

Choose:
    GigabitEthernet1
    ISP
WifiMaster0/AccessPoint2
WifiMaster1/AccessPoint1
WifiMaster0/AccessPoint3
WifiMaster0/AccessPoint0
    AccessPoint
```

```
(show)> dot1x ISP

dot1x:
    id: FastEthernet0/Vlan2
    state: CONNECTING
```

History

Version	Description
2.02	The show dot1x command has been introduced.

3.159.25 show drivers

Description Show the list of loaded kernel drivers.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **drivers**

Example

```
(show)> drivers

module:
  name: rt2860v2_sta
  size: 546736
  used: 0
  subs: -
module:
  name: rt2860v2_ap
  size: 554192
  used: 2
  subs: -
module:
  name: rndis_host
  size: 5024
  used: 0
  subs: -
module:
  name: dwc_otg
  size: 68416
  used: 0
  subs: -
module:
  name: lm
  size: 1344
  used: 1
  subs: dwc_otg,[permanent]
...
...
...
```

History

Version	Description
2.00	The show drivers command has been introduced.

3.159.26 show dyndns updaters

Description Show the list of available DynDNS providers.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **dyndns updaters**

Example (show)> **dyndns updaters**

```

    updater:
      type: dyndns
      url: https://account.dyn.com/dns/dyndns
      api: http://members.dyndns.org/nic/update

    updater:
      type: noip
      url: https://www.noip.com/
      api: http://dynupdate.no-ip.com/nic/update

```

History

Version	Description
2.12	The show dyndns updaters command has been introduced.

3.159.27 show easyconfig status

Description Show EasyConfig status and settings.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **easyconfigstatus**

Example (show)> **easyconfig status**

```

    easyconfig:
      checked: Tue Aug  6 11:50:21 2019
      enabled: yes
      reliable: yes
    gateway-accessible: yes
      dns-accessible: yes
      host-accessible: yes
      internet: yes

```

```

gateway:
  interface: GigabitEthernet1
  address: 193.0.175.2
  failures: 0
accessible: yes
excluded: no

hosts:
  host:
    name: google.com
  failures: 0
  resolved: no
  accessible: no

```

History

Version	Description
2.00	The show easyconfig status command has been introduced.

3.159.28 show eula document

Description Show [EULA](#) agreement text.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> eula document [ <version> ] [ <language> ]`

Arguments

Argument	Value	Description
version	<i>String</i>	Version of EULA . If not specified, the latest version is shown.
language	<i>String</i>	The language of EULA . If not specified, the English version is shown.

Example

```

(show)> eula document 20181001
20181001

KEENETIC LIMITED
End User License Agreement

This End User License Agreement (this "Agreement") constitutes ►
a valid and binding agreement between Keenetic Limited, including ►
all affiliates and subsidiaries ("Keenetic", "us", "our" or "we") ►
and You (as
defined below) of the Software (as defined below), including the ►
Software installed onto any one of our Keenetic products (the ►
"Product") and/or the Software legally obtained from or provided ►

```



```
by an App Platform
(as defined below) authorised by Keenetic. Keenetic and You shall ►
be collectively referred to as the “Parties”, and individually ►
as a “Party”.
```

```
(show)> eula document 20181001 ru
20181001

KEENETIC LIMITED
Лицензионное соглашение с конечным пользователем

Настоящее Лицензионное соглашение с конечным пользователем ►
(настоящее «Соглашение») представляет собой действительное и ►
обязательное соглашение между Keenetic Limited, включая все ►
связанные с ней компании и все
её подразделения («Keenetic», «нам», «наш» или «мы»), и Вами ►
(как определено ниже) о Программном обеспечении (как определено ►
ниже), включая Программное обеспечение, устанавливаемое на любом ►
из продуктов
производства Keenetic («Продукт») и/или Программное обеспечение, ►
полученное на законных основаниях или предоставленное Магазином ►
Приложений (как определено ниже), авторизованной Keenetic. ►
Keenetic и Вы вместе
упоминаетесь как «Стороны», а по отдельности – «Сторона».
```

History

Version	Description
2.15	The show eula document command has been introduced.

3.159.29 show eula list

- Description** Show the list of *EULA* available in the system.
- Prefix no** No
- Change settings** No
- Multiple input** No

Synopsis (show)> eula list

```
(show)> eula list
eula:
  version: 20181001

  document:
    lang: en

    format: md

    format: txt
```

```

document:
    lang: ru

    format: md

    format: txt

document:
    lang: tr

    format: md

    format: txt

document:
    lang: uk

    format: md

    format: txt

```

History

Version	Description
2.15	The show eula list command has been introduced.

3.159.30 show interface

Description Show information of specified interface. If you use no argument, the entire list of all network interfaces will be displayed.

Prefix no No

Change settings No

Multiple input No

Interface type IP

Synopsis (show)> **interface** *<name>*

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface to display.

Example**Example 3.1. Review the status of switch ports**

The command **show interface** displays different information depending on the interface type. In particular, for FastEthernet0 switch it shows current state of physical ports, speed and duplex, on top of general information.

```
(config)> show interface FastEthernet0
```

```

    id: GigabitEthernet0
    index: 0
    type: GigabitEthernet
description:
interface-name: GigabitEthernet0
    link: up
    connected: yes
    state: up
    mtu: 1500
    tx-queue: 2000

```

```

    port, name = 1:
        id: GigabitEthernet0/0
        index: 0
    interface-name: 1
        type: Port
        link: up
        speed: 1000
        duplex: full
    auto-negotiation: on
    flow-control: on
        eee: off
        last-change: 4578.185413
    last-overflow: 0
        public: no

```

```

    port, name = 2:
        id: GigabitEthernet0/1
        index: 1
    interface-name: 2
        type: Port
        link: down
        last-change: 4590.205656
    last-overflow: 0
        public: no

```

```

    port, name = 3:
        id: GigabitEthernet0/2
        index: 2
    interface-name: 3
        type: Port
        link: up

```

```

        role, for = GigabitEthernet0/Vlan2: inet

        speed: 100
        duplex: full
    auto-negotiation: on
    flow-control: off
        eee: off
        last-change: 4570.078144
    last-overflow: 0

```

```

        public: yes

        port, name = 4:
            id: GigabitEthernet0/3
            index: 3
        interface-name: 4
            type: Port
            link: down
            last-change: 4590.202571
            last-overflow: 0
            public: no

```

History

Version	Description
2.00	The show interface command has been introduced.

3.159.31 show interface antennas

Description Show antenna signal strength.

Prefix no No

Change settings No

Multiple input No

Interface type Usb

Synopsis

```
(show)> interface <name> antennas
```

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Output

Element	Description
channel	Antenna number.
rss_i	Received signal strength indicator.
rsrq	Reference signal received quality for 4G only.
rsrp	Reference signal received power for 4G only.
phase	Offset phase for 4G only.
ecio	Ratio of the received/good energy to the interference/bad energy for 3G only.

Example

```
(show)> interface UsbQmi0 antennas
```

```

    antenna:
      channel: 0
      rssi: -61
      rsrp: -81
      rsrq: -8
      phase: 0

    antenna:
      channel: 1
      rssi: -94
      rsrp: -120
      rsrq: -10
      phase: 6

```

History

Version	Description
3.05	The show interface antennas command has been introduced.

3.159.32 show interface bands

Description Show available 3G/LTE bands.

Prefix no No

Change settings No

Multiple input No

Interface type Usb

Synopsis (show)> **interface** *<name>* **bands**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```

(show)> interface UsbQmi0 bands

    umts:
      band: 1
      enabled: yes

    umts:
      band: 5
      enabled: yes

    lte:
      band: 1

```

```
enabled: yes
```

```
lte:
  band: 3
enabled: yes
```

```
lte:
  band: 7
enabled: yes
```

```
lte:
  band: 20
enabled: yes
```

History

Version	Description
3.05	The show interface bands command has been introduced.

3.159.33 show interface bridge

Description Display interface bridge status.

Prefix no No

Change settings No

Multiple input No

Interface type Bridge

Synopsis (show)> **interface** *<name>* **bridge**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface to display.

Output

Element	Value
members	Root node.
interface	Interface name.
link	Link state of interface.
inherited	Attribute of inheritance.

Example

```
(show)> interface Bridge1 bridge
```

```
members:
  interface, link = no, inherited = yes:
```

```

                                WifiMaster0/AccessPoint2
                                interface, link = yes: UsbLte0

```

History

Version	Description
2.03	The show interface bridge command has been introduced.

3.159.34 show interface cells

Description Show base stations in mobile networks.

Prefix no No

Change settings No

Multiple input No

Interface type Usb

Synopsis (show)> **interface** *<name>* **cells**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Output

Element	Description
phy-id	Cell identity (Cell ID).
rsi	Received signal strength indicator.

Example

```

(show)> interface UsbQmi0 cells

      cells:
        phy-id: fc
        rssi: -71

      cells:
        phy-id: 15b
        rssi: -71

      cells:
        phy-id: 187
        rssi: -72

```

History

Version	Description
3.05	The show interface cells command has been introduced.

3.159.35 show interface channel-utilization rrd

Description Show specific data from the channel utilization monitor.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(show)> interface <name> channel-utilization rrd <attribute> [
<detail>]
```

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the Wi-Fi interface.
attribute	load	Channel load percentage.
	valid	The data is valid.
detail	0	RRD detalization level 64 x 3-seconds. It is used by default if the parameter is not specified.
	1	RRD detalization level 64 x 1-minutes.
	2	RRD detalization level 64 x 3-minutes.
	3	RRD detalization level 64 x 30-minutes.

Example

```
(show)> interface WifiMaster1 channel-utilization rrd load 1
```

```
data:
    t: 578928.500000
    v: 0

data:
    t: 578868.500000
    v: 1

data:
    t: 578808.500000
    v: 1

data:
    t: 578748.500000
    v: 2

data:
    t: 578688.500000
    v: 1

data:
    t: 578628.500000
    v: 0
```



```

data:
    t: 578568.500000
    v: 1

data:
    t: 578508.500000
    v: 1

data:
    t: 578448.500000
    v: 1

data:
    t: 578388.500000
    v: 0

data:
    t: 578328.500000
    v: 1

data:
    t: 578268.500000
    v: 1

data:
    t: 578208.500000
    v: 1

data:
    t: 578148.500000
    v: 6

data:
    t: 578088.500000
    v: 1

data:
    t: 578028.500000
    v: 11

```

History

Version	Description
3.09	The show interface channel-utilization rrd command has been introduced.

3.159.36 show interface channels

Description Show information about the specified wireless interface channels.

Prefix no No

Change settings No

Multiple input No

Interface type Radio

Synopsis `(show)> interface <name> channels`

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface to display.

Output

Element	Value
channels	Root node.
channel, index	Record number in the list.
number	Channel number.
ext-40-above	Ability to expand channel above.
ext-40-below	Ability to expand channel below.
vht-80	Ability to expand channel up to 80 MHz.

Example

```
(show)> interface WifiMaster0 channels
```

```
channels:
  channel, index = 0:
    number: 1
    ext-40-above: yes
    ext-40-below: no
    vht-80: yes

  channel, index = 1:
    number: 2
    ext-40-above: yes
    ext-40-below: yes
    vht-80: yes

  channel, index = 2:
    number: 3
    ext-40-above: yes
    ext-40-below: yes
    vht-80: yes

  channel, index = 3:
    number: 4
    ext-40-above: yes
    ext-40-below: yes
    vht-80: yes

  channel, index = 4:
```

```

        number: 5
    ext-40-above: yes
    ext-40-below: yes
        vht-80: yes

    channel, index = 5:
        number: 6
    ext-40-above: yes
    ext-40-below: yes
        vht-80: yes

    channel, index = 6:
        number: 7
    ext-40-above: yes
    ext-40-below: yes
        vht-80: yes

    channel, index = 7:
        number: 8
    ext-40-above: yes
    ext-40-below: yes
        vht-80: yes
...
...
...

```

History

Version	Description
2.03	The show interface channels command has been introduced.

3.159.37 show interface chilli

Description Show information about statistics of connected clients to the [RADIUS](#) hotspot.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **interface** *<name>* **chilli**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface.

Example

```

(show)> interface Chilli0 chilli

        host:
        session-id: 4bf7c55f00000006

```

```

        user: 44w3c1
        ip: 10.1.30.3
        mac: 55:a3:f9:51:b4:11
    start-time: 3884
    end-time: 0
    idle-time: 9
idle-time-limit: 0
    tx-bytes: 695682
tx-bytes-limit: 0
    rx-bytes: 1627453
rx-bytes-limit: 0
    tx-speed: 0
tx-speed-limit: 0
    rx-speed: 0
rx-speed-limit: 0

```

History

Version	Description
2.10	The show interface chilli command has been introduced.

3.159.38 show interface country-codes

Description Show the list of available country codes on a radio interface.

Prefix no No

Change settings No

Multiple input No

Interface type Radio

Synopsis (show)> **interface** *<name>* **country-codes**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface to display.

Output

Element	Value
country-codes	Root node.
code	Country code.
country	Country name.

Example

```

(show)> interface WifiMaster0 country-codes

country-codes:
  country-code:
    code: AL

```

```

country: Albania

country-code:
  code: DZ
  country: Algeria

country-code:
  code: AR
  country: Argentina

country-code:
  code: AM
  country: Armenia

country-code:
  code: AU
  country: Australia
...
...
...

```

History

Version	Description
2.03	The show interface country-codes command has been introduced.

3.159.39 show interface mac

Description Show the table of MAC addresses of the switch.

Prefix no No

Change settings No

Multiple input No

Interface type Switch

Synopsis (show)> **interface** *<name>* **mac**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface to display.

Example

```

(show)> interface FastEthernet0 mac
=====
Port  MAC                      Aging
=====
0     b0:b2:dc:70:c4:28          6
0     f0:1b:21:6d:9a:c5          4

```

```

0      00:0c:43:76:20:77      6
0      b4:18:d1:6e:b5:6a      3
0      40:4a:03:78:01:af      2
0      84:8e:0c:3f:79:05      5
0      ec:43:f6:73:0a:99      6
0      ec:43:f6:04:2b:05      6
0      b2:b2:dc:5f:09:b3      1
0      ec:43:f6:72:4e:51      6
0      00:30:48:93:91:a7      6
0      f0:c1:f1:95:c3:fb      5
0      b8:ca:3a:8a:c7:43      6
0      ec:43:f6:da:78:79      5
0      10:7b:ef:59:7b:61      2
0      ec:43:f6:ff:f8:8b      6
0      58:8b:f3:65:8c:91      5
0      ec:43:f6:cf:0e:ef      2
0      00:ee:bd:a1:18:51      6
0      ec:43:f6:72:4e:69      6
0      90:e2:ba:07:9a:81      6
0      00:00:5e:00:01:01      6
0      00:08:9b:dc:8d:17      4
0      50:e5:49:58:2b:5a      6
0      90:e2:ba:07:99:55      6
0      ec:43:f6:04:36:8d      6
0      ec:43:f6:05:44:49      6
0      de:06:21:02:b3:e2      6
0      40:4a:03:60:80:05      6
0      00:0c:29:d5:84:c0      6
0      00:08:9b:dc:92:55      6
0      00:08:9b:dc:92:56      6
0      00:1b:0c:7f:b6:41      6
0      10:2a:b3:a6:86:18      5
0      10:7b:ef:df:83:a7      1
0      01:00:5e:00:00:fb      0
.....

```

History

Version	Description
2.00	The show interface mac command has been introduced.

3.159.40 show interface name-server

Description Show a list of current addresses of DNS resolvers used on the interface.

Prefix no No

Change settings No

Multiple input No

Synopsis | (show)> **interface** *<name>* **name-server**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface.

Example

```
(show)> interface WifiMaster1/WifiStation0 name-server

server:
  address: 1.1.1.1
  port: 0
  domain:
  global: 0
  service: Dns::Manager
  interface:

server:
  address: 9.9.9.9
  port: 0
  domain:
  global: 0
  service: Dns::Manager
  interface:

server:
  address: 8.8.8.8
  port: 0
  domain:
  global: 0
  service: Dns::Manager
  interface:

server:
  address: 192.168.133.1
  port: 0
  domain:
  global: 65318
  service: WifiMaster1/WifiStation0 DHCP client
  interface: WifiMaster1/WifiStation0

server-tls:
  address: 8.8.8.8
  port: 0
  sni: dns.google
  spki:
  interface:
  domain:
```

History

Version	Description
3.09	The show interface name-server command has been introduced.

3.159.41 show interface operators

Description Show list of available mobile operators. Before running this command, you must first run the network scan command [interface mobile scan](#). After the scan is complete, the list will be available until the modem is restarted.

Prefix no No

Change settings No

Multiple input No

Interface type Usb

Synopsis `(show)> interface <name> operators`

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(show)> interface UsbQmi0 operators

scanning: complete
age: 80

operator:
  plmn: 25011
  name: YOTA
  mobile: 4G

  status: used

  status: preferred

operator:
  plmn: 25099
  name: Beeline
  mobile: 4G

  status: available

  status: roaming

  status: forbidden

operator:
  plmn: 25020
  name: Tele2
  mobile: 3G

  status: available
```



```

        status: roaming

        status: forbidden

operator:
    plmn: 25001
    name: MTS
    mobile: 3G

    status: available

    status: roaming

    status: forbidden

operator:
    plmn: 25099
    name: Beeline
    mobile: 3G

    status: available

    status: roaming

    status: forbidden

operator:
    plmn: 25020
    name: Tele2
    mobile: 4G

    status: available

    status: roaming

    status: forbidden

operator:
    plmn: 25001
    name: MTS
    mobile: 4G

    status: available

    status: roaming

    status: forbidden

```

History

Version	Description
2.12	The show interface operators command has been introduced.

3.159.42 show interface rf e2p

Description Show the current contents of all calibration data cells.

Prefix no No

Change settings No

Multiple input No

Interface type Radio

Synopsis (show)> **interface** *<name>* **rf e2p**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface to display.

Example

```
(show)> interface WifiMaster0 rf e2p

[0x0000]:5392 [0x0002]:0103 [0x0004]:43EC [0x0006]:04F6
[0x0008]:042B [0x000A]:5392 [0x000C]:1814 [0x000E]:8001
[0x0010]:0000 [0x0012]:5392 [0x0014]:1814 [0x0016]:0000
[0x0018]:0001 [0x001A]:FF6A [0x001C]:0213 [0x001E]:FFFF
[0x0020]:FFFF [0x0022]:FFC1 [0x0024]:9201 [0x0026]:FFFF
[0x0028]:43EC [0x002A]:04F6 [0x002C]:052B [0x002E]:FFFF
[0x0030]:758E [0x0032]:4301 [0x0034]:FF22 [0x0036]:0025
[0x0038]:FFFF [0x003A]:012D [0x003C]:FFFF [0x003E]:FAD9
[0x0040]:88CC [0x0042]:FFFF [0x0044]:FF0A [0x0046]:0000
[0x0048]:0000 [0x004A]:0000 [0x004C]:0000 [0x004E]:FFFF
[0x0050]:FFFF [0x0052]:1111 [0x0054]:1111 [0x0056]:1111
[0x0058]:1011 [0x005A]:1010 [0x005C]:1010 [0x005E]:1010
[0x0060]:1111 [0x0062]:1211 [0x0064]:1212 [0x0066]:1312
[0x0068]:1313 [0x006A]:1413 [0x006C]:1414 [0x006E]:2264
[0x0070]:00F1 [0x0072]:1133 [0x0074]:0000 [0x0076]:FC62
[0x01E8]:FFFF [0x01EA]:FFFF [0x01EC]:FFFF [0x01EE]:FFFF
[0x01F0]:FFFF [0x01F2]:FFFF [0x01F4]:FFFF [0x01F6]:FFFF
[0x01F8]:FFFF [0x01FA]:FFFF [0x01FC]:FFFF [0x01FE]:FFFF
.....
```

History

Version	Description
2.04	The show interface rf e2p command has been introduced.

3.159.43 show interface rrd

Description Show network interface loading on the principle of Round Robin Database.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> interface <name> rrd <attribute> [ <detail> ]`

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface.
attribute	rxspeed	Value of data rate type.
	txspeed	
detail	0	Level of detail is 1 second.
	1	Level of detail is 2 seconds.
	2	Level of detail is 3 seconds.
	3	Level of detail is 5 seconds.
	4	Level of detail is 15 seconds.
	5	Level of detail is 30 seconds.
	6	Level of detail is 1 minute.
	7	Level of detail is 2 minutes.
	8	Level of detail is 3 minutes.
	9	Level of detail is 5 minutes.
	10	Level of detail is 15 minutes.
	11	Level of detail is 30 minutes.

Example

```
(show)> interface GigabitEthernet1 rrd rxspeed

data:
  t: 90083.990183
  v: 200880

data:
  t: 90082.990128
  v: 152392

data:
  t: 90081.990193
  v: 110976

data:
  t: 90080.990142
  v: 48000

data:
  t: 90079.990178
  v: 38366
```

```
(show)> interface GigabitEthernet1 rrd txspeed
```

```
data:
    t: 87771.249486
    v: 148202

data:
    t: 87768.248974
    v: 10694

data:
    t: 87765.248977
    v: 19070

data:
    t: 87762.249105
    v: 48909

data:
    t: 87759.249105
    v: 149277
```

```
(show)> interface GigabitEthernet1 rrd rxspeed 1
```

```
data:
    t: 90176.990054
    v: 164766

data:
    t: 90174.990061
    v: 121828

data:
    t: 90172.990052
    v: 95430

data:
    t: 90170.990085
    v: 57559

data:
    t: 90168.990119
    v: 97759
```

History

Version	Description
2.10	The show interface rrd command has been introduced.

3.159.44 show interface spectrum rrd

Description

Show specific data from the spectrum analyzer.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> interface <name> spectrum rrd <channel> <attribute> [ <detail> ]`

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the Wi-Fi interface.
channel	<i>Integer</i>	Wi-Fi channel number.
attribute	load	Channel load percentage.
	dfs	DFS enabled.
	radar	Radar detected.
	valid	The data is valid.
	active	The channel is used by the selected Wi-Fi radio interface.
detail	0	RRD detalization level 64 x 1-minute. This value is used by default if the parameter is not specified explicitly.
	1	RRD detalization level 64 x 3-minutes.
	2	RRD detalization level 64 x 30-minutes.

Example

```
(show)> interface WifiMaster1 spectrum rrd 36 active
data:
    t: 976.500000
    v: 1

data:
    t: 916.500000
    v: 1

data:
    t: 856.500000
    v: 0

data:
    t: 796.500000
    v: 0

data:
    t: 736.500000
    v: 0

data:
    t: 676.500000
    v: 0
```

```
data:
    t: 616.500000
    v: 0

data:
    t: 556.500000
    v: 0

data:
    t: 496.500000
    v: 0

data:
    t: 436.500000
    v: 0

data:
    t: 376.500000
    v: 0

data:
    t: 316.500000
    v: 0

data:
    t: 256.500000
    v: 0

data:
    t: 196.500000
    v: 0

data:
    t: 136.500000
    v: 0

data:
    t: 76.500000
    v: 0
```

History

Version	Description
3.08	The show interface spectrum rrd command has been introduced.

3.159.45 show interface stat

Description Show interface statistics.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> interface <name> stat`

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface.

Example

```
(show)> interface WifiMaster0/AccessPoint0 stat

rxpackets: 137033
rxbytes: 23915722
rxerrors: 0
rxdropped: 0
txpackets: 847802
txbytes: 1192583473
txerrors: 0
txdropped: 0
timestamp: 11754.721178
```

History

Version	Description
2.00	The show interface stat command has been introduced.

3.159.46 show interface traffic-counter

Description Show detailed information about the traffic counter status.

Prefix no No

Change settings No

Multiple input No

Interface type Usb

Synopsis `(show)> interface <name> traffic-counter`

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(show)> interface UsbQmi0 traffic-counter

enabled: true
value: 1.47
```

```

threshold: 3.96
  limit: 4
remaining: 2.46
  unit: GiB

trigger:
  limit: false
  threshold: false

saved: Fri Feb 19 18:56:29 2021

```

History

Version	Description
3.06	The show interface traffic-counter command has been introduced.

3.159.47 show interface wps pin

Description Show the access point WPS PIN.

Prefix no No

Change settings No

Multiple input No

Interface type WiFi

Synopsis

```
(show)> interface <name> wps pin
```

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface.

Output

Element	Value
pin	Pin number.

Example

```
(show)> interface WifiMaster0/AccessPoint0 wps pin

pin: 60180360
```

History

Version	Description
2.00	The show interface wps pin command has been introduced.

3.159.48 show interface wps status

Description Show the access point WPS status.

Prefix no No

Change settings No

Multiple input No

Interface type WiFi

Synopsis `(show)> interface <name> wps status`

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface.

Output

Element	Value
wps	Root node.
configured	WPS is configured for Access Point.
auto-self-pin	Auto-self-pin mode state.
status	disabled enabled active
direction	send receive
mode	pbc self-pin peer
left	Time to session closure in seconds.

Example

```
(show)> interface WifiMaster0/AccessPoint0 wps status
```

```

wps:
  configured: yes
  auto-self-pin: yes
  status: active
  direction: send
  mode: self-pin
  left: infinite

```

History

Version	Description
2.00	The show interface wps status command has been introduced.

3.159.49 show interface zerotier peers

Description Show a list of nodes.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **interface** *<name>* **zerotier peers**

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface.

Example

```
(show)> interface ZeroTier0 zerotier peers

    peer:
      address: 63f865ae71
      latency: 328
        role: PLANET
      version: -1.-1.-1

      path: 50.7.252.138/9993

      path: 50.7.252.138/9993

    peer:
      address: 458cde7190
      latency: 201
        role: PLANET
      version: -1.-1.-1

      path: 103.195.103.66/9993

    peer:
      address: 126127940c
      latency: 153
        role: LEAF
      version: 1.12.2

      path: 35.209.81.208/53871

      path: 35.209.81.208/53871

      path: 35.209.81.208/53871
```

```

peer:
  address: fdfe04eba9
  latency: 129
    role: PLANET
  version: -1.-1.-1

  path: 84.17.53.155/9993

peer:
  address: dfde9efeb9
  latency: 246
    role: PLANET
  version: -1.-1.-1

  path: 104.194.8.134/9993

```

History

Version	Description
4.01	The show interface zerotier peers command has been introduced.

3.159.50 show internet status

Description Check for an Internet connection on the device. The "Internet" LED (the globe) lights up as a result of connecting to popular internet sites.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **internet status**

Example (show)> **internet status**

```

checked: Tue Apr 24 17:14:37 2018
reliable: yes
gateway-accessible: yes
  dns-accessible: yes
  host-accessible: yes
  internet: yes

gateway:
  interface: GigabitEthernet1
  address: 192.168.1.1
  failures: 0
  accessible: yes
  excluded: no

```

```

hosts:
    host:
        name: example.net
        failures: 0
        resolved: yes
        accessible: yes

    host:
        name: google.com
        failures: 0
        resolved: no
        accessible: no

```

History

Version	Description
2.11	The show internet status command has been introduced.

3.159.51 show ip arp

Description Display the contents of the [ARP](#) cache.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ip arp**

Example

```

(show)> ip arp
=====
IP                MAC                Interface
=====
192.168.75.209    9c:b7:0d:91:e7:31    Home
82.135.72.150     00:0e:0c:09:db:60    ISP
192.168.75.106    88:53:2e:5e:07:1d    Home
192.168.75.201    7c:61:93:eb:6c:77    Home
192.168.75.203    00:19:d2:48:d6:dc    Home
10.10.30.34       a0:88:b4:40:9c:98    GuestWiFi
192.168.75.203    7c:61:93:ee:88:67    Home
192.168.75.211    00:26:c7:4a:e0:16    Home
82.138.72.163     34:51:c9:c6:53:cf    ISP
192.168.75.200    60:d8:19:cb:1b:36    Home
192.168.75.204    4c:0f:6e:4b:3c:ba    Home
82.138.72.129     00:30:48:89:b5:9f    ISP

```

History

Version	Description
2.00	The show ip arp command has been introduced.

3.159.52 show ip dhcp bindings

Description Show *DHCP server* status. If you use no argument, the entire list of issued IPs for all pools will be displayed.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ip dhcp bindings** [*pool*]

Arguments

Argument	Value	Description
pool	<i>String</i>	The pool name.

Example

```
(show)> ip dhcp bindings _WEBADMIN

      lease:
          ip: 192.168.15.211
          mac: 00:26:c7:4a:e0:16
          expires: 289
          hostname: lenovo
      lease:
          ip: 192.168.15.208
          mac: 00:19:d2:48:d6:dc
          expires: 258
          hostname: evo
      ...
      ...
```

History

Version	Description
2.00	The show ip dhcp bindings command has been introduced.

3.159.53 show ip dhcp pool

Description Show information about specified pool. If you use no argument, the information about all system pools will be displayed.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ip dhcp pool** [*pool*]

Arguments

Argument	Value	Description
pool	<i>String</i>	The pool name.

Example

```
(show)> ip dhcp pool 123

pool, name = 123:
interface, binding = auto:
  network: 0.0.0.0/0
  begin: 0.0.0.0
  end: 0.0.0.0
  router, default = yes: 0.0.0.0
  lease, default = yes: 25200
  state: down
  debug: no
```

History

Version	Description
2.03	The show ip dhcp pool command has been introduced.

3.159.54 show ip ftp

Description

Show home directories for users with **ftp** tag.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(show)> ip ftp
```

Example

```
(show)> ip ftp

enabled: yes
permissive: yes
root: ADATA SD600:
path: /tmp/mnt/ADATA SD600

user, index = 0:
  name: admin
  root: ADATA SD600:
  path: /tmp/mnt/ADATA SD600
```

History

Version	Description
2.08	The show ip ftp command has been introduced.

3.159.55 show ip hotspot

Description Show hotspot hosts.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> ip hotspot`

Example `(show)> ip hotspot`

```

    host:
      mac: 24:92:0e:92:e5:44
      via: 24:92:0e:92:e5:44
      ip: 192.168.1.41
      hostname: android-41d997d510af8ff9
      name:

    interface:
      id: Bridge0
      name: Home
      description: Home network (Wired and wireless hosts)

      expires: 207328
      registered: no
      access: permit
      schedule:
        active: yes
      rxbytes: 0
      txbytes: 0
      uptime: 4911
      link: up
      ssid: Bewilderbeast
      ap: WifiMaster0/AccessPoint0
    authenticated: yes
      txrate: 65
      ht: 20
      mode: 11n
      gi: 800
      rssi: -24
      mcs: 7

    host:
      mac: 20:aa:4b:5c:09:0e
      via: 20:aa:4b:5c:09:0e
      ip: 192.168.1.51
      hostname: Julia-PC
      name:

    interface:
```

```

        id: Bridge0
        name: Home
    description: Home network (Wired and wireless hosts)

    expires: 212967
    registered: no
    access: permit
    schedule:
    active: yes
    rxbytes: 0
    txbytes: 0
    uptime: 884
    link: up
    ssid: Bewilderbeast
    ap: WifiMaster0/AccessPoint0
    authenticated: yes
    txrate: 130
    ht: 20
    mode: 11n
    gi: 800
    rssi: -37
    mcs: 15

```

History

Version	Description
2.09	The show ip hotspot command has been introduced.

3.159.56 show ip hotspot rrd

Description Show registered host traffic information of Round Robin Database.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ip hotspot** *<mac>* **rrd** *<attribute>* [*<detail>*]

Arguments

Argument	Value	Description
mac	<i>MAC address</i>	MAC address of registered host.
attribute	rxspeed	Data rate type.
	txspeed	
	rxbytes	
	txbytes	
detail	0	Level of detail is 1 second.

Argument	Value	Description
	1	Level of detail is 2 seconds.
	2	Level of detail is 3 seconds.
	3	Level of detail is 5 seconds.
	4	Level of detail is 15 seconds.
	5	Level of detail is 30 seconds.
	6	Level of detail is 1 minute.
	7	Level of detail is 2 minutes.
	8	Level of detail is 3 minutes.
	9	Level of detail is 5 minutes.
	10	Level of detail is 15 minutes.
	11	Level of detail is 30 minutes.

Example

```
(show)> ip hotspot a8:1e:84:85:f2:11 rrd rxspeed
```

```
data:
  t: 2180.491855
  v: 16298
```

```
data:
  t: 2177.492050
  v: 9026
```

```
data:
  t: 2174.491916
  v: 11450
```

```
data:
  t: 2171.491843
  v: 626
```

```
(show)> ip hotspot a8:1e:84:85:f2:11 rrd txspeed
```

```
data:
  t: 2228.491841
  v: 952
```

```
data:
```

```

t: 2225.491920
v: 8813

data:
t: 2222.492053
v: 28746

data:
t: 2219.491845
v: 22474

```

```
(show)> ip hotspot a8:1e:84:85:f2:11 rrd rxbytes
```

```

data:
t: 2279.491860
v: 4197

data:
t: 2276.492050
v: 362

data:
t: 2273.492040
v: 14337

data:
t: 2270.491862
v: 3281

```

```
(show)> ip hotspot a8:1e:84:85:f2:11 rrd txbytes
```

```

data:
t: 2360.491865
v: 3342

data:
t: 2357.491853
v: 142

data:
t: 2354.491949
v: 3333

data:
t: 2351.491847
v: 3390

```

History

Version	Description
2.14	The show ip hotspot rrd command has been introduced.

3.159.57 show ip hotspot summary

Description Show the information about traffic usage for several registered hosts according to Round Robin Database. Sorting is in descending order.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ip hotspot summary** *<attribute>* [**detail** *<detail>*] [**count** *<count>*]

Arguments

Argument	Value	Description
attribute	rxspeed	Value of data rate type.
	txspeed	
	rxbytes	
	txbytes	
detail	0	Level of detail is 3 seconds.
	1	Level of detail is 60 seconds.
	2	Level of detail is 180 seconds.
	3	Level of detail is 1440 seconds.
count	Integer	The number of hosts. If not specified, the entire list of hosts is displayed.

Example

```
(show)> ip hotspot summary rxspeed

t: 255

host:
  active: yes
  name: toshiba
  rxspeed: 143964

host:
  active: yes
  name: lnx
  rxspeed: 24749

host:
  active: yes
  name: oneplus6
  rxspeed: 2558

(show)> ip hotspot summary rxspeed detail 0

t: 0
```

```
host:
  active: yes
  name: toshiba
  rxspeed: 186519

host:
  active: yes
  name: oneplus6
  rxspeed: 94298

host:
  active: yes
  name: lnx
  rxspeed: 8237

(show)> ip hotspot summary rxspeed count 3

t: 255

host:
  active: yes
  name: toshiba
  rxspeed: 390322

host:
  active: yes
  name: lnx
  rxspeed: 53518

host:
  active: yes
  name: oneplus6
  rxspeed: 5284
```

History

Version	Description
2.14	The show ip hotspot summary command has been introduced.

3.159.58 show ip http proxy

Description	Show HTTP proxy status.
Prefix no	No
Change settings	No
Multiple input	No
Synopsis	(show)> ip http proxy

Example

(show)> ip http proxy

```

proxy:
  name: modem
  domain: myhomemodem.keenetic.link
  upstream: http://192.168.8.1:80
  allow: public
  ndns: yes

```

History

Version	Description
2.09	The show ip http proxy command has been introduced.

3.159.59 show ip http webdav

Description Show [WebDAV](#) server status.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> ip http webdav

Example

(show)> ip http webdav

```

enabled: yes
permissive: yes
root: ext4-files:/
path: /tmp/mnt/7a976f42-a16f-d501-3017-6b42a16fd501

user, index = 0:
  name: admin
  root:
  path:

user, index = 1:
  name: enpa
  root: ext4-files:/
  path: ►
/tmp/mnt/7a976f42-a16f-d501-3017-6b42a16fd501

```

History

Version	Description
3.04	The show ip http webdav command has been introduced.

3.159.60 show ip name-server

Description Show a list of current IPv4 and IPv6 addresses of DNS servers in order of decreasing priority.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ip name-server**

Example (show)> **ip name-server**

```
server:
  address: 1.1.1.1
  port: 0
  domain:
  global: 0
  service: Dns::Manager
  interface:

server:
  address: 9.9.9.9
  port: 0
  domain:
  global: 0
  service: Dns::Manager
  interface:

server:
  address: 2001:4860:4860::8888
  port: 0
  domain: ISP
  global: 0
  service: Dns::Manager
  interface:

server:
  address: 193.0.174.21
  port: 0
  domain:
  global: 64520
  service: Dhcp::Client-GigabitEthernet1
  interface: GigabitEthernet1

server:
  address: 2a02:290:0:1::4
  port: 0
  domain:
  global: 64520
  service: Ip6::Dhcp::Client-GigabitEthernet1
```

```
interface: GigabitEthernet1

server:
  address: 10.2.0.1
  port: 0
  domain:
    global: 43
  service: Dns::InterfaceSpecific-Wireguard5
  interface: Wireguard5
```

History

Version	Description
2.00	The show ip name-server command has been introduced.

3.159.61 show ip nat

- Description** Show network address translation table.
- Prefix no** No
- Change settings** No
- Multiple input** No

Synopsis (show)> **ip nat** [**tcp**]

Arguments

Argument	Value	Description
tcp	Keyword	Only the records with <i>TCP</i> type will be displayed.

Example

```
(show)> ip nat
=====
Type | In | Source          Port Destination      Port  Packets
   | Out |                |      |                   |      |
-----
udp   |    | 10.1.30.34      6482 111.221.77.159    40005 1
      |    | 111.221.77.159  40005 82.138.7.164      6482 1
-----
udp   |    | 220.27.130.179  6896 82.138.7.164      28197 1
      |    | 192.168.15.204  28197 220.27.130.179    6896 1
-----
tcp   |    | 10.1.30.33       57474 78.141.179.15     12350 12
      |    | 78.141.179.15   12350 82.138.7.164      57474 11
-----
udp   |    | 10.1.30.34       6482 84.201.228.162    44423 11
      |    | 84.201.228.162  44423 82.138.7.164      6482 16
-----
tcp   |    | 10.1.30.34       46655 96.55.147.21      443 2
      |    | 96.55.147.21    443 82.138.7.164      46655 0
```

```
-----
udp          10.1.30.34      6482  213.199.179.158 40006  1
            213.199.179.158 40006  82.138.7.164   6482   1
-----
```

History

Version	Description
2.00	The show ip nat command has been introduced.

3.159.62 show ip neighbour

Description Show the list of discovered hosts on the network at the OSI model network level.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ip neighbour** [**alive**]

Arguments

Argument	Value	Description
alive	<i>Keyword</i>	Show active hosts.

Example

```
(show)> ip neighbour

neighbour:
    id: 1
    via: b8:88:e1:2b:30:af
    mac: b8:88:e1:2b:30:af
address-family: ipv4
    address: 192.168.22.16
    interface: Bridge0
    first-seen: 251387
    last-seen: 0
    leasetime: 7372
    expired: no
    wireless: no

neighbour:
    id: 4
    via: b8:88:e2:4b:30:af
    mac: b8:88:e2:4b:30:af
address-family: ipv6

addresses:
    address:
        address: fe80::a022:a505:fae6:c891
        status: active
```



```

last-seen: 3

interface: Bridge0
first-seen: 251371
last-seen: 251371
leasetime: 0
expired: no
wireless: no

```

History

Version	Description
2.10	The show ip neighbour command has been introduced.

3.159.63 show ip policy

Description Show the IP Policy profile status.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ip policy** [*<policy>*]

Arguments

Argument	Value	Description
policy	<i>Policy</i>	Name of IP Policy profile.

Example

```

(show)> ip policy
policy, name = Policy0, description = VPN-OpenVPN:
    mark: fffffffd00
    table: 42

    route:
    destination: 10.1.30.0/24
    gateway: 0.0.0.0
    interface: Guest
    metric: 0
    proto: boot
    floating: no

    route:
    destination: 172.16.3.33/32
    gateway: 0.0.0.0
    interface: L2TPVPN
    metric: 0
    proto: boot
    floating: no

    route:

```

```
destination: 192.168.1.0/24
gateway: 0.0.0.0
interface: Home
metric: 0
proto: boot
floating: no

policy, name = Policy3, description = Home:
mark: fffffffd03
table: 45

route:
destination: 10.1.30.0/24
gateway: 0.0.0.0
interface: Guest
metric: 0
proto: boot
floating: no

route:
destination: 172.16.3.33/32
gateway: 0.0.0.0
interface: L2TPVPN
metric: 0
proto: boot
floating: no

route:
destination: 192.168.1.0/24
gateway: 0.0.0.0
interface: Home
metric: 0
proto: boot
floating: no
```

```
(show)> ip policy Policy0
policy, name = Policy0:
mark: fffffffd00
table: 42

route:
destination: 0.0.0.0/0
gateway: 193.0.174.1
interface: ISP
metric: 0
proto: boot
floating: no

route:
destination: 10.1.30.0/24
gateway: 0.0.0.0
interface: Guest
metric: 0
proto: boot
```

```

floating: no

route:
destination: 185.230.127.84/32
gateway: 193.0.174.1
interface: ISP
metric: 0
proto: boot
floating: no

route:
destination: 192.168.1.0/24
gateway: 0.0.0.0
interface: Home
metric: 0
proto: boot
floating: no

route:
destination: 193.0.174.0/24
gateway: 0.0.0.0
interface: ISP
metric: 0
proto: boot
floating: no

route:
destination: 193.0.175.0/25
gateway: 193.0.174.10
interface: ISP
metric: 0
proto: boot
floating: no

route:
destination: 193.0.175.22/32
gateway: 193.0.174.1
interface: ISP
metric: 0
proto: boot
floating: no

```

History

Version	Description
2.12	The show ip policy command has been introduced.

3.159.64 show ip route

Description Show the current routing table.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> ip route [table <table>] [sort <criteria> <direction>]`

Arguments

Argument	Value	Description
table	<i>Integer</i>	The route number.
criteria	interface	Sorting criteria is the interface name.
	gateway	Sorting criteria is the gateway address.
	destination	Sorting criteria is the destination address.
direction	ascending	Routing table records are sorted in ascending order.
	descending	Routing table records are sorted in descending order.

Example

(show)> ip route table 254			
Destination	Gateway	Interface	
F Metric			
0.0.0.0/0	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
1.1.1.1/32	0.0.0.0	Wireguard1	►
U 0			
8.8.8.8/32	0.0.0.0	Wireguard7	►
U 0			
10.1.30.0/24	0.0.0.0	Guest	►
U 0			
10.8.0.0/24	0.0.0.0	Wireguard3	►
U 0			
13.32.99.0/24	0.0.0.0	Wireguard7	►
U 0			
82.3.116.12/32	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
108.157.4.0/24	0.0.0.0	Wireguard7	►
U 0			
162.159.192.1/32	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
172.16.85.0/24	0.0.0.0	Wireguard1	►
U 0			
176.124.212.86/32	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
188.114.96.0/22	0.0.0.0	Wireguard7	►
U 0			
192.168.1.0/24	192.168.15.88	Home	►
U 0			
192.168.15.0/24	0.0.0.0	Home	►
U 0			

```

192.168.17.0/24    0.0.0.0    Bridge2    ►
    U    0
192.168.133.0/24  0.0.0.0    WifiMaster1/WifiStation0 ►
    U    0
192.168.220.0/24  0.0.0.0    Wireguard1 ►
    U    0
194.71.130.15/32  192.168.133.1 WifiMaster1/WifiStation0 ►
    U    0

```

```
(show)> ip route sort interface ascending
```

Destination F Metric	Gateway	Interface	►
192.168.1.0/24 U 0	192.168.15.88	Home	►
192.168.15.0/24 U 0	0.0.0.0	Home	►
10.1.30.0/24 U 0	0.0.0.0	Guest	►
192.168.17.0/24 U 0	0.0.0.0	Bridge2	►
0.0.0.0/0 U 0	192.168.133.1	WifiMaster1/WifiStation0	►
84.2.111.11/32 U 0	192.168.133.1	WifiMaster1/WifiStation0	►
162.159.192.1/32 U 0	192.168.133.1	WifiMaster1/WifiStation0	►
176.124.212.86/32 U 0	192.168.133.1	WifiMaster1/WifiStation0	►
192.168.133.0/24 U 0	0.0.0.0	WifiMaster1/WifiStation0	►
194.71.130.15/32 U 0	192.168.133.1	WifiMaster1/WifiStation0	►
1.1.1.1/32 U 0	0.0.0.0	Wireguard1	►
172.16.85.0/24 U 0	0.0.0.0	Wireguard1	►
192.168.220.0/24 U 0	0.0.0.0	Wireguard1	►
10.8.0.0/24 U 0	0.0.0.0	Wireguard3	►
8.8.8.8/32 U 0	0.0.0.0	Wireguard7	►
13.32.99.0/24 U 0	0.0.0.0	Wireguard7	►
108.157.4.0/24 U 0	0.0.0.0	Wireguard7	►
188.114.96.0/22 U 0	0.0.0.0	Wireguard7	►

```
(show)> ip route sort interface descending
```

Destination	Gateway	Interface	►
-------------	---------	-----------	---

F Metric			
188.114.96.0/22	0.0.0.0	Wireguard7	►
U 0			
108.157.4.0/24	0.0.0.0	Wireguard7	►
U 0			
13.32.99.0/24	0.0.0.0	Wireguard7	►
U 0			
8.8.8.8/32	0.0.0.0	Wireguard7	►
U 0			
10.8.0.0/24	0.0.0.0	Wireguard3	►
U 0			
192.168.220.0/24	0.0.0.0	Wireguard1	►
U 0			
172.16.85.0/24	0.0.0.0	Wireguard1	►
U 0			
1.1.1.1/32	0.0.0.0	Wireguard1	►
U 0			
194.71.130.15/32	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
192.168.133.0/24	0.0.0.0	WifiMaster1/WifiStation0	►
U 0			
176.124.212.86/32	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
162.159.192.1/32	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
85.1.112.11/32	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
0.0.0.0/0	192.168.133.1	WifiMaster1/WifiStation0	►
U 0			
192.168.17.0/24	0.0.0.0	Bridge2	►
U 0			
10.1.30.0/24	0.0.0.0	Guest	►
U 0			
192.168.15.0/24	0.0.0.0	Home	►
U 0			
192.168.1.0/24	192.168.15.88	Home	►
U 0			

History

Version	Description
2.00	The show ip route command has been introduced.

3.159.65 show ip service

Description Show a list of open ports used by system services.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(show)> ip service
```

Example

```
(show)> ip service

    service:
    service-name: Telnet
      family: ipv4
      protocol: tcp
      port: 23
    security-level: private

    service:
    service-name: DNS proxy
      family: ipv4
      protocol: udp
      port: 53
    security-level: protected

    service:
    service-name: DNS proxy
      family: ipv4
      protocol: tcp
      port: 53
    security-level: protected

    service:
    service-name: DNS proxy
      family: ipv4
      protocol: udp
      port: 54321
    security-level: private
```

History

Version	Description
3.06	The show ip service command has been introduced.

3.159.66 show ipsec

Description

Show info about *IPsec/IKE* strongSwan service status.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(show)> ipsec
```

Example

```
(show)> ipsec

ipsec_statusall:
```

```

Status of IKE charon daemon (strongSwan 5.3.4, Linux 2.6.36, ▶
mips):
  uptime: 6 days, since Dec 22 10:23:36 2015
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: ▶
0/0/0/0, scheduled: 10
  loaded plugins: charon aes des sha1 sha2 md5 random nonce ▶
openssl xcbc cmac hmac attr kernel-netlink socket-default stroke ▶
updown eap-mschapv2 eap-dynamic xauth-generic xauth-eap ▶
error-notify systime-fix
Listening IP addresses:
  192.168.1.1
  10.10.10.15
Connections:
  test: %any...ipsec.example.org IKEv2, dpddelay=10s
  test: local: [ipsec.example.org] uses pre-shared key ▶
authentication
  test: remote: [ipsec.example.com] uses pre-shared key ▶
authentication
  test: child: 172.16.200.0/24 === 172.16.201.0/24 TUNNEL, ▶
dpdaction=restart
Security Associations (1 up, 0 connecting):
  test[572]: ESTABLISHED 24 minutes ago, ▶
10.10.10.15[ipsec.example.org]...10.10.10.20[ipsec.example.com]
  test[572]: IKEv2 SPIs: 00a6ebfc9d90f1c2_i* ▶
3cd201ef496df75c_r, pre-shared key reauthentication in 20 minutes
  test[572]: IKE proposal: ▶
AES_CBC=256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024/#
  test{304}: INSTALLED, TUNNEL, reqid 185, ESP in UDP SPIs: ▶
ca59bfcf_i cde23d83_o
  test{304}: AES_CBC_256/HMAC_SHA1_96, 10055 bytes_i (164 ▶
pkts, 0s ago), 10786 bytes_o (139 pkts, 0s ago), rekeying in 34 ▶
minutes
  test{304}: 172.16.200.0/24 === 172.16.201.0/24

```

History

Version	Description
2.06	The show ipsec command has been introduced.

3.159.67 show ipv6 addresses

Description Show a list of current IPv6-addresses.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ipv6 addresses**

Example

```
(show)> ipv6 addresses

address:
  address: 2001:db8::1
  interface: ISP
valid-lifetime: infinite
address:
  address: 2001:db8::ce5d:4eff:fe4f:aab2
  interface: Home
valid-lifetime: infinite
address:
  address: fd3c:4268:1559:0:ce5d:4eff:fe4f:aab2
  interface: Home
valid-lifetime: infinite
address:
  address: fd01:db8:43:0:ce5d:4eff:fe4f:aab2
  interface: Home
valid-lifetime: infinite
```

History

Version	Description
2.00	The show ipv6 addresses command has been introduced.

3.159.68 show ipv6 dhcp bindings

Description Show *DHCPv6 server* status.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ipv6 dhcp bindings**

Example

```
(show)> ipv6 dhcp bindings
subnet:
  name: Default

subnet:
  name: guest

lease:
  type: IA-NA
  duid: 00:03:00:01:a8:a1:59:61:57:69
  address: fc34:5678:0:4::cc
  expires: 299

lease:
  type: IA-PD
```

```

duid: 00:03:00:01:a8:a1:59:61:57:69
prefix: fc34:5678:0:7::/64
remote: fe80::2ecb:ff38:a778:66e8
expires: 299

```

History

Version	Description
4.00	The show ipv6 dhcp bindings command has been introduced.

3.159.69 show ipv6 prefixes

Description Show a list of current IPv6-prefixes.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ipv6 prefixes**

Example

```

(show)> ipv6 prefixes

    prefix:
      prefix: 2001:db8::/64
      interface: ISP
    valid-lifetime: infinite
  preferred-lifetime: infinite
    prefix:
      prefix: fd3c:4268:1559::/48
      interface:
    valid-lifetime: infinite
  preferred-lifetime: infinite
    prefix:
      prefix: fd01:db8:43::/48
      interface:
    valid-lifetime: infinite
  preferred-lifetime: infinite

```

History

Version	Description
2.00	The show ipv6 prefixes command has been introduced.

3.159.70 show ipv6 route

Description Show a list of current IPv6-routes.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> ipv6 route [table <table> ] [sort <criteria> <direction> ]`

Arguments

Argument	Value	Description
table	<i>Integer</i>	The route number.
criteria	interface	Sorting criteria is the interface name.
	gateway	Sorting criteria is the gateway address.
	destination	Sorting criteria is the destination address.
direction	ascending	Routing table records are sorted in ascending order.
	descending	Routing table records are sorted in descending order.

Example

```
(show)> ipv6 route table 42
```

```
route6:
destination: 2a02:290:2:65d:52ff:20ff:fe00:1e86/128
gateway: ::
interface: Home
metric: 256
flags: U
rejecting: no
proto: boot
floating: no
static: no
```

```
(show)> ipv6 route sort interface ascending
```

```
route6:
destination: 2a02:290:2:65d:52ff:20ff:fe00:1e86/128
gateway: ::
interface: Home
metric: 256
flags: U
rejecting: no
proto: kernel
floating: no
static: no
```

```
(show)> ipv6 route sort gateway descending
```

```
route6:
destination: ::/0
gateway: fe80::66a0:e7ff:fef5:6392
interface: ISP
metric: 1024
flags: U
```

```

rejecting: no
proto: boot
floating: no
static: no

```

History

Version	Description
2.00	The show ipv6 routes command has been introduced.
4.00	New command name is show ipv6 route .

3.159.71 show ipv6 subnets

Description Show a list of current IPv6-subnets.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ipv6 subnets**

Example

```

(show)> ipv6 subnets

subnet:
  name: Default
  interface: Home

prefixes:
  prefix: 2a0d:8140:2ba1::/64
  interface: TunnelSixInFour0
  valid-lifetime: infinite
  preferred-lifetime: 0
  global: no

```

History

Version	Description
4.01	The show ipv6 subnets command has been introduced.

3.159.72 show kabinet status

Description Check for the status and configuration of KASiNET authenticator.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(show)> kabinet status
```

Example

```
(show)> kabinet status

    kabinet:
      enabled: yes
      wan: yes
      state: STOPPED
      server: 10.0.0.1
      access-level: internet
      protocol-version: 2
```

History

Version	Description
2.02	The show kabinet status command has been introduced.

3.159.73 show last-change

Description

Show when and who made the latest changes in the settings.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(show)> last-change
```

Example

```
(show)> last-change

    date: Thu, 12 Jul 2012 10:01:47 GMT

    agent: cli
```

History

Version	Description
2.00	The show last-change command has been introduced.

3.159.74 show led

Description

Show information about specified LED in the system. If you use no argument, the entire list of all LEDs on the device will be displayed. Available LEDs depend on hardware configuration.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis**(show)> led [<name>]****Arguments**

Argument	Value	Description
name	SYS	The LED name. The number of available indicators depends on the selected device.
	FN	
	FW_UPD	
	ACT_ACK	
	WAN	
	DSL	
	WLAN	
	WLAN5	
	WPS_1	
	WPS_2	
	WPS_3	
	WPS_4	
	WPS5_1	
	WPS5_2	
	WPS5_3	
	WPS5_4	
	USB_1	
	USB_2	
	LTE	

Example

```
(show)> led FN_1

      leds:
        led, index = 0:
          name: FN_1
        user_configurable: yes
        virtual: no
```

History

Version	Description
2.05	The show led command has been introduced.

3.159.75 show led bindings

Description

Show the control associated with the specified LED. If you use no argument, the entire list of all LEDs with theirs controls will be displayed.

Prefix no

No

Change settings No

Multiple input No

Synopsis (show)> **led** [<name>]**bindings**

Argument	Value	Description
name	SYS	The LED name. Set of available indicators depends on the selected device.
	FN	
	FW_UPD	
	ACT_ACK	
	WAN	
	DSL	
	WLAN	
	WLAN5	
	WPS_1	
	WPS_2	
	WPS_3	
	WPS_4	
	WPS5_1	
	WPS5_2	
	WPS5_3	
	WPS5_4	
	USB_1	
	USB_2	
	LTE	

Example

```
(show)> led bindings

bindings:

  binding, index = 0:
    led: SYS
  user_configurable: no
  active_control: SystemState
  default_control: SystemState

  binding, index = 1:
    led: FN_1
  user_configurable: yes
  active_control: Usb1PortDeviceAttached
  default_control: Usb1PortDeviceAttached
```

```
        binding, index = 2:
            led: FN_2
user_configurable: yes
    active_control: Usb2PortDeviceAttached
    default_control: Usb2PortDeviceAttached

        binding, index = 3:
            led: ACT_ACK
user_configurable: no
    active_control: ButtonActivityAcknowledgement
    default_control: ButtonActivityAcknowledgement

        binding, index = 4:
            led: FW_UPD
user_configurable: no
    active_control:
    default_control:

        binding, index = 5:
            led: WAN
user_configurable: no
    active_control: WanConnected
    default_control: WanConnected

        binding, index = 6:
            led: WLAN
user_configurable: no
    active_control: WlanActivity
    default_control: WlanActivity

        binding, index = 7:
            led: WPS_1
user_configurable: no
    active_control: WlanWps1Activity
    default_control: WlanWps1Activity

        binding, index = 8:
            led: WPS_2
user_configurable: no
    active_control: WlanWps2Activity
    default_control: WlanWps2Activity

        binding, index = 9:
            led: WPS_3
user_configurable: no
    active_control: WlanWps3Activity
    default_control: WlanWps3Activity

        binding, index = 10:
            led: WPS_4
user_configurable: no
    active_control: WlanWps4Activity
    default_control: WlanWps4Activity
```



```

binding, index = 11:
    led: WPS_STA
user_configurable: no
active_control: WstaWpsActivity
default_control: WstaWpsActivity

binding, index = 12:
    led: WLAN5
user_configurable: no
active_control: Wlan5Activity
default_control: Wlan5Activity

binding, index = 13:
    led: WPS5_1
user_configurable: no
active_control: Wlan5Wps1Activity
default_control: Wlan5Wps1Activity

binding, index = 14:
    led: WPS5_2
user_configurable: no
active_control: Wlan5Wps2Activity
default_control: Wlan5Wps2Activity

binding, index = 15:
    led: WPS5_3
user_configurable: no
active_control: Wlan5Wps3Activity
default_control: Wlan5Wps3Activity

binding, index = 16:
    led: WPS5_4
user_configurable: no
active_control: Wlan5Wps4Activity
default_control: Wlan5Wps4Activity

binding, index = 17:
    led: WPS5_STA
user_configurable: no
active_control: Wsta5WpsActivity
default_control: Wsta5WpsActivity

```

History

Version	Description
2.08	The show led bindings command has been introduced.

3.159.76 show led controls**Description**

Show a list of LED controls in the system. Available controls depend on hardware configuration.

Prefix no

No

Change settings No

Multiple input No

Synopsis `(show)> led controls`

Example `(show)> led controls`

```
controls:
  control, index = 0:
    name: SystemState
  short_description: System state
    owner: ndm
  user_configurable: no

  control, index = 1:
    name: ButtonActivityAcknowledgement
  short_description: Button activity acknowledgement
    owner: ndm
  user_configurable: no

  control, index = 2:
    name: SelectedSchedule
  short_description: Selected schedule is active
    owner: ndm
  user_configurable: yes

  control, index = 3:
    name: SelectedWan
  short_description: Selected WAN interface has default route
    owner: ndm
  user_configurable: yes

  control, index = 4:
    name: BackupWan
  short_description: Backup WAN interface has default route
    owner: ndm
  user_configurable: yes

  control, index = 5:
    name: WanConnected
  short_description: WAN interface connected
    owner: ndm
  user_configurable: no

  control, index = 6:
    name: Usb1PortDeviceAttached
  short_description: USB port 1 known device attached
    owner: ndm
  user_configurable: yes

  control, index = 7:
```

```

        name: Usb2PortDeviceAttached
short_description: USB port 2 known device attached
        owner: ndm
user_configurable: yes

        control, index = 8:
            name: UpdatesAvailable
short_description: Firmware updates available
        owner: ndm
user_configurable: yes

        control, index = 9:
            name: OpkgLedControl
short_description: OPKG LED control
        owner: ndm
user_configurable: yes

        control, index = 10:
            name: Wlan5Activity
short_description: WLAN 5GHz interface activity
        owner: mt7615_ap
user_configurable: no

        control, index = 11:
            name: Wlan5Wps1Activity
short_description: WLAN 5GHz SSID 1 WPS activity
        owner: mt7615_ap
user_configurable: no

        control, index = 12:
            name: Wlan5Wps2Activity
short_description: WLAN 5GHz SSID 2 WPS activity
        owner: mt7615_ap
user_configurable: no

        control, index = 13:
            name: Wlan5Wps3Activity
short_description: WLAN 5GHz SSID 3 WPS activity
        owner: mt7615_ap
user_configurable: no

        control, index = 14:
            name: Wlan5Wps4Activity
short_description: WLAN 5GHz SSID 4 WPS activity
        owner: mt7615_ap
user_configurable: no

        control, index = 15:
            name: WlanActivity
short_description: WLAN 2.4GHz interface activity
        owner: mt7615_ap
user_configurable: no

        control, index = 16:

```

```

        name: WlanWps1Activity
short_description: WLAN 2.4GHz SSID 1 WPS activity
        owner: mt7615_ap
user_configurable: no

        control, index = 17:
            name: WlanWps2Activity
short_description: WLAN 2.4GHz SSID 2 WPS activity
            owner: mt7615_ap
user_configurable: no

        control, index = 18:
            name: WlanWps3Activity
short_description: WLAN 2.4GHz SSID 3 WPS activity
            owner: mt7615_ap
user_configurable: no

        control, index = 19:
            name: WlanWps4Activity
short_description: WLAN 2.4GHz SSID 4 WPS activity
            owner: mt7615_ap
user_configurable: no

        control, index = 20:
            name: Wsta5WpsActivity
short_description: Station 5GHz WPS activity
            owner: mt7615_ap
user_configurable: no

        control, index = 21:
            name: WstaWpsActivity
short_description: Station 2.4GHz WPS activity
            owner: mt7615_ap
user_configurable: no

```

History

Version	Description
2.08	The show led controls command has been introduced.

3.159.77 show log

Description	Show system log contents (records that are present in a circular buffer). The command executes in the background, that is, until forced to stop by the user pressing [Ctrl]+[C].
Prefix no	No
Change settings	No
Multiple input	No

Synopsis

```
(show)> log [ <max-lines> ] [once]
```

Arguments

Argument	Value	Description
max-lines	<i>Integer</i>	Limit for returned log items.
once	<i>Keyword</i>	Show current log and exit to the CLI.

Example

```
(show)> log
```

Time	Message
I [Jul 12 12:08:39]	radvd[228]: attempting to reread config file
I [Jul 12 12:08:39]	radvd[228]: resuming normal operation
I [Jul 12 12:08:40]	wmond: WifiMaster0/AccessPoint0: ► STA(d8:b3:77:36:05:c1) occurred MIC different in key handshaking.
I [Jul 12 12:08:40]	radvd[228]: attempting to reread config file
I [Jul 12 12:08:40]	radvd[228]: resuming normal operation
I [Jul 12 12:08:41]	wmond: WifiMaster0/AccessPoint0: ► STA(d8:b3:77:36:05:c1) occurred MIC different in key handshaking.
I [Jul 12 12:08:41]	radvd[228]: attempting to reread config file
I [Jul 12 12:08:41]	radvd[228]: resuming normal operation
I [Jul 12 12:08:44]	wmond: WifiMaster0/AccessPoint0: ► STA(d8:b3:77:36:05:c1) pairwise key handshaking timeout.
I [Jul 12 12:08:44]	wmond: WifiMaster0/AccessPoint0: ► STA(d8:b3:77:36:05:c1) had deauthenticated.

History

Version	Description
2.00	The show log command has been introduced.

3.159.78 show media

Description

Show info about system USB-drives and their partitions.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(show)> media
```

Example

```
(show)> media
```

```
media:
  name: Media0
```

```

        port: 1
        state: ACTIVE
    manufacturer: Western Digital
    product: My Passport 074A
    serial: 575832314139324D36383139
    size: 1000202043392

    partition:
        uuid: 01D55E919F06F5C0
        label: MyPassport
        fstype: ntfs
        state: MOUNTED
        total: 982291312640
        free: 285839884288

    partition:
        uuid: dd5e899f-915e-d501-101e-899f915ed501
        label: fls_wd_ext4
        fstype: ext4
        state: MOUNTED
        total: 15756732416
        free: 15741890560

    partition:
        uuid: 00000000-0000-0000-0000-000000000000
        label:
        fstype: swap
        state: MOUNTED
        total: 1081077760
        free: 1081077760

```

History

Version	Description
3.04	The show media command has been introduced.

3.159.79 show mws associations

Description Show the list of Access Points on the repeater(s) associated with [MWS](#) controller.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **mws associations**

Example (show)> **mws associations**

```
station:
```

```

        mac: 51:ef:22:11:17:1a
        ap: WifiMaster1/Backhaul0
authenticated: yes
    txrate: 585
    rxrate: 270
    uptime: 31
txbytes: 33569
rxbytes: 74324
    ht: 80
    mode: 11ac
    gi: 800
    rssi: -27
    mcs: 7
    txss: 2
    ebf: yes
    mu: yes

```

History

Version	Description
3.01	The show mws associations command has been introduced.

3.159.80 show mws candidate

Description Show the list of candidates or the description of specified candidate by the given identifier.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **mws candidate** [*<candidate>*]

Arguments

Argument	Value	Description
candidate	<i>String</i>	Device ID — MAC address or CID.

Example

```

(show)> mws candidate d11246e8-583d-11ef-911a-1f4569ab1720

candidate:
    mac: 51:ff:21:c4:a1:83
    cid: d11246e8-583d-11ef-911a-1f4569ab1720
    mode: extender
    model: Hopper (KN-3811)
    state: COMPATIBLE_UPDATE
    fw: 4.3.2
fw-available: 5.0 Alpha 1
    license: 1111222233334444555
eula-accepted: yes

```

```
    dpn-accepted: yes
    stp-encapsulation: yes

    port:
      label: 1

    port:
      label: 2

    port:
      label: 3

    port:
      label: 0

    rci:
```

```
(show)> mws candidate 51:ff:21:c4:a1:83
```

```
    candidate:
      mac: 51:ff:21:c4:a1:83
      cid: d11246e8-583d-11ef-911a-1f4569ab1720
      mode: extender
      model: Hopper (KN-3811)
      state: COMPATIBLE_UPDATE
      fw: 4.3.2
      fw-available: 5.0 Alpha 1
      license: 1111222233334444555
      eula-accepted: yes
      dpn-accepted: yes
      stp-encapsulation: yes

      port:
        label: 1

      port:
        label: 2

      port:
        label: 3

      port:
        label: 0

      rci:
```

History

Version	Description
2.15	The show mws candidate command has been introduced.

3.159.81 show mws log

Description Show log of connections and transitions from one Access Point to another within [MWS](#). The command executes in the background, that is, until forced to stop by the user pressing [Ctrl]+[C].

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> mws log [ <max-lines> ] [once]`

Argument	Value	Description
max-lines	<i>Integer</i>	Limit of entries in the response.
once	<i>Keyword</i>	Show recent entries in the log.

Example

```
(show)> mws log 1
```

Time	Message
[Jan 17 15:04:58]	: 64:a2:f9:51:b1:82: associated -> ▶ 50:ff:20:00:11:82 (5 GHz)

```
(show)> mws log once
```

Time	Message
[Jan 17 14:46:37]	: 64:a2:f9:51:b1:82: associated -> ▶ 50:ff:20:00:11:82 (5 GHz)
[Jan 17 15:04:50]	: 64:a2:f9:51:b1:82: 50:ff:20:00:11:82 (5 GHz) -> disassociated
[Jan 17 15:04:58]	: 64:a2:f9:51:b1:82: associated -> ▶ 50:ff:20:00:11:82 (5 GHz)

Version	Description
2.15	The show mws log command has been introduced.

3.159.82 show mws member

Description Show the list of members or the description of specified member by the given identifier.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **mws member** [<member>]

Arguments

Argument	Value	Description
member	<i>String</i>	Device ID — MAC address or CID.

Example

```
(show)> mws member 40f829b8-71a8-11ec-9396-5fb681ed4743

member:
    cid: 40f829b8-71a8-11ec-9396-5fb681ed4743
    model: Speedster (KN-3310)
    mac: 50:ff:21:69:21:7d
    known-host: Keenetic Hopper 116***591
    ip: 192.168.15.42
    mode: extender
    hw-type: router
    license: 116232491843591
    fqdn: 1fb1227d6b44e5863f46cb5a.keenetic.io
fqdn-certificate-valid: yes
    fw: 3.8 Beta 2
    fw-available: 3.8.2
    region: EU
    associations: 0
    rebooting: yes

capabilities:
    mode-hw: no
    dual-band: yes
auto-ap-shutdown: yes
    wpa3: yes
    owe: yes
    wind: yes
    wpa-eap: no
    acme: yes
    auth-token: yes
    backhaul-bss: yes
    sta-mask: yes
    country-code: yes
    notify: yes

    system:
        cpuload: 2
        memory: 97592/262144
        uptime: 567

    backhaul:
        uplink: GigabitEthernet0/Vlan1
        bridge: 8000.50:ff:21:69:21:7d
        cost: 5
        speed: 1000
```

```
duplex: full

rci:
errors: 0
```

History	Version	Description
	2.15	The show mws member command has been introduced.

3.159.83 show ndns

Description Show KeenDNS parameters from the latest request to the server (see [ndns get-booked](#) and [ndns get-update](#) commands).

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ndns**

Example

```
(show)> ndns

name: test
booked: test
domain: keenetic.pro
address: 0.0.0.0
address6: ::
updated: yes
access: cloud
access6: cloud
xns: ub5

ttp:
direct: no
interface: GigabitEthernet1
address: 193.0.174.200
address6: ::

tunnel:
client: *
target: *:80
target-local: 192.168.133.40:49840
target-remote: *:80
default-fqdn: keenetic.io
destination: 192.168.133.40:443
dialback: ndns
timeout: 30
uptime: 8
```

```
idle: 0
linger: 8073
```

History

Version	Description
2.07	The show ndns command has been introduced.

3.159.84 show netfilter

Description Show information about the firewall working. Need to provide remote technical support.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **netfilter**

History

Version	Description
2.00	The show netfilter command has been introduced.

3.159.85 show nextdns availability

Description Check and show *NextDNS* availability.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **nextdns availability**

Example (show)> **nextdns availability**

```
available: yes
port: 53
doh-supported: yes
doh-available: yes
```

History

Version	Description
3.08	The show nextdns availability command has been introduced.

3.159.86 show nextdns profiles

Description	Show <i>NextDNS</i> profiles.
Prefix no	No
Change settings	No
Multiple input	No
Synopsis	(show)> nextdns profiles

Example

```
(show)> nextdns profiles

  profiles:
    profile:
      name: No filtering
      token: 0

    profile:
      name: My First Configuration
      token: 1f3a36

NextDns::Client: Loaded profiles.
```

History	Version	Description
	3.08	The show nextdns profiles command has been introduced.

3.159.87 show ntce applications

Description	Show the list of applications supported by the <i>NTCE</i> service.
Prefix no	No
Change settings	No
Multiple input	No
Synopsis	(show)> ntce applications

Example

```
(show)> ntce applications

  application:
    id-num: 1
    short: facebook
    long: Facebook
    group-id: 2065
    group-long: Social
    groupset-id: 4
```

```
groupset-short-id: surfing
groupset-long-id: Web surfing

application:
    id-num: 2
    short: magicjack
    long: magicJack
    group-id: 2054
    group-long: Voice over IP
    groupset-id: 0
groupset-short-id: calling
groupset-long-id: Calling and conferencing

application:
    id-num: 3
    short: itunes
    long: iTunes
    group-id: 2056
    group-long: Streaming
    groupset-id: 2
groupset-short-id: streaming
groupset-long-id: Video & Audio streaming

application:
    id-num: 4
    short: myspace
    long: MySpace
    group-id: 2065
    group-long: Social
    groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing

application:
    id-num: 5
    short: facetime
    long: FaceTime
    group-id: 2054
    group-long: Voice over IP
    groupset-id: 0
groupset-short-id: calling
groupset-long-id: Calling and conferencing

application:
    id-num: 6
    short: truphone
    long: Truphone
    group-id: 2054
    group-long: Voice over IP
    groupset-id: 0
groupset-short-id: calling
groupset-long-id: Calling and conferencing

application:
```

```

        id-num: 7
        short: twitter
        long: Twitter
        group-id: 2065
        group-long: Social
        groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing

application:
    id-num: 8
    short: xbox
    long: XBOX gaming console
    group-id: 2050
    group-long: Gaming
    groupset-id: 1
groupset-short-id: gaming
groupset-long-id: Gaming

application:
    id-num: 9
    short: realmedia
    long: RealMedia
    group-id: 2088
    group-long: Removed
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

application:
    id-num: 10
    short: google-mail
    long: Google Mail
    group-id: 2059
    group-long: Mail
    groupset-id: 3
groupset-short-id: work
groupset-long-id: Work & Learn from home

```

History

Version	Description
3.07	The show ntce applications command has been introduced.

3.159.88 show ntce attributes

Description Show the list of attributes supported by the [NTCE](#) service.

Prefix no No

Change settings No

Multiple input

No

Synopsis**(show)> ntce attributes****Example**

```
(show)> ntce attributes

    attribute:
      id-num: 1
      short: encrypted
      long: Indicates that the current connection is ►
encrypted traffic.

    attribute:
      id-num: 2
      short: audio
      long: Indicates that the current connection is ►
an audio or voice signal.

    attribute:
      id-num: 3
      short: out
      long: Indicates that the current connection is ►
a landline call, e.g. a call to a home phone.

    attribute:
      id-num: 4
      short: video
      long: Indicates that the current connection is ►
a video signal.

    attribute:
      id-num: 5
      short: file-transfer
      long: Indicates that the current connection is ►
a file transfer.

    attribute:
      id-num: 6
      short: web
      long: Indicates that the current connection is ►
a surf the Internet session.

    attribute:
      id-num: 7
      short: chat
      long: Indicates that the current connection is ►
a chat session.

    attribute:
      id-num: 8
      short: mail
      long: Indicates that the current connection is ►
mail traffic.
```



```

    attribute:
      id-num: 9
      short: stream
      long: Indicates that the current connection is a ▶
a continues unidirectional stream of audio and / or video.

    attribute:
      id-num: 10
      short: android
      long: Indicates that the client side uses the ▶
operating system Android.

    attribute:
      id-num: 11
      short: ios
      long: Indicates that the client side uses the ▶
operating system iOS.

    attribute:
      id-num: 12
      short: windows-mobile
      long: Indicates that the client side uses the ▶
operating system Windows Mobile.

    attribute:
      id-num: 13
      short: blackberry
      long: Indicates that the client side uses the ▶
operating system Blackberry.

    attribute:
      id-num: 14
      short: picture
      long: Indicates that the current connection ▶
transfers pictures.

    attribute:
      id-num: 15
      short: ddl
      long: Indicates that the current connection is ▶
a Direct Download Host.

    attribute:
      id-num: 16
      short: google
      long: Indicates that the current connection is ▶
a Google service.

    attribute:
      id-num: 17
      short: outlook_web_access
      long: Indicates that the current connection ▶
uses the Microsoft Exchange Outlook Web Access as authentication ▶

```

```
mechanism.

    attribute:
        id-num: 18
        short: amazon-cloud
        long: Indicates that the current connection is a ►
a service of Amazon Cloud.

    attribute:
        id-num: 19
        short: apache
        long: Indicates that the server side is an ►
Apache server.

    attribute:
        id-num: 20
        short: mysql-server
        long: Indicates that the server side is a MySQL ►
database server.

    attribute:
        id-num: 21
        short: mariadb-server
        long: Indicates that the server side is a ►
MariaDB database server.

    attribute:
        id-num: 22
        short: ntlm
        long: Current connection uses NTLM as ►
authentication mechanism.

    attribute:
        id-num: 23
        short: microsoft-windows
        long: Indicates that the client side is the ►
operating system Microsoft Windows.

    attribute:
        id-num: 24
        short: chrome
        long: Indicates that the client side is the ►
operating system Chrome.

    attribute:
        id-num: 25
        short: akamai-cloud
        long: Indicates that the current connection is ►
a service of Akamai Cloud.

    attribute:
        id-num: 26
        short: dox
        long: Indicates that the current connection is ►
```

DoT (DNS over TLS) or DoH (DNS over HTTPS).

```

attribute:
  id-num: 27
  short: rcs
  long: Indicates that the current connection is ►
RCS (Rich Communication Services).
```

History

Version	Description
3.07	The show ntce attributes command has been introduced.

3.159.89 show ntce filter profile

Description Show system list of *NTCE* filter profiles.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ntce filter profile** [<name>]

Arguments

Argument	Value	Description
name	<i>String</i>	The <i>NTCE</i> filter name. You can see the list of available filters with help of ntce filter profile [Tab] command.

Example

```
(show)> ntce filter profile
```

```

profile:
  name: test
  type: deny
  schedule:
  schedule-active: no
```

```

profile:
  name: test2
  type: deny
  schedule:
  schedule-active: no
```

```
(show)> ntce filter profile test
```

```

profile:
  name: test
```

```

        type: deny
    schedule:
    schedule-active: no

```

History

Version	Description
4.02	The show ntce filter profile command has been introduced.

3.159.90 show ntce groups

Description Show the list of groups supported by the [NTCE](#) service.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ntce groups**

Example

```

(show)> ntce groups

    group:
        id-num: 2048
        long: Generic
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2049
        long: Peer to Peer
    groupset-id: 6
groupset-short-id: filetransferring
groupset-long-id: File transferring

    group:
        id-num: 2050
        long: Gaming
    groupset-id: 1
groupset-short-id: gaming
groupset-long-id: Gaming

    group:
        id-num: 2051
        long: Tunnel
    groupset-id: 3
groupset-short-id: work
groupset-long-id: Work & Learn from home

```

```

    group:
      id-num: 2052
      long: Business
    groupset-id: 3
groupset-short-id: work
groupset-long-id: Work & Learn from home

    group:
      id-num: 2053
      long: E-Commerce
    groupset-id: 3
groupset-short-id: work
groupset-long-id: Work & Learn from home

    group:
      id-num: 2054
      long: Voice over IP
    groupset-id: 0
groupset-short-id: calling
groupset-long-id: Calling and conferencing

    group:
      id-num: 2055
      long: Messaging
    groupset-id: 0
groupset-short-id: calling
groupset-long-id: Calling and conferencing

    group:
      id-num: 2056
      long: Streaming
    groupset-id: 2
groupset-short-id: streaming
groupset-long-id: Video & Audio streaming

    group:
      id-num: 2057
      long: Mobile
    groupset-id: 0
groupset-short-id: calling
groupset-long-id: Calling and conferencing

    group:
      id-num: 2058
      long: Remote Control
    groupset-id: 3
groupset-short-id: work
groupset-long-id: Work & Learn from home

    group:
      id-num: 2059
      long: Mail
    groupset-id: 3
groupset-short-id: work

```

```
groupset-long-id: Work & Learn from home

    group:
        id-num: 2060
        long: Network Management
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2061
        long: Database
    groupset-id: 3
groupset-short-id: work
groupset-long-id: Work & Learn from home

    group:
        id-num: 2062
        long: Filetransfer
    groupset-id: 6
groupset-short-id: filetransferring
groupset-long-id: File transferring

    group:
        id-num: 2063
        long: Web
    groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing

    group:
        id-num: 2064
        long: Conference
    groupset-id: 0
groupset-short-id: calling
groupset-long-id: Calling and conferencing

    group:
        id-num: 2065
        long: Social
    groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing

    group:
        id-num: 2066
        long: Sharehosting
    groupset-id: 6
groupset-short-id: filetransferring
groupset-long-id: File transferring

    group:
        id-num: 2067
        long: Deprecated
```

```

    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2068
        long: Industrial
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2069
        long: Encrypted
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2070
        long: Advertisement and Analytic Services
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2071
        long: News
    groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing

    group:
        id-num: 2072
        long: Health and Fitness
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2073
        long: Cloud and CDN Services
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2074
        long: Navigation
    groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing

    group:

```

```
        id-num: 2075
        long: Finance
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2076
        long: Travel and Transportation
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2077
        long: Pornography
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2078
        long: Books and Magazines
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2079
        long: Audio Entertainment
    groupset-id: 2
groupset-short-id: streaming
groupset-long-id: Video & Audio streaming

    group:
        id-num: 2080
        long: Education
    groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

    group:
        id-num: 2081
        long: M2M and IoT
    groupset-id: 3
groupset-short-id: work
groupset-long-id: Work & Learn from home

    group:
        id-num: 2082
        long: Device Security
    groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing
```



```

      group:
        id-num: 2083
        long: Multimedia Service Providers
      groupset-id: 2
groupset-short-id: streaming
groupset-long-id: Video & Audio streaming

      group:
        id-num: 2084
        long: Organizers
      groupset-id: 3
groupset-short-id: work
groupset-long-id: Work & Learn from home

      group:
        id-num: 2085
        long: Enterprise Services
      groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing

      group:
        id-num: 2086
        long: App-Stores and OS Updates
      groupset-id: 6
groupset-short-id: filetransferring
groupset-long-id: File transferring

      group:
        id-num: 2087
        long: Browsers
      groupset-id: 4
groupset-short-id: surfing
groupset-long-id: Web surfing

      group:
        id-num: 2088
        long: Removed
      groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

      group:
        id-num: 2089
        long: Moved
      groupset-id: 5
groupset-short-id: other
groupset-long-id: Other

```

History

Version	Description
3.07	The show ntce groups command has been introduced.

3.159.91 show ntce groupsets

Description Show the list of groupsets supported by the [NTCE](#) service.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> ntce groupsets`

Example `(show)> ntce groupsets`

```
groupset:
  id-num: 0
  short: calling
  long: Calling and conferencing

groupset:
  id-num: 1
  short: gaming
  long: Gaming

groupset:
  id-num: 2
  short: streaming
  long: Video & Audio streaming

groupset:
  id-num: 3
  short: work
  long: Work & Learn from home

groupset:
  id-num: 4
  short: surfing
  long: Web surfing

groupset:
  id-num: 5
  short: other
  long: Other

groupset:
  id-num: 6
  short: filetransferring
  long: File transferring
```

History	Version	Description
	3.07	The show ntce groupsets command has been introduced.

3.159.92 show ntce hosts

Description	Show application statistics, which <i>NTCE</i> service has detected for hosts.
Prefix no	No
Change settings	No
Multiple input	No

Synopsis (show)> **ntce hosts**

Example (show)> **ntce hosts**

```

    host:
      mac: 04:d4:c4:54:31:12

    application:
      id-num: 7
      short: twitter
      long: Twitter
      group-id: 2065
      group-long: Social
      groupset-id: 4
      groupset-short-id: surfing
      groupset-long-id: Web surfing
    groupset-service-class: 2
      rxbytes: 62274
      txbytes: 6020

    application:
      id-num: 43
      short: instagram
      long: Instagram
      group-id: 2065
      group-long: Social
      groupset-id: 4
      groupset-short-id: surfing
      groupset-long-id: Web surfing
    groupset-service-class: 2
      rxbytes: 57606
      txbytes: 11148

    application:
      id-num: 428
      short: spotify
      long: Spotify
```

```

        group-id: 2079
        group-long: Audio Entertainment
        groupset-id: 2
        groupset-short-id: streaming
        groupset-long-id: Video & Audio streaming
groupset-service-class: 2
        rxbytes: 155317
        txbytes: 80526

application:
        id-num: 438
        short: whatsapp
        long: WhatsApp
        group-id: 2055
        group-long: Messaging
        groupset-id: 0
        groupset-short-id: calling
        groupset-long-id: Calling and conferencing
groupset-service-class: 2
        rxbytes: 826
        txbytes: 706

application:
        id-num: 461
        short: google-cloud
        long: Google Cloud
        group-id: 2073
        group-long: Cloud and CDN Services
        groupset-id: 5
        groupset-short-id: other
        groupset-long-id: Other
groupset-service-class: 2
        rxbytes: 313
        txbytes: 352

application:
        id-num: 498
        short: telegram
        long: Telegram
        group-id: 2055
        group-long: Messaging
        groupset-id: 0
        groupset-short-id: calling
        groupset-long-id: Calling and conferencing
groupset-service-class: 2
        rxbytes: 109895
        txbytes: 15561

application:
        id-num: 559
        short: google-play
        long: Google Play
        group-id: 2086
        group-long: App-Stores and OS Updates

```

```

        groupset-id: 6
        groupset-short-id: filetransferring
        groupset-long-id: File transferring
groupset-service-class: 2
        rxbytes: 16736
        txbytes: 28451

application:
        id-num: 611
        short: zendesk
        long: ZenDesk
        group-id: 2052
        group-long: Business
        groupset-id: 3
        groupset-short-id: work
        groupset-long-id: Work & Learn from home
groupset-service-class: 2
        rxbytes: 101697
        txbytes: 187527

application:
        id-num: 621
        short: slack
        long: Slack
        group-id: 2064
        group-long: Conference
        groupset-id: 0
        groupset-short-id: calling
        groupset-long-id: Calling and conferencing
groupset-service-class: 2
        rxbytes: 30568
        txbytes: 3650

application:
        id-num: 632
        short: google-services
        long: Google Shared Services
        group-id: 2085
        group-long: Enterprise Services
        groupset-id: 4
        groupset-short-id: surfing
        groupset-long-id: Web surfing
groupset-service-class: 2
        rxbytes: 614512
        txbytes: 202174

application:
        id-num: 664
        short: microsoft-services
        long: Microsoft Services
        group-id: 2085
        group-long: Enterprise Services
        groupset-id: 4
        groupset-short-id: surfing

```

```
        groupset-long-id: Web surfing
groupset-service-class: 2
        rxbytes: 20243
        txbytes: 10699

application:
        id-num: 700
        short: fastly
        long: Fastly
        group-id: 2073
        group-long: Cloud and CDN Services
        groupset-id: 5
        groupset-short-id: other
        groupset-long-id: Other
groupset-service-class: 2
        rxbytes: 14859
        txbytes: 3147

application:
        id-num: 703
        short: cloudflare
        long: Cloudflare
        group-id: 2073
        group-long: Cloud and CDN Services
        groupset-id: 5
        groupset-short-id: other
        groupset-long-id: Other
groupset-service-class: 2
        rxbytes: 2172
        txbytes: 3593

application:
        id-num: 719
        short: google-apis
        long: Google APIs
        group-id: 2052
        group-long: Business
        groupset-id: 3
        groupset-short-id: work
        groupset-long-id: Work & Learn from home
groupset-service-class: 2
        rxbytes: 11837
        txbytes: 7602

application:
        id-num: 933
        short: bamtech-media
        long: BAMTech Media
        group-id: 2083
        group-long: Multimedia Service Providers
        groupset-id: 2
        groupset-short-id: streaming
        groupset-long-id: Video & Audio streaming
groupset-service-class: 2
```

```

        rxbytes: 4734
        txbytes: 6006

    os-id: 3
    os-long: Windows

    host:
        mac: 04:d4:c4:54:31:12
        via: 04:d4:c4:54:31:12
        ip: 192.168.11.19
        hostname: MyHost
        name: MyHost

    interface:
        id: Bridge0
        name: Home
        description: Home network

        dhcp:
            static: yes

    registered: yes
    access: permit
    schedule:
        active: yes
        rxbytes: 0
        txbytes: 0
        uptime: 9083
    first-seen: 9097
    last-seen: 1
    link: up
    auto-negotiation: yes
    speed: 1000
    duplex: yes
    port: 2

    traffic-shape:
        rx: 0
        tx: 0
        mode: mac
        schedule:

```

History

Version	Description
3.07	The show ntce hosts command has been introduced.

3.159.93 show ntce oses

Description Show the list of OSES supported by the [NTCE](#) service.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> ntce oses`

Example `(show)> ntce oses`

```
os:
id-num: 1
long: Not detected
```

```
os:
id-num: 2
long: Other
```

```
os:
id-num: 3
long: Windows
```

```
os:
id-num: 4
long: Linux
```

```
os:
id-num: 5
long: OS X
```

```
os:
id-num: 6
long: iOS
```

```
os:
id-num: 7
long: Symbian
```

```
os:
id-num: 8
long: Android
```

```
os:
id-num: 9
long: Blackberry
```

```
os:
id-num: 10
long: WindowsMobile
```

```
os:
id-num: 11
long: WindowsPhone
```

```
os:
```



```
id-num: 12
  long: Chrome

os:
id-num: 13
  long: Darwin
```

History

Version	Description
3.07	The show ntce oses command has been introduced.

3.159.94 show ntce status

Description Show *NTCE* service info.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **ntce status**

Example (show)> **ntce status**

```
conntack:
  hosts: 2
  applications: 16
  applications-flows: 63
  applications-events: 0
  groups: 12
  groups-flows: 64
  groups-events: 0

  memory:
    applications-flows: 1512
    applications-events: 0
    applications: 512
    groups-flows: 1536
    groups-events: 0
    groups: 384
    hosts: 72
    total: 4016

  event:
    count: 0

  memory:
    total: 0

database:
```

```

        hosts: 1
    applications: 54
        groups: 30
        attributes: 6

    memory:
        applications: 2372976
        groups: 1318320
        attributes: 263664
        total: 3954960

```

History

Version	Description
3.07	The show ntce status command has been introduced.

3.159.95 show ntp status

Description Show *NTP* system settings.

NTP state general info

- ❶ The time elapsed since the last synchronization in seconds.
- ❷ The indicator of the last synchronization.
- ❸ The indicator of the initial synchronization.
- ❹ Time is taken from NDSS server.
- ❺ Time is set by the user manually.

Prefix no No

Change settings No

Multiple input No

Synopsis | (show)> **ntp status**

Example (show)> **ntp status**

```

    status:
        elapsed: 435146 ❶
        server: 1.pool.ntp.org
        accurate: yes ❷
    synchronized: yes ❸
        ndsstime: no ❹
        usertime: no ❺

```

History

Version	Description
2.00	The show ntp status command has been introduced.

3.159.96 show oc-server

Description	Show current connections to the <i>OpenConnect</i> server.
Prefix no	No
Change settings	No
Multiple input	No
Synopsis	(show)> oc-server

Example

```
(show)> oc-server

      ndns-name: mywrk.keenetic.link
            fqdn: 12af.mywrk.keenetic.link
            secret: 123e45ed
has-ndns-certificate: yes

      tunnel:
clientaddress: 172.16.3.34
      username: mymy
            uptime: 30

      statistic:
            rxpackets: 121
rx-multicast-packets: 0
rx-broadcast-packets: 0
            rxbytes: 14715
            rxerrors: 0
            rxdropped: 0
            txpackets: 78
tx-multicast-packets: 0
tx-broadcast-packets: 0
            txbytes: 48265
            txerrors: 0
            txdropped: 0
            timestamp: 104530.202229
last-overflow: 0.000000
```

History	Version	Description
	4.02	The show oc-server command has been introduced.

3.159.97 show ping-check

Description	Show <i>Ping Check</i> profile status. If you use no arguments, the command displays information about all profiles.
Prefix no	No

Change settings No

Multiple input No

Synopsis (show)> **ping-check** [*profile_name*]

Arguments

Argument	Value	Description
profile_name	<i>String</i>	Profile name.

Example

```
(show)> ping-check

    pingcheck:
      profile: TEST
      host: 8.8.8.8
      port: 80
    max-fails: 7
      timeout: 1
      mode: connect

    interface: ISP
      fail count: 0
      status: pass

    pingcheck:
      profile: TEST1
      mode: icmp

    pingcheck:
      profile: TEST2
      mode: icmp
```

History

Version	Description
2.04	The show ping-check command has been introduced.

3.159.98 show printers

Description Show attached printer list.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **printers**

Example (show)> **printers**

```
printers:
  printer: Canon MF8300C Series
```

History

Version	Description
2.00	The show printers command has been introduced.

3.159.99 show processes

Description Show statistics of CPU usage by services and processes.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **processes**

Example

```
(show)> processes

process, id = NETBIOS browser:
  name: nqnd

  arg: -i

  arg: 50ff20001e87

  state: S (sleeping)
  pid: 629
  ppid: 192
  vm-size: 3188 kB
  vm-data: 1548 kB
  vm-stk: 136 kB
  vm-exe: 4 kB
  vm-lib: 1448 kB
  vm-swap: 0 kB
  threads: 1
  fds: 15

statistics:
  interval: 30

  cpu:
    now: 17319.483753
    min: 0
    max: 0
    avg: 0
    cur: 0

service:
```

```

        configured: yes
        alive: yes
        started: yes
        state: STARTED

process, id = Dns::Proxy::Policy0:
    name: ndnproxy

    arg: -c

    arg: /var/ndnproxy_Policy0.conf

    arg: -p

    arg: /var/ndnproxy_Policy0.pid

    state: S (sleeping)
    pid: 630
    ppid: 192
    vm-size: 1676 kB
    vm-data: 504 kB
    vm-stk: 136 kB
    vm-exe: 108 kB
    vm-lib: 896 kB
    vm-swap: 0 kB
    threads: 1
    fds: 10

statistics:
    interval: 30

    cpu:
        now: 17319.483764
        min: 0
        max: 0
        avg: 0
        cur: 0

service:
    configured: yes
    alive: yes
    started: yes
    state: STARTED

```

History

Version	Description
2.09	The show processes command has been introduced.

3.159.100 show running-config

Description	Show current settings, that is file system: running-config contains, just like command more does.
Prefix no	No
Change settings	No
Multiple input	No
Synopsis	<code>(show)> running-config</code>

Example

```
(show)> running-config
! $$$ Model: Keenetic Hopper
! $$$ Version: 2.06.1
! $$$ Agent: default
! $$$ Md5 checksum: 8c4b233db9ff35f1ea2fff277e36d9ea
! $$$ Username: admin
system
  set net.ipv4.ip_forward 1
  set net.ipv4.tcp_fin_timeout 30
  set net.ipv4.tcp_keepalive_time 120
  set net.ipv4.neigh.default.gc_thresh1 256
  set net.ipv4.neigh.default.gc_thresh2 1024
  set net.ipv4.neigh.default.gc_thresh3 2048
  set net.ipv6.neigh.default.gc_thresh1 256
  set net.ipv6.neigh.default.gc_thresh2 1024
  set net.ipv6.neigh.default.gc_thresh3 2048
  set net.netfilter.nf_conntrack_tcp_timeout_established 1200
  set net.netfilter.nf_conntrack_max 32768
  set vm.swappiness 60
  set vm.overcommit_memory 0
  set vm.vfs_cache_pressure 1000
  set dev.usb.force_usb2 0
  set net.ipv6.conf.all.forwarding 1
  domainname WORKGROUP
  hostname Keenetic-1111
  caption default
!
isolate-private
user admin
  tag cli
  tag http
  tag cifs
  tag printers
  tag webdav
!
interface FastEthernet0
  up
!
interface FastEthernet0/0
  rename 1
```

```
switchport mode access
switchport mode trunk
switchport access vlan 1
switchport trunk vlan 3
up
!
interface FastEthernet0/1
  rename 2
  switchport mode access
  switchport mode trunk
  switchport access vlan 1
  switchport trunk vlan 3
  up
!
interface FastEthernet0/2
  rename 3
  switchport mode access
  switchport mode trunk
  switchport access vlan 1
  switchport trunk vlan 3
  up
!
interface FastEthernet0/Vlan1
  description "Home VLAN"
  ip dhcp client dns-routes
  up
!
interface FastEthernet0/Vlan3
  description "Guest VLAN"
  ip dhcp client dns-routes
  up
!
interface GigabitEthernet1
  rename ISP
  description "Broadband connection"
  mac address factory wan
  security-level public
  ip address dhcp
  ip dhcp client dns-routes
  ip global 700
  igmp upstream
  ipv6 address auto
  ipv6 prefix auto
  ipv6 name-servers auto
  up
!
interface GigabitEthernet1/0
  rename 0
  up
!
interface WifiMaster0
  compatibility BGN+AX
  tx-burst
  rekey-interval 86400
```



```

        beamforming explicit
        vht
        downlink-mumimo
        uplink-mumimo
        spatial-reuse
        up
    !
interface WifiMaster0/AccessPoint0
    rename AccessPoint
    description "Wi-Fi access point"
    mac access-list type none
    wps
    authentication wpa-psk ns3 BMclwe4ZX9/fbJtDiM
    encryption enable
    encryption wpa2
    ip dhcp client dns-routes
    ssid Keenetic-1111
    wmm
    rrm
    ft mdid PX
    ft enable
    up
    !
interface WifiMaster0/AccessPoint1
    rename GuestWiFi
    description "Guest access point"
    mac access-list type none
    ip dhcp client dns-routes
    ssid Guest
    wmm
    rrm
    ft mdid vX
    ft enable
    down
    !
interface WifiMaster0/AccessPoint2
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
    !
interface WifiMaster0/AccessPoint3
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
    !
interface WifiMaster0/AccessPoint4
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
    !
interface WifiMaster0/AccessPoint5

```

```
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
!
interface WifiMaster0/AccessPoint6
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
!
interface WifiMaster0/WifiStation0
    security-level public
    encryption disable
    ip dhcp client dns-routes
    down
!
interface WifiMaster1
    compatibility AN+AC+AX
    tx-burst
    rekey-interval 86400
    beamforming explicit
    target-waketime
    downlink-mumimo
    uplink-mumimo
    spatial-reuse
    up
!
interface WifiMaster1/AccessPoint0
    rename AccessPoint_5G
    description "5GHz Wi-Fi access point"
    mac access-list type none
    wps
    authentication wpa-psk ns3 BMc0w7dA7GF04ZX9/fbJtDiM
    encryption enable
    encryption wpa2
    ip dhcp client dns-routes
    ssid Keenetic-1111
    wmm
    rrm
    ft mdid PX
    ft enable
    follow AccessPoint
    up
!
interface WifiMaster1/AccessPoint1
    rename GuestWiFi_5G
    description "5GHz Guest access point"
    mac access-list type none
    encryption disable
    ip dhcp client dns-routes
    ssid Guest
    rrm
    ft mdid vX
```

```

    ft enable
    follow GuestWiFi
    down
!
interface WifiMaster1/AccessPoint2
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
!
interface WifiMaster1/AccessPoint3
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
!
interface WifiMaster1/AccessPoint4
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
!
interface WifiMaster1/AccessPoint5
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
!
interface WifiMaster1/AccessPoint6
    mac access-list type none
    security-level private
    ip dhcp client dns-routes
    down
!
interface WifiMaster1/WifiStation0
    security-level public
    encryption disable
    ip dhcp client dns-routes
    down
!
interface Bridge0
    rename Home
    description "Home network"
    inherit GigabitEthernet0/Vlan1
    include AccessPoint
    include AccessPoint_5G
    mac access-list type none
    security-level private
    ip address 192.168.1.1 255.255.255.0
    ip dhcp client dns-routes
    igmp downstream
    band-steering
    iapp key ns3 4k/XpM98jF123131NK9eur5Jk7Cgq4PpBm4M6U+hwh27
    up

```

```

!
interface Bridge1
    rename Guest
    description "Guest network"
    traffic-shape rate 5120
    inherit GigabitEthernet0/Vlan3
    include GuestWiFi
    include GuestWiFi_5G
    mac access-list type none
    peer-isolation
    security-level protected
    ip address 10.1.30.1 255.255.255.0
    ip dhcp client dns-routes
    iapp key ns3 +lIvt9ohKnXsiIt131312jPtqCJfqtVjrdm/MCVxzNY0H
    down
!
ip dhcp pool _WEBADMIN
    range 192.168.1.33 192.168.1.152
    bind Home
    enable
!
ip dhcp pool _WEBADMIN_GUEST_AP
    range 10.1.30.33 10.1.30.152
    bind Guest
    enable
!
ip http security-level private
ip http lockout-policy 5 15 3
ip http ssl enable
ip http webdav
    security-level public
!
ip nat Home
ip nat Guest
ip telnet
    security-level private
    lockout-policy 5 15 3
!
ipv6 subnet Default
    bind Home
    mode slaac
    prefix length 64
    number 0
!
ipv6 local-prefix default
ppe software
ppe hardware
upnp lan Home
service dhcp
service dns-proxy
service igmp-proxy
service http
service cifs
service telnet

```

```

service ntp
service upnp
cifs
    automount
    permissive
!
dns-proxy
    rebind-protect auto
!

```

History

Version	Description
2.00	The show running-config command has been introduced.

3.159.101 show schedule

Description Show parameters of defined schedule. If you use no argument, the entire list of system schedules will be displayed.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **schedule** [<name>]

Arguments

Argument	Value	Description
name	<i>String</i>	A schedule name.

Example

```

(show)> schedule 123

    schedule, name = 123:
        action, type = start, left = 561514, next = yes:
            dow: Tue
            time: 01:29

        action, type = stop, left = 564274:
            dow: Tue
            time: 02:15

```

History

Version	Description
2.06	The show schedule command has been introduced.

3.159.102 show self-test

Description Show summary information about system activity. Need to provide remote technical support.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **self-test**

History

Version	Description
2.00	The show self-test command has been introduced.

3.159.103 show site-survey

Description Show available wireless networks.

Prefix no No

Change settings No

Multiple input No

Interface type Radio

Synopsis (show)> **site-survey** <name>

Arguments

Argument	Value	Description
name	<i>Interface</i>	Full name or an alias of the interface. You can see the list of available interfaces with help of site-survey [Tab] command.

Example

(show)> site-survey WifiMaster0				
SSID		MAC	Ch	Mode ►
Q				
Hello_123		11:22:d4:70:97:f1	1	►
11b/g/n	31			
BRT		78:69:87:b3:9d:68	1	►
11b/g/n	13			
SVH34-34		23:bf:45:7b:0e:2e	1	►
11b/g/n	5			

Keenetic-1234	56:f4:ab:56:9a:48	3	►
11b/g/n 26			
(show)> site-survey WifiMaster1			
SSID	MAC	Ch	Mode ►
Q			
Keenetic-1153 (5)	34:ff:22:3d:69:fc	36	►
11a/n/ac 2			
RT-5WiFi-87F8	15:a3:b8:e6:57:fa	44	►
11a/n/ac 42			
GPON5	23:9a:34:b1:b1:26	48	►
11a/n/ac 0			

History

Version	Description
2.00	The show site-survey command has been introduced.

3.159.104 show snmp view

Description Show *SNMP* view status.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **snmp view**

Example

```
(show)> snmp view

view:
    id: client

    include: .1.3.6.1

    exclude: .1.3.6.1.2
```

History

Version	Description
4.01	The show snmp view command has been introduced.

3.159.105 show ssh fingerprint

Description Show current SSH server keys.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> ssh fingerprint`

Example

```
(show)> ssh fingerprint

rsa: MD5:d0:b0:d4:f7:da:7b:c0:e0:d0:c8:8f:ea:85:3c:09:00

rsa: SHA1:Nhxcg8KNeE62E8zAZJngImcrJkma

rsa: SHA256:LM7MyrIaq4qFGT/dyF/t8TbJk5tCzreeGuh03zaydu4

ecdsa: ►
MD5:a6:db:b4:fb:3c:b9:ae:31:ca:6d:ca:ed:62:73:a5:7e

ecdsa: SHA1:ndWg/dx/dP/P8rMkJcVC3XB8nFo

ecdsa: ►
SHA256:Wp1K9d8MsquQBtlBeBlpVlyKdCN1Vay3BtBwbj0xs+o
```

History

Version	Description
2.12	The show ssh fingerprint command has been introduced.

3.159.106 show ssh sftp

Description Show home directories for users with **sftp** tag.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> ssh sftp`

Example

```
(show)> ssh sftp

enabled: yes
permissive: yes
root: files_ssd:/
path: /tmp/mnt/963b0583-4017-401b-9542-7ff1255add40

user, index = 0:
name: admin
root:
path: ►
```


History

Version	Description
3.04	The show ssh sftp command has been introduced.

3.159.107 show sstp-server

Description Show current connections to the [SSTP](#) server.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **sstp-server**

Example

```
(show)> sstp-server

    enabled: yes
    ndns-name: mymy.keenetic.link
has-ndns-certificate: yes

    tunnel:
    clientaddress: 172.16.3.33
      username: mymy
      uptime: 29

    statistic:
      rxpackets: 121
    rx-multicast-packets: 0
    rx-broadcast-packets: 0
      rxbytes: 14715
      rxerrors: 0
      rxdropped: 0
      txpackets: 78
    tx-multicast-packets: 0
    tx-broadcast-packets: 0
      txbytes: 48265
      txerrors: 0
      txdropped: 0
      timestamp: 104530.202229
      last-overflow: 0.000000
```

History

Version	Description
2.12	The show sstp-server command has been introduced.

3.159.108 show system

Description Show the general state of the system.

System state general info

- ❶ CPU load, percentage.
- ❷ Occupied and available memory info, kilobytes.
- ❸ Swap file usage info, kilobytes.
- ❹ System uptime from the start, seconds.

Prefix no No**Change settings** No**Multiple input** No**Synopsis** (show)> **system****Example** (config)> **show system**

```

hostname: Undefined
domainname: WORKGROUP
cpuload: 0 ❶
memory: 13984/28976 ❷
swap: 0/0 ❸
uptime: 153787 ❹

```

History

Version	Description
2.00	The show system command has been introduced.

3.159.109 show system country**Description** Show country-specific configuration status depending on the factory region.**Prefix no** No**Change settings** No**Multiple input** No**Synopsis** (show)> **system country****Example** (show)> **system country**

```

factory: EA
selected: KZ
default-language: ru

country:
    code: AM
    short-name: Armenia
    default-language: en

```

```

country:
  code: AZ
  short-name: Azerbaijan
default-language: en

country:
  code: BY
  short-name: Belarus
default-language: ru

country:
  code: KG
  short-name: Kyrgyzstan
default-language: en

country:
  code: KZ
  short-name: Kazakhstan
default-language: ru

country:
  code: RU
  short-name: Russian Federation
default-language: ru

country:
  code: UZ
  short-name: Uzbekistan
default-language: en

```

History

Version	Description
4.00	The show system country command has been introduced.

3.159.110 show system cpustat

Description Show device CPU usage.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **system cpustat**

Example (show)> **system cpustat**

```

interval: 36

```

```

    busy:
        cur: 1
        min: 0
        max: 11
        avg: 2

    user:
        cur: 0
        min: 0
        max: 10
        avg: 1

    nice:
        cur: 0
        min: 0
        max: 0
        avg: 0

    system:
        cur: 0
        min: 0
        max: 2
        avg: 0

    iowait:
        cur: 0
        min: 0
        max: 0
        avg: 0

    irq:
        cur: 0
        min: 0
        max: 0
        avg: 0

    sirq:
        cur: 0
        min: 0
        max: 0
        avg: 0

```

History

Version	Description
2.09	The show system cpustat command has been introduced.

3.159.111 show system zram

Description	Show system zRam swap status.
Prefix no	No

Change settings No

Multiple input No

Synopsis `(show)> system zram`

Example

```
(show)> system zram

      zram:
        enabled: yes
compression-algo: lzo
        disk-size: 268435456
        compressed-size: 87
        original-size: 4096
        total-memory-used: 12288
        compression-threads: 4
        compressed-ratio-pcs: 300
```

History

Version	Description
2.09	The show system zram command has been introduced.

3.159.112 show tags

Description Show available authentication tags.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> tags`

Example

```
(show)> tags

tag: cli
tag: readonly
tag: http-proxy
tag: http
tag: printers
tag: cifs
tag: ftp
tag: ipsec-xauth
tag: ipsec-l2tp
tag: opt
tag: sstp
tag: torrent
tag: vpn
```

History

Version	Description
2.00	The show tags command has been introduced.

3.159.113 show threads

Description Show the list of active threads in NDM.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **threads**

Example (show)> **threads**

```
thread:
  name: Cloud agent service
  tid: 518
lock_list_complete: yes
locks:

statistics:
  interval: 30

cpu:
  now: 17771.481435
  min: 0
  max: 0
  avg: 0
  cur: 0

thread:
  name: FTP brute force detection
  tid: 519
lock_list_complete: yes
locks:

statistics:
  interval: 30

cpu:
  now: 17771.481440
  min: 0
  max: 0
  avg: 0
  cur: 0
```

History

Version	Description
2.09	The show threads command has been introduced.

3.159.114 show torrent status

Description Show BitTorrent client status.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> torrent status`

Example `(show)> torrent status`

```
state: running
rpc-port: 8090
```

History

Version	Description
2.03	The show torrent status command has been introduced.

3.159.115 show upnp redirect

Description Show *UPnP* port translation rules. If you use no arguments, the entire list of translation rules will be displayed.

Prefix no No

Change settings No

Multiple input No

Interface type IP

Synopsis `(show)> upnp redirect [( <protocol> <interface> <port> ) | <index> ]`

Arguments

Argument	Value	Description
protocol	tcp	Rules with <i>TCP</i> protocol will be displayed.
	udp	Rules with <i>UDP</i> protocol will be displayed.
interface	<i>Interface</i>	Rules with specified interface name will be displayed.
port	<i>Integer</i>	Rules with specified port will be displayed.
index	<i>Integer</i>	Rule with specified number in the list will be displayed.

Example

```
(show)> upnp redirect udp ISP 11175

entry:
  index: 1
  interface: ISP
  protocol: udp
  port: 11175
  to-address: 192.168.15.206
  to-port: 11175
  description: Skype UDP at 192.168.12.286:11175 (2024)
  packets: 0
  bytes: 0
```

History

Version	Description
2.00	The show upnp redirect command has been introduced.

3.159.116 show usb

Description

Show list of USB-devices.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(show)> usb
```

Example

```
(show)> usb

device:
  name: 12F6-312F:
  label: PENDRIVE
  subsystem: storage
device:
  name: 69f2894d-56a1-4632-9521-dbd8c8ab5c53d:
  label: EXT3
  subsystem: storage
device:
  name: 4FCC-A585:
  label: FAT32
  subsystem: storage
device:
  name: 226F114C088FC43D:
  label: NTFS
  subsystem: storage
```

History

Version	Description
2.00	The show usb command has been introduced.

3.159.117 show version

Description	Show firmware version.
Prefix no	No
Change settings	No
Multiple input	No

Synopsis (show)> **version**

Example

```
(show)> version

      release: 2.10.C.1.0-0
      arch: mips

      ndm:
        exact: 0-d32118a
        cdate: 11 Dec 2017

      bsp:
        exact: 0-cbe0525
        cdate: 11 Dec 2017

      ndw:
        version: 4.2.3.92
        features: ►
wifi_button,flexible_menu,emulate_firmware_progress
        components: ►
ddns,dot1x,interface-extras,miniupnpd,nathelper-ftp,
        ►
nathelper-pptp,nathelper-sip,ppe,trafficcontrol,
        ►
cloudcontrol,base,components,corewireless,dhcpd,l2tp,
        ►
igmp,easyconfig,pingcheck,ppp,pptp,pppoe,ydns

      manufacturer: Keenetic Ltd.
      vendor: Keenetic
      series: KN
      model: Start (KN-1110)
      hw_version: 10118000
      hw_id: KN-1110
      device: Start
      class: Internet Center
```

History	Version	Description
	2.00	The show version command has been introduced.

3.159.118 show vpn-server

Description Show current connections to the VPN server.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **vpn-server**

Example (show)> **vpn-server**

```
tunnel:
clientaddress: 172.16.1.33
  username: test
  uptime: 3

statistic:
  rxpackets: 51
rx-multicast-packets: 0
rx-broadcast-packets: 0
  rxbytes: 5440
  rxerrors: 0
  rxdropped: 0
  txpackets: 46
tx-multicast-packets: 0
tx-broadcast-packets: 0
  txbytes: 9229
  txerrors: 0
  txdropped: 0
  timestamp: 146237.254244
last-overflow: 0.000000
```

History

Version	Description
2.04	The show vpn-server command has been introduced.

3.160 sms

Description Access to a group of commands to configure [SMS](#) on the interface.

Prefix no No

Change settings No

Multiple input No

Interface type Usb

Group entry (sms)

Synopsis (config)> **sms** <name>

Arguments

Argument	Value	Description
name	<i>Interface</i>	Interface with SMS service.

Example

```
(config)> sms UsbQmi0
(sms)>
```

History

Version	Description
3.03	The sms command has been introduced.

3.160.1 sms delete

Description Delete SMS message.

Prefix no No

Change settings No

Multiple input No

Synopsis (sms)> **delete** <id>

Arguments

Argument	Value	Description
id	<i>String</i>	Message ID.

Example

```
(sms)> delete sim-5
UsbQmi::Sms: "UsbQmi0": message deleted.
```

History

Version	Description
3.03	The sms delete command has been introduced.

3.160.2 sms list

Description Show a list of received SMS messages.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(sms)> list [ unread ] [ id <id> ] [ no-content ]
```

Arguments

Argument	Value	Description
unread	<i>Keyword</i>	Show a list of unread SMS messages only.
id	<i>Keyword</i>	Show message with the given identifier.
no-content	<i>Keyword</i>	Disable message text output.

Example

```
(sms)> list

nv-free-slots: 23
nv-total-slots: 23
sim-free-slots: 0
sim-total-slots: 15

messages, id = sim-0:
  read: yes
  from: +79658283425
  timestamp: Thu Aug 20 14:39:57 2020
  parts: 1
  total-parts: 1
  text: Accepted

messages, id = sim-1:
  read: yes
  from: MegaFon
  timestamp: Wed Sep  9 13:57:21 2020
  parts: 2
  total-parts: 2
  text: 636-269 – your personal login code.
      Do not share this code with anyone.

messages, id = sim-3:
  read: yes
  from: +79658283425
  timestamp: Wed Sep  9 16:32:26 2020
  parts: 1
  total-parts: 1
  text: Our time to your time to yes to

messages, id = sim-4:
  read: yes
  from: +79658283425
  timestamp: Mon Sep 14 17:14:11 2020
  parts: 1
  total-parts: 1
  text: Ok

messages, id = sim-5:
  read: yes
  from: MegaFon
```

```

        timestamp: Wed Sep 16 10:24:46 2020
        parts: 7
        total-parts: 7
        text: Listen to audiobooks on management, ►
leadership,
        personal efficiency and self-development ►
2 weeks free!
        Just subscribe to the MegaFon AudioBooks ►
and
        listen to them without advertising on any ►
convenient device.
        The cost after the trial period - 1 euro ►
/ day.
        Payment from the phone account without ►
card binding. Cancel
        subscriptions at any time: pay only for ►
days
        of usage. Learn more:
        http://i.megafon.com/Q2XadzRp9xusLwS1

messages, id = sim-12:
        read: no
        from: +79252384670
        timestamp: Fri Sep 18 19:02:27 2020
        parts: 3
        total-parts: 4
        text: This subscriber left you 18.09.2020 at ►
18:35
        voice message. You can listen to it for ►
free by
        number 0525. / Listen to podcasts and ►
book parodies in
        convenient application without advertising ►
for 5 e/d. Detailed[...].

(sms)> list id xnv-64

        nv-free-slots: 68
        nv-total-slots: 128
        sim-free-slots: 15
        sim-total-slots: 15
        messages-count: 1

        messages, id = xnv-64:
                read: yes
                from: mTinkoff
                timestamp: Sat Jul 3 17:30:46 2021
                parts: 2
                total-parts: 2
                text: Replenishment: 10.00 €. Available: 31.00 €.

```

```
(sms)> list no-content

nv-free-slots: 12
nv-total-slots: 23
sim-free-slots: 10
sim-total-slots: 10
messages-count: 5

messages, id = nv-3:
    read: yes

messages, id = nv-7:
    read: yes

messages, id = nv-2:
    read: yes

messages, id = nv-0:
    read: yes

messages, id = nv-1:
    read: yes
```

History

Version	Description
3.03	The sms list command has been introduced.
3.07	The id and no-content arguments were added.

3.160.3 sms read

Description Mark SMS as read.

Command with **no** prefix return unread SMS mark.

Prefix no Yes

Change settings No

Multiple input No

Synopsis `(sms)> read <id>`

Argument	Value	Description
id	String	Message ID.

Example

```
(sms)> read sim-5
UsbQmi::Sms: "UsbQmi0": message marked as read.

(sms)> no read sim-5
UsbQmi::Sms: "UsbQmi0": message marked as unread.
```

History	Version	Description
	3.03	The sms read command has been introduced.

3.160.4 sms send

Description Send SMS to specified number. The maximum value of saved incoming SMS messages in the router's memory is 128. If the memory is full, the oldest SMS from the memory will be automatically deleted when a new SMS is received.

Prefix no No

Change settings No

Multiple input No

Synopsis `(sms)> send <to> <message>`

Arguments	Argument	Value	Description
	to	<i>String</i>	The receiver's phone number.
	message	<i>String</i>	Text message to send.

Example `(sms)> send +79261122777 "hello world!"`
 UsbQmi::Sms: "UsbQmi0": message sent.

History	Version	Description
	3.03	The sms send command has been introduced.

3.161 snmp community

Description Set new name for *SNMP* community. By default, common name public is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(config)> snmp community <community>`
`(config)> no snmp community`

Arguments

Argument	Value	Description
community	<i>String</i>	New community name.

Example

```
(config)> snmp community Co_test
Snmp::Manager: SNMP community set to "Co_test".
(config)> no snmp community
Snmp::Manager: SNMP community reset to "public".
```

History

Version	Description
2.08	The snmp community command has been introduced.

3.162 snmp contact

Description

Assign the contact name of *SNMP* agent. By default, the name is not defined.

Command with **no** prefix resets setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> snmp contact <contact>
```

```
(config)> no snmp contact
```

Arguments

Argument	Value	Description
contact	<i>String</i>	<i>SNMP</i> contact info.

Example

```
(config)> snmp contact Cont_test
Snmp::Manager: SNMP contact info set to "Cont_test".
(config)> no snmp contact
Snmp::Manager: SNMP community info reset.
```

History

Version	Description
2.08	The snmp contact command has been introduced.

3.163 snmp location

Description

Assign the location of *SNMP* agent. By default, the location is not defined.

Command with **no** prefix resets setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config)> snmp location <location>
(config)> no snmp location
```

Arguments

Argument	Value	Description
location	<i>String</i>	SNMP device location.

Example

```
(config)> snmp location Odintsovo
Snmp::Manager: SNMP device location set to "Odintsovo".
(config)> no snmp location
Snmp::Manager: SNMP device location reset.
```

History

Version	Description
2.08	The snmp location command has been introduced.

3.164 snmp view

Description Create [SNMP](#) community with restricted access.

Command with **no** prefix removes community.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config)> snmp view <name>
(config)> no snmp view <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Community name in reduced form, not more than 32 characters. The maximum number of communities is 4.

Example

```
(config)> snmp view client
Snmp::Manager: Created view "client".

(config)> no snmp view client
Snmp::Manager: Removed view "client".
```

History

Version	Description
4.01	The snmp view command has been introduced.

3.165 snmp view exclude

Description

Add subtree exclusion from *SNMP* view.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> snmp view exclude <oid>
```

```
(config)> no snmp view exclude [ <oid> ]
```

Arguments

Argument	Value	Description
oid	<i>String</i>	Object identifier.

Example

```
(config)> snmp view client exclude mgmt
Snmp::Manager: "client": added excluded OID "mgmt".
```

```
(config)> no snmp view client exclude mgmt
Snmp::Manager: "client": removed excluded OID "mgmt".
```

History

Version	Description
4.01	The snmp view exclude command has been introduced.

3.166 snmp view include

Description

Add include subtree for *SNMP* view.

Command with **no** prefix removes the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config)> snmp view include <oid>
```

```
(config)> no snmp view include [ <oid> ]
```

Arguments

Argument	Value	Description
oid	<i>String</i>	Object identifier.

Example

```
(config)> snmp view client include internet
Snmp::Manager: "client": added included OID "internet".
```

```
(config)> no snmp view client include internet
Snmp::Manager: "client": removed included OID "internet".
```

History

Version	Description
4.01	The snmp view include command has been introduced.

3.167 sstp-server

Description Access to a group of commands to configure *SSTP* server parameters.

Prefix no No

Change settings No

Multiple input No

Group entry (sstp-server)

Synopsis

```
(config)> sstp-server
```

History

Version	Description
2.12	The sstp-server command has been introduced.

3.167.1 sstp-server allow-bridging

Description Enable Ethernet bridging mode for *SSTP* server. By default, this mode is disabled.

Note: The bridging mode is supported between Keenetic routers.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(sstp-server)> allow-bridging
```

```
(sstp-server)> no allow-bridging
```

Example

```
(sstp-server)> allow-bridging
SstpServer::Manager: Enabled Ethernet mode.
```

```
(sstp-server)> no allow-bridging
SstpServer::Manager: Disabled Ethernet mode.
```

History

Version	Description
3.09	The sstp-server allow-bridging command has been introduced.

3.167.2 sstp-server camouflage

Description

Enable the camouflage mode for the [SSTP](#) server, which provides greater security from remote service scanning. By default, the mode is disabled.

Command with **no** prefix disables the camouflage mode.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(sstp-server)> camouflage
```

```
(sstp-server)> no camouflage
```

Example

```
(sstp-server)> camouflage
SstpServer::Manager: Enabled camouflage mode.
```

```
(sstp-server)> no camouflage
SstpServer::Manager: Disabled camouflage mode.
```

History

Version	Description
4.02	The sstp-server camouflage command has been introduced.

3.167.3 sstp-server debug

Description

Enable debug mode for [SSTP](#) server. Detailed information about the progress of the [SSTP](#) client connection to the [SSTP](#) server is saved to the system log. By default, setting is disabled.

Command with **no** prefix disables the debug mode.

Prefix no

Yes

Change settings Yes**Multiple input** No

Synopsis

```
(sstp-server)> debug
```

```
(sstp-server)> no debug
```

Example

```
(sstp-server)> debug
SstpServer::Manager: Enabled debug.
```

```
(sstp-server)> no debug
SstpServer::Manager: Disabled debug.
```

History	Version	Description
	4.03	The sstp-server debug command has been introduced.

3.167.4 sstp-server dhcp route

Description Assign a route which is transmitted in DHCP INFORM messages to the [SSTP](#) server clients.

Command with **no** prefix cancels the specified route. If you use no arguments, the entire list of routes will be cleared.

Prefix no Yes**Change settings** Yes**Multiple input** Yes

Synopsis

```
(sstp-server)> dhcp route <address> <mask>
```

```
(sstp-server)> no dhcp route [ <address> <mask> ]
```

Arguments	Argument	Value	Description
	address	<i>IP address</i>	Network client address.
	mask	<i>IP-mask</i>	Network client mask. There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).

Example

```
(sstp-server)> dhcp route 192.168.2.0/24
SstpServer::Manager: Added DHCP INFORM route to ►
192.168.2.0/255.255.255.0.
```

```
(sstp-server)> no dhcp route
SstpServer::Manager: Cleared DHCP INFORM routes.
```

History

Version	Description
2.12	The sstp-server dhcp route command has been introduced.

3.167.5 sstp-server interface

Description

Bind *SSTP* server to the specified interface.

Command with **no** prefix unbinds the interface.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(sstp-server)> interface <interface>
```

```
(sstp-server)> no interface
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(sstp-server)> interface [Tab]
```

```
Usage template:
  interface {interface}
```

```
Choose:
```

```
  GigabitEthernet1
  ISP
  WifiMaster0/AccessPoint2
  WifiMaster1/AccessPoint1
  WifiMaster0/AccessPoint3
  WifiMaster0/AccessPoint0
  AccessPoint
  WifiMaster1/AccessPoint2
  WifiMaster0/AccessPoint1
  GuestWiFi
```

```
(sstp-server)> interface Bridge0
SstpServer::Manager: Bound to Bridge0.
```

History

Version	Description
2.12	The sstp-server interface command has been introduced.

3.167.6 sstp-server ipv6cp

Description Enable IPv6 support. DHCP IPv6 pools are created for each *SSTP* server. By default, the setting is disabled.

Command with **no** prefix disables IPv6 support.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(sstp-server)>  ipv6cp
(sstp-server)> no ipv6cp
```

Example

```
(sstp-server)> ipv6cp
SstpServer::Manager: IPv6 control protocol enabled.
```

```
(sstp-server)> no ipv6cp
SstpServer::Manager: IPv6 control protocol disabled.
```

History

Version	Description
3.00	The sstp-server ipv6cp command has been introduced.

3.167.7 sstp-server lcp echo

Description Specify the testing rules of the SSTP-connections with *LCP* echo tools.

Command with **no** prefix disables *LCP* echo.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(sstp-server)>  lcp echo <interval> <count> [adaptive]
(sstp-server)> no lcp echo
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	Interval between sending <i>LCP</i> echo, in seconds. If within the specified time interval there is no <i>LCP</i> echo request from the remote location, the same request will be sent there asking for response <i>LCP</i> reply.

Argument	Value	Description
count	<i>Integer</i>	The number of consecutive requests <i>LCP</i> echo sent, for which no response <i>LCP</i> reply was received. If count of <i>LCP</i> echo requests goes unanswered, the connection is terminated.
adaptive	<i>Keyword</i>	Pppd will send LCP echo-request frames only if no traffic was received from the peer since the last echo-request was sent.

Example

```
(sstp-server)> lcp echo 5 3
SstpServer::Manager: LCP echo parameters updated.
```

History

Version	Description
2.12	The sstp-server lcp echo command has been introduced.

3.167.8 sstp-server lcp force-pap

Description

Enforce the *PAP* authentication only for *SSTP* server.

Command with **no** prefix disables *PAP* authentication.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(sstp-server)> lcp force-pap
```

```
(sstp-server)> no lcp force-pap
```

Example

```
(sstp-server)> lcp force-pap
SstpServer::Manager: Forced PAP-only authentication.
```

```
(sstp-server)> no lcp force-pap
SstpServer::Manager: Disabled forcing PAP-only authentication.
```

History

Version	Description
3.05	The sstp-server lcp force-pap command has been introduced.

3.167.9 sstp-server mru

Description

Set *MRU* value to be transmitted to *SSTP* server. By default, 1350 value is used.

Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(sstp-server)> mru value
(sstp-server)> no mru
```

Arguments

Argument	Value	Description
value	<i>Integer</i>	<i>MRU</i> value. Can take values in the range from 128 to 1500 inclusively.

Example

```
(sstp-server)> mru 200
SstpServer::Manager: MRU set to 200.
```

History

Version	Description
2.12	The sstp-server mru command has been introduced.

3.167.10 sstp-server mtu

Description Set *MTU* value to be transmitted to *SSTP* server. By default, 1350 value is used.

Command with **no** prefix resets value to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(sstp-server)> mtu value
(sstp-server)> no mtu
```

Arguments

Argument	Value	Description
value	<i>Integer</i>	<i>MTU</i> value. Can take values in the range from 128 to 1500 inclusively.

Example

```
(sstp-server)> mtu 200
SstpServer::Manager: MTU set to 200.
```

History

Version	Description
2.12	The sstp-server mtu command has been introduced.

3.167.11 sstp-server multi-login

Description

Allow connection to [SSTP](#) server for multiple users from one account.

Command with **no** prefix disables this feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(sstp-server)> multi-login
```

```
(sstp-server)> no multi-login
```

Example

```
(sstp-server)> multi-login
SstpServer::Manager: Enabled multiple login.
```

History

Version	Description
2.12	The sstp-server multi-login command has been introduced.

3.167.12 sstp-server pool-range

Description

Assign a pool of addresses for the clients that connect to the [SSTP](#) server. By default, pool size 10 is used.

Command with **no** prefix removes a pool.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(sstp-server)> pool-range <begin> [ <size> ]
```

```
(sstp-server)> no pool-range
```

Arguments

Argument	Value	Description
begin	<i>IP address</i>	Start address of pool.
size	<i>Integer</i>	Pool size.

Example (sstp-server)> **pool-range 192.168.1.22 7**
 SstpServer::Manager: Configured pool range 192.168.1.22 to ► 192.168.1.28.

History	Version	Description
	2.12	The sstp-server pool-range command has been introduced.

3.167.13 sstp-server session-logout

Description Terminate an active or stalled session on the [SSTP](#) server.

Prefix no No

Change settings Yes

Multiple input No

Synopsis (sstp-server)> **session-logout** <session>

Arguments	Argument	Value	Description
	session	<i>Integer</i>	Identifier of the SSTP session (can be viewed using the show sstp-server command).

Example (sstp-server)> **session-logout 6**
 SstpServer::Manager: Session "6" is terminated.

History	Version	Description
	4.03	The sstp-server session-logout command has been introduced.

3.167.14 sstp-server session-preempt

Description Enable to preempt VPN sessions when [sstp-server multi-login](#) option is disabled for the [SSTP](#) server.

Command with **no** prefix disables the preempt.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis (sstp-server)> **session-preempt**

```
(sstp-server)> no session-preempt
```

Example

```
(sstp-server)> session-preempt
SstpServer::Manager: Enabled session preemption.
```

```
(sstp-server)> no session-preempt
SstpServer::Manager: Disabled session preemption.
```

History

Version	Description
4.03	The sstp-server session-preempt command has been introduced.

3.167.15 sstp-server static-ip

Description

Bind IP address to the user. User account must have sstp tag.

Command with **no** prefix removes binding.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(sstp-server)> static-ip <name> <address>
```

```
(sstp-server)> no static-ip <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Username.
address	<i>IP address</i>	IP address to bind.

Example

```
(sstp-server)> static-ip admin 192.168.1.22
SstpServer::Manager: Static IP 192.168.1.22 assigned to user ►
"admin".
```

History

Version	Description
2.12	The sstp-server static-ip command has been introduced.

3.168 system

Description

Access to a group of commands to configure global parameters.

Prefix no

No

Change settings	No
Multiple input	No
Group entry	(system)

Synopsis | (config)> **system**

History	Version	Description
	2.00	The system command has been introduced.

3.168.1 system button

Description Configure device buttons to handle specific actions. Available handlers depend on hardware configuration and installed modules.

Command with **no** prefix remove setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis | (system)> **button** <button> **on** <action> **do** <handler>
 | (system)> **no button** [<button> [**on** <action>]]

Argument	Value	Description
button	RESET	RESET button.
	WLAN	Wireless LAN button.
	FN	FN button.
action	click	Single click.
	double-click	Double click.
	hold	Push and hold for 3 seconds. RESET button hold is 10 seconds.
handler	FactoryReset	Reset system to factory defaults.
	Reboot	System reboot.
	WifiToggle	Switch Wi-Fi on/off.
	WifiGuestApToggle	Switch Guest Wi-Fi on/off.
	WpsStartMainAp	Start WPS (2.4GHz only).
	WpsStartMainAp5	Start WPS (5GHz only).

Argument	Value	Description
	WpsStartAllMainAp	Start WPS (all frequency bands).
	UnmountAll	Unmount all disks.
	DlnaDirectoryRescan	Search for new files.
	DlnaDirectoryFullRescan	Full rescan.
	TorrentAltSpeedToggle	Alternative speed on/off (component Transmission BitTorrent client required).
	TorrentClientStateToggle	Switch the BitTorrent client on/off (component Transmission BitTorrent client required).
	OpkgRunScript	Run the script on opkg-section, /etc/ndm/button.d/ folder (component OPKG required).

Example

```
(system)> button WLAN on double-click do WifiGuestApToggle
Core::Peripheral::Manager: "WLAN/double-click" handler set.
```

```
(system)> no button
Core::Peripheral::Manager: All button bindings reset.
```

```
(system)> no button FN1
Core::Peripheral::Manager: "FN1" button bindings reset.
```

History

Version	Description
2.03	The system button command has been introduced.
2.06	The OpkgRunScript handler was added.

3.168.2 system caption

Description Set the Web interface title and header for ease of navigation.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(system)> caption <template>`

Arguments

Argument	Value	Description
template	default	Combination of Brand and Model (for example, Keenetic Speedster).
	product	The Model name (for example, Speedster).
	description	The System description (for example, Speedster (KN-3010)).
	hwid	The Model identifier (for example, KN-3010).
	hostname	The System name (for example, Keenetic-Speedster).
	ndns-domain	The KeenDNS name (for example, mywork.keenetic.name).
	default-ssid	The Default Wi-Fi name (for example, Keenetic-8665).

Example

```
(system)> caption product
Core::System::Caption: Template set to product.
```

History

Version	Description
3.08	The system caption command has been introduced.

3.168.3 system clock date

Description Adjust system date and time.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(system)> clock date <date-and-time>
```

Arguments

Argument	Value	Description
date-and-time	<i>String</i>	Current date and time in DD MM YYYY HH:MM:SS format.

Example

```
(system)> clock date 18 07 2012 09:52:33
System date and time has been changed.
```

History

Version	Description
2.00	The system clock date command has been introduced.

3.168.4 system clock timezone

Description Set the system timezone.

Command with **no** prefix resets timezone to default (GMT).

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(system)> clock timezone <locality>
(system)> no clock timezone <locality>
```

Arguments

Argument	Value	Description
locality	<i>String</i>	Name of the city, indicating the time zone.

Example

```
(system)> clock timezone Dublin
the system timezone is set to "Dublin".
```

History

Version	Description
2.00	The system clock timezone command has been introduced.

3.168.5 system configuration factory-reset

Description Reset configuration to the factory settings for all modes.

Prefix no No

Change settings Yes

Multiple input No

Synopsis

```
(system)> configuration factory-reset
```

Example

```
(system)> configuration factory-reset
Core::Configuration: the system configuration reset to factory ►
defaults.
```

History

Version	Description
2.00	The system configuration factory-reset command has been introduced.

3.168.6 system configuration fail-safe commit

Description Commit all unsaved changes and stop the timer.

Prefix no No

Change settings No

Multiple input No

Synopsis `(system)> configuration fail-safe commit`

Example `(system)> configuration fail-safe commit`
 Core::System::Mtd::ConfigStorage: Committed fail-safe ►
 configuration changes.

History	Version	Description
	3.08	The system configuration fail-safe commit command has been introduced.

3.168.7 system configuration fail-safe keep-alive

Description Silently restart the fail-safe timer.

If the fail-safe mode is inactive or there are no configuration changes the command does nothing.

Prefix no No

Change settings No

Multiple input No

Synopsis `(system)> configuration fail-safe keep-alive`

Example `(system)> configuration fail-safe keep-alive`

History	Version	Description
	3.08	The system configuration fail-safe keep-alive command has been introduced.

3.168.8 system configuration fail-safe rollback

Description Rollback all unsaved changes and reboot the system. The system brings to a special rollback state while rebooting. In this state commit and timer reconfiguration actions are blocked, except timer disable.

If there are no configuration changes the command does nothing.

Prefix no No

Change settings No

Multiple input No

Synopsis `(system)> configuration fail-safe rollback`

Example

```
(system)> configuration fail-safe rollback
Core::System::Mtd::ConfigStorage: Ignored a fail-safe rollback: ►
no pending changes.
```

History	Version	Description
	3.08	The system configuration fail-safe rollback command has been introduced.

3.168.9 system configuration fail-safe timer

Description Setup or cancel the fail-safe timer. The command configures (or reconfigures) a timer state that is permanent between reboots — it does not require explicit configuration saving. Implemented for the router mode only.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(system)> configuration fail-safe timer <action> <interval>`

`(system)> no configuration fail-safe timer`

Arguments	Argument	Value	Description
	action	reboot	Action when the timer expires.
	interval	<i>Integer</i>	Timer value in the range from 60 to 86400 seconds.

Example

```
(system)> configuration fail-safe timer reboot 60
Core::System::Mtd::ConfigStorage: Enabled a 60-second fail-safe ►
"reboot" timer.
```

```
(system)> no configuration fail-safe timer
Core::System::Mtd::ConfigStorage: Turned off the fail-safe mode.
```

History	Version	Description
	3.08	The system configuration fail-safe timer command has been introduced.

3.168.10 system configuration save

Description Save the system configuration asynchronously.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(system)> configuration save`

Example `(system)> configuration save`
Saving configuration.

History	Version	Description
	2.05.B.1	The system configuration save command has been introduced.

3.168.11 system country

Description Select a country from the list of countries available in the factory region. The selected country is permanently stored in the persistent storage and does not require configuration save commands.

The country setting affects all system modes.

Command with **no** prefix resets the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(system)> country <country>`

Arguments	Argument	Value	Description
	country	<i>String</i>	The country code from ISO 3166-1 alpha-2 ¹⁸ .

¹⁸ https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2

Example

```
(system)> country EN
Core::System::Country: Set the system country code to "EN".
```

```
(system)> no country
Core::System::Country: Reset the system country code.
```

History

Version	Description
4.00	The system country command has been introduced.

3.168.12 system debug

Description

Enable system debug. By default, setting is disabled.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(system)> debug
```

```
(system)> no debug
```

Example

```
(system)> debug
Core::Debug: System debug enabled.
```

History

Version	Description
2.03	The system debug command has been introduced.

3.168.13 system description

Description

Set the system description as an arbitrary string. By default, description Carrier (KN-1711) is used.

Command with **no** prefix resets description to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(system)> description <description>
```

```
(system)> no description
```

Arguments

Argument	Value	Description
description	<i>String</i>	System description no longer than 256 bytes.

Example

```
(system)> description DEVICE
Core::System::Info: Description saved.
```

```
(config)> show version
...
  manufacturer: Keenetic Ltd.
    vendor: Keenetic
    series: KN
    model: Ultra (KN-1810)
  hw_version: 10188000
    hw_id: KN-1810
    device: Ultra
    class: Internet Center
    region: RU
  description: DEVICE
```

```
(config)> show running-config
...
  set vm.swappiness 60
  set vm.overcommit_memory 0
  set vm.vfs_cache_pressure 1000
  set dev.usb.force_usb2 0
  domainname WORKGROUP
  hostname Keenetic_Ultra
  description DEVICE
...
```

```
(system)> no description
Core::System::Info: Description reset to default.
```

```
(config)> show version
...
  manufacturer: Keenetic Ltd.
    vendor: Keenetic
    series: KN
    model: Ultra (KN-1810)
  hw_version: 10188000
    hw_id: KN-1810
    device: Ultra
    class: Internet Center
    region: RU
  description: Keenetic Ultra (KN-1810)
```

History

Version	Description
2.15	The system description command has been introduced.

3.168.14 system domainname

Description Assign domain name for the system.

Command with **no** prefix removes domain name.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(system)> domainname <domain>
```

```
(system)> no domainname
```

Arguments

Argument	Value	Description
domain	<i>String</i>	The domain name to assign.

Example

```
(system)> domainname keenetic
Domainname saved.
```

History

Version	Description
2.00	The system domainname command has been introduced.

3.168.15 system eject

Description Stop and eject SCSI/SATA USB-drive. To display all media drive names, use [show media](#) command.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(system)> eject <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Name of media drive to eject.

Example

```
(system)> eject Media0
Storage::Manager: Started "Media0" eject.
```

History	Version	Description
	3.04	The system eject command has been introduced.

3.168.16 system hostname

Description Set the host name. Host name used to identify a node in the network. It is required to enable some of the built-in services, such as CIFS.

Command with **no** prefix sets the default value, which depends on the model name.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(system)>  hostname <hostname>
(system)> no hostname
```

Arguments	Argument	Value	Description
	hostname	<i>String</i>	Name of the host.

Example

```
(system)> hostname KN1010
Core::System::Hostname: The host name set.
```

```
(system)> no hostname
Core::System::Hostname: The host name reset.
```

History	Version	Description
	2.00	The system hostname command has been introduced.

3.168.17 system led

Description Configure general purpose LEDs. By default, LED FN shows the status of device connected to USB.

Command with **no** prefix resets the setting to default.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(system)>  led <led> indicate <control>
```

```
(system)> no led [ <led> [ indicate ] ]
```

Arguments

Argument	Value	Description
led	FN	LED name.
control	UpdatesAvailable	LED notifies you the updates for your device are available.
	BackupWan	LED shows that backup connection is active at the moment.
	SelectedWan	LED shows status of the interface defined with interface led wan command.
	SelectedSchedule	LED shows status of scheduled event assigned with schedule led command.
	OpkgLedControl	LED shows status of opkg .
	UsbPortDeviceAttached	LED shows status of device connected to USB.
indicate	<i>Keyword</i>	Turn off the indicator completely.

Example

```
(system)> led FN indicate SelectedWan
Peripheral::Manager: "SelectedWan" control bound to "FN" LED.
```

```
(system)> no led FN indicate
Peripheral::Manager: "FN" LED control binding removed.
```

History

Version	Description
2.08	The system led command has been introduced.

3.168.18 system led power schedule

Description

Assign a schedule for the LEDs on the device. Schedule must be created and customized with [schedule action](#) command before execution.

Command with **no** prefix unbinds the schedule.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(system)> led power schedule <schedule>
```

```
(system)> no led power schedule
```


Arguments

Argument	Value	Description
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(system)> led power schedule schedule1
Core::Peripheral::Manager: Set LED power schedule "schedule1".
```

```
(system)> no led power schedule
Core::Peripheral::Manager: Clear LED power schedule.
```

History

Version	Description
3.06	The system led power schedule command has been introduced.

3.168.19 system led power shutdown

Description

Shutdown the LEDs on the device.

Command with **no** prefix turns LEDs on.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(system)> led power shutdown <mode>
```

```
(system)> no led power shutdown
```

Arguments

Argument	Value	Description
mode	all	Shutdown all the LEDs.
	front	Shutdown the LEDs on the front panel.
	back	Shutdown the LEDs on the back panel.

Example

```
(system)> led power shutdown all
Core::Peripheral::Manager: Set LED shutdown mode to "all".
```

```
(system)> no led power shutdown
Core::Peripheral::Manager: Set LED shutdown mode to "none".
```

History

Version	Description
3.06	The system led power shutdown command has been introduced. Previous command name is system led shutdown .

3.168.20 system log clear

Description Clear the system log.

Prefix no No

Change settings No

Multiple input No

Synopsis `(system)> log clear`

Example `(system)> log clear`
Syslog: the system log has been cleared.

History	Version	Description
	2.00	The system log clear command has been introduced.

3.168.21 system log reduction

Description Enable repeated message reduction. By default, the setting is enabled.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(system)> log reduction`

`(system)> no log reduction`

Example `(system)> log reduction`
`(system)> no log reduction`

History	Version	Description
	2.04	The system log reduction command has been introduced.

3.168.22 system log server

Description Add remote log server.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(system)> log server <address> [: <port>]
(system)> no log server [ <address> [: <port>] ]
```

Arguments

Argument	Value	Description
address	<i>IP address</i>	Remote log server address.
port	<i>Integer</i>	Remote log server port.

Example

```
(system)> log server 192.168.1.1:8080
Syslog: server 192.168.1.1:8080 added.
```

History

Version	Description
2.00	The system log server command has been introduced.

3.168.23 system log suppress

Description Add message suppression rule.

Command with **no** prefix removes the rule.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(system)> log suppress <ident>
(system)> no log suppress [ <ident> ]
```

Arguments

Argument	Value	Description
ident	<i>String</i>	Process ID which messages need to suppress.

Example

```
(system)> log suppress kernel
Core::Syslog: Added suppression "kernel".
```

```
(system)> no log suppress kernel
Core::Syslog: Deleted suppression "kernel".
```

```
(system)> log suppress transmissiond
Core::Syslog: Added suppression "transmissiond".
```

```
(system)> no log suppress transmissiond
Core::Syslog: Deleted suppression "transmissiond".
```

History

Version	Description
2.04	The system log suppress command has been introduced.

3.168.24 system mode

Description Select system operating mode for Carrier.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(system)> mode <mode>`

Arguments

Argument	Value	Description
mode	router	Main mode.
	client	Network adapter mode to connect Ethernet devices to Wi-Fi network.
	repeater	Repeater mode to extend Wi-Fi network using a wireless connection.
	ap	Access point mode to extend Wi-Fi network using a wired Ethernet connection.

Example

```
(system)> mode repeater
Core::Mode: The system switched to "repeater" mode, reboot the ►
device to apply the settings.
```

History

Version	Description
2.05	The system mode command has been introduced.

3.168.25 system mount

Description Mount USB-drive. To display all mounted drives use [show usb](#) command.

Command with **no** prefix unmount the drive.

Prefix no Yes

Change settings No

Multiple input No

Synopsis

```
(system)> mount <filesystem>
```

```
(system)> no mount <filesystem>
```

Arguments

Argument	Value	Description
filesystem	<i>String</i>	Name of filesystem to mount/unmount.

Example

```
(system)> mount 9430B54530B52EDC:
Filesystem mounted
```

History

Version	Description
2.00	The system mount command has been introduced.

3.168.26 system ndss dump-report disable

Description

Disable product improvement program. By default, setting is enabled.

Command with **no** prefix enables the program.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(system)> ndss dump-report disable
```

```
(system)> no ndss dump-report disable
```

Example

```
(system)> ndss dump-report disable
Core::Ndss: Dump-reporting disabled.
```

```
(system)> no ndss dump-report disable
Core::Ndss: Dump-reporting enabled.
```

History

Version	Description
3.05	The system ndss dump-report disable command has been introduced. Previous command name is system dump-report disable .

3.168.27 system reboot

Description

Reboot the system. If the parameter is set, reboot is executed after a timeout, in seconds. If the timer is already set, using of the command replaces the old value of the timer to the new one.

Using a scheduled reboot is convenient in the case when the device is under remote control, and the user doesn't understand the effect of the commands he/she is trying. The user can turn on a scheduled reboot for fear of losing control over the device. After reboot the system will return to its original state and become available.

Command with **no** prefix cancels reboot or removes the reboot on schedule.

Prefix no Yes

Change settings No

Multiple input No

Synopsis

```
(system)> reboot [ <interval> | schedule <schedule> ]
(system)> no reboot [ schedule ]
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	Timeout for reboot, in seconds. If not specified, the reboot will be executed immediately.
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(system)> reboot 20
Core::System::RebootManager: Rebooting in 20 seconds.
```

```
(system)> no reboot
Core::System::RebootManager: Reboot cancelled.
```

```
(system)> reboot schedule rebootroute
Core::System::RebootManager: Set reboot schedule "rebootroute".
```

```
(system)> no reboot schedule
Core::System::RebootManager: Schedule disabled.
```

History

Version	Description
2.00	The system reboot command has been introduced.
2.12	The schedule argument has been added.

3.168.28 system set

Description Set the value of the specified system parameter and save it in the current settings.

Command with **no** prefix returns the default value to the specified parameter (before the first change).

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(system)> set <name> <value>
```

```
(system)> no set <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Identifier of the system parameter.
value	<i>String</i>	New value of the system parameter.

Example

```
(config)> system
(system)> set net.ipv4.ip_forward 1
(system)> set net.ipv4.tcp_fin_timeout 30
(system)> set net.ipv4.tcp_keepalive_time 120
(system)> set ►
net.ipv4.netfilter.ip_conntrack_tcp_timeout_established 1200
(system)> set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
(system)> set net.ipv4.netfilter.ip_conntrack_max 4096
(system)> exit
(config)> show running-config
system
set net.ipv4.ip_forward 1
    set net.ipv4.tcp_fin_timeout 30
    set net.ipv4.tcp_keepalive_time 120
    set net.ipv4.netfilter.ip_conntrack_tcp_timeout_established ►
1200
    set net.ipv4.netfilter.ip_conntrack_udp_timeout 60
    set net.ipv4.netfilter.ip_conntrack_max 4096
!
...
(config)>
```

History

Version	Description
2.00	The system set command has been introduced.

3.168.29 system swap

Description Configure swap area. If the file is not found, the command tries to create it.
Command with **no** prefix disables the swap.

Prefix no Yes

Change settings Yes

Multiple input

No

Synopsis`(system)> swap (<area> | <area>) <size>``(system)> no swap`**Arguments**

Argument	Value	Description
area	<i>Filename</i>	Full path to the swap-file in <file system>:<path> format.
size	<i>Integer</i>	Swap-file size, in Kbytes.

Example

```
(system)> swap OPKG:/swap/swapfile 2097152
Storage::Swap::Manager: Swap is being initialized in background.
```

```
(system)> no swap
Storage::Swap::Manager: Swap area OPKG:/swap/swapfile disabled.
```

History

Version	Description
2.00	The system swap command has been introduced.

3.168.30 system trace lock threshold

Description

Set a trace lock threshold for the system threads. If the threshold value is exceeded, information about this thread (for example, SCGI session) is saved in the system log. By default, setting is disabled.

Command with **no** prefix disables the trace lock threshold feature.

Prefix no

Yes

Change settings

No

Multiple input

No

Synopsis`(system)> system trace lock threshold <threshold>``(system)> no system trace lock threshold`**Arguments**

Argument	Value	Description
threshold	<i>String</i>	Threshold value in milliseconds. Can take values in the range from 100 to 100000000 inclusively. The threshold value is not saved into startup-config.

Example

```
(system)> system trace lock threshold 100
Lockable: Set threshold to 100 ms.
```



```
(system)> no trace lock threshold
Lockable: Reset threshold.
```

History

Version	Description
3.03	The system trace lock threshold command has been introduced.

3.168.31 system usb power schedule

Description

Assign a schedule for the USB port. Schedule must be created and customized with **schedule action** command before execution.

Command with **no** prefix unbinds the schedule.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(system)> usb <port> power schedule <schedule>
```

```
(system)> no usb <port> power schedule <schedule>
```

Arguments

Argument	Value	Description
port	1	USB port 1.
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(system)> usb 1 power schedule schedule0
Usb::Manager: Port "1" schedule "schedule0" assigned.
```

```
(system)> no usb 1 power schedule
Usb::Manager: Port "1" schedule unassigned.
```

History

Version	Description
4.00	The system usb power schedule command has been introduced.

3.168.32 system usb power shutdown

Description

Switch off the power on the USB port.

Command with **no** prefix turns the power on.

Prefix no

Yes

Change settings Yes**Multiple input** No

Synopsis

```
(system)> port <port> power shutdown
```

```
(system)> no port <port> power shutdown
```

Arguments

Argument	Value	Description
port	1	USB port 1.

Example

```
(system)> usb 1 power shutdown
Usb::Manager: Port "1" power is shutting down.
```

```
(system)> no usb 1 power shutdown
Usb::Manager: Port "1" power is activated.
```

History

Version	Description
4.00	The system usb power shutdown command has been introduced.

3.168.33 system zram

Description Configure zRam swap file. If you use no argument, size of zRam file will be set automatically.

Command with **no** prefix removes zRam file.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(system)> zram [ <size> ]
```

```
(system)> no zram
```

Arguments

Argument	Value	Description
size	<i>Integer</i>	Size of zRam file, in Kbytes.

Example

```
(system)> zram
Zram::Manager: Enabled zram swap of size 262144Kb.
```

```
(system)> no zram
Zram::Manager: Zram swap disabled.
```

History

Version	Description
2.09	The system zram command has been introduced.

3.169 tools

Description Access to a group of commands to test the environment.

Prefix no No

Change settings No

Multiple input No

Group entry (tools)

Synopsis (config)> **tools**

History

Version	Description
2.00	The tools command has been introduced.

3.169.1 tools arping

Description Command action is analogous to **tools ping** command, but operates at the link layer of the OSI model using the **ARP** protocol.

Prefix no No

Change settings No

Multiple input No

Synopsis (tools)> **arping** *address* **source-interface** *source-interface* [**count** *count*] [**wait-time** *wait-time*]

Arguments

Argument	Value	Description
address	<i>IP address</i>	IP address of the respondent.
source-interface	<i>Interface</i>	Name of source-interface.
count	<i>Integer</i>	Quantity of requests. If not specified, the command will run until interrupted by the user.
wait-time	<i>Integer</i>	The maximum response time, in milliseconds.

Example

```
(tools)> arping 192.168.15.51 source-interface Home count 4 ►
wait-time 3000
```

```
Starting the ARP ping to "192.168.15.51"...
ARPING 192.168.15.51 from 192.168.15.1 br0.
Unicast reply from 192.168.15.51 [9c:b7:0d:ce:51:6a] 1.884 ms.
Unicast reply from 192.168.15.51 [9c:b7:0d:ce:51:6a] 1.831 ms.
Sent 4 probes, received 2 responses.
Process terminated.
```

History

Version	Description
2.00	The tools arping command has been introduced.

3.169.2 tools ping

Description

Send Echo-Request requests of ICMP protocol to specified network node and register received Echo Reply responses. The time between sending request and receiving the response Round Trip Time (RTT) allows you to define double ended delays on the route and frequency of packet losses, that is, indirectly determine loading on the channels of data transmission and intermediate devices.

Total absence of ICMP Replies can also mean that the remote node (or any of the intermediate routers) blocks ICMP Echo Reply or ignores ICMP Echo Request.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(tools)> ping <host> [ count <count> ] [ packetsize <packetsize> ] [
sequence-id <sequence-id> ] [ source ( <source-interface> |
<source-address> ) ] [ tos <tos> ] [ ttl <ttl> ]
```

Arguments

Argument	Value	Description
host	<i>String</i>	Domain name or host IP address.
count	<i>Integer</i>	Quantity of ICMP Echo Requests. If not specified, the command will run until interrupted by the user.
packetsize	<i>Integer</i>	Size of the ICMP Echo Request data field in bytes. By default, 56 value is used. Can take values in the range from 28 to 65535 inclusively.
sequence-id	<i>Integer</i>	Sequence number to aid in matching Echo Request and Echo Reply. By default, 0 value is used. Can take values in the range from 0 to 65535 inclusively.
source	source-address	Address of the outgoing interface.

Argument	Value	Description
	source-interface	Interface to be used as the source interface in outgoing probe packets.
tos	<i>Integer</i>	Type Of Service. By default, 0 value is used. Can take values in the range from 0 to 63 inclusively.
ttl	<i>Integer</i>	Maximum number of hops (max time-to-live value) traceroute will probe. By default, 30 value is used. Can take values in the range from 1 to 255 inclusively.

Example

```
(tools)> ping 8.8.8.8 count 5 size 100
Sending ICMP ECHO request to 192.168.1.33
PING 192.168.1.33 (192.168.1.33) 72 (100) bytes of data.
100 bytes from 192.168.1.33: icmp_req=1, ttl=128, time=2.35 ms.
100 bytes from 192.168.1.33: icmp_req=2, ttl=128, time=1.07 ms.
100 bytes from 192.168.1.33: icmp_req=3, ttl=128, time=1.06 ms.
--- 192.168.1.33 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss,
0 duplicate(s), time 2002.65 ms.
Round-trip min/avg/max = 1.06/1.49/2.35 ms.
Process terminated.
```

```
(tools)> ping 8.8.8.8 source Wireguard1
sending ICMP ECHO request to 8.8.8.8...
PING 8.8.8.8 (8.8.8.8) 72 (100) bytes of data.
96 bytes from 8.8.8.8: icmp_req=1, ttl=108, time=17.58 ms. ►
(truncated).
96 bytes from 8.8.8.8: icmp_req=2, ttl=108, time=17.62 ms. ►
(truncated).
96 bytes from 8.8.8.8: icmp_req=3, ttl=108, time=17.29 ms. ►
(truncated).
96 bytes from 8.8.8.8: icmp_req=4, ttl=108, time=17.17 ms. ►
(truncated).
96 bytes from 8.8.8.8: icmp_req=5, ttl=108, time=17.41 ms. ►
(truncated).
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss,
0 duplicate(s), time 4019.72 ms.
Round-trip min/avg/max = 17.17/17.41/17.62 ms.
```

History

Version	Description
2.00	The tools ping command has been introduced.
4.01	New values address and interface were added to the source argument.

3.169.3 tools ping6

Description

Send Echo-Request requests of ICMPv6 protocol to specified network node and register received Echo Reply responses. The time between sending request and receiving the response Round Trip Time (RTT) allows you to define double ended delays on the route and frequency of packet losses, that is, indirectly determine loading on the channels of data transmission and intermediate devices.

Total absence of ICMP Replies can also mean that the remote node (or any of the intermediate routers) blocks ICMP Echo Reply or ignores ICMP Echo Request.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(tools)> ping6 <host> [ count <count> ] [ packetsize <packetsize> ] [
sequence-id <sequence-id> ] [ source ( <source-interface> |
<source-address> ) ] [ tos <tos> ] [ ttl <ttl> ]
```

Arguments

Argument	Value	Description
host	<i>String</i>	Domain name or host IPv6-address.
count	<i>Integer</i>	Quantity of ICMPv6 Echo Requests. If not specified, the command will run until interrupted by the user.
packetsize	<i>Integer</i>	Size of the ICMPv6 Echo Request data field in bytes. By default, 56 value is used. Can take values in the range from 28 to 65535 inclusively.
sequence-id	<i>Integer</i>	Sequence number to aid in matching Echo Request and Echo Reply. By default, 0 value is used. Can take values in the range from 0 to 65535 inclusively.
source	source-address	Address of the outgoing interface.
	source-interface	Interface to be used as the source interface in outgoing probe packets.
tos	<i>Integer</i>	Type Of Service. By default, 0 value is used. Can take values in the range from 0 to 63 inclusively.
ttl	<i>Integer</i>	Maximum number of hops (max time-to-live value) traceroute will probe. By default, 30 value is used. Can take values in the range from 1 to 255 inclusively.

Example

```
(tools)> ping6 2001:4860:4860::8888 count 5 size 111
sending ICMPv6 ECHO request to 2001:4860:4860::8888...
PING 2001:4860:4860::8888 (2001:4860:4860::8888) 63 (111) bytes ►
of data.
71 bytes from 2001:4860:4860::8888: icmp_req=1, ttl=108, ►
time=19.84 ms.
71 bytes from 2001:4860:4860::8888: icmp_req=2, ttl=108, ►
time=19.73 ms.
71 bytes from 2001:4860:4860::8888: icmp_req=3, ttl=108, ►
time=19.96 ms.
71 bytes from 2001:4860:4860::8888: icmp_req=4, ttl=108, ►
time=19.86 ms.
71 bytes from 2001:4860:4860::8888: icmp_req=5, ttl=108, ►
time=19.76 ms.
--- 2001:4860:4860::8888 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss,
0 duplicate(s), time 4021.21 ms.
Round-trip min/avg/max = 19.73/19.83/19.96 ms.
```

```
(tools)> ping6 2001:4860:4860::8888 source ISP
sending ICMPv6 ECHO request to 2001:4860:4860::8888...
PING 2001:4860:4860::8888 (2001:4860:4860::8888) from eth3: 56 ►
(104) bytes of data.
64 bytes from 2001:4860:4860::8888: icmp_req=1, ttl=108, ►
time=19.90 ms.
64 bytes from 2001:4860:4860::8888: icmp_req=2, ttl=108, ►
time=19.75 ms.
64 bytes from 2001:4860:4860::8888: icmp_req=3, ttl=108, ►
time=19.64 ms.
64 bytes from 2001:4860:4860::8888: icmp_req=4, ttl=108, ►
time=19.66 ms.
64 bytes from 2001:4860:4860::8888: icmp_req=5, ttl=108, ►
time=19.88 ms.
64 bytes from 2001:4860:4860::8888: icmp_req=6, ttl=108, ►
time=19.72 ms.
64 bytes from 2001:4860:4860::8888: icmp_req=7, ttl=108, ►
time=19.71 ms.
--- 2001:4860:4860::8888 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss,
0 duplicate(s), time 6221.53 ms.
Round-trip min/avg/max = 19.64/19.75/19.90 ms.
```

History

Version	Description
2.00	The tools ping6 command has been introduced.
4.01	New values address and interface were added to the source argument.

3.169.4 tools traceroute**Description**

Show the route to a network host.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(tools)> tracert <host> [ count <count> ] [ interval <interval> ]
      [ wait-time <wait-time> ] [ packet-size <packet-size> ]
      [ max-ttl <max-ttl> ] [ port <port> ] [ source-address
      <source-address> ]
      [ source-interface <source-interface> ] [ type <type> ] [ tos <tos>
      ]
```

Arguments

Argument	Value	Description
host	<i>String</i>	Name of the target host.
count	<i>Integer</i>	Number of probe packets per hop. Default value — 3. Value must be in the range [1;10].
interval	<i>Integer</i>	Time in seconds between sending packets. Default value — 0. Value must be in the range [0;15].
wait-time	<i>Integer</i>	Time to wait for a response to a probe (in seconds). Default value — 1. Value must be in the range [1;15].
packet-size	<i>Integer</i>	Size of packet according to the protocol type. For tcp type default packet size is 52. Range of values [52]. For udp and icmp types default packet size is 60. Range of values [28;65535].
max-ttl	<i>Integer</i>	Maximum number of hops (max time-to-live value) traceroute will probe. Default value — 30. Value must be in the range [1;255].
port	<i>Integer</i>	Destination port. For tcp type default port is 80. For udp type default port is 33434. For icmp type default port is 1.
source-address	<i>String</i>	Address of the outgoing interface.
source-interface	<i>String</i>	Interface to be used as the source interface in outgoing probe packets.
type	tcp	<i>TCP</i> protocol.
	udp	<i>UDP</i> protocol. Used by default.
	icmp	<i>ICMP</i> protocol.

Argument	Value	Description
tos	<i>Integer</i>	Type Of Service. Default value — 0. Value must be in the range [0;255].

Example

```
(tools)> traceroute google.com count 5 interval 5
starting traceroute to google.com...
traceroute to google.com (64.233.161.113), 30 hops maximum, 60 ►
byte packets.
 1 192.168.233.1 (192.168.233.1) 2.742 ms 2.406 ms 2.460 ms ►
 2.191 ms 2.957 ms
 2 10.77.140.1 (10.77.140.1) 3.301 ms 3.847 ms 3.839 ms
process terminated
```

History

Version	Description
2.00	The tools traceroute command has been introduced.

3.170 torrent

Description Access to a group of commands to configure BitTorrent parameters.

Prefix no No

Change settings No

Multiple input No

Group entry (config-torrent)

Synopsis (config)> **torrent**

History

Version	Description
2.00	The torrent command has been introduced.

3.170.1 torrent directory

Description Specify a folder for downloads. If the folder is not found, the command tries to create it.

Command with **no** prefix removes the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(config-torrent)> directory <directory>
```

```
(config-torrent)> no directory
```

Arguments

Argument	Value	Description
directory	<i>String</i>	Path to the folder with filesystem defining. Filesystems — temp:, system:, flash:, sys:, proc:, usb:.

Example

```
(config-torrent)> directory ►  
46E243F4E243E6B1:/components/transmission/
```

```
(config-torrent)> no directory
```

History

Version	Description
2.00	The torrent directory command has been introduced.

3.170.2 torrent io-priority

Description

Configure the background disk I/O priority for the BitTorrent client. By default, normal priority is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-torrent)> io-priority <io-priority>
```

```
(config-torrent)> no io-priority
```

Arguments

Argument	Value	Description
io-priority	normal	Disk I/O priority.
	low	

Example

```
(config-torrent)> io-priority low  
Torrent::Client: Set low I/O priority.
```

```
(config-torrent)> no io-priority  
Torrent::Client: Reset I/O priority.
```

History	Version	Description
	4.03	The torrent io-priority command has been introduced.

3.170.3 torrent peer-port

Description Set peer port. By default, 51413 value is used.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(config-torrent)> peer-port <port>`

Argument	Value	Description
port	<i>Integer</i>	Incoming TCP listen port. Can take values in the range from 1024 to 65535.

Example `(config-torrent)> peer-port 11122`
 Torrent::Client: Peer port changed to 11122.

History	Version	Description
	2.00	The torrent peer-port command has been introduced.

3.170.4 torrent policy

Description Define the IP Policy for BitTorrent client.

Command with **no** prefix removes the defined IP Policy profile for BitTorrent client.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(config-torrent)> policy <policy>`
`(config-torrent)> no policy`

Argument	Value	Description
policy	<i>Policy</i>	Name of IP Policy profile.

Example

```
(config-torrent)> policy PolicyNaN
Torrent::Client: Policy PolicyNaN applied.
```

```
(config-torrent)> no policy
Torrent::Client: Policy cleared.
```

History

Version	Description
3.01	The torrent policy command has been introduced.

3.170.5 torrent reset

Description Reset settings of BitTorrent client.

Prefix no No

Change settings No

Multiple input No

Synopsis (config-torrent)> **reset**

Example

```
(config-torrent)> reset
Torrent::Client: Reset performed.
```

History

Version	Description
2.10	The torrent reset command has been introduced.

3.170.6 torrent rpc-port

Description Set *RPC* port. By default, 8090 value is used.

Prefix no No

Change settings Yes

Multiple input No

Synopsis (config-torrent)> **rpc-port** *<port>* [**public**]

Arguments

Argument	Value	Description
port	<i>Integer</i>	Webadmin listen port. Can take values in the range from 1024 to 65535.
public	<i>Keyword</i>	Access to BitTorrent client managing by public interfaces.

Example

```
(config-torrent)> rpc-port 9945
Torrent::Client: RPC port changed to 9945 (private).
```

```
(config-torrent)> rpc-port 9945 public
Torrent::Client: RPC port changed to 9945 (public).
```

History

Version	Description
2.00	The torrent rpc-port command has been introduced.

3.171 udpxy

Description Access to a group of commands to configure [udpxy](#) parameters.

Prefix no No

Change settings No

Multiple input No

Group entry (udpxy)

Synopsis (config)> **udpxy**

History

Version	Description
2.03	The udpxy command has been introduced.

3.171.1 udpxy buffer-size

Description Set [udpxy](#) buffer size. By default, 2048 value is used.
Command with **no** prefix resets buffer size to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis (udpxy)> **buffer-size** <size>
(udpxy)> **no buffer-size**

Arguments

Argument	Value	Description
size	<i>Integer</i>	Buffer size in bytes. Can take values in the range from 1 to 1048576.

Example

```
(udpxy)> buffer-size 500
Udpxy::Manager: a buffer size set to 500 bytes.
```

History

Version	Description
2.04	The udpxy buffer-size command has been introduced.

3.171.2 udpxy buffer-timeout

Description

Set *udpxy* timeout to hold data in the buffer. By default, 1 value is used.

Command with **no** prefix resets timeout to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(udpxy)> buffer-timeout <timeout>
```

```
(udpxy)> no buffer-timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	Timeout value in seconds. Can take values in the range from -1 to 60. -1 — unlimited timeout.

Example

```
(udpxy)> buffer-timeout 10
Udpxy::Manager: a hold data timeout set to 10 sec.
```

History

Version	Description
2.04	The udpxy buffer-timeout command has been introduced.

3.171.3 udpxy interface

Description

Bind *udpxy* to the specified interface. By default, current default gateway is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(udpxy)> interface <interface>
```

```
(udpxy)> no interface
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(udpxy)> interface [Tab]
```

```
Usage template:
    interface {interface}
```

```
Choose:
```

```
    GigabitEthernet1
        ISP
    WifiMaster0/AccessPoint2
    WifiMaster1/AccessPoint1
    WifiMaster0/AccessPoint3
    WifiMaster0/AccessPoint0
        AccessPoint
```

```
(udpxy)> interface ISP
```

```
UdpXy::Manager: bound to FastEthernet0/Vlan2.
```

History

Version	Description
2.02	The udpxy interface command has been introduced.

3.171.4 udpxy port

Description

Specify port for HTTP requests. By default, 4022 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(udpxy)> port <port>
```

```
(udpxy)> no port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	Port number. Can take values in the range from 0 to 65535.

Example

```
(udpxy)> port 2323
Udpxy::Manager: a port set to 2323.
```

History

Version	Description
2.03	The udpxy port command has been introduced.

3.171.5 udpxy renew-interval

Description

Set renew interval of subscription to the multicast channel. By default, 0 value is used, i.e. the subscription is not renewed.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(udpxy)> renew-interval <renew-interval>
```

```
(udpxy)> no renew-interval
```

Arguments

Argument	Value	Description
renew-interval	<i>Integer</i>	Renew interval of subscription in seconds. Can take values in the range from 0 to 3600.

Example

```
(udpxy)> renew-interval 120
Udpxy::Manager: a renew subscription interval value set to 120 ►
sec.
```

History

Version	Description
2.03	The udpxy renew-interval command has been introduced.

3.171.6 udpxy timeout

Description

Set connection timeout. By default, 5 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(udpxy)> timeout <timeout>
```

```
(udpxy)> no timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	Timeout in seconds. Can take values in the range from 5 to 60.

Example

```
(udpxy)> timeout 10
Udpxy::Manager: a stream timeout set to 10 sec.
```

History

Version	Description
2.03	The udpxy timeout command has been introduced.

3.172 upnp forward

Description

Add [UPnP](#) forwarding rule.

Command with **no** prefix removes rule from the list.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

IP

Synopsis

```
(config)> upnp forward <protocol> [ <interface> ] <address> <port>
```

```
(config)> no upnp forward [ <index> | ( <protocol> <address> <port> ) ]
```

Arguments

Argument	Value	Description
protocol	tcp	Rule for TCP protocol will be added/deleted.
	udp	Rule for UDP protocol will be added/deleted.
interface	<i>Interface</i>	Rule for specified interface name will be added.
address	<i>IP address</i>	Rule for specified IP address will be added/deleted.
port	<i>Integer</i>	Rule for specified port will be added/deleted.
index	<i>Integer</i>	Rule with specified number in the list will be removed.

History

Version	Description
2.00	The upnp lan command has been introduced.

3.173 upnp lan

Description

Set LAN interface where the *UPnP* service is running. The service works for one network segment only.

Command with **no** prefix removes setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Interface type

IP

Synopsis

```
(config)> upnp lan <interface>
```

```
(config)> no upnp lan
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(config)> upnp lan [Tab]

Usage template:
    lan {interface}

Choose:
    GigabitEthernet1
    ISP
    WifiMaster0/AccessPoint2
    WifiMaster1/AccessPoint1
    WifiMaster0/AccessPoint3
    WifiMaster0/AccessPoint0
    AccessPoint
    WifiMaster1/AccessPoint2
    WifiMaster0/AccessPoint1
    GuestWiFi
```

```
(config)> upnp lan PPTP0
using LAN interface: PPTP0.
```

History

Version	Description
2.00	The upnp lan command has been introduced.

3.174 upnp redirect

Description

Add *UPnP* port translation rule.

Command with **no** prefix removes rule from the list. If you use no arguments, the entire list of rules will be removed.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Interface type

IP

Synopsis

```
(config)> upnp redirect <protocol> <interface> <port> <to-address> [
to-port ]
```

```
(config)> no upnp redirect [and forward | [ <index> | ( <protocol> <port> )
]]
```

Arguments

Argument	Value	Description
protocol	tcp	Rule for <i>TCP</i> protocol will be added/deleted.
	udp	Rule for <i>UDP</i> protocol will be added/deleted.
interface	<i>Interface</i>	Rule for specified interface name will be added.
port	<i>Integer</i>	Rule for specified port will be added/deleted.
to-address	<i>IP address</i>	Rule for specified destination address will be added.
to-port	<i>Integer</i>	Rule for specified destination port will be added.
and forward	<i>Keyword</i>	Lists of forwarding and redirecting rules will be cleared.
index	<i>Integer</i>	Rule with specified number in the list will be removed.

History

Version	Description
2.00	The upnp redirect command has been introduced.

3.175 user

Description

Access to a group of commands to configure user account parameters. If specified user is not found, the command tries to create it.

Note: Account with reserved name **admin** can not be removed. In addition, the **admin** user can not lose the access right to command line.

Command with **no** prefix removes user account.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Group entry

(config-user)

Synopsis

```
(config)> user <name>
```

```
(config)> no user <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	The user name.

History

Version	Description
2.00	The user command has been introduced.

3.175.1 user home

Description

Set home directory for user.

Command with **no** prefix resets the setting.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-user)> home <directory>
```

```
(config-user)> no home
```

Arguments

Argument	Value	Description
directory	<i>String</i>	Path to the home directory for FTP server, SFTP server and WeDAV server.

Example

```
(config-user)> home files_ssd:/
Core::Authenticator: "test" user root directory set to ►
"files_ssd:/".
```

```
(config-user)> no home
(config-user)>
```

History

Version	Description
3.04	The user home command has been introduced.

3.175.2 user password

Description

Set the user password. The password is stored as MD5-hash, computed from the *"user:realm:password"* string. *realm* is the device model name from startup-config.txt file.

The command takes open string or hash-function value as argument. Saved password is used for user authentication.

Command with **no** prefix removes the password so that the user can access to the device unauthenticated.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(config-user)> password ( md5 <hash> | <password> )
```

```
(config-user)> no password
```

Arguments

Argument	Value	Description
hash	<i>String</i>	MD5-hash value.
password	<i>String</i>	Value of the password in open form, from which the hash value is calculated automatically.

Example

```
(config-user)> password 1111
Core::Authenticator: Password set has been changed for user ►
"test".
```

History

Version	Description
2.00	The user password command has been introduced.

3.175.3 user tag

Description

Assign a special tag to the user account, which presence is checked at the time of user authorization as well as performing any action in the system. Set of permitted tag values depends on the system functionality. The full list is shown in the table below.

Several different tags can be assigned to one account by entering the command several times. Each tag can be viewed as granting or revoking certain permissions.

Command with **no** prefix removes the specified tag.

Note: The admin account can not be untagged cli.

The admin account can not be untagged http in Repeater mode.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(config-user)> tag <tag>
```

```
(config-user)> no tag [ <tag> ]
```

Arguments

Argument	Value	Description
tag	cli	Access to the command line (TELNET and SSH).
	readonly	Restrict commands that change the settings.
	http-proxy	Access to the HTTP proxy.
	http	Access to the Web-interface.
	afp	Access to USB drives via Apple File Protocol.
	printers	Access to USB printers via SMB/CIFS.
	cifs	Connection to the Windows files and printers service.
	vpn-dlna	Access to the DLNA for PPTP, L2TP/IPSec, SSTP tunnels.
	ftp	Connection to an integrated FTP server.
	ipsec-xauth	Connection to an integrated IPsec/XAuth server.
	ipsec-l2tp	Connection to an integrated L2TP/IPSec server.
	vpn-oc	Connection to an integrated OpenConnect server.
	opt	Access to services managed by OptWare.

Argument	Value	Description
	sftp	Access to SFTP file server.
	sstp	Connection to an integrated SSTP server.
	torrent	Access to the BitTorrent client GUI.
	vpn	Connection to an integrated PPTP server.
	webdav	Access to WebDAV file server.

Example

```
(config-user)> tag cli
Core::Authenticator: User "test" tagged with "cli".
```

```
(config-user)> tag readonly
Core::Authenticator: User "test" tagged with "readonly".
```

```
(config-user)> tag http-proxy
Core::Authenticator: User "test" tagged with "http-proxy".
```

```
(config-user)> tag http
Core::Authenticator: User "test" tagged with "http".
```

```
(config-user)> tag afp
Core::Authenticator: User "test" tagged with "afp".
```

```
(config-user)> tag printers
Core::Authenticator: User "test" tagged with "printers".
```

```
(config-user)> tag cifs
Core::Authenticator: User "test" tagged with "cifs".
```

```
(config-user)> tag vpn-dlna
Core::Authenticator: User "test" tagged with "vpn-dlna".
```

```
(config-user)> tag ftp
Core::Authenticator: User "test" tagged with "ftp".
```

```
(config-user)> tag ipsec-xauth
Core::Authenticator: User "test" tagged with "ipsec-xauth".
```

```
(config-user)> tag ipsec-l2tp
Core::Authenticator: User "test" tagged with "ipsec-l2tp".
```

```
(config-user)> tag vpn-oc
Core::Authenticator: User "test" tagged with "vpn-oc".
```

```
(config-user)> tag opt
Core::Authenticator: User "test" tagged with "opt".
```

```
(config-user)> tag sftp
Core::Authenticator: User "test" tagged with "sftp".
```

```
(config-user)> tag sstp
Core::Authenticator: User "test" tagged with "sstp".
```

```
(config-user)> tag torrent
Core::Authenticator: User "test" tagged with "torrent".
```

```
(config-user)> tag vpn
Core::Authenticator: User "test" tagged with "vpn".
```

```
(config-user)> tag webdav
Core::Authenticator: User "test" tagged with "webdav".
```

```
(config-user)> no tag readonly
Core::Authenticator: User "test": "readonly" tag deleted.
```

History

Version	Description
2.00	The user tag command has been introduced.
2.04	The vpn tag has been added.
2.06	The opt , ipsec-xauth tags have been added.
2.10	The http-proxy tag has been added.
2.11	The ipsec-l2tp tag has been added.
2.12	The sstp tag has been added.
3.04	The vpn-dlna sftp and webdav tags have been added.

Version	Description
4.02	The vpn-oc tags have been added.

3.176 ussd send

Description Send [USSD](#) request to the mobile operator.

Prefix no No

Change settings No

Multiple input No

Interface type Usb

Synopsis `(config)> ussd <interface> send <request>`

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.
request	<i>String</i>	USSD command.

Example

```
(config)> ussd UsbQmi0 send *100#

      request: *100#
      response: Your number: +79953332211
                Available: 10 dol
                4.01 / 5 GB
```

History

Version	Description
3.05	The ussd send command has been introduced.

3.177 vpn-server

Description Access to a group of commands to configure VPN server parameters.

Prefix no No

Change settings No

Multiple input No

Group entry (vpn-server)

Synopsis

```
(config)> vpn-server
```

History

Version	Description
2.04	The vpn-server command has been introduced.

3.177.1 vpn-server dhcp route

Description Assign a route which is transmitted in DHCP INFORM messages to the VPN server clients.

Command with **no** prefix cancels the specified route. If you use no arguments, the entire list of routes will be cleared.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(vpn-server)> dhcp route <address> <mask>
```

```
(vpn-server)> no dhcp route [ <address> <mask> ]
```

Arguments

Argument	Value	Description
address	IP address	Network client address.

Argument	Value	Description
mask	<i>IP-mask</i>	Network client mask. There are two ways to enter the mask: the canonical form (for example, 255.255.255.0) and the form of prefix bit length (for example, /24).

Example

```
(vpn-server)> dhcp route 192.168.2.0/24
VpnServer::Manager: Added DHCP INFORM route to ►
192.168.2.0/255.255.255.0.
```

```
(vpn-server)> no dhcp route
VpnServer::Manager: Cleared DHCP INFORM routes.
```

History

Version	Description
2.12	The vpn-server dhcp route command has been introduced.

3.177.2 vpn-server interface

Description

Bind VPN server to the specified interface.

Command with **no** prefix unbinds the interface.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(vpn-server)> interface <interface>
```

```
(vpn-server)> no interface
```

Arguments

Argument	Value	Description
interface	<i>Interface</i>	Full interface name or an alias. You can see the list of available interfaces with help of interface [Tab] command.

Example

```
(vpn-server)> interface [Tab]
```

```
Usage template:
  interface {interface}
```

```
Choose:
```

```
    GigabitEthernet1
    ISP
    WifiMaster0/AccessPoint2
    WifiMaster1/AccessPoint1
```

```
WifiMaster0/AccessPoint3
WifiMaster0/AccessPoint0
AccessPoint
```

```
(vpn-server)> interface FastEthernet0/Vlan1
VpnServer::Manager: Bound to FastEthernet0/Vlan1
```

```
(vpn-server)> no interface
VpnServer::Manager: Reset interface binding.
```

History

Version	Description
2.04	The vpn-server interface command has been introduced.

3.177.3 vpn-server ipv6cp

Description Enable IPv6 support. DHCP IPv6 pools are created for each VPN server. By default, the setting is disabled.

Command with **no** prefix disables IPv6 support.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(vpn-server)> ipv6cp
```

```
(vpn-server)> no ipv6cp
```

Example

```
(vpn-server)> ipv6cp
VpnServer::Manager: IPv6 control protocol enabled.
```

```
(vpn-server)> no ipv6cp
VpnServer::Manager: IPv6 control protocol disabled.
```

History

Version	Description
3.00	The vpn-server ipv6cp command has been introduced.

3.177.4 vpn-server lcp echo

Description Specify the testing rules of the PPTP connections with **LCP** echo tools.

Command with **no** prefix disables **LCP** echo.

Prefix no Yes

Change settings Yes

Multiple input

No

Synopsis`(vpn-server)> lcp echo <interval> <count> [adaptive]``(vpn-server)> no lcp echo`**Arguments**

Argument	Value	Description
interval	<i>Integer</i>	Interval between sending <i>LCP</i> echo, in seconds. If within the specified time interval there is no <i>LCP</i> echo request from the remote location, the same request will be sent there asking for response <i>LCP</i> reply.
count	<i>Integer</i>	The number of consecutive requests <i>LCP</i> echo sent, for which no response <i>LCP</i> reply was received. If count of <i>LCP</i> echo requests goes unanswered, the connection is terminated.
adaptive	<i>Keyword</i>	Pppd will send LCP echo-request frames only if no traffic was received from the peer since the last echo-request was sent.

Example

```
(vpn-server)> lcp echo 5 3
LCP echo parameters updated.
```

History

Version	Description
2.06	The vpn-server lcp echo command has been introduced.

3.177.5 vpn-server lockout-policy

Description

Set VPN server bruteforce detection parameters. By default, feature is enabled. If you use 0 as an argument, all bruteforce detection parameters will be reset to default.

Command with **no** prefix disables bruteforce detection.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis`(vpn-server)> lockout-policy <threshold> [<duration> [<observation-window>]]``(vpn-server)> no lockout-policy`

Arguments

Argument	Value	Description
threshold	<i>Integer</i>	The number of failed attempts to log in. By default, 5 value is used. Can take values in the range from 2 to 20.
duration	<i>Integer</i>	An authorization ban duration for the specified IP in minutes. By default, 15 value is used. Can take values in the range from 1 to 120.
observation-window	<i>Integer</i>	Duration of suspicious activity observation in minutes. By default, 3 value is used. Can take values in the range from 1 to 20.

Example

```
(vpn-server)> lockout-policy 10 30 2  
VpnServer::Manager: Bruteforce detection is reconfigured.
```

```
(vpn-server)> no lockout-policy  
VpnServer::Manager: Bruteforce detection is disabled.
```

```
(vpn-server)> lockout-policy 0  
VpnServer::Manager: Bruteforce detection reset to default.
```

History

Version	Description
3.01	The vpn-server lockout-policy command has been introduced.

3.177.6 vpn-server mppe

Description

Set mode for *MPPE* encryption. 40-bit key is used by default.

Command with **no** prefix disables selected mode.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(vpn-server)> mppe <mode>
```

```
(vpn-server)> no mppe <mode>
```

Arguments

Argument	Value	Description
mode	40	Length of the encryption key is 40 bits.
	128	Length of the encryption key is 128 bits.

Example

```
(vpn-server)> mppe 40
VpnServer::Manager: Set encryption 40.
```

History

Version	Description
2.05	The vpn-server mppe command has been introduced.

3.177.7 vpn-server mppe-optional

Description

Allow connections without [MPPE](#) encryption. By default, the feature is enabled.

Command with **no** prefix deny unencrypted connections.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(vpn-server)> mppe-optional
```

```
(vpn-server)> no mppe-optional
```

Example

```
(vpn-server)> mppe-optional
VpnServer::Manager: Unencrypted connections enabled.
```

```
(vpn-server)> no mppe-optional
VpnServer::Manager: Unencrypted connections disabled.
```

History

Version	Description
2.04	The vpn-server mppe-optional command has been introduced.

3.177.8 vpn-server mru

Description

Set [MRU](#) value to be transmitted to PPTP server. By default, 1350 value is used.

Command with **no** prefix resets value to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(vpn-server)> mru <value>
```

```
(vpn-server)> no mru
```

Arguments

Argument	Value	Description
value	<i>Integer</i>	<i>MRU</i> value. Can take values in the range from 128 to 1500 inclusively.

Example

```
(vpn-server)> mru 200
VpnServer::Manager: mru set to 200.
```

History

Version	Description
2.04	The vpn-server mru command has been introduced.

3.177.9 vpn-server mtu

Description

Set *MTU* value to be transmitted to PPTP server. By default, 1350 value is used.

Command with **no** prefix resets value to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(vpn-server)> mtu <value>
```

```
(vpn-server)> no mtu
```

Arguments

Argument	Value	Description
value	<i>Integer</i>	<i>MTU</i> value. Can take values in the range from 128 to 1500 inclusively.

Example

```
(vpn-server)> mtu 200
VpnServer::Manager: mtu set to 200.
```

History

Version	Description
2.04	The vpn-server mtu command has been introduced.

3.177.10 vpn-server multi-login

Description

Allow connection to VPN server for multiple users from one account.

Command with **no** prefix disables this feature.

Prefix no

Yes

Change settings

Yes

Multiple input No

Synopsis

```
(vpn-server)> multi-login
(vpn-server)> no multi-login
```

Example

```
(vpn-server)> multi-login
VpnServer::Manager: multi login enabled.
```

History

Version	Description
2.04	The vpn-server multi-login command has been introduced.

3.177.11 vpn-server pool-range

Description Assign a pool of addresses for the clients that connect to the VPN server.
Command with **no** prefix removes a pool.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(vpn-server)> pool-range <begin> [ <size> ]
(vpn-server)> no pool-range
```

Arguments

Argument	Value	Description
begin	<i>IP address</i>	Start address of pool.
size	<i>Integer</i>	Pool size. Can take values in the range from 1 to 64 inclusively. If the size is not specified, it is determined automatically depending on the device.

Example

```
(vpn-server)> pool-range 172.168.1.22 20
VpnServer::Manager: Configured pool range 172.168.1.22 to ►
172.168.1.41.
```

```
(vpn-server)> no pool-range
VpnServer::Manager: Reset pool range.
```

History

Version	Description
2.04	The vpn-server pool-range command has been introduced.

3.177.12 vpn-server session-logout

Description Terminate an active or stalled session on the VPN server.

Prefix no No

Change settings Yes

Multiple input No

Synopsis `(vpn-server)> session-logout <session>`

Arguments

Argument	Value	Description
session	<i>Integer</i>	Identifier of the PPTP session (can be viewed using the show vpn-server command).

Example

```
(vpn-server)> session-logout 1
VpnServer::Manager: Session "1" is terminated.
```

History

Version	Description
4.03	The vpn-server session-logout command has been introduced.

3.177.13 vpn-server session-preempt

Description Enable to preempt VPN sessions when [vpn-server multi-login](#) option is disabled for the PPTP server.

Command with **no** prefix disables the preempt.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(vpn-server)> session-preempt`

`(vpn-server)> no session-preempt`

Example

```
(vpn-server)> session-preempt
VpnServer::Manager: Enabled sessions preemption.
```

```
(vpn-server)> no session-preempt
VpnServer::Manager: Disabled session preemption.
```

History

Version	Description
4.03	The vpn-server session-preempt command has been introduced.

3.177.14 vpn-server static-ip

Description

Bind IP address to the user. User account must have vpn tag.

Command with **no** prefix removes binding.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(vpn-server)> static-ip <name> <address>
```

```
(vpn-server)> no static-ip <name>
```

Arguments

Argument	Value	Description
name	<i>String</i>	Username.
address	<i>IP address</i>	IP address to bind.

Example

```
(vpn-server)> static-ip test 172.16.1.35  
VpnServer::Manager: Static IP 172.16.1.35 assigned to user "test".
```

```
(vpn-server)> static-ip test  
VpnServer::Manager: Static IP address removed for user "test".
```

History

Version	Description
2.04	The vpn-server static-ip command has been introduced.

Glossary

Address and Control Field Compression	LCP configuration option that provides a method to negotiate the compression of the Data Link Layer Address and Control fields.
Address Resolution Protocol	is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.
Airtime Fairness	it is a technology intended to increase the overall performance of the wireless network by solving a problem with slow clients. With a high activity of a slow device, the Wi-Fi network bandwidth is reduced. So that fast clients don't have to wait for their data transfer queues, Airtime Fairness technology limits the session of communication with the client device not by the number of packets, but by the time of their transmission.
Apple Filing Protocol	is a proprietary network protocol, and part of the Apple File Service (AFS), that offers file services for macOS and the classic Mac OS.
Authenticated Encryption with Associated Data	this form of encryption which simultaneously assure the confidentiality and authenticity of data. AEAD is a variant of AE that allows a recipient to check the integrity of both the encrypted and unencrypted information in a message.
Automatic Certificate Management Environment	is a communications protocol for automating interactions between certificate authorities and their users' web servers, allowing the automated deployment of public key infrastructure at very low cost. It was designed by the Internet Security Research Group (ISRG) for their Let's Encrypt service.
Band Steering	is a feature that encourages dual-band capable wireless clients to connect to the less crowded 5GHz network, and leave the 2.4GHz network available for those clients who support 2.4GHz only; thus, Wi-Fi performance can be improved for all clients.
Challenge-Handshake Authentication Protocol	widely used algorithm for authentication, which provides the transfer of indirect information about user password. CHAP provides better security than Password Authentication Protocol .

Change of Authorization	is a provides a mechanism for changing RADIUS authentication and authorization session attributes. Allows you to set up an active client session.
Command Line Interface	is a user interface to a computer's operating system or an application in which the user responds to a visual prompt by typing in a command on a specified line, receives a response back from the system, and then enters another command, and so forth.
Common Applications Kept Enhanced	is a shaping-capable queue discipline which uses both AQM and FQ. It combines COBALT, which is an AQM algorithm combining Codel and BLUE, a shaper which operates in deficit mode, and a variant of DRR++ for flow isolation. 8-way set-associative hashing is used to virtually eliminate hash collisions. Priority queuing is available through a simplified diffserv implementation. CAKE uses a deficit-mode shaper, which does not exhibit the initial burst typical of token-bucket shapers. It will automatically burst precisely as much as required to maintain the configured throughput.
Common Internet File System	is a protocol that lets programs make requests for files and services on remote computers on the Internet. CIFS uses the client/server programming model. A client program makes a request of a server program (usually in another computer) for access to a file or to pass a message to a program that runs in the server computer. The server takes the requested action and returns a response.
Compression Control Protocol	is used for establishing and configuring data compression algorithms over PPP .
Dead Peer Detection	is a method that network devices use to verify the current existence and availability of other peer devices.
Device Privacy Notice	is a Keenetic device privacy notice on data processing.
DHCP	is a network protocol that is used to configure network devices so that they can communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server. The DHCP client then uses this information to configure its host. Once the configuration process is complete, the host is able to communicate on the Internet.
DHCP server	manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, other servers such as time servers, and so forth. On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. Depending on implementation, the DHCP server may have three methods of allocating IP-addresses: • <i>dynamic allocation</i>: A network administrator assigns a range of IP addresses to DHCP, and each client computer on the LAN is configured to request an IP address from the DHCP server during network initialization. The request-and-grant process uses a lease

concept with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed.

- *automatic allocation*: The DHCP server permanently a free IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.
- *static allocation*: The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled in (perhaps by a network administrator). Only requesting clients with a MAC address listed in this table will be allocated an IP address. This feature (which is not supported by all DHCP servers) is variously called Static DHCP Assignment (by DD-WRT), fixed-address (by the dhcpd documentation), Address Reservation (by Netgear), DHCP reservation or Static DHCP (by Cisco/Linksys), and IP reservation or MAC/IP binding (by various other router manufacturers).

DHCPv6 server	is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes, default route, local segment MTU, and other configuration data required to operate in an IPv6 network. IPv6 hosts may automatically generate IP addresses internally using stateless address autoconfiguration ¹ (SLAAC), or they may be assigned configuration data with DHCPv6.
Diffie-Hellman	is that part of the IKE protocol used for exchanging the material from which the symmetrical keys are built. The Diffie-Hellman algorithm builds an encryption key known as a "shared secret" from the private key of one party and the public key of the other. Since the IPsec symmetrical keys are derived from this DH key shared between the peers, at no point are symmetric keys actually exchanged.
DLNA	standard that allows compatible devices to transfer media content (images, music, videos) over the home network and display it in real time. This technology is to connect home computers, mobile phones, notebooks and home electronics in a single digital network. DLNA-certified devices can be configured and combined in a home network automatically.
Domain Name System	is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. A Domain Name Service resolves queries for these names into IP addresses for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.
DNS over HTTPS	is a domain name system, computer distributed system for obtaining information about domains using secure data transfer between internet nodes resolution via the HTTPS protocol. The method is to increase

¹ [https://en.wikipedia.org/wiki/IPv6#Stateless_address_autoconfiguration_\(SLAAC\)](https://en.wikipedia.org/wiki/IPv6#Stateless_address_autoconfiguration_(SLAAC))

	user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks. The standard is described in RFC 8484 ² .
DNS over TLS	is a domain name system, computer distributed system for obtaining information about domains using secure data transfer between internet nodes. The standard is described in RFC 7858 ³ and RFC 8310 ⁴ .
DNS rebinding	is a method of manipulating resolution of domain names. In this attack, a malicious web page causes visitors to run a client-side script that attacks machines elsewhere on the network. This attack can be used to breach a private network by causing the victim's web browser to access computers at private IP addresses and return the results to the attacker.
Encapsulating Security Payload	is a member of the IPsec protocol suite. In IPsec it provides origin authenticity, integrity, and confidentiality protection of packets.
End-user license agreement	is a legal contract between a software application author or publisher and the user of that application.
Fast Transition	is a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.
Fair Queuing Controlled Delay	is queuing discipline that combines Fair Queuing with the CoDel AQM scheme. FQ_Codel uses a stochastic model to classify incoming packets into different flows and is used to provide a fair share of the bandwidth to all the flows using the queue. Each such flow is managed by the CoDel queuing discipline.
Fully Qualified Domain Name	is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System . It specifies all domain levels, including the top-level domain and the root zone. A fully qualified domain name is distinguished by its lack of ambiguity: it can be interpreted only in one way.
Full Cone NAT	also Static NAT, one to one NAT, port forwarding is the only type of NAT where the port is permanently open and allows inbound connections from any external host. A full cone NAT maps a public IP address and port to a LAN IP and port. Any external host can send data to the LAN IP through the mapped NAT IP and port. If it tries to send data through a different port it will fail. Static NAT is required when a network device on a private network must be accessible from the Internet.
Generic Routing Encapsulation	is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.
Hash Message Authentication Code	is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a

² <https://tools.ietf.org/html/rfc8484>³ <https://tools.ietf.org/html/rfc7858>⁴ <https://tools.ietf.org/html/rfc8310>

	secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authentication of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key.
HTTP Proxy	Hypertext Transfer Protocol (HTTP) and HTTPS (HyperText Transfer Protocol Secure) Proxy is a proxy server that uses the Hypertext Transfer Protocol (HTTP) to connect to a web server and a client (browser). HTTPS (HyperText Transfer Protocol Secure) proxies work with SSL (Secure Socket Layer), which is an additional layer of security imposed on HTTP to protect its data. It supports security certificates, which are used to end-to-end encrypt traffic and prevent data interception during transmission. A proxy server that supports SSL establishes a secure connection to the client and to the web server to avoid any outside interference.
Idempotence	is the property of certain operations in computer science, that they can be applied multiple times without changing the result beyond the initial application.
Inter-Access Point Protocol	is a standard IEEE 802.11F protocol exchange of service information for data transfer between access points. The protocol is responsible for combining the wireless network, secure data exchange between the current access point and the new access point in the specified period.
Internet Control Message Protocol	is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.
Internet Control Message Protocol version 6	is the implementation of the Internet Control Message Protocol (ICMP) for Internet Protocol version 6 (IPv6). ICMPv6 is an integral part of IPv6 and performs error reporting and diagnostic functions. ICMPv6 is defined in RFC 4443⁵.
Internet Group Management Protocol	is an Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send content to multiple other computers. Multicasting can be used for streaming media to an audience that has "tuned in" by setting up a multicast group membership.
Internet Key Exchange	is a standard protocol IPsec, used to ensure the safety of interaction in virtual private networks. IKE purpose is to establish a secure authenticated communication channel by using the Diffie-Hellman key exchange algorithm to generate a shared secret key to encrypt further IPsec communications.

⁵ <https://datatracker.ietf.org/doc/html/rfc4443>

Internet Protocol	is the principal communications protocol in the Internet. The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6).
Internet Protocol Control Protocol	is a network control protocol for establishing and configuring Internet Protocol over a Point-to-Point Protocol (PPP) link. IPCP uses the same packet exchange mechanism as the Link Control Protocol. IPCP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase, and any IPCP packets received before this phase is reached should be silently discarded.
Internet Protocol Security	commonly called IPsec, is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.
IPsec Passthrough	is technology that allows VPN-traffic to pass through NAT.
IPsec Security Association	is fundamental to IPsec. An SA is a relationship between two or more entities that describes how the entities will use security services to communicate securely. Each IPsec connection can provide encryption, integrity, authenticity, or all three. When the security service is determined, the two IPsec peers must determine exactly which algorithms to use (for example, DES or 3DES for encryption, MD5 or SHA for integrity). After deciding on the algorithms, the two devices must share session keys. The Security Association is the method that IPsec uses to track all the particulars concerning a given IPsec communication session.
IP in IP	is an IP tunneling protocol that encapsulates one IP packet in another IP packet.
IPv6CP	is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the Point-to-Point (PPP) link. IPv6CP uses the same packet exchange mechanism as the Link Control Protocol . IPv6CP packets may not be exchanged until PPP has reached the Network-Layer Protocol phase. IPv6CP packets received before this phase is reached should be silently discarded.
Layer 2 Tunneling Protocol	is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.
Link Control Protocol	establishes, configures, and tests data-link Internet connections in the Point-to-Point Protocol (PPP). Before establishing communications over

	a point-to-point link, each end of the PPP link must send out LCP packets. The LCP packet either accepts or rejects the identity of its linked peer, agrees up on packet size limits, and looks for common misconfiguration errors. LCP packets are divided into three classes: • Link configuration packets used to establish and configure a link • Link termination packets used to terminate a link • Link maintenance packets used to manage and debug a link
Link Layer Discovery Protocol	is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. Information gathered with LLDP is stored in the device as a management information database (MIB) and can be queried with the Simple Network Management Protocol (SNMP).
Low-Density Parity-Check	is a linear error correcting code, a method of transmitting a message over a noisy transmission channel. An LDPC is constructed using a sparse bipartite graph. LDPC codes are capacity-approaching codes, which means that practical constructions exist that allow the noise threshold to be set very close (or even arbitrarily close on the BEC) to the theoretical maximum (the Shannon limit) for a symmetric memoryless channel. The noise threshold defines an upper bound for the channel noise, up to which the probability of lost information can be made as small as desired. Using iterative belief propagation techniques, LDPC codes can be decoded in time linear to their block length.
Master Browser	is a tool that provides information about, and typically a way to access, SMB/CIFS files and printer shares. It is responsible for the browse host list within its respective subnet and portion of the domain on its subnet. Is used to host information of other Windows computers within the same Windows domain or TCP/IP network.
Maximum Receive Unit	is the maximum size (in bytes) of the frame, which can be received at the data link layer of communication protocol.
Maximum Segment Size	is a parameter of the options field of the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment. It does not count the TCP header or the IP header.
Maximum Transmission Unit	is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. Most computer operating systems provide a default MTU value that is suitable for most users. In general, Internet users should follow the advice of their Internet service provider (ISP) about whether to change the default value and what to change it to.

Microsoft Point-to-Point Encryption	encrypts data in Point-to-Point Protocol based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) connections. 128-bit key (strong), 56-bit key, and 40-bit key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.
Modular Wi-Fi System	a system that allows several Keenetic devices to be combined into a single Internet space distributed over an area. One of the devices is defined as the controller, the others as the members.
Multicast DNS	is a way of using familiar DNS programming interfaces, packet formats and operating semantics, in a small network where no conventional DNS server has been installed. The mDNS protocol uses IP multicast UDP packets, and is implemented by the Apple Bonjour and open source Avahi software packages.
Network Access Control List	rules that are applied to IP interfaces that are available on a router, each with a list of hosts or networks that are permitted or denied to use the service. Access control lists can be configured to control both inbound and outbound traffic.
Network Flow	network protocol for network traffic accounting, uses UDP or SCTP protocols to send traffic data to the collector. Collector is an application that runs on a server and collects statistics received from sensors. A sensor is a device that collects traffic statistics and sends it to a collector. The sensor can be a Cisco third-level router or switch.
NEXTDNS	service of NextDNS protects you from all kinds of security threats, blocks ads and trackers on websites and in apps and provides a safe and supervised Internet for kids — on all devices and on all networks.
Network Time Protocol	is a protocol that is used to synchronize computer clock times in a network of computers. Developed by David Mills at the University of Delaware, NTP is now an Internet standard. In common with similar protocols, NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.
Network Traffic Classification Engine	also DPI, Deep Deep Packet Inspection is a technology for accumulating statistics and inspecting network packets based on their contents. Deep Packet Inspection analyzes not only packet headers, but also the full content of traffic at OSI layers 2 and above. Deep Packet Inspection can determine which network application has generated or received data, collecting detailed connection statistics for each device and application individually. With quality of service Deep Packet Inspection controls the transmission speed of individual packets by raising or lowering it. The Traffic Classification Engine component operates completely independently and does not make any calls to external services.

OpenConnect	is a free and open-source cross-platform multi-protocol virtual private network (VPN) client software which implement secure point-to-point connections.
Open Package	lightweight package management system. It is intended for use on embedded Linux devices and is used in this capacity in the OpenWrt ⁶ and Entware ⁷ projects. Opkg packages use the .ipk extension.
Opportunistic Wireless Encryption	is an extension of the IEEE 802.11 standard, similar encryption method Simultaneous Authentication of Equals (SAE). This encryption method provides users with better protection when connected to an open Wi-Fi network.
Password Authentication Protocol	is an authentication protocol that uses a password. PAP is used by Point-to-Point Protocol to validate users before allowing them access to the remote network. PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure.
Protected Extensible Authentication Protocol	is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel. The purpose was to correct deficiencies in EAP; EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided.
Perfect Forward Secrecy	is a property of secure communication protocols: a secure communication protocol is said to have forward secrecy if compromise of long-term keys does not compromise past session keys. PFS protects past sessions against future compromises of secret keys or passwords.
Ping Check	performs ICMP and TCP based tests to verify if the internet connection is working fine. Test results may be used to switch between primary and backup connections.
Pairwise Master Key	is a cryptographic private key used in wireless networks to establish secure communication between devices. PMK is derived from a pre-shared key (PSK) or another authentication mechanism, and it serves as the foundation for generating encryption keys for pairwise communication. The PMK is primarily used in the IEEE 802.11i standard.
Point-to-Point Protocol	is a protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression. PPP is used over many types of physical networks including serial cable, phone line, cellular telephone, specialized radio links, and fiber optic links. After the link has been established, additional network (layer 3) configuration may take place. Most commonly, the Internet Protocol Control Protocol (IPCP) is used.
Public Land Mobile Network	is a combination of wireless communication services offered by a specific operator in a specific country. PLMN typically consists of several cellular technologies like GSM/2G, UMTS/3G, LTE/4G, offered by a operator cellular network.

⁶ <https://www.openwrt.org/>⁷ <https://github.com/Entware/Entware>

Preamble	it is the first part of the Physical Layer Convergence Protocol/Procedure (PLCP) Protocol Data Unit (PDU). A header is the remaining part of the data packets and has more information identifying the modulation scheme, transmission rate, and length of time to transmit the whole data frame. The Preamble type in IEEE 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the Access Point and roaming wireless adapters. Long preamble: • PLCP with long preamble is transmitted at 1 Mbps regardless of transmit rate of data frames • Total long preamble transfer time is a constant at 192 usec • Compatible with legacy IEEE 802.11 systems running at 1 and 2 Mbps Short preamble: • Preamble is transmitted at 1 Mbps and header at 2 Mbps • Total short preamble transfer time is a constant at 96 usec • Not compatible with legacy IEEE 802.11 systems operating at 1 and 2 Mbps
Protected Management Frames	IEEE 802.11w is the Protected Management Frames standard for the IEEE 802.11 family of standards. This functionality is necessary to improve security by ensuring data confidentiality in control frames.
Protocol Field Compression	is a method to negotiate the compression of the PPP Protocol field. By default, all implementations MUST transmit packets with two octet PPP Protocol fields.
Pseudo-Random Function	is similar to an integrity algorithm, but instead of being used to authenticate messages, it is only used to provide randomness for purposes such as keying material. PRFs are primarily used with an authenticated encryption algorithm type such as AES-GCM.
Radio Resource Management	is the system level management of co-channel interference, radio resources, and other radio transmission characteristics in wireless communication systems. RRM includes control parameters such as transmit power, user allocation, beamforming, data rates, handover criteria, modulation scheme, coding scheme errors.
Remote Authentication in Dial-In User Service	is a protocol to implement authentication, authorization, and resource collection. It is used for charging the used resources by a specific user. Used to authenticate users on open Wi-Fi wireless networks.
Remote Procedure Call	is a protocol that one program can use to request a service from a program located in another computer in a network without having to understand network details. (A procedure call is also sometimes known

	as a function call or a subroutine call.) RPC uses the client/server model. The requesting program is a client and the service-providing program is the server. Like a regular or local procedure call, an RPC is a synchronous operation requiring the requesting program to be suspended until the results of the remote procedure are returned.
Restricted NAT	also Dynamic NAT works in the same way as a Full Cone NAT but applies additional restrictions based on an IP address. The internal client must first have sent packets to IP address (X) before it can receive packets from X. In terms of restrictions the only requirement is that packets come in on the mapped port and from an IP address that the internal client has sent packets to.
Secure Socket Tunneling Protocol	is a type of VPN tunnel that utilizes an SSL 3.0 channel to send PPP or L2TP traffic. SSL allows for transmission and data encryption, as well as traffic integrity checking. Due to this, SSTP can pass through most firewalls and proxy servers by using the SSL channel over TCP port 443.
Service Set Identifier	is a sequence of characters that uniquely names a wireless local area network (WLAN). An SSID is sometimes referred to as a "network name". This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.
Simple Network Management Protocol	is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.
Simple Network Time Protocol	is an Internet Protocol (IP) used to synchronize the clocks of networks of computers. SNTP is based upon the TCP/IP protocol suite. It is an application layer time protocol, part of the Network Time Protocol base protocol. Along with NTP, SNTP communicates using the User Datagram Protocol (UDP). By default, UDP port 123 is used. SNTP can operate on IPv4 and IPv6 networks. The standard is described in RFC 4330⁸.
SOCKS	is an Internet protocol that exchanges network packets between a client and server through a proxy server. SOCKS5 optionally provides authentication so only authorized users may access a server. SOCKS server proxies TCP connections to an arbitrary IP address, and provides a means for UDP packets to be forwarded.
Shared key	is a mode by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy protocol. With Shared Key, a computer equipped with a wireless modem can fully access any WEP network and exchange encrypted or unencrypted data.

⁸ <https://www.rfc-editor.org/rfc/rfc4330>

Short Message Service	is a text messaging service component of most telephone, Internet, and mobile device systems. It uses standardized communication protocols to enable mobile devices to exchange short text messages.
SSH File Transfer Protocol	is a application layer protocol for transferring files over a reliable and secure connection over TCP port 22.
Transmission Control Protocol	is a core protocol of the Internet Protocol suite. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network.
Temporal Key Integrity Protocol	is a security protocol used in the IEEE 802.11 wireless networking standard. TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as an interim solution to replace WEP without requiring the replacement of legacy hardware.
Universal Access Method	is a method that allows a subscriber to access a wireless Wi-Fi network. The Internet browser will open a login page where the user should fill in his credentials before he can access. UAM uses the RADIUS client and the RADIUS server for authorization.
User Datagram Protocol	is a core protocol of the Internet Protocol suite. UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network protocol. There is no guarantee of delivery, ordering, or duplicate protection. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system.
udpxy	is a UDP-to-HTTP multicast traffic relay daemon: it forwards UDP traffic from a given multicast subscription to the requesting HTTP client.
Universal Plug and Play	is a standard that uses Internet and Web protocols to enable devices such as PCs, peripherals, intelligent appliances, and wireless devices to be plugged into a network and automatically know about each other. With UPnP, when a user plugs a device into the network, the device will configure itself, acquire a TCP/IP address, and use a discovery protocol based on the HTTP to announce its presence on the network to other devices.
Unstructured Supplementary Service Data	is a communications protocol used by cellular telephones to communicate with the mobile network operator's computers. USSD is commonly used by prepaid cellular phones to query the available balance.
Variable Gain Amplifiers	are signal-conditioning amplifiers with electronically settable voltage gain. Used to improve wireless communication.
Virtual LAN	is a local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application). The virtual LAN controller can change or add workstations and manage loadbalancing and bandwidth allocation more easily than with a physical picture of the LAN.

Web Distributed Authoring and Versioning	is a extension of the Hypertext Transfer Protocol (HTTP) that allows clients to perform remote Web content authoring operations. Supports web server authentication and SSL encryption for HTTPS using the default TCP port 443.
Web Proxy Auto-Discovery Protocol	is a method used by clients to locate the URL of a configuration file using DHCP and/or DNS discovery methods. Once detection and download of the configuration file is complete, it can be executed to determine the proxy for a specified URL.
WireGuard	is a free and open-source software application and virtual private network (VPN) protocol to create secure point-to-point connections in routed configurations. WireGuard protocol uses modern cryptography options Curve25519 for key exchange, ChaCha20 for encryption, and Poly1305 for data authentication, SipHash for hashtable keys, and BLAKE2s for hashing. Supports layer 3 for both protocols IPv4 and IPv6.
Wi-Fi Multimedia	previously known as Wireless Multimedia Extensions (WME), is a subset of the 802.11e wireless LAN (WLAN) specification that enhances quality of service (QoS) on a network by prioritizing data packets according to four access categories (AC). Ranging from highest priority to lowest, these categories are: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK). WMM also features a Power Save certification that helps small devices on a network conserve battery life. Power Save allows small devices, such as phones and PDAs, to transmit data while in a low-power "dozing" status. The certification gives software developers and hardware manufacturers a way to fine-tune battery use in the ever-increasing number of small devices that have Wi-Fi capabilities.
Wi-Fi Protected Access	Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are three security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP. WPA advantages are enhanced data security and tightened access control for wireless networks. Important characteristic is the compatibility between multiple wireless devices at the hardware level as well as at software level. WPA3 uses 128-bit encryption in WPA3-Personal mode (192-bit in WPA3-Enterprise). The WPA3 standard also replaces the Pre-Shared Key exchange with Simultaneous Authentication of Equals as defined in IEEE 802.11-2016 resulting in a more secure initial key exchange in personal mode. WPA Enterprise is a protocol-based authentication mode IEEE 802.1X using an external authentication server RADIUS and local client Supplicant.
Wi-Fi Protected Setup	provides an industry-wide mechanism to set up and configure networks for home and small office (SOHO) environments. Wi-Fi Protected Setup enables typical users who possess little understanding of traditional Wi-Fi configuration and security settings to easily configure new wireless networks, to add new devices and to enable security.

Wired Equivalent Privacy	is a security algorithm for IEEE 802.11 wireless networks. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools. In 2004, with the ratification of the full 802.11i standard (i.e. WPA2), the IEEE declared that both WEP-40 and WEP-104 have been deprecated.
Wireless Internet Service Provider	is an Internet service provider (ISP) that allows subscribers to connect to a server at designated hotspots (access points) using a wireless connection such as Wi-Fi. This type of ISP offers Broadband service and allows subscriber computers, called stations, to access the Internet and the Web from anywhere within the zone of coverage provided by the server antenna. This is usually a region with a radius of several kilometers. The simplest WISP is a basic service set (BSS) consisting of one server and numerous stations all linked to that server by wireless. More sophisticated WISP networks employ the extended service set (ESS) topology, consisting of two or more BSSs linked together at access points (APs). Both BSS and ESS are supported by the IEEE 802.11b specification.
Extended Authentication	or XAUTH, provides an additional level of authentication by allowing the IPsec gateway to request extended authentication from remote users, thus forcing remote users to respond with their credentials before being allowed access to the VPN.
XFRM	is an IP framework for transforming packets (such as encrypting their payloads) and used to implement the IPsec protocol suite. It is also used for the IP Payload Compression Protocol and features of Mobile IPv6.
ZeroTier	is a distributed network hypervisor built atop a cryptographically secure global peer to peer network. It provides advanced network virtualization and management capabilities on par with an enterprise SDN switch, but across both local and wide area networks and connecting almost any kind of app or device. All traffic is encrypted end to end on OSI layer 1 using 256-bit Salsa20 and authenticated using the Poly1305 message authentication (MAC) algorithm. MAC is computed after encryption (encrypt-then-MAC) and the cipher/MAC composition used is identical to the NaCl reference implementation. The ZeroTier world is controlled by two types of identifier: 40-bit/10-digit <i>ZeroTier addresses</i> and 64-bit/16-digit <i>network IDs</i>. These identifiers are easily distinguished by their length. A ZeroTier address identifies a node or "device" (laptop, phone, server, VM, app, etc.) while a network ID identifies a virtual Ethernet network that can be joined by devices. A ZeroTier address looks like 8056c2e21c and a network ID looks like 8056c2e21c000001. Network IDs are composed of the ZeroTier address of that network's primary controller and an arbitrary 24-bit ID that identifies the network on this controller.

Interface Hierarchy

Figure A.1. Core interfaces

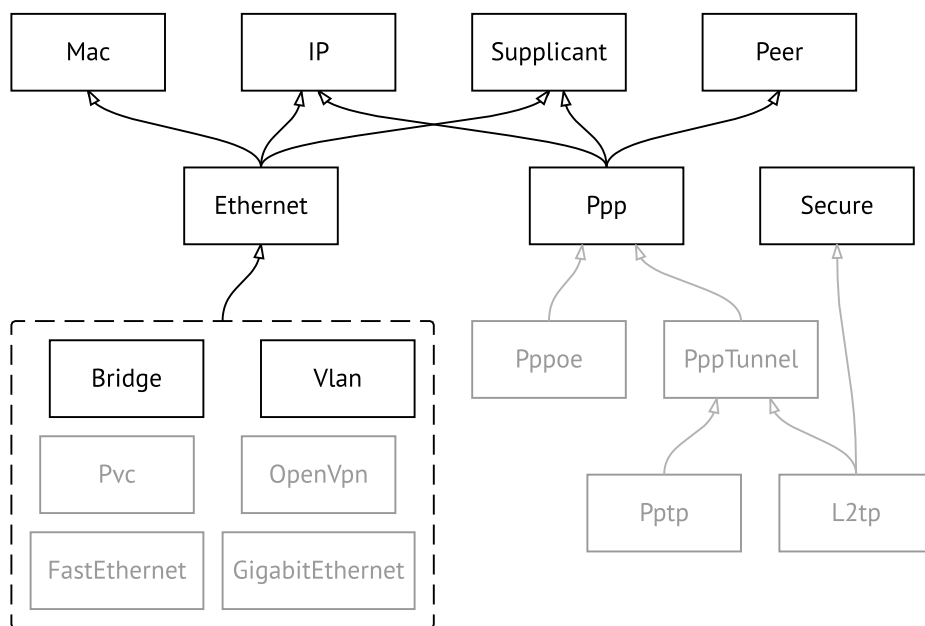


Figure A.2. Tunnel interfaces

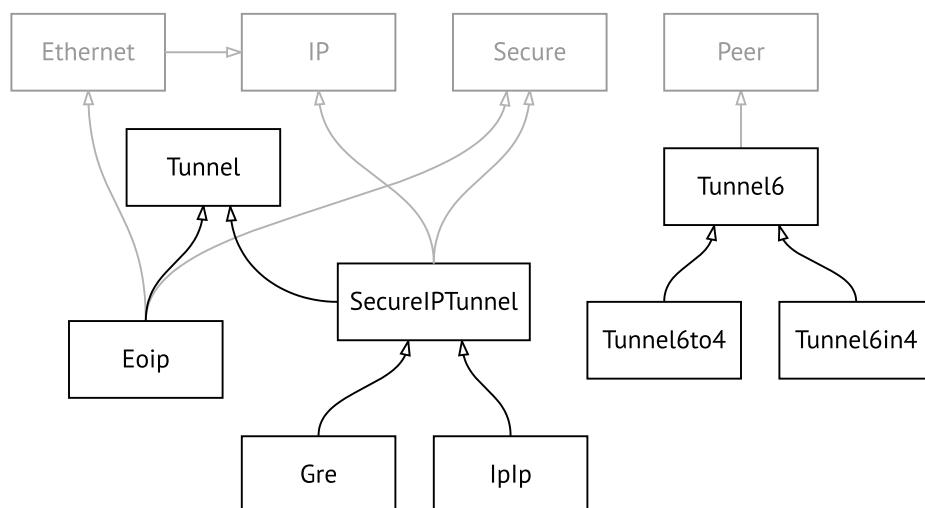
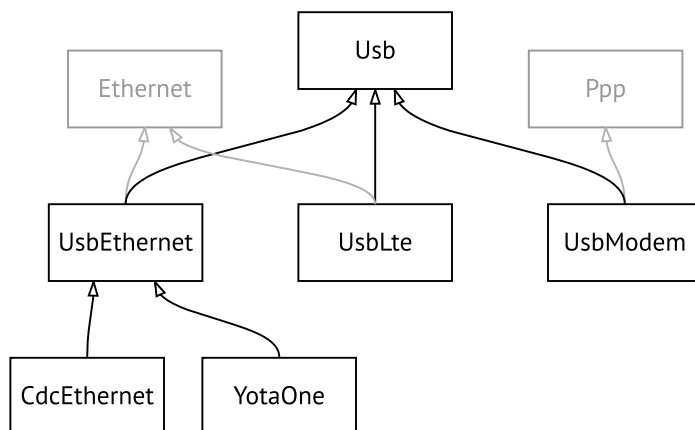
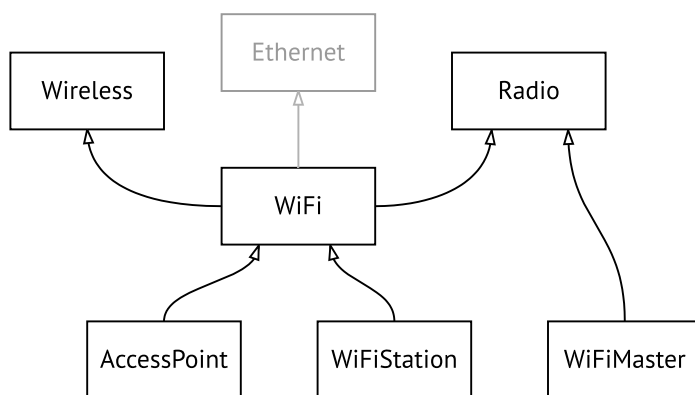


Figure A.3. USB interfaces**Figure A.4. Wi-Fi interfaces**

HTTP API

B.1 REST Core Interface

Carrier HTTP API lets you develop a custom application, that will access Carrier settings using simple HTTP methods, such as GET and POST.

The base URL for all operations is `/rci`, that simply stands for REST Core Interface. It replaces the [XML Core Interface](#), which is now deprecated but continues to be functional.

B.1.1 Resource Location

RCI is based on the Carrier command tree. Device settings are mapped to RCI resources in such a way that every “a b c” command corresponds to the `/rci/a/b/c` URL.

As a result, hereby [Command Reference](#) gives you a complete picture of all RCI resources and their parameters. The words “command” and “resource” are used interchangeably in this manual.

Parameters are listed in the Arguments table of each command. They can be passed as part of the request using HTTP query: `/rci/a/b/c?parameter=value`. Unless otherwise specified for a certain command, query parameters are optional. Multiple parameters should be separated by ampersand (&) characters.

Parameters can also be passed in the POST request body, as described in [Section B.1.3 on page 748](#).

B.1.2 Methods

Method semantics depend on the type of resource. There are three types of resources in RCI:

- Settings
- Actions
- Background processes

B.1.2.1 Settings

Settings are device configuration elements. You can view, modify, or delete settings using standard HTTP methods.

GET Retrieve settings.

- POST Create or modify settings.
- DELETE Delete settings (reset to default).

B.1.2.2 Actions

Actions are commands that do not modify settings. Actions run instantly as opposed to background processes, see also [Section B.1.2.3 on page 748](#)

- GET Mapped to POST for /rci/show. Not applicable to other actions.
- POST Execute a command and return its output.
- DELETE Not applicable.

B.1.2.3 Background processes

Background processes are instances that can be created and polled for updates. Such processes are bound to a particular session, and cannot be accessed from anywhere else.

- GET Retrieve updates from existing process. Returns 404 if there is no such process.
- POST Create a background process.
- DELETE Terminate a background process.

B.1.3 Data Format

HTTP POST requests must be submitted in a free-form JSON,¹ that is interpreted as a batch of parameters and nested settings, depending on the data type. Conversely, HTTP GET returns JSON data that was previously POSTed to the specified resource.

The primary data type is Object. This is unordered collection of key-value pairs, enclosed in curly brackets {}. Each key must be unique within an object.

Objects can be put one into another, or be combined in arrays as detailed in [Section B.1.3.2 on page 749](#) and [Section B.1.3.3 on page 749](#)

B.1.3.1 Parameters

String, boolean and number values of an object are interpreted as parameters of the resource being addressed.

```
{  
  "parameter": value  
}
```

Example B.1. Set hotspot policy

Set policy “permit” for the Home network. Refer to [Section 3.47.10 on page 356](#) to see how “interface” and “access” parameters are mentioned in the Arguments table.

¹In compliance with RFC 7159.

```
POST /rci/ip/hotspot/policy HTTP/1.1
Host: 192.168.1.1
Content-length: 48
Content-type: application/json

{
  "interface": "Home",
  "access": "permit"
}
```

B.1.3.2 Nested resources

Object and array values of a parent object are interpreted as nested resources.

```
{
  "command": {
    "parameter": value
  }
}
```

In particular, empty object denotes a command with no parameters.

```
{
  "command": {}
}
```

Using this rule, you can address multiple resources at a time. RCI engine will process your request from top to bottom, recursing over the JSON structure. Parameters of a parent resource apply to all nested resources within the nearest surrounding scope.

Example B.2. Create and enable a PPP interface

Call “interface” to create a new PPPoE connection, as described in [Section 3.29 on page 153](#), and enable it with “interface up”. The “name” parameter applies to both “interface” and “up”.

```
POST /rci HTTP/1.1
Host: 192.168.1.1
Content-length: 39
Content-type: application/json

{"interface":{"name":"PPPoE1","up":{}}}
```

B.1.3.3 Arrays

Arrays can be used to operate on a specific resource multiple times. The important thing is that arrays preserve the order of their elements, in contrast to object members.

```
{
  "command": [
    {"parameter1": value1},
    {"parameter2": value2} ]
}
```

B.1.3.4 Response structure

The structure of POST output strictly corresponds to input. RCI reproduces input arrays and nested objects, and replaces input parameters with output data. This approach lets you locate any part of the response using a resource name.

Example B.3. Show version and interface Home

Run two different “show” commands in a certain order.

```
POST /rci/show HTTP/1.1
Host: 192.168.1.1
Content-length: 46
Content-type: application/json

[{"version":{}}, {"interface":{"name":"Home"}}]
```

Response is an array of two elements, in accordance with the request.

```
[
  {
    "version": {
      "release": "2.12.A.1.0-1",
      "arch": "mips",
      "ndm": {
        "exact": "0-cbf8590",
        "cdate": "15 Jan 2018"
      },
      "bsp": {
        "exact": "0-06ee10b",
        "cdate": "15 Jan 2018"
      },
      "ndw": {
        "version": "0.2.1",
        "features": "wifi_button,single_usb_port,dual_image",
        "components": "base,cloudcontrol,..."
      },
      "manufacturer": "Keenetic Ltd.",
      "vendor": "Keenetic",
      "series": "KN",
      "model": "4G (KN-1210)",
      "hw_version": "10128000",
      "hw_id": "KN-1210",
      "device": "4G",
      "class": "Internet Center"
    },
    "interface": {
      "id": "Bridge0",
      "index": 0,
      "type": "Bridge",
      "description": "Home network",
      "interface-name": "Home",
    }
  },
  {
    "interface": {
      "id": "Bridge0",
      "index": 0,
      "type": "Bridge",
      "description": "Home network",
      "interface-name": "Home",
    }
  }
]
```

```

    "link": "up",
    "connected": "yes",
    "state": "up",
    "mtu": 1500,
    "tx-queue": 1000,
    "address": "192.168.1.1",
    "mask": "255.255.255.0",
    "uptime": 2621,
    "global": false,
    "security-level": "private",
    "mac": "50:ff:20:00:00:08",
    "auth-type": "none"
  }
}
]

```

B.2 XML Core Interface

Warning: XML Core Interface is deprecated and is maintained for backward compatibility.

Carrier provides an HTTP XML API. The API is implemented as /ci resource that accepts POST XML requests and returns XML after the user agent has been authenticated.

If Carrier is reset to factory defaults, authentication is not required.

Example B.4. XML API call

Execute the “**show interface**” command for the WAN interface named ISP. This interface exists by default in Carrier.

```

POST /ci HTTP/1.1
Host: 192.168.1.1
Connection: keep-alive
Content-Length: 177
Origin: http://192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
Content-Type: application/xml
Referer: http://192.168.1.1/

<packet ref="/">
  <request id="1" ref="former.ifaces[load]">
    <command name="show interface">
      <name>ISP</name>
    </command>
  </request>
</packet>

```

The device responds with the current status of ISP:

```

HTTP/1.0 200 OK
Server: Ag [47]
Set-Cookie: _authorized=*; path=/

```

```

Content-type: text/xml
Content-Length: 760

<packet>
  <response id="1">
    <interface name="ISP">
      <mac>ec:43:f6:d3:22:d9</mac>
      <id>FastEthernet0/Vlan2</id>
      <index>2</index>
      <type>VLAN</type>
      <description>Broadband connection</description>
      <link>down</link>
      <connected>no</connected>
      <state>up</state>
      <mtu>1500</mtu>
      <tx-queue>1000</tx-queue>
      <global>yes</global>
      <defaultgw>no</defaultgw>
      <priority>700</priority>
      <security-level>public</security-level>
      <auth-type>none</auth-type>
    </interface>
    <message code="268370345" ident="Network::Interface::Base"
source="">done</message>
  </response>
</packet>

```

The `<request>` element is always sent from the user agent to the device. The device always responds with a `<response>`. The `id` attribute can be used to establish one-to-one correspondence between them.

Figure B.1. Request Element

```

<request id="identifier">
  <!-- request content -->
</request>

```

Figure B.2. Response Element

```

<response id="identifier">
  <!-- response content -->
</response>

```

There are two basic types of XML requests:

Command Request	Execute a specific command on the device. Available commands are described in Chapter 3 on page 41
Configuration Request	Get parameters that have been configured by a specific command.

B.2.1 Command Request

Command request can be used to execute a specific command on the device.

Figure B.3. Command Request

```
<request id="identifier">
  <command name="command">
    <no/>
    <argument>value</argument>
    ...
  </command>
</request>
```

command Space separated name of the command. Available commands are listed in [Chapter 3 on page 41](#).

argument Name of the argument. Available arguments for each command are listed in [Chapter 3 on page 41](#). Some commands do not require any arguments.

value Value of the argument.

no Optional element that is used to negate the action of the command. It has the same effect as the prefix *no*, see [Section 2.3 on page 37](#).

B.2.2 Configuration Request

Configuration request can be used to get configured parameters. Web interface uses this kind of request to fill out the HTML forms.

Figure B.4. Configuration Request

```
<request id="identifier">
  <config name="command" />
</request>
```

B.2.3 Request Packet

Multiple requests can be arranged in packets to optimize the performance.

Figure B.5. Request Packet

```
<packet>
  <request id="1">
    <!-- request content -->
  </request>
  <request id="2">
    <!-- request content -->
  </request>
  ...
</packet>
```

Response elements are returned as a packet. Response identifiers are used to bind response elements to requests. If there is no response, an empty `<response/>` element is returned.

Figure B.6. Response Packet

```
<packet>
  <response id="1">
    <!-- response content -->
  </response>
  <response id="2"/>
    <!-- no response for id=2 -->
  ...
</packet>
```

NVOX CLI commands

NVOX is an IP telephony application designed to work with Keenetic Linear USB module. Allows you to connect telephones to your Keenetic router to make and receive calls over the Internet using SIP.

Why the prefix substitution rule is used

In some cases, in incoming calls, the calling numbers are defined in a format that is not compatible with the dialing rules of the IP telephony operator. This makes it impossible to call back the number from the phone's call log.

For example: during an incoming call on the phone display, you can see +393921234567 and to call back the subscriber, you need to dial 3921234567. In this case, the prefix substitution rule **(+39>)x.** can remove **+39** from the caller's number. With this rule, when a call comes in, the handset display shows the number 3921234567, compatible with the operator's dialing rules.

Syntax of prefix substitution rules

01234567890*#+ABCDx[]()|-> — allowed characters.

T — waiting for the next digit of the number.

x — any digit from 0 to 9.

[146] — any of the numbers in square brackets (1, 4, or 6).

[1-6] — any of the digits in the range specified in square brackets (1,2,3,4,5 or 6).

(8>+7) — replacement/substitution/deletion. To the left of the > symbol, there is a sequence of digits that should be replaced with the sequence to the right of the >. If only the sequence on the left is specified, it will be deleted from the dialed number. If only the sequence on the right is specified, it will be added. The expression must be enclosed in parentheses.

2. — the digit to the left of the dot is repeated any number of times.

The **|** character separates two or more prefix replacement rules in a string.

Note: A string of several rules written with the separator **|** must be enclosed in quotation marks.

Examples of a prefix substitution rules

(+7>8)49(589)x. — in numbers with the prefix **+7** and code **495**, **498** or **499** the prefix changes to **8**, the rest of the number remains unchanged.

8[49]xxxxxxxxxx — any number with 11 digits, the first digit of which is **8** and the second digit of which is **4** or **9**.

10xx — any four-digit number in which the first digits are **10**.

xx#** — a four-digit sequence in which the first character is **, followed by any two digits and the character **#**.

[1-79]xxxxxx — any number of seven digits in which the first digit is any digit except 8.

x. — any number consists of digits from 0 to 9.

"0T|00T|000" — the numbers 0, 00 or 000. The **T** symbol is used to wait for dialing to continue after dialling 0 and 00. It should be used if you need to dial in conversational mode (press the call button, then dial the number).

(0>+4)x. — in any number, the first digit of **0** will be replaced by **+4**.

(*2>84951234567) — dialing ***2** will send a call to 84951234567. You can configure a speed dialing.

"8[49]xxxxxxxxxx|10xx|*xx#" — the three rules discussed above are written on one line, separated by **|**. The telephone exchange checks such rules one by one, from left to the right.

"76543210|1234x.|+749[589]xxxxxxxx" — a list of one number and two templates.

C.1 nvox

Description Access to a group of commands to manage the telephone station.

Prefix no No

Change settings No

Multiple input No

Group entry (nvox)

Synopsis (config)> **nvox**

Example

```
(config)> nvox
Core::Configurator: Done.
(nvox)>
```

History

Version	Description
2.00	The nvox command has been introduced.

C.2 nvox call-history clear

Description Delete all entries from the call log.

Prefix no No

Change settings No

Multiple input No

Synopsis `(nvox)> call-history clear`

Example `(nvox)> call-history clear`
 Nvox::CallHistory: Call history cleared.

History

Version	Description
2.06	The dect call-history clear command has been introduced.
3.05	The command renamed to nvox call-history clear .

C.3 nvox call-history delete-call

Description Delete a call log entry.

Prefix no No

Change settings No

Multiple input No

Synopsis `(nvox)> call-history delete-call <call-index>`

Arguments

Argument	Value	Description
call-index	Hex	Four-digit entry identifier.

Example `(nvox)> call-history delete-call 000f`

History

Version	Description
3.05	The nvox call-history delete-call command has been introduced.

C.4 nvox call-history directory

Description Specify a directory on the external USB drive to store call log files. By default, the call log is stored in the Keenetic router's RAM and is cleared after a reboot.

Command with **no** prefix resets setting to default.

Note: The phone book is stored in the same directory as the call log.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> call-history directory <directory>

(nvox)> no call-history directory
```

Arguments	Argument	Value	Description
	directory	<i>Filename</i>	Path to the folder on the external drive.

Example

```
(nvox)> call-history directory DATA:/call-history
Nvox::Manager: Set call history directory to DATA:/call-history.

(nvox)> no call-history directory
Nvox::Manager: Call history directory reset to default.
```

History	Version	Description
	3.05	The nvox call-history directory command has been introduced.

C.5 nvox call-history dump

Description Save the call log to a *.csv file.

Prefix no No

Change settings No

Multiple input No

Synopsis

```
(nvox)> call-history dump
```

Example

```
(nvox)> call-history dump
Nvox::CallHistory: Dump call history to file: ►
/tmp/mnt/ff085e00-8850-4ac3-9f46-3c209fcf3a13/nvox/nvox.history_calls.
```

History	Version	Description
	3.05	The nvox call-history dump command has been introduced.

C.6 nvox call-history filter

Description Configure a filter to output the call history by the [show nvox call-history](#) command.

Command with **no** prefix disables the filter.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> call-history filter <time-from> <time-to> <type> [text]
```

```
(nvox)> no call-history filter
```

Arguments

Argument	Value	Description
time-from	<i>String</i>	Date and time of the period start in DD MM YYYY HH:MM:SS format.
	*	The beginning of the interval is not set.
time-to	<i>String</i>	Date and time of the period end in DD MM YYYY HH:MM:SS format.
	*	The end of the interval is not set.
type	in	Search in incoming calls.
	out	Search in outgoing calls.
	missed	Search in missed calls.
	*	Search in any calls.
text	<i>String</i>	Text to find.

Example

```
(nvox)> call-history filter "12 Aug 2021 00:00:00" "15 Aug 2021 23:59:59" in 1234567
Nvox::CallHistory: Filter enabled.
```

```
(nvox)> no call-history filter
Nvox::CallHistory: Filter disabled.
```

History

Version	Description
3.05	The nvox call-history filter command has been introduced.

C.7 nvox call-history length

Description Set the maximum number of records in the call log. By default, value 500 is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> call-history length <length>
```

```
(nvox)> no call-history length
```

Arguments

Argument	Value	Description
length	<i>Integer</i>	The number of entries in the call log in the range from 2 to 8000.

Example

```
(nvox)> call-history length 400
Nvox::CallHistory: Set history length to 400.
```

```
(nvox)> no call-history length
Nvox::CallHistory: Reset history length to default value (500).
```

History

Version	Description
3.05	The nvox call-history length command has been introduced.

C.8 nvox fxs

Description Access to a group of commands to configure the USB FXS adapter.

Prefix no No

Change settings No

Multiple input No

Group entry (nvox - fxs)

Synopsis

```
(config)> nvox fxs
```

Example

```
(config)> nvox fxs
Core::Configurator: Done.
(nvox-fxs)>
```


History

Version	Description
2.00	The nvox fxs command has been introduced.

C.8.1 nvox fxs country

Description

Set the national FXS settings profile. Tones, ringtone, port impedance, etc. will be configured according to the standards in force in that country.

Command with **no** prefix resets the country code value to what is hardwired into the router.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-fxs)> country <country>
```

```
(nvox-fxs)> no country
```

Arguments

Argument	Value	Description
country	BG	Two-letter country code (ISO 3166-1 alpha-2).
	CA	
	CS	
	DE	
	DK	
	EE	
	ES	
	FI	
	FR	
	GR	
	HR	
	HU	
	IT	
	KZ	
	LT	
	LV	
	NO	
	PL	
	PT	

Argument	Value	Description
	R0	
	RS	
	RU	
	SE	
	SI	
	SK	
	TR	
	UA	

Example

```
(nvox-fxs)> country DE
Nvox::Manager: Set FXS Country for FXS configuration to "DE".
```

```
(nvox-fxs)> no country
Nvox::Manager: Reset FXS Country for FXS configuration to "TR".
```

History

Version	Description
3.05	The nvox fxs country command has been introduced.

C.8.2 nvox fxs echo-canc-mode

Description

Set echo cancellation mode on FXS ports. By default, 2 value is used.

Command with **no** prefix resets the mode to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-fxs)> echo-canc-mode mode
```

```
(nvox-fxs)> no echo-canc-mode
```

Arguments

Argument	Value	Description
mode	0	Echo cancellation is off.
	1	Weak echo cancellation.
	2	Medium echo cancellation.
	3	Maximum echo cancellation.

Example

```
(nvox-fxs)> echo-canc-mode 3
Nvox::Manager: Set FXS Echo cancellation mode to "3".
```

```
(nvox-fxs)> no echo-canc-mode
Nvox::Manager: Reset FXS Echo cancellation mode.
```

History

Version	Description
3.05	The nvox fxs echo-canc-mode command has been introduced.

C.8.3 nvox fxs echo-canc-thresholds

Description

Set the threshold levels of the audio signal to activate echo cancellation. By default, 20 and 15 values is used. The upper threshold must be higher than the lower threshold.

Command with **no** prefix resets settings to default.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(nvox-fxs)> echo-canc-thresholds <mute_threshold> <unmute_threshold>
```

```
(nvox-fxs)> no echo-canc-thresholds
```

Arguments

Argument	Value	Description
mute_threshold	<i>Integer</i>	Upper threshold signal level between 1 and 127.
unmute_threshold	<i>Integer</i>	Lower threshold signal level between 1 and 127.

Example

```
(nvox-fxs)> echo-canc-thresholds 15 10
```

Nvox::Manager: Set FXS Echo cancellation mute threshold to "15" and Echo cancellation unmute threshold to "10".

```
(nvox-fxs)> no echo-canc-thresholds
```

Nvox::Manager: Reset FXS Echo cancellation mute threshold and Echo cancellation unmute threshold.

History

Version	Description
3.05	The nvox fxs echo-canc-thresholds command has been introduced.

C.8.4 nvox fxs force-calibration

Description

Perform LB calibration for FXS ports each time FXS is initialized.

	Command with no prefix disables LB calibration, using factory calibration data.				
Prefix no	Yes				
Change settings	Yes				
Multiple input	No				
Synopsis	<pre>(nvox-fxs)> force-calibration</pre> <pre>(nvox-fxs)> no force-calibration</pre>				
Example	<pre>(nvox-fxs)> force-calibration</pre> Nvox::Manager: Set FXS Force FXS longitudinal balance calibration ► on start to "1". <pre>(nvox-fxs)> no force-calibration</pre> Nvox::Manager: Set FXS Force FXS longitudinal balance calibration ► on start to "0".				
History	<table border="1"> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>3.05</td><td>The nvox fxs force-calibration command has been introduced.</td></tr> </tbody> </table>	Version	Description	3.05	The nvox fxs force-calibration command has been introduced.
Version	Description				
3.05	The nvox fxs force-calibration command has been introduced.				

C.8.5 nvox fxs init-timer

Description	Set FXS initialisation waiting timer in milliseconds. By default, 15000 value is used. Command with no prefix resets setting to default.						
Prefix no	Yes						
Change settings	Yes						
Multiple input	No						
Synopsis	<pre>(nvox-fxs)> init-timer <timer></pre> <pre>(nvox-fxs)> no init-timer</pre>						
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td>timer</td><td><i>Integer</i></td><td>Timer value in milliseconds. Can take values in the range from 1000 to 300000.</td></tr></table>	Argument	Value	Description	timer	<i>Integer</i>	Timer value in milliseconds. Can take values in the range from 1000 to 300000.
Argument	Value	Description					
timer	<i>Integer</i>	Timer value in milliseconds. Can take values in the range from 1000 to 300000.					
Example	<pre>(nvox-fxs)> init-timer 1000</pre> Nvox::Manager: Set FXS Timer to exit on DECT dongle ► initialization failure to "1000".						

```
(nvox-fxs)> no init-timer
Nvox::Manager: Reset FXS Timer to exit on DECT dongle ►
initialization failure.
```

History

Version	Description
3.05	The nvox fxs init-timer command has been introduced.

C.8.6 nvox fxs led-blinking-timer

Description Set the switching period (flashing frequency) of the FXS port status LEDs in talk mode. By default, 15000 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-fxs)> led-blinking-timer <timer>
(nvox-fxs)> no led-blinking-timer
```

Arguments

Argument	Value	Description
timer	<i>Integer</i>	Timer value in milliseconds. Can take values in the range from 0 to 60000.

Example

```
(nvox-fxs)> led-blinking-timer 1000
Nvox::Manager: Set FXS LED blinking period during calls to "1000".
```

```
(nvox-fxs)> no led-blinking-timer
Nvox::Manager: Reset FXS LED blinking period during calls.
```

History

Version	Description
3.05	The nvox fxs led-blinking-timer command has been introduced.

C.8.7 nvox fxs port-paging

Description Enable FXS port paging.

Command with **no** prefix disables the paging.

Prefix no Yes

Change settings No

Multiple input No

Synopsis

```
(nvox-fxs)> port-paging <id>
(nvox-fxs)> no port-paging
```

Arguments

Argument	Value	Description
id	1	FXS port ID.
	2	

Example

```
(nvox-fxs)> port-paging 1
Nvox::Fxs: Start paging FXS port 1.
```

```
(nvox-fxs)> no port-paging
Nvox::Fxs: Stop paging FXS ports.
```

History

Version	Description
3.05	The nvox fxs port-paging command has been introduced.

C.8.8 nvox fxs pulse-dial-mode

Description Set the pulse detection mode on the FXS ports. By default, 1 value is used.
Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-fxs)> pulse-dial-mode <mode>
(nvox-fxs)> no pulse-dial-mode
```

Arguments

Argument	Value	Description
mode	0	Pulse dialing is not detected.
	1	Pulse dialing is not detected during a call.
	2	Pulse dialing is detected all the time.

Example

```
(nvox-fxs)> pulse-dial-mode 2
Nvox::Manager: Set FXS Pulse dialing mode to "2".
```

```
(nvox-fxs)> no pulse-dial-mode
Nvox::Manager: Reset FXS Pulse dialing mode to 1.
```

History	Version	Description
	3.05	The nvox fxs pulse-dial-mode command has been introduced.

C.8.9 nvox fxs unmute-timer

Description Set the timer to delay the sound on the FXS ports in milliseconds after connecting the audio channel during a call. The turn-on delay helps to eliminate noises and other unwanted sounds when answering a call. By default, the 200 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-fxs)> unmute-timer <timer>
(nvox-fxs)> no unmute-timer
```

Arguments	Argument	Value	Description
	timer	<i>Integer</i>	Timer value in milliseconds. Can take values in the range from 0 to 5000.

Example

```
(nvox-fxs)> unmute-timer 300
Nvox::Manager: Set FXS Delay before unmuting the voice channel ►
to "300".
```

```
(nvox-fxs)> no unmute-timer
Nvox::Manager: Reset FXS Delay before unmuting the voice channel.
```

History	Version	Description
	3.05	The nvox fxs unmute-timer command has been introduced.

C.9 nvox parallel accept

Description Set the code to answer a parallel incoming call. Dial this code to answer a call that comes in during a call. By default, the R value is used.

Command with **no** prefix disables the answer to a parallel incoming call function.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> parallel accept <accept>
(nvox)> no parallel accept
```

Argument	Value	Description
accept	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or #. The second and third characters are numbers from 0 to 9 or characters R,* or #.

Example

```
(nvox)> parallel accept **R
Nvox::Manager: Handset info "012345ABCD" created.

(nvox)> no parallel accept
Nvox::Manager: Disabled an action to accept a call.
```

Version	Description
3.05	The nvox parallel accept command has been introduced.

C.10 nvox parallel disable

Description Disable support for parallel calls on the Keenetic telephone station. By default, the parallel calls are enabled.

Command with **no** prefix enables support for parallel calls.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> parallel disable
(nvox)> no parallel disable
```

Example

```
(nvox)> parallel disable
Nvox::Manager: Disabled parallel calls.

(nvox)> no parallel disable
Nvox::Manager: Enabled parallel calls.
```


History

Version	Description
3.05	The nvox parallel disable command has been introduced.

C.11 nvox parallel call-external

Description

Set the code to create a parallel outgoing external call. To call another caller during a call, dial this code, then the caller's number. By default, the R value is used.

Command with **no** prefix disables the parallel outgoing external call function.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox)> parallel call-external <call-external>
```

```
(nvox)> no parallel call-external
```

Arguments

Argument	Value	Description
call-external	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or #. The second and third characters are numbers from 0 to 9 or characters R,*or #.

Example

```
(nvox)> parallel call-external **R
Nvox::Manager: "***R" sequence set to start an external call.
```

```
(nvox)> no parallel call-external
Nvox::Manager: Disabled an action to start an external call.
```

History

Version	Description
3.05	The nvox parallel call-external command has been introduced.

C.12 nvox parallel call-internal

Description

Set the code to create a parallel outgoing internal call. To call another phone port or DECT-handset during a call, dial this code, then the extension number of the port or handset. By default, the * value is used.

Command with **no** prefix disables this feature.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(nvox)> parallel call-internal <call-internal>
```

```
(nvox)> no parallel call-internal
```

Arguments

Argument	Value	Description
call-internal	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or#. The second and third characters are numbers from 0 to 9 or characters R,*or#.

Example

```
(nvox)> parallel call-internal ***
Nvox::Manager: "****" sequence set to start an internal call.
```

```
(nvox)> no parallel call-internal
Nvox::Manager: Disabled an action to start an internal call.
```

History

Version	Description
3.05	The nvox parallel call-internal command has been introduced.

C.13 nvox parallel hold-resume

Description Configure code to put on hold and unholding a call on phone during a conversation. Dial this code during the call to put the caller on hold. To remove the hold and continue the call, dial this code again. By default, the R value is used.

Command with **no** prefix disables this feature.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(nvox)> parallel hold-resume <hold-resume>
```

```
(nvox)> no parallel hold-resume
```

Arguments	Argument	Value	Description
	hold-resume	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or #. The second and third characters are numbers from 0 to 9 or characters R,*or #.

Example

```
(nvox)> parallel hold-resume **R
Nvox::Manager: "**R" sequence set to hold or resume a call.
```

```
(nvox)> no parallel hold-resume
Nvox::Manager: Disabled an action to hold or resume a call.
```

History	Version	Description
	3.05	The nvox parallel hold-resume command has been introduced.

C.14 nvox parallel intercept

Description Configure code to intercept the call. Dial this code, which to transfer the caller from another handset to this handset. When incoming call to the other handset, dial this code to answer the call. By default, the R value is used.

Command with **no** prefix disables this feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> parallel intercept <intercept>
(nvox)> no parallel intercept
```

Arguments	Argument	Value	Description
	intercept	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or #. The second and third characters are numbers from 0 to 9 or characters R,*or #.

Example

```
(nvox)> parallel intercept **R
Nvox::Manager: "**R" sequence set to intercept a call.
```

```
(nvox)> no parallel intercept
Nvox::Manager: Disabled an action to intercept a call.
```

History

Version	Description
3.05	The nvox parallel intercept command has been introduced.

C.15 nvox parallel reject

Description

Configure code to reject an incoming parallel call. Dial this code to reject a call that comes in during a call. By default, the # value is used.

Command with **no** prefix disables this feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox)> parallel intercept <reject>
```

```
(nvox)> no parallel intercept
```

Arguments

Argument	Value	Description
reject	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or #. The second and third characters are numbers from 0 to 9 or characters R,*or #.

Example

```
(nvox)> parallel reject **#
```

```
Nvox::Manager: "***#" sequence set to reject a call.
```

```
(nvox)> no parallel reject
```

```
Nvox::Manager: Disabled an action to reject a call.
```

History

Version	Description
3.05	The nvox parallel reject command has been introduced.

C.16 nvox parallel release-active

Description

Configure code to end of an active parallel call. Dial this code to end an active call and continue the conversation with the caller on hold. By default, the # value is used.

Command with **no** prefix disables this feature.

Prefix no

Yes

Change settings Yes**Multiple input** No

Synopsis

```
(nvox)> parallel release-active <release-active>
```

```
(nvox)> no parallel release-active
```

Arguments

Argument	Value	Description
release-active	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or #. The second and third characters are numbers from 0 to 9 or characters R,*or #.

Example

```
(nvox)> parallel release-active **1
```

Nvox::Manager: "**1" sequence set to release an active call.

```
(nvox)> no parallel release-active
```

Nvox::Manager: Disabled an action to release an active call.

History

Version	Description
3.05	The nvox parallel release-active command has been introduced.

C.17 nvox parallel release-passive

Description Configure code to end of a parallel call on hold. Dial this code to end the connection with the caller on hold and continue the conversation with the current caller. By default, the # value is used.

Command with **no** prefix disables this feature.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(nvox)> parallel release-passive <release-passive>
```

```
(nvox)> no parallel release-passive
```

Arguments

Argument	Value	Description
release-passive	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or #. The second and third characters are numbers from 0 to 9 or characters R,*or #.

Example

```
(nvox)> parallel release-passive **0
Nvox::Manager: "**0" sequence set to release a passive call.
```

```
(nvox)> no parallel release-passive
Nvox::Manager: Disabled an action to release a passive call.
```

History

Version	Description
3.05	The nvox parallel release-passive command has been introduced.

C.18 nvox parallel toggle

Description

Configure code to switch between two parallel calls. Dial this code to continue a call on hold and put the current call on hold. By default, the R value is used.

Command with **no** prefix disables this feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox)> parallel toggle <toggle>
```

```
(nvox)> no parallel toggle
```

Arguments

Argument	Value	Description
toggle	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or#. The second and third characters are numbers from 0 to 9 or characters R,*or#.

Example

```
(nvox)> parallel toggle **5
Nvox::Manager: "**5" sequence set to toggle a call.
```

```
(nvox)> no parallel toggle
Nvox::Manager: Disabled an action to toggle a call.
```

History

Version	Description
3.05	The nvox parallel toggle command has been introduced.

C.19 nvox parallel transfer

Description Configure code to transfer the caller on hold to another caller or phone port/DECT-handset. Dial this code to connect the caller on hold with the caller who is talking to you at the moment. By default, the * value is used.

Command with **no** prefix disables this feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> parallel transfer <transfer>
```

```
(nvox)> no parallel transfer
```

Arguments

Argument	Value	Description
transfer	<i>String</i>	A string from 1 to 3 characters in length. The first character is R,*or#. The second and third characters are numbers from 0 to 9 or characters R,*or#.

Example

```
(nvox)> parallel transfer ***
Nvox::Manager: "***" sequence set to transfer a call.
```

```
(nvox)> no parallel transfer
Nvox::Manager: Disabled an action to transfer a call.
```

History

Version	Description
3.05	The nvox parallel transfer command has been introduced.

C.20 nvox phone

Description Access to a group of commands to configure the FXS ports and DECT handsets.

Prefix no No

Change settings No

Multiple input No

Group entry (nvox-phone)

Synopsis

```
(config)> nvox phone
```

Example

```
(config)> nvox phone
Core::Configurator: Done.
(nvox-phone)>
```

History

Version	Description
3.05	The nvox phone command has been introduced.

C.20.1 nvox phone cadence

Description

Set the parameters for one of the six ringtones, each of which can be linked to a specific type of incoming call (external, internal, paging, call from a particular number). Such a setting will allow you to identify the type of call by the sound of the ringtone.

Default values:

Ringtone N	active1	passive1	active2	passive2	active3	passive3
0	400	500	400	2000	0	0
1	1000	4000	0	0	0	0
2	400	500	0	0	0	0
3	400	2000	1200	1200	0	0
4	400	500	400	2000	2000	2000
5	4000	2000	0	0	0	0

Command with **no** prefix resets settings to default.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(nvox-phone)> cadence <cadence> <active1> <passive1> <active2>
<passive2> <active3> <passive3>
```

```
(nvox-phone)> no cadence [<cadence>]
```

Arguments

Argument	Value	Description
cadence	<i>Integer</i>	Ringtone number in the range from 0 to 5.
active1	<i>Integer</i>	First signal duration in the range from 200 to 5000 ms or 0.
passive1	<i>Integer</i>	Second pause duration in the range from 200 to 5000 ms or 0.
active2	<i>Integer</i>	Second signal duration in the range from 200 to 5000 ms or 0.

Argument	Value	Description
passive2	<i>Integer</i>	First pause duration in the range from 200 to 5000 ms or 0.
active3	<i>Integer</i>	Third signal duration in the range from 200 to 5000 ms or 0.
passive3	<i>Integer</i>	Third pause duration in the range from 200 to 5000 ms or 0.

Example

```
(nvox-phone)> cadence 1 800 320 0 0 0 0
Nvox::Phone: Set phone cadence 1 to 800/320, 0/0, 0/0 ►
(active/passive periods).
```

```
(nvox-phone)> no cadence 1
Nvox::Phone: Reset phone cadence 1 to 1000/4000, 0/0, 0/0 ►
(active/passive periods).
```

History

Version	Description
3.05	The nvox phone cadence command has been introduced.

C.20.2 nvox phone dial-digit-timer

Description

Set the timer in milliseconds to wait for the next digit to be dialed in the dialing mode during an outgoing call. When the timer countdown finishes, the outgoing call is made on the dialed number. By default, 5000 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-phone)> dial-digit-timer <timer>
```

```
(nvox-phone)> no dial-digit-timer
```

Arguments

Argument	Value	Description
timer	<i>Integer</i>	The timer duration is in the range from 100 to 10000 ms.

Example

```
(nvox-phone)> dial-digit-timer 7000
Nvox::Manager: Set dial digit timer.
```

```
(nvox-phone)> no dial-digit-timer
Nvox::Manager: Reset dial digit timer.
```

History

Version	Description
3.05	The nvox phone dial-digit-timer command has been introduced.

C.20.3 nvox phone intercom-cadence

Description

Set a ringtone for internal calls. By default, 0 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-phone)> intercom-cadence <cadence>
```

```
(nvox-phone)> no intercom-cadence
```

Arguments

Argument	Value	Description
cadence	<i>Integer</i>	Ringtone number in the range from 0 to 5.

Example

```
(nvox-phone)> intercom-cadence 4  
Nvox::Phone: Set intercom cadence to 4.
```

```
(nvox-phone)> no intercom-cadence  
Nvox::Phone: Reset intercom cadence to 0.
```

History

Version	Description
3.05	The nvox phone intercom-cadence command has been introduced.

C.20.4 nvox phone offhook-timer

Description

Set the timer in milliseconds to wait for the first digit to be dialed after activating the talk mode for an outgoing call. When the timer countdown is over, the waiting stops and a short beep sounds. By default, 10000 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-phone)> offhook-timer <timer>
```

```
(nvox-phone)> no offhook-timer
```

Arguments

Argument	Value	Description
timer	<i>Integer</i>	The timer duration is in the range from 100 to 10000 ms.

Example

```
(nvox-phone)> offhook-timer 8000  
Nvox::Manager: Set offhook timer.
```

```
(nvox-phone)> no offhook-timer  
Nvox::Manager: Reset offhook timer.
```

History

Version	Description
3.05	The nvox phone offhook-timer command has been introduced.

C.20.5 nvox phone paging-cadence

Description

Set a ringtone for paging. By default, 0 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-phone)> paging-cadence <cadence>
```

```
(nvox-phone)> no paging-cadence
```

Arguments

Argument	Value	Description
cadence	<i>Integer</i>	Ringtone number in the range from 0 to 5.

Example

```
(nvox-phone)> paging-cadence 3  
Nvox::Phone: Set paging cadence to 3.
```

```
(nvox-phone)> no paging-cadence  
Nvox::Phone: Reset paging cadence to 0.
```

History

Version	Description
3.05	The nvox phone paging-cadence command has been introduced.

C.21 nvox phonebook delete

Description Delete all contacts from the phonebook.

Prefix no No

Change settings No

Multiple input No

Synopsis `(nvox)> nvox phonebook delete`

Example `(nvox)> nvox phonebook delete`
Nvox::Manager: All contacts have been deleted from the phonebook.

History

Version	Description
4.02	The nvox phonebook delete command has been introduced.

C.22 nvox phonebook handset-edit

Description Allow DECT handsets to edit the phonebook.
Command with **no** prefix denies editing the phonebook.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis `(nvox)> phonebook handset-edit`

`(nvox)> no phonebook handset-edit`

Example `(nvox)> phonebook handset-edit`
Nvox::Manager: Enabled a DECT handset to edit a phonebook.

`(nvox)> no phonebook handset-edit`
Nvox::Manager: Disabled a DECT handset to edit a phonebook.

History

Version	Description
3.05	The nvox phonebook handset-edit command has been introduced.

C.23 nvox phonebook import

Description

Import contacts in vCard format from a *.vcf file to the phonebook. Each contact must contain the subscriber's first name, last name and up to three phone numbers up to 20 digits long with standard labels - home, work, cell, etc.

You can create a contact group using Google Contacts and/or iCloud Contacts in an Internet browser and then export it in vCard format.

The contacts.vcf file obtained during export is suitable for importing into the phonebook. It should be downloaded to the built-in storage of the Internet Center, then run this command, specifying the path to the /storage/contacts.vcf file and the contacts reading mode.

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(nvox)> phonebook import <filename> <mode>
```

Arguments

Argument	Value	Description
filename	<i>String</i>	Path to the *.vcf file with contacts to import. If the contacts.vcf file is located on the router's built-in storage, you must specify the path /storage/contacts.vcf
mode	replace	All contacts in the phonebook will be deleted and replaced by contacts from the file.
	overwrite	New contacts will be added when the first and last name of a contact in the phonebook matches a contact in the file. The contact numbers in the phonebook are replaced by the contact numbers from the file.
	expand	New contacts will be added when the first and last name of a contact in the phonebook matches a contact in the file. The new numbers of the contact from the file are added to the contact from the phonebook. Note: this addition of numbers occurs if the phonebook contact has less than three numbers.

Argument	Value	Description
	duplicate	Contacts from the file are added to the phonebook even if they match contacts in the phonebook.

Example

```
(nvox)> nvox phonebook import /storage/contacts_google.vcf replace
```

```
(nvox)> nvox phonebook import /storage/contacts_icloud.vcf ►
overwrite
```

History

Version	Description
4.02	The nvox phonebook import command has been introduced.

C.24 nvox phonebook last-name-first

Description

Display the last name first (last name, first name) when viewing the phone book on DECT handsets. By default, the first name is displayed first (first name, last name).

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox)> phonebook last-name-first
```

```
(nvox)> no phonebook last-name-first
```

Example

```
(nvox)> phonebook last-name-first
Nvox::Manager: Show last name first in a DECT phonebook.
```

```
(nvox)> no phonebook last-name-first
Nvox::Manager: Show name first in a DECT phonebook.
```

History

Version	Description
3.05	The nvox phonebook last-name-first command has been introduced.

C.25 nvox phonebook length

Description Set the maximum number of phonebook entries that are supported by DECT handsets connected to the Keenetic Plus DECT base. By default, 500 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> phonebook length <length>
```

```
(nvox)> no phonebook length
```

Arguments

Argument	Value	Description
length	<i>Integer</i>	Number of entries in the range from 2 to 500.

Example

```
(nvox)> phonebook length 100
Nvox::Manager: Set DECT phonebook length to 100.
```

```
(nvox)> no phonebook length
Nvox::Manager: Reset DECT phonebook length to default (500).
```

History

Version	Description
3.05	The nvox phonebook length command has been introduced.

C.26 nvox phonebook match-length

Description Set the length of the caller's number fragment that is used for comparison with the numbers in the phonebook. When a call comes in, the system compares the number fragment with the phonebook numbers and, if it matches, displays the caller's name from the corresponding phonebook entry on the phone display. By default, 7 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> phonebook match-length <length>
```

```
(nvox)> no phonebook match-length
```

Arguments

Argument	Value	Description
length	<i>Integer</i>	Number of digits for comparison in the range from 0 to 20.

Example

```
(nvox)> phonebook match-length 6
Nvox::Manager: Set a DECT phonebook match length to 6.
```

```
(nvox)> no phonebook match-length
Nvox::Manager: Reset a DECT phonebook match length to 7.
```

History

Version	Description
3.05	The nvox phonebook match-length command has been introduced.

C.27 nvox postdial key

Description

Set the postdial key. The part of the number to the right of the postdial key is transmitted to the line after connecting to the number to the left of this key. By default, *** value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox)> postdial key <key>
```

```
(nvox)> no postdial key
```

Arguments

Argument	Value	Description
key	<i>String</i>	A postdial key of 1 to 3 digits in the range from 0 to 9 or R, *, # characters in any combination.

Example

```
(nvox)> postdial key ***#
Nvox::Manager: Set postdial key.
```

```
(nvox)> no postdial key
Nvox::Manager: Reset postdial key.
```


History	Version	Description
	3.05	The nvox postdial key command has been introduced.

C.28 nvox postdial mid-timer

Description Set the duration of pauses between digits transmitted to the line during postdialing. By default, 250 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> postdial mid-timer <timeout>
```

```
(nvox)> no postdial mid-timer
```

Arguments	Argument	Value	Description
	timeout	<i>Integer</i>	Pause duration in the range from 250 to 10000 ms.

Example

```
(nvox)> postdial mid-timer 300
Nvox::Manager: Set postdial mid timer.
```

```
(nvox)> no postdial mid-timer
Nvox::Manager: Reset postdial mid timer.
```

History	Version	Description
	3.05	The nvox postdial mid-timer command has been introduced.

C.29 nvox postdial post-timer

Description Set the sound delay timer after postdialing. By default, 250 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox)> postdial post-timer <timeout>
```

```
(nvox)> no postdial post-timer
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	Delay duration in the range from 250 to 10000 ms.

Example

```
(nvox)> postdial post-timer 500
Nvox::Manager: Set postdial post timer.
```

```
(nvox)> no postdial post-timer
Nvox::Manager: Reset postdial post timer.
```

History

Version	Description
3.05	The nvox postdial post-timer command has been introduced.

C.30 nvox postdial pre-timer

Description

Set the postdialing delay after a connection is established (SIP 200 OK). By default, 6000 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox)> postdial pre-timer <timeout>
```

```
(nvox)> no postdial pre-timer
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	Delay duration in the range from 250 to 10000 ms.

Example

```
(nvox)> postdial pre-timer 8000
Nvox::Manager: Set postdial pre timer.
```

```
(nvox)> no postdial pre-timer
Nvox::Manager: Reset postdial pre timer.
```

History	Version	Description
	3.05	The nvox postdial pre-timer command has been introduced.

C.31 nvox sip

Description Access to a group of commands to configure the selected SIP line. If the line is not found, the command tries to create it. The maximum number of telephone lines supported by the telephone station is 10.

Command with **no** prefix deletes the line.

Prefix no Yes

Change settings No

Multiple input Yes

Group entry (nvox-sip)

Synopsis

```
(nvox)> sip <id>
(nvox)> no sip <id>
```

Arguments	Argument	Value	Description
	id	<i>String</i>	SIP line identifier of Latin letters and numbers from 0 to 9. The maximum string length is 64 characters.

Example

```
(nvox)> sip sipline1
Nvox::Manager: Created SIP line "sipline1".
(nvox-sip)>
```

```
(nvox)> no sip sipline1
Nvox::Manager: Deleted SIP line "sipline1".
```

History	Version	Description
	2.00	The nvox sip command has been introduced.

C.31.1 nvox sip audio-protocol

Description Select the audio transport protocol for the SIP line. By default, RTP value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes**Multiple input** No

Synopsis

```
(nvov-sip)> audio-protocol <protocol>
```

```
(nvov-sip)> no audio-protocol
```

Arguments

Argument	Value	Description
protocol	rtp	RTP protocol.
	srtp	SRTP protocol.
	both	Where possible, SRTP is used, otherwise RTP.

Example

```
(nvov-sip)> audio-protocol srtp
```

Nvox::Manager: Set SIP line sipline1 audio protocol to "srtp".

```
(nvov-sip)> no audio-protocol
```

Nvox::Manager: Reset SIP line sipline1 audio protocol.

History

Version	Description
3.05	The nvov sip audio-protocol command has been introduced.

C.31.2 nvov sip blacklist

Description

Create a blacklist of numbers from which incoming calls are prohibited through this line. By default, blacklist is not configured.

When you receive an incoming call from a subscriber whose number is blacklisted and is not on the whitelist, the phones and handsets do not ring. The caller is notified that the user is busy, and the call information is recorded in the call log and system log.

When checking the number against the blacklist, the system sequentially compares the number with each of the numbers and patterns in the line from left to right until the first match.

When the command is executed, the previously configured blacklist is overwritten with the new list.

Command with **no** prefix removes the blacklist.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(nvox-sip)> blacklist <map>
```

```
(nvox-sip)> no blacklist
```

Arguments

Argument	Value	Description
map	<i>String</i>	A string of up to 600 characters in length. Phone numbers and number patterns are separated from each other by the character. Valid characters: 01234567890*#+ABCDx[] -.>

Example

```
(nvox-sip)> blacklist 1234x  
Nvox::Manager: Set SIP line 1 blacklist to "1234x".
```

```
(nvox-sip)> blacklist +749[589]1234567  
Nvox::Manager: Set SIP line 1 blacklist to "+749[589]1234567".
```

```
(nvox-sip)> blacklist "[1-69]x.|+792[67]x.|000x.|1234567"  
Nvox::Manager: Set SIP line test blacklist to ►  
"[1-69]x.|+792[67]x.|000x.|1234567".
```

```
(nvox-sip)> no blacklist  
Nvox::Manager: Reset SIP line 1 blacklist.
```

History

Version	Description
4.01	The nvox sip blacklist command has been introduced.

C.31.3 nvox sip cadence

Description

Select the ringtone that will sound for incoming calls on this line. By default, the 1 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> cadence <cadence>
```

```
(nvox-sip)> no cadence
```

Arguments

Argument	Value	Description
cadence	<i>Integer</i>	Ringtone number in the range from 0 to 5.

Example

```
(nvox-sip)> cadence 3
Nvox::Manager: Set SIP line 1 Cadence for incoming calls (0 is for internal calls) to "3".
```

```
(nvox-sip)> no cadence
Nvox::Manager: Reset SIP line 1 Cadence for incoming calls (0 is for internal calls).
```

History

Version	Description
3.05	The nvox sip cadence command has been introduced.

C.31.4 nvox sip cadence-rule

Description

Set a rule to select a melody that will sound for incoming calls from specific numbers on this line. You can recognize by the sound of the ringtone who is calling you.

Command with **no** prefix removes the rule.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(nvox-sip)> cadence-rule <rule> <cadence> <digitmap>
```

```
(nvox-sip)> no cadence-rule
```

Arguments

Argument	Value	Description
rule	<i>Integer</i>	Rule number of 0 to 2.
cadence	<i>Integer</i>	Ringtone number of 0 to 5.
digitmap	<i>String</i>	The pattern to which the caller's number must correspond. For more information see Syntax of prefix substitution rules .

Example

```
(nvox-sip)> cadence-rule 0 4 4951234567
Nvox::Sip: Add SIP sipline1 cadence rule 0: cadence 4 for digit map "4951234567".
```

```
(nvox-sip)> no cadence-rule 0
Nvox::Sip: Reset SIP sipline1 cadence rule 0.
```

History

Version	Description
3.05	The nvox sip cadence-rule command has been introduced.

C.31.5 nvox sip codec

Description Allow use of audio codec for calls on this line. When configuring codecs with this command, you should consider:

- 1) Keenetic Linear only supports codecs G.711a and G.711u;
- 2) Codec G.722 only supports DECT-handset with support CAT-iq 1/CAT-iq 2.x (handset Gigaset).

Command with **no** prefix denies the use of this codec or resets configuration.

Prefix no Yes

Change settings Yes

Multiple input Yes

Synopsis

```
(nvox-sip)> codec <codec>
```

```
(nvox-sip)> no codec
```

Arguments

Argument	Value	Description
codec	g711u	Codec G.711u (ULAW, PCMU).
	g711a	Codec G.711a (ALAW, PCMA).
	g726	Codec G.726-32.
	g722	Codec G.722.

Example

```
(nvox-sip)> codec g726
Nvox::Manager: Added g726 to SIP line "sipline1" codecs.
```

```
(nvox-sip)> no codec g726
Nvox::Manager: Removed g726 from SIP line "sipline1" codecs.
```

```
(nvox-sip)> no codec
Nvox::Manager: Reset SIP line "sipline1" codecs.
```

History

Version	Description
3.05	The nvox sip codec command has been introduced.

C.31.6 nvox sip deny-interception

Description Prohibit interception of connections on this line (user 1 is on the phone, user 2 dials a special code, intercepts the call and talks with the interlocutor of the user 1). By default, the connection interception is allowed.

Command with **no** prefix allows the connection interception.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> deny-interception
(nvox-sip)> no deny-interception
```

Example

```
(nvox-sip)> deny-interception
Nvox::Manager: Set SIP line sipline1 deny interception to "1".

(nvox-sip)> no deny-interception
Nvox::Manager: Set SIP line sipline1 deny interception to "0".
```

History

Version	Description
3.05	The nvox sip deny-interception command has been introduced.

C.31.7 nvox sip deny-pickup

Description Prohibit interception of incoming calls on this line (user 1 is on the phone, user 2 dials a special code on his phone/DECT-handset and answers the phone instead of user 1). By default, the incoming calls interception is allowed.

Command with **no** prefix allows the incoming calls interception.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> deny-pickup
(nvox-sip)> no deny-pickup
```

Example

```
(nvox-sip)> deny-pickup
Nvox::Manager: Set SIP line sipline1 deny pickup to "1".

(nvox-sip)> no deny-pickup
Nvox::Manager: Set SIP line sipline1 deny pickup to "0".
```

History

Version	Description
3.05	The nvox sip deny-pickup command has been introduced.

C.31.8 nvox sip digit-map

Description Create dialing rules the number, outgoing calls to which are allowed through this line. If the dialed number doesn't match any of the dialing rules, the outgoing call will be dismiss. If there are no dialing rules, calls to any number are allowed. By default, dialing rules is not configured.

For more information see [Syntax of prefix substitution rules](#).

Command with **no** prefix removes the dialing rules.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> digit-map <map>
(nvox-sip)> no digit-map
```

Argument	Value	Description
map	<i>String</i>	String to 250 characters long. Valid characters: 01234567890*#+ABCDxT[]() >.-

Example

```
(nvox-sip)> digit-map "8[49]xxxxxxxx|10xx|*xx#"
Nvox::Manager: Set SIP line test digit map to ►
"8[49]xxxxxxxx|10xx|*xx#".
```

```
(nvox-sip)> no digit-map
Nvox::Manager: Reset SIP line sipline1 digit map.
```

Version	Description
3.05	The nvox sip digit-map command has been introduced.

C.31.9 nvox sip disable

Description Shutdown the telephone line. If the line is off, outgoing and incoming calls cannot be made through this line.

Command with **no** prefix enables the telephone line.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> disable
```

```
(nvox-sip)> no disable
```

Example

```
(nvox-sip)> deny-pickup
Nvox::Manager: Disabled SIP line "sipline1".
```

```
(nvox-sip)> no deny-pickup
Nvox::Manager: Enabled SIP line "sipline1".
```

History

Version	Description
3.05	The nvox sip disable command has been introduced.

C.31.10 nvox sip disable-extended-keepalive

Description

Disable Extended Keep Alive feature, which sends keepalive packets to all servers resolved from the DNS SRV record. By default, the feature is enabled.

Note: If Extended Keep Alive is disabled, keepalive packets should only be sent to the server where SIP registration is performed.

Command with **no** prefix enables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> disable-extended-keepalive
```

```
(nvox-sip)> no disable-extended-keepalive
```

Example

```
(nvox-sip)> disable-extended-keepalive
Nvox::Manager: Set SIP line test disable extended keepalive to ►
"1".
```

```
(nvox-sip)> no disable-extended-keepalive
Nvox::Manager: Reset SIP line test disable extended keepalive ►
to 0.
```

History

Version	Description
4.01	The nvox sip disable-extended-keepalive command has been introduced.

C.31.11 nvox sip disable-force-registration-retry

Description	Disable sending retry SIP registration requests in situations where registration was rejected or there is no response to the request. By default, the request sending is enabled. Command with no prefix enables retry registration requests.				
Prefix no	Yes				
Change settings	Yes				
Multiple input	No				
Synopsis	<pre>(nvox-sip)> disable-force-registration-retry</pre> <pre>(nvox-sip)> no disable-force-registration-retry</pre>				
Example	<pre>(nvox-sip)> disable-force-registration-retry Nvox::Manager: Set SIP line sipline1 disable force registration ► retry to "1".</pre> <pre>(nvox-sip)> no disable-force-registration-retry Nvox::Manager: Reset SIP line sipline1 disable force registration ► retry.</pre>				
History	<table border="1"> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>3.05</td><td>The nvox sip disable-force-registration-retry command has been introduced.</td></tr> </tbody> </table>	Version	Description	3.05	The nvox sip disable-force-registration-retry command has been introduced.
Version	Description				
3.05	The nvox sip disable-force-registration-retry command has been introduced.				

C.31.12 nvox sip disable-stun

Description	Shutdown the STUN client used to successfully pass SIP messages and RTP audio data through NAT. By default, STUN client is enabled. Command with no prefix enables the STUN client.
Prefix no	Yes
Change settings	Yes
Multiple input	No
Synopsis	<pre>(nvox-sip)> disable-stun</pre> <pre>(nvox-sip)> no disable-stun</pre>
Example	<pre>(nvox-sip)> disable-stun Nvox::Manager: Set SIP line sipline1 disable STUN to "1".</pre>

```
(nvox-sip)> no disable-stun
Nvox::Manager: Reset SIP line sipline1 disable STUN.
```

History

Version	Description
3.05	The nvox sip disable-stun command has been introduced.

C.31.13 nvox sip display-name

Description Specify the name that will be displayed on the phone of the called party during an outgoing call on this line. By default, the name is not specified.

Command with **no** prefix removes the name.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> display-name <name>
(nvox-sip)> no display-name
```

Arguments

Argument	Value	Description
name	<i>String</i>	String of printed symbols of the set ASCII. Maximum string length is 100 characters.

Example

```
(nvox-sip)> display-name office_12
Nvox::Manager: Set SIP line sipline1 display name to "office_12".

(nvox-sip)> no display-name
Nvox::Manager: Reset SIP line sipline1 display name.
```

History

Version	Description
3.05	The nvox sip display-name command has been introduced.

C.31.14 nvox sip dnd

Description Enable DND (Do Not Disturb) mode for this line. When DND is enabled, phones and handsets do not ring on incoming calls, callers are receive a notification that the user is busy and information about missed calls is entered into the call log and system log. By default, the setting is disabled.

Command with **no** prefix disables DND (Do Not Disturb) function.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(nvox-sip)> dnd
(nvox-sip)> no dnd
```

Example

```
(nvox-sip)> dnd
Nvox::Manager: Set SIP line sipline1 Do Not Disturb to "1".

(nvox-sip)> no dnd
Nvox::Manager: Reset SIP line sipline1 Do Not Disturb.
```

History

Version	Description
3.05	The nvox sip dnd command has been introduced.

C.31.15 nvox sip dnd-schedule

Description Assign a schedule work to the DND (Do Not Disturb). Schedule must be created and customized with [schedule action](#) command before execution.

Command with **no** prefix unbinds the schedule.

Prefix no Yes**Change settings** Yes**Multiple input** No

Synopsis

```
(nvox-sip)> dnd-schedule <schedule>
(nvox-sip)> no dnd-schedule
```

Arguments

Argument	Value	Description
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(nvox-sip)> dnd-schedule
Nvox::Sip: SIP line "sipline1" set schedule "schedule0" for dnd.

(nvox-sip)> no dnd-schedule
Nvox::Sip: SIP line "sipline1" delete schedule for dnd.
```

History

Version	Description
3.05	The nvox sip dnd-schedule command has been introduced.

C.31.16 nvox sip domain

Description

Specify the domain name of the IP Telephony operator to which this line is connected.

Command with **no** prefix removes the domain name.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> domain <domain>
```

```
(nvox-sip)> no domain
```

Arguments

Argument	Value	Description
domain	<i>String</i>	The domain name. Maximum domain name length is 100 characters.

Example

```
(nvox-sip)> domain voipprovider
Nvox::Manager: Set SIP line sipline1 domain to "voipprovider".
```

```
(nvox-sip)> no domain
Nvox::Manager: Reset SIP line sipline1 domain.
```

History

Version	Description
3.05	The nvox sip domain command has been introduced.

C.31.17 nvox sip dtmf-flash-signal

Description

Enable FLASH signal transmission (calibrated loop plume) in SIP INFO messages. By default, the feature is disabled.

Command with **no** prefix disables the feature.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> dtmf-flash-signal
```

```
(nvox-sip)> no dtmf-flash-signal
```

Example

```
(nvox-sip)> dtmf-flash-signal
Nvox::Manager: Set SIP line sipline1 DTMF flash signal to "1".
```

```
(nvox-sip)> no dtmf-flash-signal
Nvox::Manager: Reset SIP line sipline1 DTMF flash signal.
```

History

Version	Description
3.05	The nvox sip dtmf-flash-signal command has been introduced.

C.31.18 nvox sip dtmf-mode

Description

Set the DTMF transmission method for this line. By default, method rfc2833 is used.

Command with **no** prefix resets transmission method to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> dtmf-mode <mode>
```

```
(nvox-sip)> no dtmf-mode
```

Arguments

Argument	Value	Description
mode	rfc2833	Transmission of DTMF signals by RTP protocol messages.
	sip-info	Transmission of DTMF signals with SIP INFO requests.
	inband	Transmission of DTMF signals in the media stream along with voice. Can only be used with G.711a and G.711u codecs.

Example

```
(nvox-sip)> dtmf-mode rfc2833
Nvox::Manager: Set SIP line sipline1 DTMF mode to "rfc2833".
```

```
(nvox-sip)> no dtmf-mode
Nvox::Manager: Reset SIP line sipline1 DTMF mode.
```

History

Version	Description
3.05	The nvox sip dtmf-mode command has been introduced.

C.31.19 nvox sip enable-blacklist

Description

Enable blacklist. By default, setting is disabled.

Command with **no** prefix disables the setting.

Note: The **nvox sip blacklist** command is used to create a blacklist.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> enable-blacklist
```

```
(nvox-sip)> no enable-blacklist
```

Example

```
(nvox-sip)> enable-blacklist
Nvox::Manager: Set SIP line 1 Enable blacklist for a line to "1".
```

```
(nvox-sip)> no enable-blacklist
Nvox::Manager: Set SIP line 1 Enable blacklist for a line to "0".
```

History

Version	Description
4.01	The nvox sip enable-blacklist command has been introduced.

C.31.20 nvox sip enable-whitelist

Description

Enable whitelist. By default, setting is disabled.

Command with **no** prefix disables the setting.

Note: The **nvox sip whitelist** command is used to create a whitelist.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> enable-whitelist
(nvox-sip)> no enable-whitelist
```

Example

```
(nvox-sip)> enable-whitelist
Nvox::Manager: Set SIP line 1 Enable whitelist for a line to "1".

(nvox-sip)> no enable-whitelist
Nvox::Manager: Set SIP line 1 Enable whitelist for a line to "0".
```

History	Version	Description
	4.01	The nvox sip enable-whitelist command has been introduced.

C.31.21 nvox sip enable-whitelist-phonebook

Description Enable whitelist from phonebook numbers. By default, setting is disabled.

When you receive an incoming call from a subscriber whose number is listed in the phonebook, the phone rings even if the number is blacklisted. If the whitelist of phonebook numbers is enabled while the blacklist is absent or disabled, only calls from phonebook numbers are allowed.

Command with **no** prefix disables the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> enable-whitelist-phonebook
(nvox-sip)> no enable-whitelist-phonebook
```

Example

```
(nvox-sip)> enable-whitelist-phonebook
Nvox::Manager: Set SIP line test Enable to use phonebook as a ►
whitelist to "1".

(nvox-sip)> no enable-whitelist-phonebook
Nvox::Manager: Set SIP line test Enable to use phonebook as a ►
whitelist to "0".
```

History	Version	Description
	4.02	The nvox sip enable-whitelist-phonebook command has been introduced.

C.31.22 nvox sip forward

Description Enable unconditional forwarding of incoming calls to a specified SIP ID through this line. By default, the feature is disabled.

Command with **no** prefix resets the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> forward <number>
(nvox-sip)> no forward
```

Arguments

Argument	Value	Description
number	<i>String</i>	The caller ID consists of ASCII characters (not more than 100 characters). The call is forwarded to the SIP URL sip:sipid@domain.

Example

```
(nvox-sip)> forward +49301234567
Nvox::Manager: Set SIP line 1 unconditional forward to ►
"+49301234567".
```

```
(nvox-sip)> no forward
Nvox::Manager: Reset SIP line 1 unconditional forward.
```

History

Version	Description
3.05	The nvox sip forward command has been introduced.

C.31.23 nvox sip forward-if-busy

Description Enable forwarding of incoming calls to a specified SIP ID through this line, if the phones/DECT-handsets, which are allowed to make incoming calls from this line at the time of the call are busy.

Command with **no** prefix resets the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> forward-if-busy <{number}>
(nvox-sip)> no forward-if-busy
```

Arguments	Argument	Value	Description
	number	<i>String</i>	The caller ID consists of ASCII characters (not more than 100 characters). The call is forwarded to the SIP URL sip:sipid@domain.

Example

```
(nvox-sip)> forward-if-busy +49301234567
Nvox::Manager: Set SIP line 1 forward if busy to "+49301234567".
```

```
(nvox-sip)> no forward-if-busy
Nvox::Manager: Reset SIP line 1 forward if busy.
```

History	Version	Description
	3.05	The nvox sip forward-if-busy command has been introduced.

C.31.24 nvox sip forward-if-busy-schedule

Description Assign a schedule for the forwarding of incoming calls on busy. Schedule must be created and customized with [schedule action](#) command before execution.

Command with **no** prefix unbinds the schedule.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> forward-if-busy-schedule <schedule>
(nvox-sip)> no forward-if-busy-schedule
```

Arguments	Argument	Value	Description
	schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(nvox-sip)> forward-if-busy-schedule telephony-fwd-busy
Nvox::Sip: SIP line "1" set schedule "telephony-fwd-busy" for ►
forward-if-busy.
```

```
(nvox-sip)> no forward-if-busy-schedule
Nvox::Sip: SIP line "1" delete schedule for forward-if-busy.
```

History	Version	Description
	3.05	The nvox sip forward-if-busy-schedule command has been introduced.

C.31.25 nvox sip forward-if-timeout

Description Enable forwarding of incoming calls to a specified SIP ID through this line, if the phones/DECT-handsets, which are allowed to make incoming calls from this line do not answer within a specified time.

Command with **no** prefix resets the setting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> forward-if-timeout <number> <timeout>
(nvox-sip)> no forward-if-timeout
```

Arguments

Argument	Value	Description
number	<i>String</i>	The caller ID consists of ASCII characters (not more than 100 characters). The call is forwarded to the SIP URL sip:sipid@domain.
timeout	<i>Integer</i>	Response time in the range from 1 to 60 seconds.

Example

```
(nvox-sip)> forward-if-timeout +49301234567 10
Nvox::Manager: Set SIP line 1 forward timeout to "10".
```

```
(nvox-sip)> no forward-if-timeout
Nvox::Manager: Reset SIP line 1 forward timeout.
```

History

Version	Description
3.05	The nvox sip forward-if-timeout command has been introduced.

C.31.26 nvox sip forward-if-timeout-schedule

Description Assign a schedule for the forwarding of incoming calls on timeout. Schedule must be created and customized with **schedule action** command before execution.

Command with **no** prefix unbinds the schedule.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> forward-if-timeout-schedule <schedule>
```

```
(nvox-sip)> no forward-if-timeout-schedule
```

Arguments

Argument	Value	Description
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(nvox-sip)> forward-if-timeout-schedule telephony-fwd-timeout
Nvox::Sip: SIP line "1" set schedule "telephony-fwd-timeout" for ►
forward-if-timeout.
```

```
(nvox-sip)> no forward-if-timeout-schedule
Nvox::Sip: SIP line "1" delete schedule for forward-if-timeout.
```

History

Version	Description
3.05	The nvox sip forward-if-timeout-schedule command has been introduced.

C.31.27 nvox sip forward-schedule

Description

Enable unconditional forwarding by schedule. Schedule must be created and customized with [schedule action](#) command before execution.

Command with **no** prefix unbinds the schedule.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> forward-schedule <schedule>
```

```
(nvox-sip)> no forward-schedule
```

Arguments

Argument	Value	Description
schedule	<i>Schedule</i>	The name of the schedule that was created with schedule group of commands.

Example

```
(nvox-sip)> forward-schedule telephony-fwd
Nvox::Sip: SIP line "1" set schedule "telephony-fwd" for forward.
```

```
(nvox-sip)> no forward-schedule
Nvox::Sip: SIP line "1" delete schedule for forward.
```

History

Version	Description
3.05	The nvox sip forward-schedule command has been introduced.

C.31.28 nvox sip identity

Description

Set the SIP user ID for this line received from your IP telephony provider.

Command with **no** prefix removes SIP ID.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> identity <identity>
```

```
(nvox-sip)> no identity
```

Arguments

Argument	Value	Description
identity	<i>String</i>	The caller ID consists of ASCII characters (not more than 100 characters).

Example

```
(nvox-sip)> identity sipuser1001  
Nvox::Manager: Set SIP line 1 identity to "sipuser1001".
```

```
(nvox-sip)> no identity  
Nvox::Manager: Reset SIP line 1 identity.
```

History

Version	Description
3.05	The nvox sip identity command has been introduced.

C.31.29 nvox sip incoming-mask

Description

Allow a telephone (Keenetic Linear) or DECT handset with a given ID to receive incoming calls on this line. By default, all phones and handsets are not allowed to receive incoming calls through this line.

Command with **no** prefix denies incoming calls for this handset.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(nvox-sip)> incoming-mask <ipui>
```

```
(nvox-sip)> no incoming-mask <ipui>
```

Arguments

Argument	Value	Description
ipui	1	Keenetic Linear Adapter Port 1 ID.
	2	Keenetic Linear Adapter Port 2 ID.
	<i>String</i>	Ten-digit DECT handset identifier (IPUI). Consists of 10 characters A, B, C, D, E, F and digits from 0 to 9.

Example

```
(nvox-sip)> incoming-mask 01234ABCDE  
Nvox::Manager: Added phone 01234ABCDE to SIP "1" incoming-mask.
```

```
(nvox-sip)> no incoming-mask 01234ABCDE  
Nvox::Manager: Removed phone 01234ABCDE from SIP "1" ►  
incoming-mask.
```

History

Version	Description
3.05	The nvox sip incoming-mask command has been introduced.

C.31.30 nvox sip keepalive

Description

Set a timeout for sending keepalive messages to the SIP proxy server signal port to keep the server connection open through NAT. By default, 15 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> keepalive <keepalive>
```

```
(nvox-sip)> no keepalive
```

Arguments

Argument	Value	Description
keepalive	<i>Integer</i>	Keepalive timeout in the range from 10 to 3600 seconds. 0 value disables the sending of keepalive messages.

Example

```
(nvox-sip)> keepalive 50  
Nvox::Manager: Set SIP line 1 keepalive to "50".
```

```
(nvox-sip)> no keepalive  
Nvox::Manager: Reset SIP line 1 keepalive.
```

```
(nvox-sip)> keepalive 0  
Nvox::Manager: Set SIP line 1 keepalive to "0".
```

History

Version	Description
3.05	The nvox sip keepalive command has been introduced.

C.31.31 nvox sip lock-codec

Description

Force a single codec for the connection by requesting re-INVITE when the remote party chooses multiple codecs.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> lock-codec
```

```
(nvox-sip)> no lock-codec
```

Example

```
(nvox-sip)> lock-codec  
Nvox::Manager: Set SIP line 3 lock SIP audio codec to "1".
```

```
(nvox-sip)> no lock-codec  
Nvox::Manager: Set SIP line 3 lock SIP audio codec to "0".
```

History

Version	Description
3.05	The nvox sip lock-codec command has been introduced.

C.31.32 nvox sip login

Description

Set SIP Auth ID — the name used for authentication on the IP-telephony provider's servers. By default, SIP Auth ID is not configured.

Command with **no** prefix removes the SIP Auth ID from the line parameters.

Prefix no

Yes

Change settings

Yes

Multiple input No

Synopsis

```
(nvox-sip)> login <login>
(nvox-sip)> no login
```

Argument	Value	Description
login	<i>String</i>	A string of ASCII characters. The maximum length of the string is 64 characters.

Example

```
(nvox-sip)> login user1001
Nvox::Manager: Set SIP line 1 login to "user1001".

(nvox-sip)> no login
Nvox::Manager: Reset SIP line 1 login.
```

Version	Description
3.05	The nvox sip login command has been introduced.

C.31.33 nvox sip name

Description Set the line name, which is displayed in the call log and system log. By default, the line name is not configured.

Command with **no** prefix removes the line name from the line parameters.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> name <name>
(nvox-sip)> no name
```

Argument	Value	Description
name	<i>String</i>	A string of ASCII characters. The maximum length of the string is 100 characters.

Example

```
(nvox-sip)> name line-1001
Nvox::Manager: Set SIP line 3 line name to "line-1001".

(nvox-sip)> no name
Nvox::Manager: Reset SIP line 3 line name.
```

History

Version	Description
3.05	The nvox sip name command has been introduced.

C.31.34 nvox sip outgoing-mask

Description

Allow a telephone (Keenetic Linear) or DECT handset with a given ID to perform outgoing calls via this line. By default, for all phones and handsets outgoing calls are denied via this line.

Command with **no** prefix denies outgoing calls for this handset.

Prefix no

Yes

Change settings

Yes

Multiple input

Yes

Synopsis

```
(nvox-sip)> outgoing-mask <ipui>
```

```
(nvox-sip)> no outgoing-mask <ipui>
```

Arguments

Argument	Value	Description
ipui	1	Keenetic Linear Adapter Port 1 ID.
	2	Keenetic Linear Adapter Port 2 ID.
	<i>String</i>	Ten-digit DECT handset identifier (IPUI). Consists of 10 characters A, B, C, D, E, F and digits from 0 to 9.

Example

```
(nvox-sip)> outgoing-mask 1  
Nvox::Manager: Added phone 1 to SIP "1" outgoing-mask.
```

```
(nvox-sip)> outgoing-mask 034725D054  
Nvox::Manager: Added phone 034725D054 to SIP "1" outgoing-mask.
```

```
(nvox-sip)> no outgoing-mask 2  
Nvox::Manager: Removed phone 2 from SIP "1" outgoing-mask.
```

History

Version	Description
3.05	The nvox sip outgoing-mask command has been introduced.

C.31.35 nvox sip password

Description

Set the password used for authentication on the IP-telephony provider's servers. By default, the password is not configured.

Command with **no** prefix removes the password from the line parameters.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> password <password>
(nvox-sip)> no password
```

Arguments

Argument	Value	Description
password	<i>String</i>	A string of ASCII characters. The maximum length of the string is 64 characters.

Example

```
(nvox-sip)> password 1234567
Nvox::Manager: Set SIP line 1 password.
```

```
(nvox-sip)> no password
Nvox::Manager: Reset SIP line 1 password.
```

History

Version	Description
3.05	The nvox sip password command has been introduced.

C.31.36 nvox sip priority

Description Set the priority for this line. Line priorities are taken into account when selecting a line for an outgoing call: the system selects the line with the highest priority of those that are allowed for the phone or handset and have dialing rules that correspond to the dialed number.

Command with **no** prefix sets priority to 1 for this line, rearranging the priorities of the other lines accordingly if necessary.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> priority <priority>
(nvox-sip)> no priority
```

Arguments

Argument	Value	Description
priority	<i>Integer</i>	The priority number in the range from 0 to 9, where 0 is the lowest priority; 9 — highest priority.

Example

```
(nvox-sip)> priority 7
Nvox::Manager: Set SIP line 1 priority to "7".
```

```
(nvox-sip)> no priority
Nvox::Manager: Reset SIP line 1 priority.
```

History

Version	Description
3.05	The nvox sip priority command has been introduced.

C.31.37 nvox sip proxy

Description

Set the domain name or IP address of the IP telephony operator's SIP proxy for this line. By default, the SIP proxy is not configured.

Command with **no** prefix removes the SIP proxy from the line parameters.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> proxy <proxy>
```

```
(nvox-sip)> no proxy
```

Arguments

Argument	Value	Description
proxy	<i>String</i>	Domain name or IP address. If the SIP proxy uses a non-standard port (other than 5060), it must be specified to the right of the domain name/IP address with a colon.

Example

```
(nvox-sip)> proxy sip.proxy.local:5090
Nvox::Manager: Set SIP line 1 proxy URI to "sip.proxy.local:5090".
```

```
(nvox-sip)> no proxy
Nvox::Manager: Reset SIP line 1 proxy URI.
```

History

Version	Description
3.05	The nvox sip proxy command has been introduced.

C.31.38 nvox sip reg-timeout

Description Set the SIP registration validity period on the IP-telephony operator's server, after which the registration should be resumed. This parameter can be changed during the registration process by the server. By default, 180 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> reg-timeout <timeout>
(nvox-sip)> no reg-timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	SIP registration validity period in the range from 10 to 3600 seconds.

Example

```
(nvox-sip)> reg-timeout 1800
Nvox::Manager: Set SIP line 1 registration timeout to "1800".
```

```
(nvox-sip)> no reg-timeout
Nvox::Manager: Reset SIP line 1 registration timeout.
```

History

Version	Description
3.05	The nvox sip reg-timeout command has been introduced.

C.31.39 nvox sip registration-first-retry

Description Set the first SIP registration retry timeout. Registration attempts are repeated if the IP telephony operator's SIP server does not respond to SIP registration requests. By default, 120 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> registration-first-retry <timeout>
```

```
(nvox-sip)> no registration-first-retry
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	First SIP registration repeat timeout in the range from 0 to 1800 seconds.

Example

```
(nvox-sip)> registration-first-retry 180
Nvox::Manager: Set SIP line 1 registration first retry to "180".
```

```
(nvox-sip)> no registration-first-retry
Nvox::Manager: Reset SIP line 1 registration first retry.
```

History

Version	Description
3.05	The nvox sip registration-first-retry command has been introduced.

C.31.40 nvox sip registration-retry

Description

Set the SIP registration retry timeout. Registration attempts are repeated if the IP telephony operator's server does not respond to SIP registration requests. By default, 120 value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> registration-retry <timeout>
```

```
(nvox-sip)> no registration-retry
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	SIP registration repeat timeout in the range from 0 to 1800 seconds.

Example

```
(nvox-sip)> registration-retry 180
Nvox::Manager: Set SIP line 1 registration retry to "180".
```

```
(nvox-sip)> no registration-retry
Nvox::Manager: Reset SIP line 1 registration retry.
```

History	Version	Description
	3.05	The nvox sip registration-retry command has been introduced.

C.31.41 nvox sip registration-uri

Description Set the domain name or IP address of the SIP registration server of the IP telephony operator for this line. By default, the registration server is not set.

Command with **no** prefix removes the registration server from parameters.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> registration-uri <uri>
(nvox-sip)> no registration-uri
```

Arguments	Argument	Value	Description
	uri	<i>String</i>	Domain name or IP address. If the SIP proxy uses a non-standard port (other than 5060), it must be specified to the right of the domain name/IP address with a colon.

Example

```
(nvox-sip)> registration-uri sip.registrar.local:5090
Nvox::Manager: Set SIP line 1 registration URI to ►
"sip.registrar.local:5090".
```

```
(nvox-sip)> no registration-uri
Nvox::Manager: Reset SIP line 1 registration URI.
```

History	Version	Description
	3.05	The nvox sip registration-uri command has been introduced.

C.31.42 nvox sip sdp-nat-rewrite

Description Enable receiving your IP address (or NAT IP address) from the registration server and overwriting by it the appropriate fields in the Via, Contact headers, as well as in SIP/SDP in all further outgoing SIP messages. This ensures the successful exchange of SIP signaling messages and two-way audibility. Use this option when a secondary channel, such as a VPN tunnel, is used to communicate with the server, or when there is a symmetric NAT between

the Keenetic device and the operator's public server that STUN technology does not work with. By default, the feature is disabled.

Command with **no** prefix disables IP address rewriting.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> sdp-nat-rewrite
(nvox-sip)> no sdp-nat-rewrite
```

Example

```
(nvox-sip)> sdp-nat-rewrite
Nvox::Manager: Set SIP line 1 SDP NAT, Contact and Via rewrite ►
to "1".

(nvox-sip)> no sdp-nat-rewrite
Nvox::Manager: Reset SIP line 1 SDP NAT, Contact and Via rewrite.
```

History

Version	Description
3.05	The nvox sip sdp-nat-rewrite command has been introduced.

C.31.43 nvox sip selection-id

Description Set the line selection code 0...9, which allows you to select this line for an outgoing call. To select a line, dial #, the line selection code and the subscriber number. When you select a line with a dialing code, the dialing rules are ignored and you can call a number that does not match the dialing rules of that line. With the code you can select only the lines, outgoing calls through which are allowed for this phone or DECT handset. The default selection code is not configured.

Command with **no** prefix removes the selection code from the line settings.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> selection-id <sel-id>
(nvox-sip)> no selection-id
```

Arguments

Argument	Value	Description
sel-id	<i>Integer</i>	Line selection code in the range from 0 to 9.

Example

```
(nvox-sip)> selection-id 9
Nvox::Manager: Set SIP line 1 selection id to "9".
```

```
(nvox-sip)> no selection-id
Nvox::Manager: Reset SIP line 1 selection id.
```

History	Version	Description
	3.05	The nvox sip selection-id command has been introduced.

C.31.44 nvox sip session-timer

Description Set the SIP session timer for this line. By default, the 120 value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> session-timer <timer>
```

```
(nvox-sip)> no session-timer
```

Arguments	Argument	Value	Description
	timer	<i>Integer</i>	Timer value in the range from 90 to 86400 seconds.

Example

```
(nvox-sip)> session-timer 180
Nvox::Manager: Set SIP line 1 session timer to "180".
```

```
(nvox-sip)> no session-timer
Nvox::Manager: Reset SIP line 1 session timer.
```

History	Version	Description
	3.05	The nvox sip session-timer command has been introduced.

C.31.45 nvox sip session-timer-mode

Description Set the SIP-session timer mode for this line. By default, the optional value is used.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> session-timer-mode <mode>
```

```
(nvox-sip)> no session-timer-mode
```

Arguments

Argument	Value	Description
mode	disable	The session timer is not used, except when required by the remote party.
	optional	The session timer is used if the remote party supports and uses it.
	required	Session timer support is a requirement for the remote party to establish a connection.
	always	Session timer is used in every connection, regardless of whether the remote party supports it or not.

Example

```
(nvox-sip)> session-timer-mode always
Nvox::Manager: Set SIP line 1 session timer mode to "always".
```

```
(nvox-sip)> no session-timer-mode
Nvox::Manager: Reset SIP line 1 session timer mode.
```

History

Version	Description
3.05	The nvox sip session-timer-mode command has been introduced.

C.31.46 nvox sip substitute

Description

Set up a prefix substitution rule to delete some digits or a group of digits in the caller's number that appears on the handset display when a call comes in. The symbol > is used for substitution. To the left of the > must be a sequence of numbers, which should be replaced by the sequence to the right of this symbol. The substitution expression must be enclosed in parentheses. In a substitution rule there can be several substitution expressions. By default, the prefix substitution rule is not configured. Numbers that do not comply with the prefix substitution rule are displayed on the phone screen unchanged.

For more information see [Syntax of prefix substitution rules](#).

Command with **no** prefix removes the prefix substitution rule.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip)> substitute <substitute>
```

```
(nvox-sip)> no substitute
```

Arguments

Argument	Value	Description
substitute	<i>String</i>	A string up to 100 characters long. Valid characters: 01234567890*#+ABCDx[]() >.-.

Example

```
(nvox-sip)> substitute "(+39>)x.|(+>00)x."
Nvox::Manager: Set SIP line test substitute to ►
"(+39>)x.|(+>00)x."
```

```
(nvox-sip)> no substitute
Nvox::Manager: Reset SIP line 1 substitute.
```

History

Version	Description
3.05	The nvox sip substitute command has been introduced.

C.31.47 nvox sip tls-security-mode

Description

Set the security mode when using the TLS transport protocol. By default, the sip-tls value is used.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> tls-security-mode <mode>
```

```
(nvox-sip)> no tls-security-mode
```

Arguments

Argument	Value	Description
mode	sip-tls	The SIP URI scheme is used. During a call, the TLS transport is only used to transmit SIP signaling between the Keenetic router and your IP telephony provider's proxy server.
	sips	The SIPS URI scheme is used. It is designed to ensure that during a phone call, secure transport protocols are used to send SIP signaling all the way between the Keenetic router and the remote caller.

Example

```
(nvox-sip)> tls-security-mode sips
Nvox::Manager: Set SIP line 1 TLS security mode to "sips".
```

```
(nvox-sip)> no tls-security-mode
Nvox::Manager: Reset SIP line 1 TLS security mode to sip-tls.
```

History

Version	Description
3.05	The nvox sip tls-security-mode command has been introduced.

C.31.48 nvox sip transport

Description

Set the transport protocol used to transmit SIP signaling messages. By default, the udp value is used.

Note: If communication is only possible over IPv4, the UDP over IPv4 transport will be used, even if UDP over IPv6 was selected.

Command with **no** prefix resets setting to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> transport <transport>
```

```
(nvox-sip)> no transport
```

Arguments

Argument	Value	Description
transport	udp	The UDP transport protocol over IPv4 is the most commonly used transport. It is supported by most SIP servers and subscriber devices.
	udp6	The UDP transport protocol over IPv6.
	tcp	Transport protocol TCP over IPv4. It guarantees the delivery of messages, including long messages that cannot be transmitted by the UDP transport without fragmentation.
	tcp6	Transport protocol TCP over IPv6.
	tls	TLS transport protocol over IPv4. It ensures secure exchange of SIP signaling messages with the operator's proxy server. Helps prevent theft of credentials and other important information transmitted in SIP signaling messages.
	tls6	TLS transport protocol over IPv6.

Example

```
(nvox-sip)> transport tls
Nvox::Manager: Set SIP line 1 transport to "tls".
```

```
(nvox-sip)> transport udp6
Nvox::Manager: Set SIP line 1 transport to "udp6".
```

```
(nvox-sip)> no transport
Nvox::Manager: Reset SIP line 1 transport to udp.
```

History

Version	Description
3.05	The nvox sip transport command has been introduced.
4.00	The udp6, tcp6, tls6 arguments were added.

C.31.49 nvox sip whitelist

Description

Create a whitelist list of numbers from which incoming calls are allowed through this line. By default, whitelist is not configured.

When you receive an incoming call from a subscriber whose number is in the whitelist, the phone rings even if this number corresponds to the blacklist. If the whitelist is created and enabled, while the blacklist is absent or disabled, only calls from numbers in the whitelist are allowed.

When checking the number against the whitelist, the system sequentially compares the number with each of the numbers and patterns in the line from left to right until the first match.

When the command is executed, the previously configured whitelist is overwritten with the new list.

Command with **no** prefix removes the whitelist.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip)> whitelist <map>
```

```
(nvox-sip)> no whitelist
```

Arguments

Argument	Value	Description
map	<i>String</i>	A string of up to 600 characters in length. Phone numbers and number patterns are separated from each other by the character. Valid characters: 01234567890*#+ABCDx[] .->

Example

```
(nvox-sip)> whitelist 1234x
Nvox::Manager: Set SIP line 1 whitelist to "1234x".

(nvox-sip)> whitelist +749[589]1234567
Nvox::Manager: Set SIP line 1 whitelist to "+749[589]1234567".

(nvox-sip)> whitelist "1234567890|+79261234567|000123456|1234567"
Nvox::Manager: Set SIP line test whitelist to ►
"1234567890|+79261234567|000123456|1234567".

(nvox-sip)> no whitelist
Nvox::Manager: Reset SIP line 1 whitelist.
```

History

Version	Description
4.01	The nvox sip whitelist command has been introduced.

C.32 nvox sip-common

Description Access to a group of commands to configure the SIP common settings.

Prefix no No

Change settings No

Multiple input No

Group entry (nvox-sip-common)

Synopsis (nvox)> **sip-common**

Example (nvox)> **sip-common**
Core::Configurator: Done.
(nvox-sip-common)>

History

Version	Description
2.00	The nvox sip-common command has been introduced.

C.32.1 nvox sip-common 100rel

Description Enable support of 100rel for reliable SIP Class 100 messaging on incoming and outgoing calls. By default, 100rel is enabled.

Command with **no** prefix disables 100rel support.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> 100rel
(nvox-sip-common)> no 100rel
```

Example

```
(nvox-sip-common)> 100rel
Nvox::Manager: Set SIP enable 100rel/PRACK SIP extension to "1".

(nvox-sip-common)> no 100rel
Nvox::Manager: Set SIP enable 100rel/PRACK SIP extension to "0".
```

History	Version	Description
	3.05	The nvox sip-common 100rel command has been introduced.

C.32.2 nvox sip-common agent

Description Configure the User Agent name. By default, the name is used of the router's model, for example "Keenetic Giga (KN-1011)".

Command with **no** prefix removes the User Agent name configured by the user.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> agent <agent>
(nvox-sip-common)> no agent
```

Arguments	Argument	Value	Description
	agent	<i>String</i>	String of printed symbols of the set ASCII. Maximum string length is 100 characters.

Example

```
(nvox-sip-common)> agent Keenetic
Nvox::Manager: Set SIP user agent to "Keenetic".
```

```
(nvox-sip-common)> no agent
Nvox::Manager: Reset SIP user agent.
```

History	Version	Description
	3.05	The nvox sip-common agent command has been introduced.

C.32.3 nvox sip-common disable-dns-srv

Description Disable the DNS SRV resolving feature. With this feature, the system gets the IP address and signal port of the SIP proxy server from the DNS SRV record. By default, the feature is enabled.

Note: If the DNS SRV resolving function is disabled, the system gets the IP address of the SIP proxy server from entry A, and gets its signal port from the SIP line settings.

Command with **no** prefix enables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> disable-dns-srv
(nvox-sip-common)> no disable-dns-srv
```

Example

```
(nvox-sip-common)> disable-dns-srv
Nvox::Manager: Set SIP disable DNS SRV to "1".
```

```
(nvox-sip-common)> no disable-dns-srv
Nvox::Manager: Reset SIP disable DNS SRV.
```

History

Version	Description
3.05	The nvox sip-common disable-dns-srv command has been introduced.

C.32.4 nvox sip-common disable-tls-validation

Description Disable the SIP proxy validation when using SIP TLS transport. By default, the SIP proxy validation is enabled.

Validation is performed when a TLS connection is established with a SIP proxy server. A proxy server is considered valid if the following conditions are met:

1) The x.509 certificate of the proxy server is signed by one of the trusted certificate authorities whose root certificates are in the certificate store of the Keenetic device.

2) The SIP proxy server domain name in the SIP telephone line settings must match the "commonName" field in the SIP proxy certificate.

Keenetic establishes a TLS connection if the validation is successful and starts exchanging SIP messages with the SIP proxy server. Keenetic terminates the TLS connection if a validation error occurs, and displays "503 SSL certificate validation error" in the system log.

Command with **no** prefix enables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> disable-tls-validation
(nvox-sip-common)> no disable-tls-validation
```

Example

```
(nvox-sip-common)> disable-tls-validation
Nvox::Manager: Set SIP disable proxy verification to "1".

(nvox-sip-common)> no disable-tls-validation
Nvox::Manager: Set SIP disable proxy verification to "0"
```

History

Version	Description
3.09	The nvox sip-common disable-tls-validation command has been introduced.

C.32.5 nvox sip-common g726-dynamic-payload

Description Configure the dynamic payload type for the G.726 codec. By default, 109 value is used.

Note: G.726 codec is not supported with Keenetic Linear.

Command with **no** prefix resets the dynamic payload to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> g726-dynamic-payload <payload>
(nvox-sip-common)> no g726-dynamic-payload
```

Arguments

Argument	Value	Description
payload	<i>Integer</i>	Dynamic payload type ranging from 96 to 127.

Example

```
(nvox-sip-common)> g726-dynamic-payload 98
Nvox::Manager: Set SIP G726 dynamic payload to "98".

(nvox-sip-common)> no g726-dynamic-payload
Nvox::Manager: Reset SIP G726 dynamic payload.
```

History

Version	Description
3.05	The nvox sip-common g726-dynamic-payload command has been introduced.

C.32.6 nvox sip-common outbound-proxy

Description

Configure the domain name or IP address of the outgoing SIP proxy server for all SIP telephone lines configured in the system. By default, the proxy server is not configured.

Note: If the outgoing proxy uses a non-standard port (other than 5060), it must be specified to the right of the domain name/IP address with a colon.

Command with **no** prefix deletes the outgoing SIP proxy server.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip-common)> outbound-proxy <proxy>
```

```
(nvox-sip-common)> no outbound-proxy
```

Arguments

Argument	Value	Description
proxy	<i>String</i>	Domain name or IP address.

Example

```
(nvox-sip-common)> outbound-proxy sip.proxy.local:5090  
Nvox::Manager: Set SIP outbound proxy to "sip.proxy.local:5090".
```

```
(nvox-sip-common)> no outbound-proxy  
Nvox::Manager: Reset SIP outbound proxy.
```

History

Version	Description
3.05	The nvox sip-common outbound-proxy command has been introduced.

C.32.7 nvox sip-common qos

Description

Access to a group of commands to configure the QoS. These settings apply to all SIP lines in the system.

Prefix no

No

Change settings

No

Multiple input	No				
Group entry	(sip-common-qos)				
Synopsis	(nvox-sip)> qos				
Example	<pre>(nvox-sip)> qos Core::Configurator: Done. (sip-common-qos)></pre>				
History	<table border="1"> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>3.05</td><td>The nvox sip qos command has been introduced.</td></tr> </tbody> </table>	Version	Description	3.05	The nvox sip qos command has been introduced.
Version	Description				
3.05	The nvox sip qos command has been introduced.				

C.32.7.1 nvox sip-common qos rtp-dscp

Description	Set the priority in the IP header DS field of outgoing packets with audio data transmitted over RTP. The upstream network equipment can read the DS field and prioritize packets according to the priority specified in this field. The default setting is lowest priority. Command with no prefix sets lowest priority (0) to DS.								
Prefix no	Yes								
Change settings	Yes								
Multiple input	No								
Synopsis	<pre>(sip-common-qos)> rtp-dscp <dscp></pre> <pre>(sip-common-qos)> no rtp-dscp</pre>								
Arguments	<table><tr><th>Argument</th><th>Value</th><th>Description</th></tr><tr><td>dscp</td><td><i>Integer</i></td><td>The priority number in the range from 0 to 63.</td></tr></table>			Argument	Value	Description	dscp	<i>Integer</i>	The priority number in the range from 0 to 63.
Argument	Value	Description							
dscp	<i>Integer</i>	The priority number in the range from 0 to 63.							
Example	<pre>(sip-common-qos)> rtp-dscp 46</pre> Nvox::Manager: Set SIP Default RTP ToS/DSCP (Type of Service) ► to "46". <pre>(sip-common-qos)> no rtp-dscp</pre> Nvox::Manager: Reset SIP Default RTP ToS/DSCP (Type of Service).								
History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>3.05</td><td>The nvox sip-common qos rtp-dscp command has been introduced.</td></tr></table>			Version	Description	3.05	The nvox sip-common qos rtp-dscp command has been introduced.		
Version	Description								
3.05	The nvox sip-common qos rtp-dscp command has been introduced.								

C.32.7.2 nvox sip-common qos rtp-so-prio

Description Set the priority in the 3-bit PCP field of the IEEE 802.1Q header of outgoing packets with audio data transmitted via RTP over VLAN. The upstream network equipment can read the PCP field and prioritize packets according to the priority specified in this field. The default setting is lowest priority.

Command with **no** prefix sets 0 priority to PCP.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(sip-common-qos)> rtp-so-prio <so_prio>
(sip-common-qos)> no rtp-so-prio
```

Arguments

Argument	Value	Description
so_prio	<i>Integer</i>	The priority number in the range from 0 to 7, where 0 is the lowest priority; 7 — highest priority.

Example

```
(sip-common-qos)> rtp-so-prio 7
Nvox::Manager: Set SIP Default RTP CoS (Class of Service) to "7".
```

```
(sip-common-qos)> no rtp-so-prio
Nvox::Manager: Reset SIP Default RTP CoS (Class of Service).
```

History

Version	Description
3.05	The nvox sip-common qos rtp-so-prio command has been introduced.

C.32.7.3 nvox sip-common qos sip-dscp

Description Set the priority in the DS field of the IP header packets with outgoing messages transmitted via the SIP protocol. The upstream network equipment can read the DS field and prioritize packets according to the priority specified in this field. The default setting is lowest priority.

Command with **no** prefix sets lowest priority (0) to DS.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(sip-common-qos)> sip-dscp <dscp>
```

```
(sip-common-qos)> no sip-dscp
```

Arguments

Argument	Value	Description
dscp	<i>Integer</i>	The priority number in the range from 0 to 63.

Example

```
(sip-common-qos)> sip-dscp 24  
Nvox::Manager: Set SIP Default SIP ToS/DSCP (Type of Service) ►  
to "24".
```

```
(sip-common-qos)> no sip-dscp  
Nvox::Manager: Reset SIP Default SIP ToS/DSCP (Type of Service).
```

History

Version	Description
3.05	The nvox sip-common qos sip-dscp command has been introduced.

C.32.7.4 nvox sip-common qos sip-so-prio**Description**

Set the priority in the 3-bit PCP field of the IEEE 802.1Q header of outgoing packets with audio data transmitted via SIP over VLAN. The upstream network equipment can read the PCP field and prioritize packets according to the priority specified in this field. The default setting is lowest priority.

Command with **no** prefix sets 0 priority to PCP.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(sip-common-qos)> sip-so-prio <so_prio>
```

```
(sip-common-qos)> no sip-so-prio
```

Arguments

Argument	Value	Description
so_prio	<i>Integer</i>	The priority number in the range from 0 to 7, where 0 is the lowest priority; 7 — highest priority.

Example

```
(sip-common-qos)> sip-so-prio 7  
Nvox::Manager: Set SIP Default SIP CoS (Class of Service) to "7".
```

```
(sip-common-qos)> no sip-so-prio
Nvox::Manager: Reset SIP Default SIP CoS (Class of Service).
```

History

Version	Description
3.05	The nvox sip-common qos sip-so-prio command has been introduced.

C.32.8 nvox sip-common rtp-port

Description Configure the range of UDP ports that the system uses to exchange RTP audio data during a telephone connection. By default, the range of UDP ports is from 4000 to 4015.

Command with **no** prefix resets the range of UDP ports by default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> rtp-port <port> through <end-port>
(nvox-sip-common)> no rtp-port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	The first port of the range. Valid values are from 1 to 65534.
end-port	<i>Integer</i>	The last port of the range. Valid values are from 1 to 65534.

Example

```
(nvox-sip-common)> rtp-port 10000 through 10200
Nvox::Manager: Set RTP port range from 10000 to 10200.
```

```
(nvox-sip-common)> no rtp-port
Nvox::Manager: Reset SIP RTP port range to default, the transport ►
will be bound to any available port.
```

History

Version	Description
3.05	The nvox sip-common rtp-port command has been introduced.

C.32.9 nvox sip-common sdp rtcp

Description Enable RTCP parameter negotiation in SDP. By default, function is disabled.

Command with **no** prefix disables the feature.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> sdp rtcp
(nvox-sip-common)> no sdp rtcp
```

Example

```
(nvox-sip-common)> sdp rtcp
Nvox::Manager: Set SIP RTCP in SDP to "1".

(nvox-sip-common)> no sdp rtcp
Nvox::Manager: Reset SIP RTCP in SDP.
```

History

Version	Description
3.05	The nvox sip-common sdp rtcp command has been introduced.

C.32.10 nvox sip-common sdp tias

Description Add TIAS bandwidth modifier to SDP (SDP bandwidth modifier TIAS, RFC3890). By default, the TIAS is absent in SDP.

Command with **no** prefix removes TIAS from SDP.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> sdp tias
(nvox-sip-common)> no sdp tias
```

Example

```
(nvox-sip-common)> sdp tias
Nvox::Manager: Set SIP TIAS in SDP to "1".

(nvox-sip-common)> no sdp tias
Nvox::Manager: Reset SIP TIAS in SDP.
```

History

Version	Description
3.05	The nvox sip-common sdp tias command has been introduced.

C.32.11 nvox sip-common stun-server

Description Configure the domain name or IP address of the STUN server common to all SIP telephone lines configured in the system.

By default, the STUN server is `stun.l.google.com:19302`.

Command with **no** prefix resets configuration by default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> stun-server <stun>
(nvox-sip-common)> no stun-server
```

Arguments	Argument	Value	Description
	stun	<i>String</i>	Domain name or IP address.

Example

```
(nvox-sip-common)> stun-server stun.sipnet.ru:3478
Nvox::Manager: Set SIP STUN server to "stun.sipnet.ru:3478".
```

```
(nvox-sip-common)> no stun-server
Nvox::Manager: Reset SIP STUN server.
```

History	Version	Description
	3.05	The nvox sip-common stun-server command has been introduced.

C.32.12 nvox sip-common tcp-keepalive

Description Set the interval of keepalive packet sending to the SIP proxy's TCP signaling port to keep an open connection to the server through NAT. By default, 90 value is set.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> tcp-keepalive <interval>
(nvox-sip-common)> no tcp-keepalive
```


Arguments

Argument	Value	Description
interval	<i>Integer</i>	The interval of keepalive packet sending in seconds. Can take values in the range from 5 to 600 inclusively. 0 value disables the sending of keepalive messages.

Example

```
(nvox-sip-common)> tcp-keepalive 120
Nvox::Manager: Set SIP TCP keepalive to "120".
```

```
(nvox-sip-common)> no tcp-keepalive
Nvox::Manager: Reset SIP TCP keepalive.
```

```
(nvox-sip-common)> tcp-keepalive 0
Nvox::Manager: Set SIP TCP keepalive to "0".
```

History

Version	Description
3.05	The nvox sip-common tcp-keepalive command has been introduced.

C.32.13 nvox sip-common tcp-port

Description

Configure the number of the local TCP port used to exchange SIP signaling messages with IP-telephony providers servers over the TCP transport protocol. By default, 5060 value is set.

Command with **no** prefix resets port to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip-common)> tcp-port <port>
```

```
(nvox-sip-common)> no tcp-port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	TCP port number in the range from 1 to 65534. Use 0 value to force the system to select a random free TCP port automatically.

Example

```
(nvox-sip-common)> tcp-port 8075
Nvox::Manager: Set SIP TCP port to "8075".
```

```
(nvox-sip-common)> no tcp-port
Nvox::Manager: Reset SIP TCP port.
```

```
(nvbox-sip-common)> tcp-port 0
Nvox::Manager: Set SIP TCP port to "0".
```

History

Version	Description
3.05	The nvbox sip-common tcp-port command has been introduced.

C.32.14 nvbox sip-common td-timeout

Description

Set the timeout for switching SIP proxies. Switching becomes possible if the DNS SRV record contains a list of several servers. The system selects from a list the server with the highest priority for SIP messaging. If this server does not respond, the system switches to the next highest priority server.

Note: This command is relevant if the [DNS SRV resolving](#) is enabled.

By default, 10000 value is set.

Command with **no** prefix resets timeout to default.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvbox-sip-common)> td-timeout <timeout>
```

```
(nvbox-sip-common)> no td-timeout
```

Arguments

Argument	Value	Description
timeout	<i>Integer</i>	The switchover timeout to another server in the range from 10000 to 100000 ms.

Example

```
(nvbox-sip-common)> td-timeout 12000
Nvox::Manager: Set SIP wait time for response retransmissions ►
to "12000".
```

```
(nvbox-sip-common)> no td-timeout
Nvox::Manager: Reset SIP wait time for response retransmissions.
```

History

Version	Description
3.05	The nvbox sip-common td-timeout command has been introduced.

C.32.15 nvox sip-common tls-keepalive

Description Set the interval of keepalive packet sending to the SIP proxy's TLS signaling port to keep an open connection to the server through NAT. By default, 90 value is set.

Note: This command is relevant when using the TLS transport protocol.

Command with **no** prefix resets setting to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> tls-keepalive <interval>
(nvox-sip-common)> no tls-keepalive
```

Arguments

Argument	Value	Description
interval	<i>Integer</i>	The interval of keepalive packet sending in seconds. Can take values in the range from 5 to 600 inclusively. 0 value disables the sending of keepalive messages.

Example

```
(nvox-sip-common)> tls-keepalive 120
Nvox::Manager: Set SIP TLS keepalive to "120".
```

```
(nvox-sip-common)> no tls-keepalive
Nvox::Manager: Reset SIP TLS keepalive.
```

```
(nvox-sip-common)> tls-keepalive 0
Nvox::Manager: Set SIP TLS keepalive to "0".
```

History

Version	Description
3.05	The nvox sip-common tls-keepalive command has been introduced.

C.32.16 nvox sip-common tls-port

Description Configure the number of the local TLS port used to exchange SIP signaling messages with IP-telephony providers servers over the TLS protocol. By default, 5061 value is set.

Note: Local TLS port number must not be the same as the local UDP and TCP port numbers that the system uses to exchange SIP messages.

Command with **no** prefix resets port to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> tcp-port <port>
(nvox-sip-common)> no tcp-port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	TLS port number in the range from 1 to 65534. Use 0 value to force the system to select a random free TLS port automatically.

Example

```
(nvox-sip-common)> tls-port 8076
Nvox::Manager: Set SIP TLS port to "8076".
```

```
(nvox-sip-common)> no tls-port
Nvox::Manager: Reset SIP TLS port.
```

```
(nvox-sip-common)> tls-port 0
Nvox::Manager: Set SIP TLS port to "0".
```

History

Version	Description
3.05	The nvox sip-common tls-port command has been introduced.

C.32.17 nvox sip-common udp-port

Description Configure the number of the local UDP port used to exchange SIP signaling messages with IP-telephony providers servers over the UDP protocol. By default, 5060 value is set.

Command with **no** prefix resets port to default.

Prefix no Yes

Change settings Yes

Multiple input No

Synopsis

```
(nvox-sip-common)> udp-port <port>
(nvox-sip-common)> no udp-port
```

Arguments

Argument	Value	Description
port	<i>Integer</i>	UDP port number in the range from 1 to 65534. Use 0 value to force the system to select a random free UDP port automatically.

Example

```
(nvox-sip-common)> udp-port 34577
Nvox::Manager: Set SIP UDP port to "34577".
```

```
(nvox-sip-common)> no udp-port
Nvox::Manager: Reset SIP UDP port.
```

```
(nvox-sip-common)> udp-port 0
Nvox::Manager: Set SIP UDP port to "0".
```

History

Version	Description
3.05	The nvox sip-common udp-port command has been introduced.

C.32.18 nvox sip-common unescape-hash-char

Description

Allow the # symbol in Request URI of INVITE requests in ASCII encoding, which is necessary for normal work with some IP-telephony operators. By default, the feature is disabled.

Command with **no** prefix disables the setting. The # symbol is encoded as %23, which corresponds to RFC2396.

Prefix no

Yes

Change settings

Yes

Multiple input

No

Synopsis

```
(nvox-sip-common)> unescape-hash-char
```

```
(nvox-sip-common)> no unescape-hash-char
```

Example

```
(nvox-sip-common)> unescape-hash-char
Nvox::Manager: Set SIP unescape # char in outgoing SIP URI to "1".
```

```
(nvox-sip-common)> no unescape-hash-char
Nvox::Manager: Reset SIP unescape # char in outgoing SIP URI.
```

History

Version	Description
3.05	The nvox sip-common unescape-hash-char command has been introduced.

C.33 show nvox active-calls

Description Show the list of active calls that are being made at the moment.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **nvox active-calls**

Example (show)> **nvox active-calls**

```
active_calls:
  call:
    type: outgoing
    index: 0
    status: hold
    hs: phone 1
    line: 1001
    number: 9999
    start_time: Fri Dec 17 12:04:06 2021
    duration: 30
    matched_name:

  call:
    type: outgoing
    index: 1
    status: connected
    hs: phone 1
    line: 1001
    number: 1002
    start_time: Fri Dec 17 12:04:17 2021
    duration: 12
    matched_name:

  call:
    type: incoming
    index: 2
    status: connected
    hs: phone 2
    line: 1002
    number: 1001
    start_time: Fri Dec 17 12:04:21 2021
    duration: 12
    matched_name:
```

History

Version	Description
3.05	The show nvox active-calls command has been introduced.

C.34 show nvox blacklist

Description Show the blacklist configured for the SIP line.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> nvox blacklist <id>`

Arguments

Argument	Value	Description
id	<i>String</i>	SIP line identifier of Latin letters and numbers from 0 to 9. The maximum string length is 64 characters.

Example

```
(show)> nvox blacklist 1

line:
    id: 1
    name: nonoh
    blacklist: [1-69]x.|+792[67]x.|000x.|1234567
```

History

Version	Description
4.01	The show nvox blacklist command has been introduced.

C.35 show nvox cadences

Description Show the settings of the selected ringtone. If you use no argument, the settings of all ringtones will be displayed.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> nvox cadences [cadence]`

Arguments

Argument	Value	Description
cadence	<i>Integer</i>	Ringtone number in the range from 0 to 5.

Example

```
(show)> nvox cadences

cadences:
```

```
cadence:
    id: 0
    active1: 400
    passive1: 500
    active2: 400
    passive2: 2000
    active3: 0
    passive3: 0
```

```
cadence:
    id: 1
    active1: 1000
    passive1: 4000
    active2: 0
    passive2: 0
    active3: 0
    passive3: 0
```

```
cadence:
    id: 2
    active1: 400
    passive1: 500
    active2: 0
    passive2: 0
    active3: 0
    passive3: 0
```

```
cadence:
    id: 3
    active1: 400
    passive1: 2000
    active2: 1200
    passive2: 1200
    active3: 0
    passive3: 0
```

```
cadence:
    id: 4
    active1: 400
    passive1: 500
    active2: 400
    passive2: 2000
    active3: 2000
    passive3: 2000
```

```
cadence:
    id: 5
    active1: 4000
    passive1: 2000
    active2: 0
    passive2: 0
    active3: 0
    passive3: 0
```



```
(show)> nvox cadences 1
```

```
cadence:
  id: 1
  active1: 1000
  passive1: 4000
  active2: 0
  passive2: 0
  active3: 0
  passive3: 0
```

History

Version	Description
3.05	The show nvox cadences command has been introduced.

C.36 show nvox call-history

Description Show list of calls registered since the router is switched on. If you use no arguments, the entire call log will be displayed.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> nvox call-history [ <offset> [ <count> ] ]`

Arguments

Argument	Value	Description
offset	<i>Integer</i>	The number of call log entries, starting from the last entry, that you want to skip when displaying on the screen. The offset must not exceed the maximum number of records specified by the nvox call-history length command.
count	<i>Integer</i>	The number of records to be shown. The records are displayed in descending order. If this parameter is absent, all records with the specified offset are displayed.

Example

```
(show)> nvox call-history
```

```
call_history:
  call:
    type: outgoing
    index: 3
    start_time: Wed Dec 29 13:15:17 2021
    line: 1002
    hs: phone 2
```

```
other_party_number: 9996
  other_party_name:
    duration: 47
    release_code:
    release_reason:

    call:
      type: outgoing
      index: 2
      start_time: Wed Dec 29 13:15:17 2021
      line: 1001
      hs: phone 1
other_party_number: 9997
  other_party_name:
    duration: 48
    release_code:
    release_reason:

    call:
      type: outgoing
      index: 1
      start_time: Wed Dec 29 13:13:39 2021
      line: 1002
      hs: phone 2
other_party_number: 9998
  other_party_name:
    duration: 13
    release_code:
    release_reason:

    call:
      type: outgoing
      index: 0
      start_time: Wed Dec 29 13:13:36 2021
      line: 1001
      hs: phone 1
other_party_number: 9999
  other_party_name:
    duration: 18
    release_code:
    release_reason:
```

```
(show)> nvox call-history 2 2
```

```
call_history:
  call:
    type: outgoing
    index: 1
    start_time: Wed Dec 29 13:13:39 2021
    line: 1002
    hs: phone 2
other_party_number: 9998
other_party_name:
  duration: 13
```

```

        release_code:
        release_reason:

        call:
            type: outgoing
            index: 0
            start_time: Wed Dec 29 13:13:36 2021
            line: 1001
            hs: phone 1
        other_party_number: 9999
        other_party_name:
            duration: 18
        release_code:
        release_reason:

```

History

Version	Description
2.06	The show dect call-history command has been introduced.
3.05	The command renamed to show nvox call-history .

C.37 show nvox fxs

Description Show Keenetic Linear USB module settings.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **nvox fxs**

Example (show)> **nvox fxs**

```

        fxs-status:
            country-codes: BG CA CS DE DK EE ES FI FR GR HR
                           HU IT KZ LT LV NO PL PT RO RS RU ►
SE SI SK TR UA
        selected-country: DE
        force-calibration: disabled
        pulse-dial-modes: 0 - disabled, 1 - disabled
                           during voice calls, 2 - always ►
enabled
        selected-pulse-dial-mode: 1
        led-blinking-timer: 1000
        unmute-timer: 200

```

History

Version	Description
3.05	The show nvox fxs command has been introduced.

C.38 show nvox fxs-ports

Description Show phone port settings of Keenetic Linear USB module.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **nvox fxs-ports**

Example (show)> **nvox fxs-ports**

```
ports:
  port:
    id: 1
    name: phone 1
    int-number: 1
    status: enabled
    volume-rx: -4
    volume-tx: -4
    impedance: 220_820_115
    hash-ends-dial: enabled
    echo-cancellation: enabled

  port:
    id: 2
    name: phone 2
    int-number: 2
    status: enabled
    volume-rx: -4
    volume-tx: -4
    impedance: 220_820_115
    hash-ends-dial: enabled
    echo-cancellation: enabled
```

History

Version	Description
3.05	The show nvox fxs-ports command has been introduced.

C.39 show nvox info

Description Show information about the IP telephony system application installed on Keenetic OS.

Prefix no No**Change settings** No**Multiple input** No**Synopsis** (show)> **nvox info****Example** (show)> **nvox info**

```

info:
  app_name: nvox
  app_version: 0.8.2.53
  app_suffix: singledongle
  compile_date: Dec 15 2021
  sip_name: pjsip
  sip_version: 2.6
  sip_status: stopped
  tel_type: FXS
  tel_name: Si32287
tel_api_version: 9.2.0
  tel_serial: S2135NS000404
  tel_fw_date: 17:28:49 Feb 24 2021
  tel_fw_version: 0044
  plugged: yes
supported_codecs: g711u,g711a,g726,g722

```

History

Version	Description
3.05	The show nvox info command has been introduced.

C.40 show nvox license

Description Show information about the connected USB module service code.**Prefix no** No**Change settings** No**Multiple input** No**Synopsis** (show)> **nvox license****Example** (show)> **nvox license**

```

plugged: yes
license: 123456789012345
integrity: ok

```

History

Version	Description
3.05	The show nvox license command has been introduced.

C.41 show nvox phonebook

Description Show the phonebook. If you execute the command without parameters, the entire phonebook is displayed.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **nvox phonebook** [<sort_by_field> [<offset> <count>]]

Arguments

Argument	Value	Description
sort_by_field	fn	Sort by first name.
	ln	Sort by last name.
offset	<i>Integer</i>	The number of contacts, starting from the first record, to be skipped when displaying on the screen. The offset mustn't exceed the maximum number of phone contacts specified by the nvox phonebook length command.
count	<i>Integer</i>	The number of contacts to be displayed. If this parameter is absent, all contacts with the offset specified by the offset parameter are displayed.

Example

```
(show)> show nvox phonebook ln 5 3

phonebook:
  record:
    index: 5
    first_name: Dan
    last_name: Lazovski
    number1: 11231234567
  number1_type: mobile
    number2: 4912341234567
  number2_type: mobile
    number3: 57945678900
  number3_type: mobile

  record:
    index: 6
    first_name: Lana
    last_name: Rey
```

```
        number1: 6545613854
    number1_type: mobile

    record:
        index: 7
        first_name: Sam
        last_name: Sorin
        number1: 4912312345678980
    number1_type: mobile
        number2: 5754329764534
    number2_type: work
        number3: 5334838376261234
    number3_type: fixed
```

History

Version	Description
4.02	The show nvox phonebook command has been introduced.

C.42 show nvox sip-lines

Description Show SIP registration status of telephone lines and the status of blacklists and whitelists configured in the system.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **nvox sip-lines**

Example

```
(show)> nvox sip-lines

    lines:
        line:
            id: 2
            name: 1002
            code: 401
            status: failure
        description: Unauthorized
        blacklist: configured, enabled
        whitelist: configured, disabled

        line:
            id: 1
            name: 1001
            code: 200
            status: registered
        description: OK
```

```

blacklist: empty, disabled
whitelist: configured, disabled

```

History

Version	Description
3.05	The show nvox sip-lines command has been introduced.

C.43 show nvox sip-profiles

Description Show settings profiles for connecting to IP telephony operators, which are used to configure phone lines in the web interface.

Prefix no No

Change settings No

Multiple input No

Synopsis (show)> **nvox sip-profiles [default]**

Arguments

Argument	Value	Description
default	<i>Keyword</i>	Show the default settings profile that is used when no operator is selected.

Example

```

(show)> nvox sip-profiles

    profile:
      provider: Actionvoip
registration-uri: sip.actionvoip.com
      proxy: sip.actionvoip.com:5060
      domain: sip.actionvoip.com
      reg-timeout: 180

    profile:
      provider: Chief 070
registration-uri:
      proxy: 202.133.231.17
      domain: chiefcall.com.tw

    profile:
      provider: Deutsche Telekom (UDP)
      domain: tel.t-online.de
registration-uri: tel.t-online.de
      proxy: tel.t-online.de
      substitute: (+49>0)x.
      reg-timeout: 480

    profile:
      provider: Deutsche Telekom (TCP)
      domain: tel.t-online.de

```



```

registration-uri: tel.t-online.de
    proxy: tel.t-online.de
    substitute: (+49>0)x.
    transport: tcp
    reg-timeout: 480

    profile:
        provider: FreeCall
registration-uri: sip.voiparound.com
    proxy: sip.voiparound.com:5060
    domain: sip.voiparound.com
    reg-timeout: 180

    profile:
        provider: Nonoh
registration-uri: sip.nonoh.net
    proxy: sip.nonoh.net:5060
    domain: sip.nonoh.net
    reg-timeout: 180

    profile:
        provider: Telbo
registration-uri: telbo.com
    proxy: telbo.com
    domain: telbo.com

    profile:
        provider: TIM Telecom Italia
registration-uri: telecomitalia.it
    domain: telecomitalia.it
    transport: udp
    keepalive: 30
    substitute: (+39>)x.|(+>00)x.

    codec: g711a

    codec: g711u

    reg-timeout: 3600

    profile:
        provider: VoipDiscount
registration-uri: sip.voipdiscount.com
    proxy: sip.voipdiscount.com:5060
    domain: sip.voipdiscount.com
    reg-timeout: 180

    profile:
        provider: WebCallDirect
registration-uri: webcalldirect.com
    proxy: webcalldirect.com
    domain: webcalldirect.com
    reg-timeout: 180

```

```
(show)> nvox sip-profiles default
```

```

  profile:
    provider: CUSTOM
    name: CUSTOM
  registration-uri:
    reg-timeout: 180
    proxy:
    domain:
    transport: udp
  tls-security-mode: SIP-TLS
  dtmf-mode: rfc2833
  lock-codec: yes
  disable-stun: yes
  sdp-nat-rewrite: no
  keepalive: 30

  codec: g711u

  codec: g711a

  digit-map:
  substitute:

```

History

Version	Description
3.05	The show nvox sip-profiles command has been introduced.

C.44 show nvox try-dial

Description Show the telephone line through which an outgoing call will go to a specified telephone number from a specified DECT handset or telephone port.

Prefix no No

Change settings No

Multiple input No

Synopsis `(show)> nvox try-dial <ipui> <number>`

Arguments

Argument	Value	Description
ipui	<i>Hex Integer</i>	Ten-digit DECT handset identifier or telephone port number (1 or 2).
number	<i>String</i>	Phone number, a string consisting of digits from 0 to 9 as well as the symbols # and *. The length of the string is up to 19 characters.

Example

```
(show)> nvox try-dial 034725D054 1234567
```

```
    line: 1
    line_id: 1
    line_name: 1001
    status: registered
    code: 200
    description: OK
```

```
(show)> nvox try-dial 1 1234567
```

```
    line: 1
    line_id: 1
    line_name: 1001
    status: registered
    code: 200
    description: OK
```

History

Version	Description
3.05	The show nvox try-dial command has been introduced.

C.45 show nvox try-dial-ext

Description

Show the routing of an outgoing call to a specified telephone number for all DECT handsets or telephone ports registered in the system. The command output for each handset displays a list of phone lines that are allowed to make an outgoing call from that handset. The lines in the list are displayed according to their priority — the higher the line in the list, the higher its priority. For the outgoing call the system selects the line with the highest priority and successful SIP registration (status "registered").

Prefix no

No

Change settings

No

Multiple input

No

Synopsis

```
(show)> nvox try-dial-ext <number>
```

Arguments

Argument	Value	Description
number	<i>String</i>	Phone number, a string consisting of digits from 0 to 9 as well as the symbols # and *. The length of the string is up to 19 characters.

Example

```
(show)> nvox try-dial-ext 1234567
```

```
    number: 1234567
```

```
    handset:
```

```
name: phone 1

line:
  id: 1
  name: 1001
  status: registered

handset:
  name: phone 2

line:
  id: 3
  name: 1003
  status: registered

line:
  id: 2
  name: 1002
  status: unregistered
```

History

Version	Description
3.05	The show nvox try-dial-ext command has been introduced.

C.46 show nvox whitelist

Description	Show the whitelist configured for the SIP line.
Prefix no	No
Change settings	No
Multiple input	No

Synopsis (show)> nvox whitelist <id>

Arguments

Argument	Value	Description
id	String	SIP line identifier of Latin letters and numbers from 0 to 9. The maximum string length is 64 characters.

Example

```
(show)> nvox whitelist 1

line:
  id: 1
  name: nonoh
whitelist: 1234567890|+79261234567|000123456|1234567
```

History

Version	Description
4.01	The show nvox whitelist command has been introduced.

SNMP MIB

Management Information Bases (MIBs) are read-only.

The following MIBs are supported:

D.1 SNMPv2-MIB

OID: 1.3.6.1.2.1.1

The following data elements are supported:

- SNMPv2-MIB::sysDescr
- SNMPv2-MIB::sysUpTime
- SNMPv2-MIB::sysContact
- SNMPv2-MIB::sysName
- SNMPv2-MIB::sysLocation
- SNMPv2-MIB::sysServices

D.2 IF-MIB

OID: 1.3.6.1.2.1.2 and 1.3.6.1.2.1.31

The following data elements are supported:

Basical

OID: 1.3.6.1.2.1.2

- IF-MIB::ifNumber
- IF-MIB::ifIndex
- IF-MIB::ifDescr
- IF-MIB::ifType
- IF-MIB::ifMtu
- IF-MIB::ifSpeed
- IF-MIB::ifPhysAddress
- IF-MIB::ifAdminStatus

- IF-MIB::ifOperStatus
- IF-MIB::ifLastChange
- IF-MIB::ifInOctets
- IF-MIB::ifInUcastPkts
- IF-MIB::ifInDiscards
- IF-MIB::ifInErrors
- IF-MIB::ifOutOctets
- IF-MIB::ifOutUcastPkts
- IF-MIB::ifOutDiscards
- IF-MIB::ifOutErrors

Advanced

OID 1.3.6.1.2.1.31

- IF-MIB::ifName
- IF-MIB::ifInMulticastPkts
- IF-MIB::ifInBroadcastPkts
- IF-MIB::ifOutMulticastPkts
- IF-MIB::ifOutBroadcastPkts
- IF-MIB::ifHCInOctets
- IF-MIB::ifHCInUcastPkts
- IF-MIB::ifHCInMulticastPkts
- IF-MIB::ifHCInBroadcastPkts
- IF-MIB::ifHCOctets
- IF-MIB::ifHCOUcastPkts
- IF-MIB::ifHCOMulticastPkts
- IF-MIB::ifHCOBroadcastPkts
- IF-MIB::ifLinkUpDownTrapEnable
- IF-MIB::ifHighSpeed
- IF-MIB::ifPromiscuousMode
- IF-MIB::ifConnectorPresent
- IF-MIB::ifAlias

- IF-MIB::ifCounterDiscontinuityTime

Main chipset	Switch	Device	Description
MT7621/RT63368	MT7530	Keenetic Giga III	64-bit per port octet counters. 32-bit per port packet counters. Separate per port broadcast, multicast and unicast packet counters.
	RTL8370M	Keenetic Ultra II Keenetic LTE	
MT7620	RTL8367B	Keenetic Viva Keenetic Extra	
	Integrated	Keenetic 4G III Keenetic Lite II Keenetic Lite III Keenetic Omni Keenetic Omni II	32-bit per port octet counters & 16-bit per port packet counters. Last counter overflow event time set in IF-MIB::ifCounterDiscontinuityTime.
MT7628	Integrated	Keenetic Start II Keenetic Lite III rev.B Keenetic 4G III rev.B Keenetic Air Keenetic Extra II	16-bit per port packet counters only. Last counter overflow event time set in IF-MIB::ifCounterDiscontinuityTime.

D.3 IP-MIB

OID: 1.3.6.1.2.1.6

The following data elements are supported:

- TCP-MIB::tcpRtoAlgorithm
- TCP-MIB::tcpRtoMin
- TCP-MIB::tcpRtoMax
- TCP-MIB::tcpMaxConn
- TCP-MIB::tcpActiveOpens
- TCP-MIB::tcpPassiveOpens
- TCP-MIB::tcpAttemptFails

- TCP-MIB::tcpEstabResets
- TCP-MIB::tcpCurrEstab
- TCP-MIB::tcpInSegs
- TCP-MIB::tcpOutSegs
- TCP-MIB::tcpRetransSegs
- TCP-MIB::tcpInErrs
- TCP-MIB::tcpOutRsts

D.4 UDP-MIB

OID: 1.3.6.1.2.1.7

The following data elements are supported:

- UDP-MIB::udpInDatagrams
- UDP-MIB::udpNoPorts
- UDP-MIB::udpInErrors
- UDP-MIB::udpOutDatagrams
- UDP-MIB::udpHCInDatagrams
- UDP-MIB::udpHCOutDatagrams

D.5 HOST-RESOURCES-MIB

OID: 1.3.6.1.2.1.25

The following data elements are supported:

- HOST-RESOURCES-MIB::hrSystemUptime

D.6 UCD-SNMP-MIB

OID 1.3.6.1.4.1.2021

The following data elements are supported:

- | | |
|-----------------|---|
| RAM info | <ul style="list-style-type: none">• UCD-SNMP-MIB::memTotalReal• UCD-SNMP-MIB::memAvailReal• UCD-SNMP-MIB::memShared• UCD-SNMP-MIB::memBuffer |
|-----------------|---|

- UCD-SNMP-MIB::memCached

USB-storage info

- UCD-SNMP-MIB::dskIndex
- UCD-SNMP-MIB::dskPath
- UCD-SNMP-MIB::dskTotal
- UCD-SNMP-MIB::dskAvail
- UCD-SNMP-MIB::dskUsed
- UCD-SNMP-MIB::dskPercent
- UCD-SNMP-MIB::dskPercentNode

System load info

- UCD-SNMP-MIB::laIndex
- UCD-SNMP-MIB::laNames
- UCD-SNMP-MIB::laLoad
- UCD-SNMP-MIB::laConfig
- UCD-SNMP-MIB::laLoadInt
- UCD-SNMP-MIB::ssCpuRawUser
- UCD-SNMP-MIB::ssCpuRawNice
- UCD-SNMP-MIB::ssCpuRawSystem
- UCD-SNMP-MIB::ssCpuRawIdle
- UCD-SNMP-MIB::ssRawInterrupts
- UCD-SNMP-MIB::ssRawContexts

IPsec Encryption Levels

The encryption level defines a set of *IKE* and *IPsec SA* algorithms.

Below a complete list of algorithms is displayed for each level in order of decreasing priority, as well as a set of commands **crypto ike proposal** to setup this profile manually.

In the list of algorithms is indicated:

- encryption with key length
- hash function for *HMAC* forming
- *PFS* mode (NO if disabled)

E.1 weak

Protocol	Encryption	Proposal
IKEv1	AES-128-CBC/SHA1/MODP1024	encryption aes-128-cbc
	AES-128-CBC/SHA1/MODP768	encryption 3des
	AES-128-CBC/MD5/MODP1024	encryption des
	AES-128-CBC/MD5/MODP768	integrity sha1
	3DES-CBC/SHA1/MODP1024	integrity md5
	3DES-CBC/SHA1/MODP768	dh-group 2
	3DES-CBC/MD5/MODP1024	dh-group 1
	3DES-CBC/MD5/MODP768	
	DES-CBC/SHA1/MODP1024	
	DES-CBC/SHA1/MODP768	
	DES-CBC/MD5/MODP1024	
	DES-CBC/MD5/MODP768	
IKEv2	AES-128-CBC/SHA1/MODP1024	encryption aes-128-cbc
	AES-128-CBC/SHA1/MODP768	encryption 3des
	AES-128-CBC/MD5/MODP1024	encryption des
	AES-128-CBC/MD5/MODP768	integrity sha1

Protocol	Encryption	Proposal
	3DES-CBC/SHA1/MODP1024	integrity md5
	3DES-CBC/SHA1/MODP768	dh-group 2
	3DES-CBC/MD5/MODP1024	dh-group 1
	3DES-CBC/MD5/MODP768	
	DES-CBC/SHA1/MODP1024	
	DES-CBC/SHA1/MODP768	
	DES-CBC/MD5/MODP1024	
	DES-CBC/MD5/MODP768	
IPsec SA	DES/MD5	cypher esp-des
	AES-128-CBC/SHA1	cypher esp-3des
	3DES-CBC/SHA1	cypher esp-aes-128
	DES/SHA1	hmac esp-md5-hmac
	AES-128-CBC/MD5	hmac esp-sha1-hmac
	3DES-CBC/MD5	

E.2 weak-pfs

Protocol	Encryption	Proposal
IKEv1	AES-128-CBC/SHA1/MODP1024	encryption aes-128-cbc
	AES-128-CBC/SHA1/MODP768	encryption 3des
	AES-128-CBC/MD5/MODP1024	encryption des
	AES-128-CBC/MD5/MODP768	integrity sha1
	3DES-CBC/SHA1/MODP1024	integrity md5
	3DES-CBC/SHA1/MODP768	dh-group 2
	3DES-CBC/MD5/MODP1024	dh-group 1
	3DES-CBC/MD5/MODP768	
	DES-CBC/SHA1/MODP1024	
	DES-CBC/SHA1/MODP768	
	DES-CBC/MD5/MODP1024	
	DES-CBC/MD5/MODP768	

Protocol	Encryption	Proposal
IKEv2	AES-128-CBC/SHA1/MODP1024	encryption aes-128-cbc
	AES-128-CBC/SHA1/MODP768	encryption 3des
	AES-128-CBC/MD5/MODP1024	encryption des
	AES-128-CBC/MD5/MODP768	integrity sha1
	3DES-CBC/SHA1/MODP1024	integrity md5
	3DES-CBC/SHA1/MODP768	dh-group 2
	3DES-CBC/MD5/MODP1024	dh-group 1
	3DES-CBC/MD5/MODP768	
	DES-CBC/SHA1/MODP1024	
	DES-CBC/SHA1/MODP768	
	DES-CBC/MD5/MODP1024	
	DES-CBC/MD5/MODP768	
IPsec SA	DES/MD5/MODP1024	cypher esp-des
	AES-128-CBC/SHA1	cypher esp-3des
	3DES-CBC/SHA1	cypher esp-aes-128
	DES/SHA1	hmac esp-md5-hmac
	AES-128-CBC/MD5	hmac esp-sha1-hmac
	3DES-CBC/MD5	dh-group 2
	AES-128-CBC/SHA1/MODP1024	dh-group 1
	3DES-CBC/SHA1/MODP1024	
	DES-CBC/SHA1/MODP1024	
	AES-128-CBC/SHA1/MODP768	
	3DES-CBC/SHA1/MODP768	
	DES-CBC/SHA1/MODP768	
	AES-128-CBC/MD5/MODP1024	
	3DES-CBC/MD5/MODP1024	
	AES-128-CBC/MD5/MODP768	
	3DES-CBC/MD5/MODP768	
	DES-CBC/MD5/MODP768	

E.3 normal

Protocol	Encryption	Proposal
IKEv1	AES-256-CBC/SHA1/MODP1536	encryption aes-256-cbc
	AES-256-CBC/SHA1/ECP384	encryption aes-128-cbc
	AES-256-CBC/SHA1/MODP2048	encryption 3des
	AES-256-CBC/SHA1/MODP1024	integrity sha1
	AES-128-CBC/SHA1/MODP1536	integrity sha256
	AES-128-CBC/SHA1/ECP256	dh-group 5
	AES-128-CBC/SHA1/MODP1024	dh-group 20
	3DES-CBC/SHA1/MODP2048	dh-group 14
	3DES-CBC/SHA1/MODP1536	dh-group 2
	3DES-CBC/SHA1/MODP1024	dh-group 26
	AES-256-CBC/SHA256/MODP1024	
	AES-128-CBC/SHA256/MODP1024	
	3DES-CBC/SHA256/MODP1024	
IKEv2	AES-256-CBC/SHA256/MODP1024	encryption aes-256-cbc
	AES-128-CBC/SHA256/MODP1024	encryption aes-128-cbc
	3DES-CBC/SHA256/MODP1024	encryption 3des
	AES-256-CBC/SHA1/MODP1024	integrity sha256
	AES-256-CBC/SHA1/ECP384	integrity sha1
	AES-256-CBC/SHA1/MODP2048	dh-group 2
	AES-128-CBC/SHA1/MODP1024	dh-group 20
	AES-128-CBC/SHA1/ECP256	dh-group 14
	AES-256-CBC/SHA256/MODP2048	dh-group 5
	3DES-CBC/SHA1/MODP2048	dh-group 26
	3DES-CBC/SHA1/MODP1536	
	3DES-CBC/SHA1/MODP1024	
IPsec SA	AES-128-CBC/SHA1	cypher esp-aes-128
	AES-256-CBC/SHA1	cypher esp-aes-256

Protocol	Encryption	Proposal
	3DES-CBC/SHA1	cypher esp-3des
	AES-128-CBC/SHA256	hmac esp-sha1-hmac
	AES-256-CBC/SHA256	hmac esp-sha256-hmac
	3DES-CBC/SHA256	

E.4 normal-pfs

Protocol	Encryption	Proposal
IKEv1	AES-256-CBC/SHA1/MODP1536	encryption aes-256-cbc
	AES-256-CBC/SHA1/ECP384	encryption aes-128-cbc
	AES-256-CBC/SHA1/MODP2048	encryption 3des
	AES-256-CBC/SHA1/MODP1024	integrity sha1
	AES-128-CBC/SHA1/MODP1536	integrity sha256
	AES-128-CBC/SHA1/ECP256	dh-group 5
	AES-128-CBC/SHA1/MODP1024	dh-group 20
	3DES-CBC/SHA1/MODP2048	dh-group 14
	3DES-CBC/SHA1/MODP1536	dh-group 2
	3DES-CBC/SHA1/MODP1024	dh-group 26
	AES-256-CBC/SHA256/MODP1024	
	AES-128-CBC/SHA256/MODP1024	
	3DES-CBC/SHA256/MODP1024	
IKEv2	AES-256-CBC/SHA256/MODP1024	encryption aes-256-cbc
	AES-128-CBC/SHA256/MODP1024	encryption aes-128-cbc
	3DES-CBC/SHA256/MODP1024	encryption 3des
	AES-256-CBC/SHA1/MODP1024	integrity sha256
	AES-256-CBC/SHA1/ECP384	integrity sha1
	AES-256-CBC/SHA1/MODP2048	dh-group 2
	AES-128-CBC/SHA1/MODP1024	dh-group 20
	AES-128-CBC/SHA1/ECP256	dh-group 14
	AES-256-CBC/SHA256/MODP2048	dh-group 5

Protocol	Encryption	Proposal
IPsec SA	3DES-CBC/SHA1/MODP2048	dh-group 26
	3DES-CBC/SHA1/MODP1536	
	3DES-CBC/SHA1/MODP1024	
	AES-128-CBC/SHA1/MODP1024	esp-aes-128
	AES-128-CBC/SHA1	cypher esp-aes-256
	AES-256-CBC/SHA1	cypher esp-3des
	3DES-CBC/SHA1	hmac esp-sha1-hmac
	AES-256-CBC/SHA1/MODP1536	hmac esp-sha256-hmac
	AES-128-CBC/SHA1/MODP1536	dh-group 2
	3DES-CBC/SHA1/MODP1536	dh-group 14
	AES-256-CBC/SHA1/MODP1024	
	3DES-CBC/SHA1/MODP1024	

E.5 normal-3des

Protocol	Encryption	Proposal
IKEv1	AES-256-CBC/SHA1/MODP1536	encryption aes-256-cbc
	AES-256-CBC/SHA1/ECP384	encryption aes-128-cbc
	AES-256-CBC/SHA1/MODP2048	encryption 3des
	AES-256-CBC/SHA1/MODP1024	integrity sha1
	AES-128-CBC/SHA1/MODP1536	integrity sha256
	AES-128-CBC/SHA1/ECP256	dh-group 5
	AES-128-CBC/SHA1/MODP1024	dh-group 20
	3DES-CBC/SHA1/MODP2048	dh-group 14
	3DES-CBC/SHA1/MODP1536	dh-group 2
	3DES-CBC/SHA1/MODP1024	dh-group 26
	AES-256-CBC/SHA256/MODP1024	
	AES-128-CBC/SHA256/MODP1024	
	3DES-CBC/SHA256/MODP1024	
IKEv2	AES-256-CBC/SHA256/MODP1024	encryption aes-256-cbc

Protocol	Encryption	Proposal
	AES-128-CBC/SHA256/MODP1024	encryption aes-128-cbc
	3DES-CBC/SHA256/MODP1024	encryption 3des
	AES-256-CBC/SHA1/MODP1024	integrity sha256
	AES-256-CBC/SHA1/ECP384	integrity sha1
	AES-256-CBC/SHA1/MODP2048	dh-group 2
	AES-128-CBC/SHA1/MODP1024	dh-group 20
	AES-128-CBC/SHA1/ECP256	dh-group 14
	AES-256-CBC/SHA256/MODP2048	dh-group 5
	3DES-CBC/SHA1/MODP2048	dh-group 26
	3DES-CBC/SHA1/MODP1536	
	3DES-CBC/SHA1/MODP1024	
IPsec SA	3DES-CBC/SHA1	cypher esp-3des
	AES-256-CBC/SHA1	cypher esp-aes-256
	AES-128-CBC/SHA1	cypher esp-aes-128
	3DES-CBC/SHA256	hmac esp-sha1-hmac
	AES-256-CBC/SHA256	hmac esp-sha256-hmac
	AES-128-CBC/SHA256	

E.6 normal-3des-pfs

Protocol	Encryption	Proposal
IKEv1	AES-256-CBC/SHA1/MODP1536	encryption aes-256-cbc
	AES-256-CBC/SHA1/ECP384	encryption aes-128-cbc
	AES-256-CBC/SHA1/MODP2048	encryption 3des
	AES-256-CBC/SHA1/MODP1024	integrity sha1
	AES-128-CBC/SHA1/MODP1536	integrity sha256
	AES-128-CBC/SHA1/ECP256	dh-group 5
	AES-128-CBC/SHA1/MODP1024	dh-group 20
	3DES-CBC/SHA1/MODP2048	dh-group 14
	3DES-CBC/SHA1/MODP1536	dh-group 2

Protocol	Encryption	Proposal
	3DES-CBC/SHA1/MODP1024 AES-256-CBC/SHA256/MODP1024 AES-128-CBC/SHA256/MODP1024 3DES-CBC/SHA256/MODP1024	dh-group 26
IKEv2	AES-256-CBC/SHA256/MODP1024 AES-128-CBC/SHA256/MODP1024 3DES-CBC/SHA256/MODP1024 AES-256-CBC/SHA1/MODP1024 AES-256-CBC/SHA1/ECP384 AES-256-CBC/SHA1/MODP2048 AES-128-CBC/SHA1/MODP1024 AES-128-CBC/SHA1/ECP256 AES-256-CBC/SHA256/MODP2048 3DES-CBC/SHA1/MODP2048 3DES-CBC/SHA1/MODP1536 3DES-CBC/SHA1/MODP1024	encryption aes-256-cbc encryption aes-128-cbc encryption 3des integrity sha256 integrity sha1 dh-group 2 dh-group 20 dh-group 14 dh-group 5 dh-group 26
IPsec SA	3DES-CBC/SHA1/MODP1024 3DES-CBC/SHA1 AES-256-CBC/SHA1 AES-128-CBC/SHA1 AES-256-CBC/SHA1/MODP1536 AES-128-CBC/SHA1/MODP1536 3DES-CBC/SHA1/MODP1536 AES-256-CBC/SHA1/MODP1024 AES-128-CBC/SHA1/MODP1024	cypher esp-3des cypher esp-aes-256 cypher esp-aes-128 hmac esp-sha1-hmac hmac esp-sha256-hmac dh-group 2 dh-group 14

E.7 high

Protocol	Encryption	Proposal
IKEv1	AES-256-CBC/SHA256/MODP1024	encryption aes-256-cbc

Protocol	Encryption	Proposal
	AES-256-CBC/SHA256/ECP384	encryption aes-128-cbc
	AES-256-CBC/SHA256/MODP1536	integrity sha256
	AES-256-CBC/SHA1/MODP2048	integrity sha1
	AES-256-CBC/SHA1/ECP384	dh-group 2
	AES-256-CBC/SHA1/MODP1536	dh-group 20
	AES-128-CBC/SHA1/MODP2048	dh-group 5
	AES-128-CBC/SHA1/ECP256	dh-group 14
	AES-128-CBC/SHA1/MODP1536	dh-group 26
IKEv2	AES-256-CBC/SHA256/MODP1024	encryption aes-256-cbc
	AES-256-CBC/SHA256/ECP384	encryption aes-128-cbc
	AES-256-CBC/SHA256/MODP1536	integrity sha256
	AES-256-CBC/SHA1/MODP2048	integrity sha1
	AES-256-CBC/SHA1/ECP384	dh-group 2
	AES-256-CBC/SHA1/MODP1536	dh-group 20
	AES-128-CBC/SHA1/MODP2048	dh-group 5
	AES-128-CBC/SHA1/ECP256	dh-group 14
IPsec SA	AES-256-CBC/SHA256	dh-group 26
	AES-128-CBC/SHA256	cypher esp-aes-256
		cypher esp-aes-128
		hmac esp-hmac-sha256

E.8 strong

Protocol	Encryption	Proposal
IKEv1	AES-256-CBC/SHA1/MODP2048	encryption aes-256-cbc
	AES-256-CBC/SHA1/ECP384	encryption aes-128-cbc
	AES-256-CBC/SHA1/MODP1536	integrity sha1
	AES-128-CBC/SHA1/MODP2048	dh-group 14
	AES-128-CBC/SHA1/ECP256	dh-group 20
	AES-128-CBC/SHA1/MODP1536	dh-group 5

Protocol	Encryption	Proposal
		dh-group 26
IKEv2	AES-256-CBC/SHA1/MODP2048	encryption aes-256-cbc
	AES-256-CBC/SHA1/ECP384	encryption aes-128-cbc
	AES-256-CBC/SHA1/MODP1536	integrity sha1
	AES-128-CBC/SHA1/MODP2048	dh-group 14
	AES-128-CBC/SHA1/ECP256	dh-group 20
	AES-128-CBC/SHA1/MODP1536	dh-group 5
		dh-group 26
IPsec SA	AES-256-CBC/SHA1/MODP1536	cypher esp-aes-256
	AES-256-CBC/SHA1/MODP2048	cypher esp-aes-128
	AES-128-CBC/SHA1/MODP2048	hmac esp-sha1-hmac
	AES-128-CBC/SHA1/MODP1536	dh-group 5
		dh-group 14

E.9 strong-aead

Protocol	Encryption	Proposal
IKEv1	AES-256-GCM-16/PRF-SHA384/ECP384	aead
		encryption aes-256-gcm-16
		prf sha384
		dh-group 20
IKEv2	AES-256-GCM-16/PRF-SHA384/ECP384	aead
		encryption aes-256-gcm-16
		prf sha384
		dh-group 20
IPsec SA	AES-256-GCM-16	aead
	CHACHA20POLY1305	cypher aes-256-gcm-16

E.10 strong-aead-pfs

Protocol	Encryption	Proposal
IKEv1	AES-256-GCM-16/PRF-SHA384/ECP384	aead

Protocol	Encryption	Proposal
		encryption aes-256-gcm-16 prf sha384 dh-group 20
IKEv2	AES-256-GCM-16/PRF-SHA384/ECP384	aead encryption aes-256-gcm-16 prf sha384 dh-group 20
IPsec SA	AES-256-GCM-16/ECP384 CHACHA20POLY1305-ECP384	aead cypher aes-256-gcm-16 dh-group 20

