

Application Note

Command Line Interface



© 2026 Advantech Czech s.r.o. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photography, recording, or any information storage and retrieval system, without prior written consent. Information in this manual is subject to change without notice and does not represent a commitment by Advantech.

Advantech Czech s.r.o. shall not be liable for any incidental or consequential damages arising from the use, performance, or furnishing of this manual.

All brand names used in this manual are registered trademarks of their respective owners. The use of trademarks or other designations in this publication is for reference purposes only and does not imply endorsement by the trademark holder.

Used symbols



Important

Important — Indicates a risk to personal safety or potential damage to the router. Follow these instructions precisely to prevent injury or equipment damage.



Warning

Warning — Highlights conditions that may cause malfunction, loss of data, or unexpected behavior in specific situations. Read carefully before proceeding.



Info

Info — Provides helpful tips, context, or references that improve understanding but are not strictly required to complete the task.

Firmware Version

This manual applies to firmware version **6.6.2 (July 28, 2026)**. Features introduced after this version may not be covered.

Contents

1. Document Introduction	1
1.1 Document Contents	1
1.2 Command Line Access	2
1.3 Permissions Notes	2
2. Commands	3
2.1 HW Control Commands	4
2.1.1 cdmaat	4
2.1.2 cdmapwr	5
2.1.3 esim	6
2.1.4 gsminfo	7
2.1.5 gsmat	9
2.1.6 gsmat2	9
2.1.7 gsmpwr	10
2.1.8 gsmpwr2	11
2.1.9 gsmsms	11
2.1.10 halt	11
2.1.11 hwclock	12
2.1.12 io	13
2.1.13 led	14
2.1.14 lpm	15
2.1.15 mac	16
2.1.16 port1	16
2.1.17 port2	17
2.1.18 portd	18
2.1.19 pse	20
2.1.20 reboot	21
2.1.21 report	22
2.1.22 sms	23
2.1.23 status	24
2.1.24 stty	27
2.1.25 tpm2	28
2.1.26 xbus	29
2.2 File/Directory Management Commands	30
2.2.1 basename	30
2.2.2 cat	30
2.2.3 cd	31
2.2.4 chdir	31
2.2.5 cmp	32
2.2.6 cp	33
2.2.7 cut	34
2.2.8 dd	35
2.2.9 decode	35
2.2.10 dirname	36
2.2.11 find	36
2.2.12 grep	37
2.2.13 gunzip	38
2.2.14 gzip	38
2.2.15 head	39
2.2.16 jq	40

2.2.17	less	41
2.2.18	ln	42
2.2.19	ls	43
2.2.20	mkdir	44
2.2.21	mv	44
2.2.22	pwd	45
2.2.23	readlink	45
2.2.24	realpath	46
2.2.25	rm	46
2.2.26	rmdir	47
2.2.27	sed	48
2.2.28	shred	49
2.2.29	split	50
2.2.30	sync	50
2.2.31	tail	51
2.2.32	tar	52
2.2.33	touch	53
2.2.34	vi	54
2.2.35	wc	54
2.2.36	xxd	55
2.2.37	zcat	56
2.3	System Commands	57
2.3.1	adduser	57
2.3.2	backup	58
2.3.3	chmod	59
2.3.4	chown	59
2.3.5	chpasswd	60
2.3.6	clog	61
2.3.7	date	61
2.3.8	deluser	62
2.3.9	df	63
2.3.10	dmesg	63
2.3.11	doas	64
2.3.12	faillock	65
2.3.13	free	66
2.3.14	fwupdate	67
2.3.15	id	68
2.3.16	kill	69
2.3.17	killall	69
2.3.18	klog	70
2.3.19	logger	70
2.3.20	losetup	71
2.3.21	mount	72
2.3.22	openssl	73
2.3.23	passwd	74
2.3.24	pidof	75
2.3.25	ps	75
2.3.26	restore	76
2.3.27	rlog	77
2.3.28	slog	77
2.3.29	service	78
2.3.30	sudo	79
2.3.31	sysctl	79
2.3.32	taskset	80
2.3.33	times	80

2.3.34	top	81
2.3.35	umask	82
2.3.36	umount	83
2.3.37	umupdate	83
2.4	Network Commands	84
2.4.1	arp	84
2.4.2	brctl	85
2.4.3	bridge	86
2.4.4	conntrack	88
2.4.5	curl	90
2.4.6	dig	91
2.4.7	dhcrelay	93
2.4.8	ebtables	95
2.4.9	email	97
2.4.10	ether-wake	98
2.4.11	ethtool	99
2.4.12	ftpput	100
2.4.13	hostname	101
2.4.14	ifconfig	102
2.4.15	ip	103
2.4.16	ipcalc	104
2.4.17	iptables	105
2.4.18	iw	106
2.4.19	nc	107
2.4.20	net-snmpinform	108
2.4.21	net-snmptrap	109
2.4.22	netstat	110
2.4.23	nsupdate	111
2.4.24	ntpdate	112
2.4.25	ping	113
2.4.26	ping6	114
2.4.27	route	115
2.4.28	scp	116
2.4.29	sipcalc	118
2.4.30	snmpget	119
2.4.31	snmpset	120
2.4.32	snmptrap	121
2.4.33	ssh	122
2.4.34	tc	123
2.4.35	tcpdump	124
2.4.36	telnet	124
2.4.37	traceroute	125
2.4.38	traceroute6	126
2.4.39	vconfig	127
2.4.40	wget	128
2.5	Scripting/Shell Commands	129
2.5.1	awk	129
2.5.2	break	130
2.5.3	clear	130
2.5.4	continue	130
2.5.5	echo	131
2.5.6	eval	132
2.5.7	exec	133
2.5.8	exit	134
2.5.9	export	135

2.5.10	hash	136
2.5.11	inc	137
2.5.12	let	138
2.5.13	local	139
2.5.14	nohup	140
2.5.15	printf	141
2.5.16	read	142
2.5.17	readonly	143
2.5.18	return	144
2.5.19	shlock	145
2.5.20	set	146
2.5.21	shift	147
2.5.22	sleep	148
2.5.23	source	149
2.5.24	test	150
2.5.25	trap	152
2.5.26	type	153
2.5.27	unset	154
2.5.28	wait	155
2.5.29	watch	156
2.5.30	xargs	157

3. Related Resources 158

Appendix: Command Index 159

List of Tables

1	esim commands	6
2	esim options	6
3	gsminfo output fields	7
4	gsmat options	9
5	gsmat2 options	9
6	gsmpwr commands	10
7	hwclock options	12
8	io options	13
9	led options	14
10	led commands	14
11	lpm options	15
12	port1 options	16
13	port2 options	17
14	portd options	18
15	pse port options	20
16	pse command options	20
17	reboot options	21
18	report options	22
19	sms arguments	23
20	status options	24
21	stty options	27
22	tpm2 subcommands	28
23	xbus commands	29

24	cd options	31
25	cmp options	32
26	cp options	33
27	cut options	34
28	dd options	35
29	find expressions	36
30	grep options	37
31	gunzip options	38
32	gzip options	38
33	head options	39
34	jq options	40
35	less options	41
36	ln options	42
37	ls options	43
38	mkdir options	44
39	mv options	44
40	rm options	46
41	rmdir options	47
42	sed options	48
43	shred options	49
44	split options	50
45	sync options	50
46	tail options	51
47	tar options	52
48	touch options	53
49	vi options	54
50	wc options	54
51	xxd options	55
52	adduser options	57
53	backup options	58
54	chmod options	59
55	chown options	59
56	chpasswd options	60
57	date options	61
58	deluser options	62
59	df options	63
60	dmesg options	63
61	doas options	64
62	faillock options	65
63	free output columns	66
64	fwupdate options	67
65	id options	68
66	kill options	69
67	killall options	69
68	logger options	70
69	losetup options	71
70	mount flags	72
71	mount options	72
72	passwd options	74
73	pidof options	75
74	ps options	75
75	restore options	76
76	slog options	77
77	sysctl options	79
78	taskset options	80

79	top options	81
80	top keys	81
81	umask options	82
82	umount options	83
83	umupdate options	83
84	arp options	84
85	brctl commands	85
86	global bridge options	86
87	bridge link commands	86
88	bridge fdb commands	87
89	bridge vlan commands	87
90	conntrack commands	88
91	conntrack tables	88
92	conntrack options	88
93	expectation options	88
94	conntrack and expectation options	89
95	curl options	90
96	dig options	91
97	dhcrelay options available in DHCPv4 mode only	93
98	dhcrelay options available for both DHCPv4 and DHCPv6	93
99	dhcrelay options available in DHCPv6 mode only:	93
100	ebtables commands	95
101	ebtables options	95
102	email options	97
103	ether-wake options	98
104	ftpput options	100
105	hostname options	101
106	ifconfig options	102
107	ip common options	103
108	ip common objects	103
109	ipcalc options	104
110	iw options	106
111	iw commands	106
112	nc options	107
113	net-snmpinform options	108
114	net-snmptrap options	109
115	netstat options	110
116	nsupdate options	111
117	ntpdate options	112
118	ping options	113
119	ping6 options	114
120	route options	115
121	scp options	116
122	sipcalc – global options	118
123	sipcalc – IPv4 options	118
124	sipcalc – IPv6 options	118
125	snmpget options	119
126	snmpset options	120
127	type options	120
128	snmptrap options	121
129	ssh options	122
130	tc options	123
131	traceroute options	125
132	traceroute6 options	126
133	vconfig commands and options	127

134	wget options	128
135	awk options	129
136	break options	130
137	continue options	130
138	echo options	131
139	eval options	132
140	exec options	133
141	exit options	134
142	export options	135
143	hash options	136
144	inc options	137
145	let options	138
146	local options	139
147	nohup options	140
148	printf format specifiers	141
149	read options	142
150	return options	144
151	commonly used tests	150
152	common signals	152
153	watch options	156
154	xargs options	157

1. Document Introduction

1.1 Document Contents

This document provides a complete list of available **console commands** for Advantech routers. Commands are grouped into the following categories based on their usage:

- **HW Control Commands** — see Chapter [2.1](#).
- **File/Directory Management Commands** — see Chapter [2.2](#).
- **System Commands** — see Chapter [2.3](#).
- **Network Commands** — see Chapter [2.4](#).
- **Scripting/Shell Commands** — see Chapter [2.4](#).

Warning

You may find some commands available on the system that are not documented in this manual. These commands are not intended for regular user operations, and their incorrect use may cause system malfunction.

Info

For a comprehensive list of all commands, please refer to Appendix *Command Index*.

1.2 Command Line Access

The command-line interface (CLI) is a non-GUI alternative that allows you to manage the router. It provides an interactive interface enabling you to perform advanced configurations and troubleshoot the device directly.

SSH Connection

You can use an SSH (Secure Shell) connection to access the router's console. A commonly used application for this is [PuTTY](#). To connect securely without requiring credentials, you can use Passwordless Console Login with a public key. For detailed instructions, refer to the Configuration Manual, Chapter *Administration* → *Modify User* → *Passwordless Console Login*.

Note: Ensure that SSH is enabled under *Configuration* → *Services* → *SSH*.

Web Terminal Router App

The *Web Terminal Router App* allows you to access the router's console directly from the web GUI. This Router App is available for free on the [Engineering Portal](#).

1.3 Permissions Notes

Please note that only a user with the `admin` role is permitted to access the router's console; a user with the `user` role does not have this access.

Commands that modify device status or configuration require privileged mode. When you log in to the console on the `flexible` platform, you are already in privileged mode, indicated by the # symbol on the prompt line.

2. Commands

In the ecosystem of Unix-like operating systems, commands are the essential tools through which users interact with the system, automate tasks, manage resources, and configure services. Whether you are a system administrator, a network engineer, or a software developer, understanding these commands is key to harnessing the full potential of the system.

This chapter covers an array of commands used in daily operations and specialized tasks alike. Scripting and shell command essentials form the backbone of system automation and task scheduling; administration commands ensure system security and integrity; network commands enable configuring, analyzing, and securing network communications; and file and directory management commands provide the means to navigate and manipulate the filesystem. The text processing and analysis commands section demonstrates the power of Unix-like systems in handling textual data — searching, editing, and transforming text in various ways.

Each command entry includes a synopsis, a description of available options, and practical usage examples, catering to both users seeking foundational knowledge and those looking to refine their expertise.

2.1 HW Control Commands

These commands are specific to router and network device management, offering functionalities to configure interfaces, manage routing tables, and control device-specific features.

2.1.1 cdmaat

Info

This command is not supported by routers of *v1* production line.

This command interfaces with a CDMA module to send AT commands, facilitating direct communication and control over the module's functionality. This utility is especially useful for developers and administrators working with CDMA technology for diagnostics, configuration, or testing purposes.

Synopsis:

```
cdmaat <AT command>
```

Description:

`cdmaat` sends specified AT commands to the connected CDMA module, allowing for a wide range of actions, from querying the module status to configuring its settings. The command's ability to interact directly with the CDMA module makes it a powerful tool for advanced device management.

Examples:

Check the signal quality of the CDMA module:

```
cdmaat AT+CSQ
```

Reset the CDMA module:

```
cdmaat ATZ
```

2.1.2 cdmawr

Info

This command is not supported by routers of *v1* production line.

This command controls the power supply to the CDMA module, enabling or disabling it as required. This command is crucial for managing the module's power state, especially for conserving energy or resetting the module.

Synopsis:

```
cdmawr [on | off]
```

Description:

By specifying `on` or `off`, the `cdmawr` command toggles the power state of the CDMA module. Turning the module off can be particularly useful for saving battery life in portable devices or when the module is not in use. Conversely, powering on the module restores its operational state, ready for communication or configuration.

Examples:

Power on the CDMA module:

```
cdmawr on
```

Power off the CDMA module:

```
cdmawr off
```

2.1.3 esim

Info

This command is available only on selected devices, depending on the cellular module used, and is intended for use in customer project deployments.

This command manages eSIM profiles on the eUICC of the cellular module. It can list the installed profiles, download a new profile, and delete, enable, or disable an existing profile.

Synopsis:

```
esim [-h] [-i] list | download <actcode> [<confcode>] | delete <iccid> | enable  
| disable <iccid> | notify
```

Commands:

Command	Description
list	List the eSIM profiles installed on the eUICC, including their status, ICCID, and provider.
download <actcode> [<confcode>]	Download a new eSIM profile from the operator's SM-DP+ server using the activation code. Some operators also require a confirmation code.
delete <iccid>	Delete the profile with the specified ICCID.
enable <iccid>	Enable the profile with the specified ICCID.
disable <iccid>	Disable the profile with the specified ICCID.
notify	Send pending profile management notifications (install, enable, disable, and delete events) to the operator's SM-DP+ server.

Table 1: esim commands

Options:

Option	Description
-h	Format the output as HTML.
-i	Insecure mode — do not verify the HTTPS certificate of the SM-DP+ server.

Table 2: esim options

Examples:

List the installed eSIM profiles:

```
esim list
```

Enable the profile with the given ICCID:

```
esim enable 89440000000000000000
```


2.1.4 gsminfo

This command retrieves and displays detailed information about the cellular module’s status, including signal quality, network registration, and connection details. This tool is invaluable for diagnosing connectivity issues and optimizing signal reception.

Synopsis:

```
gsminfo
```

Description:

`gsminfo` provides a concise overview of the current cellular module’s status, including the signal strength, network operator, and the communication channel. This information aids in assessing the quality of the connection and troubleshooting network problems.

Output Fields:

Field	Description
Manufacturer	Cellular module manufacturer.
Model	Cellular module model designation.
Revision	Firmware revision of the cellular module.
IMEI	International Mobile Equipment Identity number.
ICCID	Integrated Circuit Card Identifier of the active SIM card.
IMSI	International Mobile Subscriber Identity of the active SIM card.
Registration	Current network registration status.
Operator	Name of the mobile network operator.
Technology	Active cellular technology (e.g., LTE, 5G).
PLMN	Public Land Mobile Network code of the operator.
Cell	Identifier of the currently connected cell.
Channel	Channel number used for communication.
Band	Active cellular frequency band.
Signal Strength	Signal strength of the connected cell (dBm).
Signal Quality	Signal quality of the connected cell (dB).
RSSI	Received Signal Strength Indicator (dBm).
RSRP	Reference Signal Received Power (dBm).
RSRQ	Reference Signal Received Quality (dB).
CSQ	Signal strength number (0 to 31).

Table 3: gsminfo output fields

Examples:

Display the current cellular module status:

```
gsminfo
```

Output:

```
Manufacturer      : Quectel
Model             : EC25-EUX
Revision          : EC25EUXGAR08A05M1G
Firmware Release  : EC25EUXGAR08A05M1G_01.001.01.001
IMEI              : 86584_____

ICCID             : 89420310_____
IMSI              : 23003_____
SMS Center        : +420_____
Registration      : Home Network
Operator          : Vodafone CZ
Technology        : LTE
PLMN              : 23003
Cell              : 10A804
TAC               : 947C
Channel           : 1849
Band              : B3
Signal Strength   : -90 dBm
Signal Quality    : -12 dB

RSSI              : -57 dBm
RSRP              : -90 dBm
RSRQ              : -12 dB
CSQ               : 11
```

2.1.5 gsmat

This command sends an AT command to the cellular module.

Synopsis:

```
gsmat [-t <timeout>] <AT command>
```

Options:

Option	Description
-t	The timeout for the response from the cellular module. If not specified, the default value is 10 seconds.

Table 4: gsmat options

Examples:

Determine the type and firmware version of the cellular module.

```
gsmat ATI
```

Determine the IMEI code of the module.

```
gsmat AT+GSN
```

2.1.6 gsmat2

Info

This command is not supported by routers of *v1* production line.

This command sends an AT command to the second cellular module, if one is installed in the router.

Synopsis:

```
gsmat2 [-t <timeout>] <AT command>
```

Options:

Option	Description
-t	The timeout for the response from the cellular module. If not specified, the default value is 10 seconds.

Table 5: gsmat2 options

Examples:

Determine the type and firmware version of the second cellular module.

```
gsmat2 ATI
```

Determine the IMEI code of the second cellular module.

```
gsmat2 AT+GSN
```

2.1.7 gsmppwr

Info

This command is not supported by routers of the v1 production line.

The `gsmppwr` utility is used to control the power supply of the primary cellular module.

Synopsis:

```
gsmppwr on [<sim>] | off | shutdown
```

Commands:

Command	Description
on [<sim>]	Turn on the power for the cellular module. You can optionally specify the SIM card slot (1 or 2) to activate a specific SIM upon power-up.
off	Turn off the power for the cellular module abruptly.
shutdown	Gracefully shut down the cellular module using an AT command and then turn off its power. Please note that execution may take a few seconds.

Table 6: gsmppwr commands

Warning

It is highly recommended to use the `gsmppwr shutdown` command prior to using the `gsmppwr off` command to increase the lifetime of the cellular module.

Examples:

Turn on the cellular module using the first SIM card:

```
gsmppwr on 1
```

Gracefully shut down the cellular module:

```
gsmppwr shutdown
```

Turn off the power for the cellular module abruptly:

```
gsmppwr off
```

2.1.8 gsmpwr2

Info

This command is not supported by routers of the *v1* production line.

The `gsmpwr2` utility is used to control the power supply of the **second** cellular module, provided that the router is equipped with one. Its syntax and behavior are identical to the `gsmpwr` command.

Synopsis:

```
gsmpwr2 on [<sim>] | off | shutdown
```

Warning

It is highly recommended to use the `gsmpwr2 shutdown` command prior to using the `gsmpwr2 off` command to increase the lifetime of the cellular module.

Examples:

Turn on the second cellular module using the first SIM card:

```
gsmpwr2 on 1
```

Gracefully shut down the second cellular module:

```
gsmpwr2 shutdown
```

2.1.9 gsmsms

This program has been deprecated and was removed starting with firmware version 6.6.x. Please use the `sms` command instead, as described in Chapter 2.1.22.

2.1.10 halt

This command shuts down the router so it can be safely powered off. It properly stops all running services, turns off the *PWR* LED, and then waits for 100 seconds, during which the router can be safely unplugged from the power supply. If the router remains powered after this period, it reboots automatically.

Synopsis:

```
halt
```

Example:

Shut down the router for safe power-off:

```
halt
```

2.1.11 hwclock

This command queries and sets the hardware clock (RTC).

Synopsis:

```
hwclock [-swul] [--systz] [-f DEV]
```

Options:

Option	Description
-s	Set the system time from the hardware clock.
-w	Set the hardware clock to the current system time.
--systz	Set the in-kernel timezone and correct the system time if the RTC is kept in local time.
-f DEV	Use the specified RTC device (e.g., <code>/dev/rtc2</code>).
-u	Assume the hardware clock is kept in UTC.
-l	Assume the hardware clock is kept in local time. If neither -u nor -l is specified, the setting is read from <code>/etc/adjtime</code> .

Table 7: hwclock options

Examples:

Display the current hardware clock:

```
hwclock
```

Example output:

```
Wed Apr 22 08:24:52 2026 0.000000 seconds
```

Set the hardware clock to the current system time, assuming UTC:

```
hwclock -w -u
```

Set the system time from the hardware clock:

```
hwclock -s
```

2.1.12 io

This command reads binary inputs and controls binary outputs of the router. If an expansion board is installed, it also supports the router's expansion ports.

Synopsis:

```
io [get <pin>] | [set <pin> <value>]
```

Options:

Option	Description
get	Get the state of the specified input pin.
set	Set the state of the specified output pin.

Table 8: io options

Examples:

Get the state of digital input BIN0.

```
io get bin0
```

Get the state of analog input AN1 on expansion port XC-CNT.

```
io get an1
```

Get the state of counter input CNT1 on expansion port XC-CNT.

```
io get cnt1
```

Set the state of digital output OUT0 to 1.

```
io set out0 1
```

2.1.13 led

Info

This command is not supported by routers of *v1* production line.

This command controls the USR or PWR LED of the router.

Synopsis:

```
led [-p] [-u] <command>
```

Options:

Option	Description
-p	Control of PWR LED
-u	Control of USR LED (default)

Table 9: led options

Commands:

Command	Description
on	Power on the LED.
off	Power off the LED.
slow	Start blinking the LED slowly.
fast	Start blinking the LED fast.

Table 10: led commands

Examples:

Turn on the USR LED:

```
led on
```

Start blinking the USR LED slowly:

```
led slow
```

Control the PWR LED — turn it off:

```
led -p off
```


2.1.14 lpm

Info

This command is not supported by routers of *v1*, *v2*, ICR-2000, ICR-2400, ICR-2500, and ICR-2600 production lines.

This command switches the router into Low Power Mode (LPM) to minimize power consumption. The router can be woken from this state by one of two events: the expiration of a specified time interval or a signal change on a binary input. If both wake-up conditions are configured, the router will wake up as soon as the first event occurs.

Synopsis:

```
lpm [-b] [-i <interval>]
```

Options:

Option	Description
-b	Wakes up the router upon activation of a binary input. The specific input used depends on the router platform: • <i>BIN1</i> for <i>SmartFlex</i>, <i>SmartMotion</i>, <i>ICR-2800</i>, <i>ICR-4200</i>, and <i>ICR-4400</i> platforms. • <i>BIN0</i> for <i>SmartStart</i> and <i>ICR-3200</i> platforms. Note: This option is not supported by routers of the <i>ICR-2700</i> production line.
-i	Wakes up the router after the specified time interval has elapsed. The interval is defined in seconds, ranging from 1 to 16,777,215. The interval represents the duration of the actual low power sleep only; it does not include the time required for system shutdown and startup.

Table 11: lpm options

Examples:

Put the router to sleep for five minutes.

```
lpm -i 300
```

Put the router to sleep, to be woken up by the activation of the binary input.

```
lpm -b
```

Put the router to sleep for a maximum of five minutes. It will wake up sooner if the binary input is activated.

```
lpm -b -i 300
```

2.1.15 mac

This command displays the MAC address of the `eth0` interface.

Synopsis:

```
mac [<separator>]
```

Examples:

Display the MAC address of `eth0` using "-" as the separator instead of the default ":".

```
mac -
```

2.1.16 port1

This command controls the first expansion port.

Synopsis:

```
port1 [on|off|auto|rs232|rs485|type]
```

Options:

Option	Description
on	Turn on the first expansion port.
off	Turn off the first expansion port.
auto	Turn on the first expansion port and set the flow control (CTS signal) to RS232 or RS485 mode depending on the type of the expansion board.
rs232	Turn on the first expansion port and set the flow control (CTS signal) to RS232 mode.
rs485	Turn on the first expansion port and set the flow control (CTS signal) to RS485 mode.
type	Display the type of the expansion board installed (e.g., RS-232 or RS-485).

Table 12: port1 options

Examples:

Enable the first expansion port in RS485 mode:

```
port1 rs485
```

Disable the first expansion port:

```
port1 off
```

Show the type of the installed expansion board:

```
port1 type
```

2.1.17 port2

This command controls the second expansion port.

Synopsis:

```
port2 [on|off|auto|rs232|rs485|type]
```

Options:

Option	Description
on	Turn on the second expansion port.
off	Turn off the second expansion port.
auto	Turn on the second expansion port and set the flow control (CTS signal) to RS232 or RS485 mode depending on the type of the expansion board.
rs232	Turn on the second expansion port and set the flow control (CTS signal) to RS232 mode.
rs485	Turn on the second expansion port and set the flow control (CTS signal) to RS485 mode.
type	Display the type of the expansion board installed (e.g., RS-232 or RS-485).

Table 13: port2 options

Examples:

Enable the second expansion port in RS232 mode:

```
port2 rs232
```

Disable the second expansion port:

```
port2 off
```

Show the type of the installed expansion board:

```
port2 type
```

2.1.18 portd

This program facilitates the transparent transfer of data between a serial line and a network using TCP or UDP protocols. It can operate in two primary modes: as a server that waits for incoming connections, or as a client that connects to a specified host.

Synopsis:

```
portd -c <device> [-b <baudrate>] [-d <databits>] [-p <parity>] [-s <stopbits>]
[-l <split timeout>] [-4] [-h <hostname>] [-o <proto>] -t <port> [-k <keepalive time>]
[-i <keepalive interval>] [-r <keepalive probes>] [-x] [-z] [-j <inactivity timeout>]
[-u <user>] [-n] [-f]
```

Options:

Option	Description
-c <device>	Specifies the serial line device path, e.g., <code>/dev/ttyS0</code> . This option is mandatory.
-b <baudrate>	Sets the communication speed in bits per second (baud rate). Default is 9600.
-d <databits>	Sets the number of data bits. Valid values are 5, 6, 7, or 8. Default is 8.
-p <parity>	Sets the parity. Use 'N' for None, 'E' for Even, or 'O' for Odd. Default is None.
-s <stopbits>	Sets the number of stop bits. Valid values are 1 or 2. Default is 1.
-l <split timeout>	Sets the timeout in milliseconds for data packetization. If the time between consecutive characters received from the serial port exceeds this value, the buffered data is sent as a single network packet. Default is 20 ms.
-4	Forces RS485 mode. This typically involves managing the RTS signal for controlling the line driver.
-h <hostname>	Specifies the hostname or IP address of the remote server to connect to. When this option is used, <code>portd</code> operates in client mode. If omitted, it runs in server mode, listening for incoming connections.
-o <proto>	Sets the communication protocol. Specify <code>tcp</code> or <code>udp</code> . Default is TCP.
-t <port>	Specifies the TCP or UDP port number to listen on (server mode) or connect to (client mode). This option is mandatory.
-k <time>	Sets the TCP keepalive time in seconds. This is the duration of inactivity before the first keepalive probe is sent. A value of 0 disables keepalive.
-i <interval>	Sets the interval in seconds between individual TCP keepalive probes. Default is 10 seconds.
-r <probes>	Sets the number of unacknowledged TCP keepalive probes to send before considering the connection to be dead. Default is 5 probes.
-x	Use Carrier Detect (CD) signal to indicate TCP connection status. The router's DTR pin is asserted (high) when a TCP connection is active and de-asserted (low) when disconnected. This can be used to signal connection status to an attached device.

Table 14: portd options

Option	Description
-z	Use Data Terminal Ready (DTR) signal to control the TCP connection. The program monitors the serial port's CD pin, and if it is de-asserted by the connected device, the TCP connection is terminated.
-j <timeout>	Sets an inactivity timeout in seconds. If no data is transferred over the network socket for this duration, the connection is closed. A value of 0 disables this feature.
-n	Rejects new connections in server mode. If a client is already connected, any new incoming connection attempts will be rejected until the current one is closed.
-u <user>	Specifies a user to drop privileges to after the program has been initialized (e.g., after binding to a privileged port).
-f	Enables hardware flow control (RTS/CTS). The RTS pin is asserted when a network connection is active.

Table 14: portd options (continued)

Examples:

Run a TCP server listening on port 1000. After a client establishes a TCP connection, the program transparently transfers data from the serial port `/dev/ttyS0`, which is configured for 115200 bit/s, 8 data bits, no parity, and 1 stop bit (8N1). The process runs in the background.

```
portd -c /dev/ttyS0 -b 115200 -t 1000 &
```

Run as a TCP client connecting to a server at IP address 192.168.1.100 on port 2000. Data from the local serial port `/dev/ttyS1` (at 9600, 8N1) is forwarded to the remote server. The connection has TCP keepalive enabled with a 60-second idle time.

```
portd -c /dev/ttyS1 -b 9600 -h 192.168.1.100 -t 2000 -k 60 &
```

2.1.19 pse

Info

This program is only supported on models supporting the PoE PSE functionality.

This command enables or disables the PoE PSE feature on the router.

Synopsis:

```
pse [port] [command]
```

port:

port	Description
eth0	Ethernet ETH0 interface (port).
eth1	Ethernet ETH1 interface (port), if equipped on the router.
lanx	Port of an Ethernet switch interface, if equipped on the router. Replace x with a port number.

Table 15: pse port options

command:

command	Description
on	Enable the PoE PSE on the specified interface (port).
off	Disable the PoE PSE on the specified interface (port).

Table 16: pse command options

Examples:

Enable the PoE PSE on the *eth1* Ethernet interface:

```
pse eth1 on
```

Enable the PoE PSE on the *lan2* port of the Ethernet switch interface:

```
pse lan2 on
```

2.1.20 reboot

This command reboots the router.

Synopsis:

```
reboot [-d <delay>] [-n] [-f]
```

Options:

Option	Description
-d	Delay interval in seconds before rebooting.
-n	Do not call <code>sync()</code> before rebooting.
-f	Force reboot without calling shutdown.

Table 17: reboot options

Examples:

Reboot the router immediately:

```
reboot
```

Reboot the router after a 10-second delay:

```
reboot -d 10
```

2.1.21 report

This command generates and displays a diagnostic report for the router.

Warning

Sensitive data from the report are filtered out for security reasons.

Synopsis:

```
report [<options>]
```

Options:

Option	Description
<i>no option</i>	Report all sections except the configuration one.
-a	Report all sections.
-s	Report status section.
-m	Report router apps section.
-l	Report log section.
-c	Report configuration section.

Table 18: report options

Examples:

Generate a full diagnostic report (all sections except configuration):

```
report
```

Generate a report including the configuration section:

```
report -a
```

Generate only the status and log sections:

```
report -s -l
```


2.1.22 sms

This command is used to send an SMS message from the router's cellular module.

Synopsis:

```
sms <phone_number> "<text>"
```

Arguments:

Argument	Description
<phone_number>	The recipient's telephone number. It is recommended to use the international format (e.g., +420123456789).
<text>	The content of the SMS message. The text must be enclosed in double quotes if it contains spaces or special characters.

Table 19: sms arguments

Examples:

Send the SMS `Hello world` to the phone number +420123456789:

```
sms +420123456789 "Hello world"
```

2.1.23 status

This command displays the status of the router's interfaces and system components. It provides information equivalent to what is available on the *General Status* and *Mobile WAN Status* pages in the router's web administration interface.

Synopsis:

```
status [-h] [-v] [eth | geoloc | gnss | vlan | mobile | module | mwan | sim | bard  
| ports | security | sys | hw | usb | wifi ap | wifi sta]
```

Options:

Item	Description
-h	Generates HTML output, which is used when the command is called by the web interface.
-v	Enables verbose mode, which provides more detailed information. Data amounts are shown in bytes only, not in dynamic units (e.g., KB, MB).
eth	Displays the status of Ethernet interfaces (e.g., eth0, eth1), including link state, speed, and data statistics.
geoloc	Displays the router's last known geographical coordinates (latitude and longitude), determined by the GNSS receiver.
gnss	Shows the current status of the GNSS receiver, including the UTC time, fix type (e.g., 2D, 3D), dilution of precision (HDOP), and the number of satellites in use versus in view.
vlan	Lists the status of configured Virtual LAN (VLAN) interfaces, including their names, associated physical interfaces, and VLAN IDs.
mobile	Shows the status of the mobile radio connection, including registration status, operator, network technology (e.g., LTE, 5G), and signal quality metrics.
module	Displays the status of the cellular module(s), which can be module 1, module 2, etc., if available.
mwan	Provides the status of the Mobile WAN network interface, including IP address, DNS servers, and connection uptime.
status sim or status sim 1	Reports daily statistics for the first SIM card, including data usage (RX/TX), connection count, signal history, cell changes, and network availability. status sim is an alias for status sim 1.
status sim 2	Reports the same daily statistics as above, but for the second SIM card.
status sim 1 full or status sim 2 full	Provides a comprehensive statistical report for the specified SIM card (1 or 2). This extended view includes data for multiple time intervals: Today, Yesterday, This Week, Last Week, This Period, and Last Period.
bard	Displays the status of the Backup and Recovery Daemon (BARD), indicating whether it is active and monitoring backup routes.
ports	Shows the status of the router's peripheral ports — the type of the expansion ports (e.g., RS-232, RS-485), the state of the digital inputs and outputs, and the USB port status (on models equipped with a USB port).
security	Shows recent user login activity, including the last successful login, the count of failed login attempts, and the source IP address for each event.
sys	Provides general system information, such as uptime, memory usage, and supply voltage.

Table 20: status options

Item	Description
hw	Displays hardware capabilities of the router, including the presence of wireless modules (Mobile WAN, GNSS, Wi-Fi, Bluetooth) and eSIM support, the number of serial ports, digital inputs and outputs, and USB ports, PoE capabilities (PD/PSE), and the product's designated region.
usb	Displays detailed information about connected USB devices (manufacturer, product, vendor/product ID, class, USB version, speed, and driver), on models equipped with a USB port.
wifi ap	Displays the status of the WiFi Access Point.
wifi sta	Displays the status of the WiFi Station (client) connection.

Table 20: status options (continued)

Examples:

Show the verbose status of the mobile connection:

```
status -v mobile
```

Output:

```
Registration      : Home Network
Operator         : Vodafone CZ
Technology       : LTE
PLMN             : 23003
Cell             : 10A804
TAC              : 947C
Channel          : 1849
Band             : B3
Signal Strength  : -90 dBm
Signal Quality   : -7 dB

RSSI             : -63 dBm
RSRP             : -90 dBm
RSRQ             : -7 dB
SINR             : 18 dB
CSQ              : 11
```

Show the system information:

```
status sys
```

Output:

```
Part Number      : ICR-3211B
Firmware Version : 6.6.0 (2025-12-17)
Serial Number    : ACZ1100000011434
Product Revision : N/A
Profile          : Standard
Free Space       : 696.6 MiB for apps, 450.2 MiB for data
RTC Battery      : Ok
Supply Voltage   : 23.8 V
Temperature      : 37 °C
Time             : 2026-04-13 11:48:30
Uptime           : 112 days, 16 hours, 49 minutes
```

Show the status of the peripheral ports:

```
status ports
```

Output:

```
Expansion Port 1 : RS-232
Expansion Port 2 : RS-485
Digital Input    : On
Digital Output   : Off
USB Port         : disabled
```

Show hardware feature information:

```
status hw
```

Output:

```
Mobile WAN      : 1
eSIM            : 0
GNSS            : 0
WiFi           : 1
Bluetooth       : 0
Serial Ports    : 2
PoE PD          : 0
PoE PSE         : 0
Digital Inputs  : 1
Digital Outputs : 1
USB Ports       : 1
Region          : Outside North America
```

2.1.24 stty

This command prints or changes terminal line settings.

Synopsis:

```
stty [-a|g] [-F DEVICE] [SETTING]...
```

Options:

Option	Description
-F DEVICE	Open device instead of stdin
-a	Print all current settings in human-readable form
-g	Print in stty-readable form
[SETTING]	See manpage

Table 21: stty options

Examples:

Get the current parameters of the first UART serial port:

```
stty -F /dev/ttyS0
```

To only get actual speed of the second UART serial port.

```
stty -F /dev/ttyS1 speed
```

To set parameters of the first UART serial port to:

- speed to 1200 bps
- character size to 7 bits
- 2 stop bits
- disable software output flow control
- reset parameters to system default raw mode

```
stty -F /dev/ttyS0 1200 cs7 cstopb -ixon raw
```

2.1.25 tpm2

Info

TPM features are available only on products that are equipped with a TPM module. TPM support can be verified either in the Hardware Manual or directly in the router console, as described below.

This command provides tools for working with the TPM 2.0 (Trusted Platform Module) chip mounted directly on the router mainboard.

Note: To verify whether TPM functionality is supported on your device, use one of the following procedures:

1. In the router console, execute the following command: `ls /dev/tpm0`
 - If the response is `No such file or directory`, the TPM chip is not available.
 - If the response is `/dev/tpm0`, the TPM chip is available.
2. In the router console, execute the TPM command to display fixed TPM properties: `tpm2 getcap properties-fixed`
 - If multiple error messages are displayed, the TPM chip is not available.
 - If a list of TPM properties is displayed, the TPM chip is available.

Synopsis:

```
tpm2 <subcommand> [<options>...]
```

The table below lists the most important `tpm2` subcommands. For more details about the subcommands, see <https://github.com/tpm2-software/tpm2-tools/tree/5.1.X/man>.

tpm2 subcommands

Subcommand	Description
getcap	Display TPM capabilities in a human readable form.
create	Create a child object.
createek	Generate TCG profile compliant endorsement key.
createak	Generate attestation key with given algorithm under the endorsement hierarchy.
createprimary	Create a primary key.
load	Load an object into the TPM.
loadexternal	Load an external object into the TPM.
readpublic	Read the public area of a loaded object.
evictcontrol	Make a transient object persistent or evict a persistent object.
clear	Clear lockout, endorsement and owner hierarchy authorization values.
getrandom	Retrieve random bytes from the TPM.
hash	Perform a hash operation with the TPM.
hmac	Perform an HMAC operation with the TPM.
sign	Sign a hash or message using the TPM.
verifysignature	Validate a signature using the TPM.
encryptdecrypt	Perform symmetric encryption or decryption.

Table 22: tpm2 subcommands

Subcommand	Description
ecdzhgen	Recover the shared secret value (Z) from a public point and a specified private key.
nvdefine	Define a TPM Non-Volatile (NV) index.
nvundefine	Delete a Non-Volatile (NV) index.
nvread	Read the data stored in a Non-Volatile (NV) index.
nvwrite	Write data to a Non-Volatile (NV) index.

Table 22: tpm2 subcommands (continued)

2.1.26 xbus

This program is primarily used for internal process communication. It can also function as a watchdog for user processes.

Synopsis:

```
xbus [command]
```

xbus commands:

Command	Description
subscribe <topic> [<script>]	Subscribe to a particular topic.
publish <topic> <payload>	Publish the payload for the topic ¹ .
write <topic> <payload>	Publish and store the payload for the topic ¹ .
read <topic>	Read stored payload of the topic.
list	List all the stored topics.

Table 23: xbus commands

Examples:

Set the watchdog for process `user_process` to 10 seconds. If this command is not re-executed within 10 seconds, the router will reboot:

```
xbus write watchdog/proc/user_process "Timeout:10"
```

Suspend the watchdog for process `user_process`:

```
xbus write watchdog/proc/user_process "Timeout:0"
```

¹Do not execute this command more than once per second.

2.2 File/Directory Management Commands

Essential for navigating and manipulating the filesystem, these commands allow users to create, list, modify, and remove files and directories, making them indispensable for day-to-day operations on a Unix-like system.

2.2.1 basename

This command strips the directory path and an optional suffix from a filename.

Synopsis:

```
basename FILE [SUFFIX]
```

Examples:

Strip the directory from the path `/home/myfile.txt`:

```
basename /home/myfile.txt
```

Output:

```
myfile.txt
```

Strip the directory and the `.txt` extension from the path `/home/myfile.txt`:

```
basename /home/myfile.txt .txt
```

Output:

```
myfile
```

2.2.2 cat

This command concatenates files and prints to standard output.

Synopsis:

```
cat [<file>] ...
```

Options:

This command does not support any options.

Examples:

View the contents of the file `/proc/tty/driver/atmel_serial` (serial port information on v2i routers):

```
cat /proc/tty/driver/atmel_serial
```

Output:

```
serinfo:1.0 driver revision:
0: uart:ATMEL_SERIAL mmio:0xF8028200 irq:38 tx:0 rx:0 DSR|CD|RI
1: uart:ATMEL_SERIAL mmio:0xF0004200 irq:37 tx:0 rx:0 DSR|CD|RI
5: uart:ATMEL_SERIAL mmio:0xFFFFF200 irq:36 tx:0 rx:0 CTS|DSR|CD|RI
```

Merge all router configuration files into a single file `/tmp/my.cfg`:

```
cat /etc/settings.* > /tmp/my.cfg
```


2.2.3 cd

This command changes the current working directory.

Synopsis:

```
cd [-P] [-L] [<directory>]
```

Options:

Option	Description
-P	Do not follow symbolic links.
-L	Follow symbolic links (default).

Table 24: cd options

Examples:

Change to the home directory (`/root`):

```
cd
```

Change to the directory `/mnt` :

```
cd /mnt
```

2.2.4 chdir

The `chdir` command is an alias for `cd`. See the [2.2.3 cd](#) command for full documentation.

2.2.5 cmp

The `cmp` utility compares two files of any type and writes the results to the standard output.

Synopsis:

```
cmp [-l] [-s] [-n <num>] <file1> [<file2>]
```

Options:

Option	Description
-l	Print the byte number (decimal) and the differing byte values (octal) for each difference.
-s	Print nothing for differing files; return exit status only.
-n <num>	Compare at most <num> bytes.

Table 25: cmp options

By default, `cmp` is silent if the files are the same; if they differ, the byte and line number at which the first difference occurred is reported. Bytes and lines are numbered beginning with one. If *<file2>* is not specified, standard input is used instead.

Examples:

Compare two files and report the first difference:

```
cmp file1.txt file2.txt
```

Check silently whether two files are identical (useful in scripts):

```
cmp -s file1.bin file2.bin && echo "identical" || echo "differ"
```

2.2.6 cp

This command copies files and directories.

Synopsis:

```
cp [<option>] <source> <dest>
```

Options:

Option	Description
-a	Preserve all attributes.
-R, -r	Copy directories recursively.
-d, -P	Never follow symbolic links.
-H, -L	Follow command-line symbolic links.
-p	Preserve the mode, ownership, and timestamps attributes.
-f	If an existing destination file cannot be opened, remove it and try again.
-i	Prompt before overwrite.
-n	Don't overwrite.
-l, -s	Create (sym)links
-T	Refuse to copy if DEST is a directory
-t DIR	Copy all SOURCES into DIR
-u	Copy only newer files

Table 26: cp options

Examples:

Copy the system log files to the directory `/mnt`:

```
cp /var/log/messages* /mnt
```

Copy configuration profile *Alternative 1* to profile *Standard*:

```
cp -r /etc/alt1/* /etc
```

2.2.7 cut

This command prints selected fields from each input FILE to standard output.

Synopsis:

```
cut [OPTIONS] [FILE]...
```

Options:

Option	Description
-b LIST	Output only bytes from LIST
-c LIST	Output only characters from LIST
-d CHAR	Field delimiter for input (default -f TAB, -F run of whitespace)
-O CHAR	Field delimiter for output (default = -d for -f, one space for -F)
-D	Don't sort/collate sections or match -fF lines without delimiter
-f LIST	Print only these fields (-d is single char)
-s	Output only the lines containing delimiter
-n	Ignored

Table 27: cut options

Examples:

Display the first field of each line, using tab as the field separator:

```
cut -f1 file.txt
```

Display the second field of each line, using colon as the field separator:

```
echo a:b | cut -d: -f2
```

Output:

b

Display the second and all subsequent fields:

```
echo a b c d | cut -d" " -f2-
```

Output:

b c d

Display the third and fourth characters:

```
echo abcd | cut -c3,4
```

Output:

cd

2.2.8 dd

This command copies a file and optionally converts the data format according to the specified operands.

Synopsis:

```
dd [if=FILE] [of=FILE] [bs=N] [count=N] [skip=N] [seek=N]
```

Options:

Option	Description
if=FILE	Read from FILE instead of stdin
of=FILE	Write to FILE instead of stdout
bs=N	Read and write N bytes at a time
count=N	Copy only N input blocks
skip=N	Skip N input blocks
seek=N	Skip N output blocks
N	May be suffixed by c (1), w (2), b (512), kB (1000), k (1024), MB, M, GB, G

Table 28: dd options

Examples:

Erase the microSD card available as `/dev/sda`:

```
dd if=/dev/zero of=/dev/sda bs=4k
```

Create a backup image of a device:

```
dd if=/dev/sda of=/mnt/backup.img bs=1M
```

2.2.9 decode

This command decodes Base64-encoded values. The decoded result is printed to standard output.

Synopsis:

```
decode <base64>
```

Description:

The `decode` command takes a single Base64-encoded string as its argument and prints the decoded value. This is particularly useful for reading encoded values from configuration files.

Examples:

Decode a Base64-encoded string:

```
decode SGVsbG8sIFdvcmxkIQ==
```

Output:

Hello, World!

2.2.10 **dirname**

This command strips the non-directory suffix from a filename.

Synopsis:

```
dirname FILENAME
```

Examples:

Strip the filename from the path `/home/MyFolder/myfile.txt`:

```
dirname /home/MyFolder/myfile.txt
```

Output:

```
/home/MyFolder
```

2.2.11 **find**

This command searches for files in a directory hierarchy.

Synopsis:

```
find [<path> ...] [<expression>]
```

Options:

The default path is the current directory and the default expression is `-print`. Expression may consist of:

Option	Description
<code>-follow</code>	Dereference symbolic links.
<code>-name <pattern></code>	File name (leading directories removed) matches <i><pattern></i> .
<code>-print</code>	Print (default and assumed).
<code>-type X</code>	Filetype matches X (where X is one of: f, d, l, b, c, ...).
<code>-perm <perms></code>	Permissions match any of (+NNN), all of (-NNN), or exactly (NNN).
<code>-mtime <days></code>	Modified time is greater than (+N), less than (-N), or exactly (N) days.
<code>-mmin <mins></code>	Modified time is greater than (+N), less than (-N), or exactly (N) minutes.
<code>-exec <cmd></code>	Execute command with all instances of { } replaced by the files matching <i><expression></i> .

Table 29: find expressions

Examples:

Search for files in the home directory modified in the last 24 hours:

```
find $HOME -mtime 0
```

Search for files with read and write permission for owner and group, but read-only for others:

```
find . -perm 664
```

2.2.12 grep

The `grep` command searches the named input files (or standard input) for lines containing a match to a given pattern. By default, it prints the matching lines. It is an essential tool for parsing logs and filtering command outputs.

Synopsis:

```
grep [options] {PATTERN | -e PATTERN... | -f FILE...} [FILE]...
```

Options:

Option	Description
<code>-H / -h</code>	Print (-H) or suppress (-h) the filename prefix for each match.
<code>-n</code>	Prefix each line of output with its line number.
<code>-l / -L</code>	Show only the names of files that match (-l) or do not match (-L).
<code>-c</code>	Show only a count of matching lines per file.
<code>-o</code>	Show only the matching part of the line, not the entire line.
<code>-q</code>	Quiet mode. Do not write anything to standard output. Returns 0 if found.
<code>-v</code>	Invert the match, selecting non-matching lines.
<code>-s</code>	Suppress error messages about nonexistent or unreadable files.
<code>-r / -R</code>	Recurse through directories (-R also dereferences symlinks).
<code>-i</code>	Ignore case distinctions.
<code>-w / -x</code>	Match whole words only (-w) or whole lines only (-x).
<code>-F</code>	Interpret the pattern as a literal fixed string (not a regular expression).
<code>-E</code>	Interpret the pattern as an extended regular expression.
<code>-m N</code>	Stop reading a file after N matches.
<code>-A N</code>	Print N lines of trailing context (after the match).
<code>-B N</code>	Print N lines of leading context (before the match).
<code>-C N</code>	Print N lines of output context (same as <code>-A N -B N</code>).
<code>-e PTRN</code>	Use PTRN as the pattern. Useful if the pattern begins with a hyphen.
<code>-f FILE</code>	Obtain patterns from FILE, one per line.

Table 30: grep options

Examples:

Find all lines in the system log containing the word `error`:

```
grep error /var/log/messages
```

Search the process list for processes containing the string `ppp`:

```
ps | grep ppp
```

Find the word `error` and print 2 lines of context before and after each match:

```
grep -C 2 "error" /var/log/messages
```

2.2.13 gunzip

This command decompresses a file. If the filename is `-`, data is read from standard input.

Synopsis:

```
gunzip [-c] [-f] [-t] <filename>
```

Options:

Option	Description
-c	Write output to standard output
-f	Force decompression even if the file has multiple links or the corresponding file already exists, or if the compressed data is read from or written to a terminal.
-t	Test. Check the compressed file integrity.

Table 31: gunzip options

Examples:

Decompress the file `test.tar.gz` (creates `test.tar`):

```
gunzip test.tar.gz
```

Decompress and write output to standard output (useful in pipes):

```
gunzip -c test.tar.gz | tar -xf -
```

2.2.14 gzip

This command compresses a file using maximum compression.

Synopsis:

```
gzip [-c] [-d] [-f] <filename>
```

Options:

Option	Description
-c	Write output to standard output
-d	Decompress
-f	Force compression even if the file has multiple links or the corresponding file already exists, or if the compressed data is read from or written to a terminal

Table 32: gzip options

Examples:

Compress the file `test.tar` (creates `test.tar.gz`):

```
gzip test.tar
```

Decompress a file using `gzip`:

```
gzip -d test.tar.gz
```


2.2.15 head

This command prints the first 10 lines of each file to standard output. With more than one file, each output is preceded by a header with the file name. With no file, or when the file is a dash (`-`), read standard input.

Synopsis:

```
head [<option(s)>] [<file(s)>]
```

Options:

Option	Description
-n NUM	Print the first NUM lines instead of the first 10.
-c NUM	Output the first NUM bytes.
-q	Never output headers giving file names.
-v	Always output headers giving file names.

Table 33: head options

Examples:

Display the first 5 lines of the system log:

```
head -n 5 /var/log/messages
```

Display the first 100 bytes of a file:

```
head -c 100 /var/log/messages
```

2.2.16 jq

Info

This command is not supported by routers of *v1* and *v2* production lines.

This command is a powerful tool for processing JSON inputs, applying filters to JSON text, and producing the output as JSON. It can manipulate, filter, and transform structured data.

Synopsis:

```
jq [options] <jq filter> [file...]
```

```
jq [options] --args <jq filter> [strings...]
```

```
jq [options] --jsonargs <jq filter> [JSON_TEXTS...]
```

Options:

Option	Description
-r	Output raw strings, not JSON texts.
-c	Produce compact output instead of pretty-printed output.
-f	Load a jq program from a file.
-arg name value	Pass argument to the filter.

Table 34: jq options

Examples:

Output a JSON object unmodified with pretty-printing:

```
echo '{"foo": 0}' | jq .
```

Extract the value of the key `bar`:

```
echo '{"foo": 0, "bar": 1}' | jq '.bar'
```

Output:

```
1
```

Apply a filter to each element in a JSON array:

```
echo '["foo": 0], {"foo": 1}]' | jq '.[ ] | .foo'
```

2.2.17 less

This command is a terminal pager that displays the contents of a text file one screen at a time. Unlike most pager programs, `less` allows backward as well as forward movement through the file.

Synopsis:

`less [-EFIN] [file] ...` **Options:**

Option	Description
-E	Quit once the end of a file is reached.
-F	Quit if the entire file fits on the first screen.
-I	Ignore case in all searches.
-N	Prefix a line number to each line.
-	Suppress the characters displayed past the end of the file.

Table 35: less options

Examples:

Display the contents of `file.txt`:

```
less file.txt
```

Display `file.txt` with line numbers:

```
less -N file.txt
```

Open `log.txt`, quitting once the whole file fits on the first screen:

```
less -F log.txt
```

2.2.18 ln

This command creates hard or symbolic links between files.

Synopsis:

```
ln [option] <target> ... <link_name> | <directory>
```

Options:

Option	Description
-s	Make symbolic links instead of hard links.
-f	Remove existing destination files.
-n	Do not dereference symlinks — treat like a normal file.
-b	Make a backup of the target (if it exists) before the link operation.
-S	Use the specified suffix instead of <code>~</code> when making backup files.

Table 36: ln options

Examples:

Create a symbolic link named `my.log` pointing to `/var/log/messages`:

```
ln -s /var/log/messages my.log
```

Create a hard link:

```
ln /var/log/messages /tmp/messages.lnk
```

2.2.19 ls

This command lists directory contents.

Synopsis:

```
ls [ option ] < filename > ...
```

Options:

Option	Description
-1	List files in a single column
-A	Do not list implied . and ..
-a	Do not hide entries starting with .
-C	List entries by columns
-c	With -l: show ctime
-d	List directory entries instead of contents
-full-time	List both full date and full time
-i	List the i-node for each file
-l	Use a long listing form
-n	List numeric UIDs and GIDs instead of names
-L	List entries pointed to by symbolic links
-r	Sort the listing in reverse order
-S	Sort the listing by file size
-s	List the size of each file, in blocks
-t	With -l: show modification time
-u	With -l: show access time
-v	Sort the listing by version
-x	List entries by lines instead of by columns
-X	Sort the listing by extension

Table 37: ls options

Examples:

List the contents of the `/mnt` directory in long format:

```
ls -l /mnt
```

List all files including hidden ones in the current directory:

```
ls -a
```

2.2.20 mkdir

This command creates directories.

Synopsis:

```
mkdir [<option>] directory ...
```

Options:

Option	Description
-m	Set permission mode (as in <code>chmod</code>).
-p	No error if the directory already exists; create parent directories as needed.

Table 38: mkdir options

Examples:

Create the directory `/tmp/test/example` , including any missing parent directories:

```
mkdir -p /tmp/test/example
```

2.2.21 mv

This command moves or renames files.

Synopsis:

```
mv [-f] [-fin] <source> ... <dest>
```

Options:

Option	Description
-f	Don't prompt before overwriting
-i	Interactive, prompt before overwrite
-n	Don't overwrite an existing file
-T	Refuse to move if DEST is a directory
-t DIR	Move all SOURCES into DIR

Table 39: mv options

Examples:

Rename the file `abc.txt` to `def.txt` :

```
mv abc.txt def.txt
```

Move all `.txt` files to the directory `/mnt` :

```
mv *.txt /mnt
```

2.2.22 pwd

This command prints the path of the current working directory.

Synopsis:

```
pwd
```

Examples:

Print the path of the current directory, which is `/home/httpd` in this case.

```
pwd
```

Output:

```
/home/httpd
```

Store the current directory path in a variable for later use.

```
DIR=$(pwd)
```

```
echo "Working in: $DIR"
```

Output:

```
Working in: /home/httpd
```

2.2.23 readlink

The `readlink` command is used to display the target of a symbolic link.

Synopsis:

```
readlink FILE
```

Description:

When given a symbolic link as an argument, `readlink` displays the path to which the symlink points. If the specified file is not a symbolic link, `readlink` produces no output.

Examples:

Display the target of the symbolic link `/usr/bin/report`:

```
readlink /usr/bin/report
```

```
/usr/bin/abox
```

2.2.24 realpath

This command returns the absolute pathname of the given filename.

Synopsis:

```
realpath FILE
```

Examples:

Return the absolute pathname of `myfile.txt` located in the current directory (here `/home/MyFolder/`):

```
realpath myfile.txt
```

Output:

```
/home/MyFolder/myfile.txt
```

2.2.25 rm

This command removes files or directories.

Synopsis:

```
rm [-i] [-f] [-r] <file> ...
```

Options:

Option	Description
-i	Always prompt before removing each destination
-f	Remove existing destinations, never prompt
-r	Remove the contents of directories recursively

Table 40: rm options

Examples:

Remove all files with the `.txt` extension in the current directory:

```
rm *.txt
```

Remove the directory `/tmp/test` and all its contents recursively:

```
rm -rf /tmp/test
```


2.2.26 rmdir

This command removes empty directories.

Synopsis:

```
rmdir [-p] [--ignore-fail-on-non-empty] <filename>
```

Options:

Option	Description
-p	Remove the directory and its ancestors; e.g., <code>rmdir -p a/b/c</code> is similar to <code>rmdir a/b/c a/b a</code> .
--ignore-fail-on-non-empty	Ignore each failure that is solely because a directory is non-empty.

Table 41: rmdir options

Examples:

Remove empty directory `/tmp/test`.

```
rmdir /tmp/test
```

Remove directory `/tmp/test` and its parent `/tmp` if both are empty.

```
rmdir -p /tmp/test
```

2.2.27 sed

This command filters and transforms text.

Synopsis:

```
sed [ -e ] [ -f ] [ -i ] [ -n ] [ -r ] pattern [ -files ]
```

Options:

Option	Description
-e	Add the script to the commands to be executed
-f	Add script-file contents to the commands to be executed
-i	Edit files in place (makes backup if extension supplied)
-n	Suppress automatic printing of pattern space
-r	Use extended regular expression syntax

Table 42: sed options

Info

If no `-e` or `-f` is given, the first non-option argument is taken as the sed script to interpret. All remaining arguments are names of input files; if no input files are specified, then the standard input is read. Source files will not be modified unless `-i` option is given.

Examples:

Change the parameter `PPP_APN` in the file `/etc/settings.ppp` to the value `internet`:

```
sed -e "s/\(PPP_APN=\).*\/\1internet/" -i /etc/settings.ppp
```

Delete all blank lines from a file:

```
sed '/^$/d' file.txt
```

2.2.28 shred

This command securely deletes a file from non-volatile memory by overwriting its contents multiple times with patterns designed to maximize data destruction, making recovery difficult even with specialized hardware.

Synopsis:

```
shred [OPTIONS] [FILE]
```

Options:

Option	Description
-f	Change permissions to allow writing if necessary.
-n N	Overwrite N times instead of the default (default is 3 time).
-z	Add a final overwrite with zeros to hide shredding.
-u	Truncate and remove file after overwriting.

Table 43: shred options

Examples:

Overwrite the data of `file1.txt` and `file2.txt` using the default shredding method:

```
shred file1.txt file2.txt
```

Overwrite and then delete `file1.txt`:

```
shred -u file1.txt
```

Overwrite `file1.txt` 10 times:

```
shred -n 10 file1.txt
```

2.2.29 split

This command splits a single file (INPUT) into multiple smaller files. A custom PREFIX for the output filenames can be specified.

Synopsis:

```
split [OPTIONS] [INPUT [PREFIX]]
```

Options:

Option	Description
-b N[k m]	Split the input file into chunks of N (kilo mega)bytes.
-l N	Split the input file by N lines (default is 1000 lines).
-a N	Use N letters as the suffix for output filenames (default is 2 letters).

Table 44: split options

Examples:

Split `file.img` into 50 kB chunks (`xaa`, `xab`, `xac`, ...):

```
split -b 50k file.img
```

Split `file.txt` into files of 200 lines each (`file_a`, `file_b`, ...):

```
split -l 200 -a 1 file.txt file_
```

2.2.30 sync

This command forces an immediate transfer of buffered data blocks in memory (or in specified files) to disk.

Synopsis:

```
sync [OPTIONS] [FILEs]...
```

Options:

Option	Description
-d	Avoid syncing metadata.
-f	Sync the filesystems underlying the specified files.

Table 45: sync options

Examples:

Flush all pending writes to disk:

```
sync
```

Sync only the data of a specific file without updating metadata:

```
sync -d /var/log/messages
```

2.2.31 tail

This command outputs the last part of files.

Synopsis:

```
tail [-n <number>] [-f] [file ...]
```

Options:

Option	Description
-n	Print the last N lines instead of the last 10.
-f	Output appended data as the file grows.

Table 46: tail options

Examples:

Show the last 30 lines of the system log:

```
tail -n 30 /var/log/messages
```

Follow the system log in real time:

```
tail -f /var/log/messages
```

2.2.32 tar

This command creates, extracts, or lists files in a tar archive.

Synopsis:

```
tar -[czxtvok0] [-f tarfile] [-C dir] [file] ...
```

Options:

Option	Description
c	Create an archive.
x	Extract files from an archive.
t	List the contents of an archive.
-f FILE	Name of the archive file, or <code>-</code> for stdin.
-C DIR	Change to directory DIR before performing the operation.
-v	Verbosely list files processed.
-O	Extract to stdout.
-o	Do not restore user:group ownership.
-k	Do not replace existing files.
-z	(De)compress using gzip.
-a	(De)compress based on file extension.
-h	Follow symlinks.

Table 47: tar options

Examples:

Create a `log.tar` archive from the directory `/var/log`:

```
tar -cf log.tar /var/log
```

Extract all files from the archive `log.tar`:

```
tar -xf log.tar
```

Create a compressed archive using gzip:

```
tar -czf log.tar.gz /var/log
```

2.2.33 touch

This command updates the timestamp of a file, or creates an empty file if it does not exist.

Synopsis:

```
touch [-c] [-h] <file> [<file> ...]
```

Options:

Option	Description
-c	Do not create any files.
-h	Do not follow symbolic links.

Table 48: touch options

Examples:

Create an empty file or update the timestamp of `/tmp/test` :

```
touch /tmp/test
```

Update the timestamps of multiple files at once:

```
touch file1.txt file2.txt file3.txt
```

2.2.34 vi

This command opens a text editor for creating or modifying files.

Synopsis:

```
vi [-H] [<file> ...]
```

Options:

Option	Description
-H	List available features.

Table 49: vi options

Examples:

Open the file `/etc/rc.local` for editing:

```
vi /etc/rc.local
```

2.2.35 wc

This command prints newline, word, and byte counts for each file, and a total line if more than one file is specified. With no file, or when the file is a dash (`-`), read standard input.

Synopsis:

```
wc [<option(s)>] [<file(s)>]
```

Options:

Option	Description
-c	Print the byte counts.
-l	Print the newline counts.
-L	Print the length of the longest line.
-w	Print the word counts.

Table 50: wc options

Examples:

Count the number of lines in the system log:

```
wc -l /var/log/messages
```

Count the number of words in a file:

```
wc -w file.txt
```


2.2.36 xxd

`xxd` is a command-line utility that creates a hex dump of a given file or standard input. It can also convert a hex dump back to its original binary form. This tool is commonly used for debugging, examining binary files, and performing binary file analysis.

Synopsis:

```
xxd [-pri] [-g N] [-c N] [-l LEN] [-s OFS] [-o OFS] [FILE]
```

Options:

Option	Description
<code>-g N</code>	Bytes per group
<code>-c N</code>	Bytes per line
<code>-p</code>	Show only hex bytes, assumes <code>-c30</code>
<code>-i</code>	C include file style
<code>-l LENGTH</code>	Show only first LENGTH bytes
<code>-s OFFSET</code>	Skip OFFSET bytes
<code>-o OFFSET</code>	Add OFFSET to displayed offset
<code>-r</code>	Reverse (with <code>-p</code> , assumes no offsets in input)

Table 51: xxd options

Examples:

Generate a hex dump of `file.txt`:

```
xxd file.txt
```

Create a plain hex dump of a binary file:

```
xxd -p file.bin > file.hex
```

Convert a hex dump back to its original binary form:

```
xxd -r file.hex > file.bin
```

2.2.37 zcat

This command displays the contents of gzip-compressed files without explicitly decompressing them first. It is equivalent to running `gunzip -c`.

Synopsis:

```
zcat [file ...]
```

Description:

`zcat` concatenates the uncompressed contents of compressed files to standard output. When no files are specified, or when the filename `-` is used, `zcat` reads from standard input. Since `zcat` is a symlink to `gzip`, additional `gzip` options may be passed.

Examples:

View the contents of a compressed file:

```
zcat file.gz
```

Concatenate and view multiple compressed files:

```
zcat file1.gz file2.gz file3.gz
```

Pipe the contents of a compressed file into `grep`:

```
zcat file.gz | grep 'search_pattern'
```

2.3 System Commands

System administration commands provide the necessary tools for managing users, system services, and hardware settings. They are crucial for maintaining the system’s integrity, security, and performance.

2.3.1 adduser



Warning

Incorrect usage of this command may lead to system malfunction.

The `adduser` command is used to create a new user or add an existing user to a specified group.

Synopsis:

```
adduser [OPTIONS] USER [GROUP]
```

Options:

Option	Description
-s SHELL	Specify the login shell for the new user.
-G GRP	Add the user to the specified group.
	Undocumented options are not recommended for use if you are not sure what you are doing, as their incorrect usage may lead to system malfunction.

Table 52: adduser options

Examples:

Create a new user `john` with the `user` role:

```
adduser -s /bin/false -G users john
```

Create a new user `george` with the `admin` role:

```
adduser -s /bin/sh -G root george
```

2.3.2 backup

This program is used to create a backup of the router configuration. The backup data is written to the standard output (`stdout`) and can be redirected to a file using shell redirection, as shown in the examples below. A previously saved configuration can be restored using the `restore` command; see Chapter 2.3.26 [restore](#) for details.

The backup output is generated in a plain-text, key-value format that is suitable for storage, transfer, and later restoration. Sensitive data can optionally be filtered out or encrypted.

Synopsis:

```
backup [<options>] > <filename>
```

Info

The output filename is specified using shell redirection (`>`), not as a command argument.

Options:

Option	Description
-c	Back up the configuration excluding user account data (default if no option is specified).
-u	Back up only user account data.
-a	Back up the complete configuration, including user accounts, scripts, and Router Apps settings.
-f	Filter sensitive information (passwords, keys, secrets, and passphrases are replaced by ###REMOVED###).
-p <password>	Encrypt the backup using AES-256; the output is Base64 encoded.

Table 53: backup options

Examples:

Back up the complete configuration to a file:

```
backup -a > /tmp/my.cfg
```

Back up only the configuration (without user accounts):

```
backup -c > /tmp/config-only.cfg
```

Back up only user accounts:

```
backup -u > /tmp/users.cfg
```

Back up the configuration while filtering sensitive data:

```
backup -a -f > /tmp/support-safe.cfg
```

Create an encrypted backup:

```
backup -a -p MySecretPass > /tmp/backup.enc
```

View the backup directly on the console:

```
backup -c
```

2.3.3 **chmod**

This command is used to change file and directory permissions (mode bits) in a Unix-like system. It allows you to control who can read, write, or execute a file or directory.

For a detailed explanation of permission modes and their numeric or symbolic notation, see: [chmod\(1\) — Linux manual page](#)

Synopsis:

```
chmod [-R] <mode> <filename>
```

Options:

Option	Description
-R	Change permissions of files and directories recursively.

Table 54: chmod options

Examples:

Make a script executable by its owner and readable by others:

```
chmod 755 /tmp/script.sh
```

Allow full access for the owner and read-only access for others:

```
chmod 744 /tmp/config.cfg
```

Change permissions for all files in a directory recursively:

```
chmod -R 755 /opt/custom
```

2.3.4 **chown**

This command changes the user and/or group ownership of files and directories. It is commonly used by administrators to manage access rights and file control in Unix-like systems.

For detailed usage and syntax, see: [chown\(1\) — Linux manual page](#)

Synopsis:

```
chown [-R] <user>[:<group>] <filename>
```

Options:

Option	Description
-R	Change ownership of files and directories recursively.

Table 55: chown options

Examples:

Change the owner of a file to user `root`:

```
chown root /tmp/config.cfg
```

Change both owner and group of a directory recursively:

```
chown -R admin:admin /opt/custom
```

Change only the group of a file:

```
chown :network /tmp/log.txt
```

2.3.5 chpasswd

This utility updates user passwords non-interactively, which is useful for bulk password updates or use in scripts.

Synopsis:

```
chpasswd [options]
```

Options:

Option	Description
-c, -crypt-method METHOD	Specify the crypt method (one of NONE, DES, MD5, SHA256, SHA512, BCRYPT, YESCRYPT)
-e, -encrypted	Supplied passwords are encrypted
-h, -help	Display this help message and exit
-m, -md5	Encrypt the clear text password using the MD5 algorithm
-R, -root CHROOT_DIR	Directory to chroot into
-P, -prefix PREFIX_DIR	Directory prefix
-s, -sha-rounds	Number of rounds for the SHA, BCRYPT, or YESCRYPT crypt algorithms

Table 56: chpasswd options

Examples:

Update the password for a user, encrypting the password with MD5:

```
chpasswd -m «EOF
username:newpassword
EOF
```

Update the password for a user, providing an already encrypted password:

```
chpasswd -e «EOF
username:encryptedpassword
EOF
```

Update the password for two users, specifying the crypt method to SHA512:

```
chpasswd -c SHA512 «EOF
username:newpassword
username2:newpassword
EOF
```

2.3.6 clog

This command prints the connection log.

Synopsis:

```
clog
```

Examples:

Display the connection log:

```
clog
```

2.3.7 date

This command displays the current date and time in the specified format, or sets the system date and time.

Synopsis:

```
date [-R] [-d <string>] [-s] [-r <file>] [-u] [MMDDhhmm[[CC]YY][.ss]]
```

Options:

Option	Description
-R	Output date and time in RFC 2822 format.
-d <string>	Display the time described by STRING, not the current time.
-s	Set the time described by STRING.
-r <file>	Display the last modification time of FILE.
-u	Print or set Coordinated Universal Time (UTC).

Table 57: date options

Examples:

Display the current date and time:

```
date
```

Set the date and time to December 24, 2011 at 20:00:

```
date 122420002011
```

2.3.8 deluser

Warning

Incorrect usage of this command may lead to system malfunction.

The `deluser` command is used to delete a user from the system.

Synopsis:

```
deluser [--remove-home] USER
```

Description:

The `deluser` command removes the specified user from the system. If the `--remove-home` option is used, the user's home directory and mail spool will also be deleted.

Options:

Option	Description
<code>--remove-home</code>	Remove the user's home directory and mail spool along with the user account

Table 58: deluser options

Examples:

Delete the user `testuser` from the system:

```
deluser testuser
```

Delete the user `testuser` and remove their home directory:

```
deluser --remove-home testuser
```


2.3.9 df

This command reports file system disk space usage.

Synopsis:

```
df [-Pkt] [-t TYPE] [FILESYSTEM ...]
```

Options:

Option	Description
-P	POSIX output format.
-k	Print sizes in kilobytes.
-T	Print the filesystem type.
-t TYPE	Print only mounts of this type.

Table 59: df options

Examples:

Display disk usage for all mounted filesystems:

```
df
```

Display disk usage including filesystem type:

```
df -T
```

2.3.10 dmesg

This command displays kernel log messages.

Synopsis:

```
dmesg [-R] [-T] [-c]
```

Options:

Option	Description
-R	Display relative time since the router booted in <i>sec.nanosec</i> format.
-T	Display human-readable timestamp in <i>YYYY-MM-DD hh:mm:ss</i> format.
-c	Read and clear all messages.

Table 60: dmesg options

Examples:

Display the latest kernel log messages and clear the ring buffer:

```
dmesg -c
```

Display kernel log messages with human-readable timestamps:

```
dmesg -T
```

2.3.11 doas

This command executes commands as another user. The command argument is mandatory unless `-C`, `-L`, or `-s` is specified. The user must authenticate with their password unless configured otherwise.

By default, a new environment is created. The variables `HOME`, `LOGNAME`, `PATH`, `SHELL`, and `USER` and the `umask` are set to values appropriate for the target user. `DOAS_USER` is set to the name of the user executing `doas`. The variables `DISPLAY` and `TERM` are inherited from the current environment. This behavior may be modified by the config file. The working directory is not changed.

Synopsis:

```
doas [-Lns] [-C config] [-u user] command [args]
```

Options:

Option	Description
<code>-L</code>	Clear any persisted authentications from previous invocations, then immediately exit. No command is executed.
<code>-n</code>	Non-interactive mode; fails if the matching rule does not have the <code>nopass</code> option.
<code>-s</code>	Execute the shell from <code>SHELL</code> or <code>/etc/passwd</code> .
<code>-C config</code>	Parse and check the configuration file <i>config</i> , then exit. If a command is supplied, <code>doas</code> will also perform command matching. In the latter case, either <code>permit</code> , <code>permit nopass</code> , or <code>deny</code> will be printed on standard output. No command is executed.
<code>-u user</code>	Execute the command as <i>user</i> . The default is <i>root</i> .

Table 61: doas options

Exit Status:

The `doas` utility exits 0 on success, and > 0 if an error occurs. It may fail for one of the following reasons:

- The config file `/etc/doas.conf` could not be parsed.
- The user attempted to run a command which is not permitted.
- The password was incorrect.
- The specified command was not found or is not executable.

2.3.12 faillock



Info

This command is not supported by routers of *v1* production line.

This program is used to handle user login failures. It allows listing failures for each user, resetting failures, or eventually resetting locked users. Note that this feature is associated with account locking after exceeding the allowed number of unsuccessful login attempts and is not related to the administrative account locking function in the GUI.

Synopsis:

```
faillock [--user username] [--reset] [--legacy-output]
```

Options:

Option	Description
-user username	Apply the command to the specified user.
-reset	Reset the failure records. This can be used to manually unlock accounts or reset the failure count.
-legacy-output	Display output in the legacy format.

Table 62: faillock options

Examples:

View the authentication failure records for all users:

```
faillock
```

View the authentication failure records for the user `john`:

```
faillock --user john
```

john:				
When	Type	Source	Valid	
2024-07-25 12:31:22	RHOST	10.64.0.1	V	
2024-08-22 11:30:30	RHOST	10.64.0.25	V	

Reset the failure records for the user `john`:

```
faillock --user john --reset
```

2.3.13 free

The `free` command displays information about free and used memory, reported in kilobytes (kB).

Synopsis:

```
free
```

Examples:

Display current memory usage:

```
free
```

```
Mem:      total        used        free      shared  buff/cache   available
Swap:      0            0            0            0           0            0
```

The output columns have the following meaning:

Column	Description
total	Total physical memory (in kB).
used	Memory currently used by running processes.
free	Memory that is completely unallocated.
shared	Memory used by temporary shared memory segments.
buff/cache	Memory used by the kernel for buffers and caches. Can be quickly reclaimed when needed.
available	Estimate of memory available for new applications without swapping. Includes free memory and reclaimable buff/cache.

Table 63: free output columns

Difference Between Free and Available Memory

- **Free Memory:** This refers to the portion of RAM that is not being used at all. It is completely idle and unallocated. However, relying solely on this metric can be misleading because modern Linux systems deliberately use much of the free memory for caching to speed up system performance.
- **Available Memory:** This is a more meaningful metric for determining how much memory is truly available for applications. It not only accounts for the free memory but also includes the memory used for caching and buffers that can be quickly reclaimed. Therefore, even if the "free" memory appears low, a high "available" memory indicates that the system can still allocate memory for new processes without resorting to swap space.

2.3.14 fwupdate

This command updates the router's ICR-OS firmware.

Synopsis:

```
fwupdate [-i <filename> [-h] [-n]] [-f] [-c]
```

Options:

Option	Description
-i <filename>	Path to the new ICR-OS firmware file.
-h	Generate HTML output (used when called from the web interface).
-n	Do not reboot after the firmware update.
-f	Finish update procedures (restore configuration, complete firmware switch).
-c	Check firmware update status.

Table 64: fwupdate options

Examples:

Update the firmware from a file on the router:

```
fwupdate -i /tmp/firmware.bin
```

Check the current firmware update status:

```
fwupdate -c
```

2.3.15 id

This command displays user and group information for the specified user, or for the current user if no user is specified.

Synopsis:

```
id [OPTIONS] [USER]
```

Options:

Option	Description
-u	Print the user ID (UID).
-g	Print the primary group ID (GID).
-G	Print all supplementary group IDs.
-n	Print the name instead of the numeric ID (used with -u, -g, or -G).
-r	Print the real ID instead of the effective ID.

Table 65: id options

Examples:

Print the current user’s UID, GID, and supplementary groups:

```
id
```

Print the UID of the current user:

```
id -u
```

Print the primary group name of the current user:

```
id -gn
```

Print all supplementary group names of the current user:

```
id -Gn
```

For a comprehensive guide on the `id` command and its options, consult the man pages or official documentation available on your system or online.

2.3.16 kill

This command sends a signal to a running process, by default SIGTERM which requests graceful termination.

Synopsis:

```
kill [-<signal>] <PID> [<PID> ...]
```

```
kill -l
```

Options:

Option	Description
-l	Print a list of signal names. These are found in <i>/usr/include/linux/signal.h</i> .

Table 66: kill options

Examples:

Terminate the process with PID 1234 gracefully (SIGTERM):

```
kill 1234
```

Force-kill the process with PID 1234 (SIGKILL):

```
kill -9 1234
```

2.3.17 killall

This command sends a signal to all processes matching the specified name, by default SIGTERM.

Synopsis:

```
killall [-q] [-<signal>] <process-name> [<process-name> ...]
```

Options:

Option	Description
-l	Print a list of signal names. These are found in <i>/usr/include/linux/signal.h</i> .
-q	Do not report an error if no processes were found.

Table 67: killall options

Examples:

Terminate all `pppd` processes gracefully (SIGTERM):

```
killall pppd
```

Force-kill all `pppd` processes (SIGKILL):

```
killall -9 pppd
```

2.3.18 klog

This command prints kernel log messages.

Synopsis:

```
klog
```

Examples:

Display the kernel log:

```
klog
```

2.3.19 logger

This program makes entries in the system log. It provides a shell command interface to the system log module.

Synopsis:

```
logger [OPTIONS] [MESSAGE ...]
```

Options:

Option	Description
-s	Log the message to standard error, as well as the system log.
-p <priority>	Enter the message with the specified priority. The priority may be specified numerically or as a facility.level pair.
-t <tag>	Mark every line in the log with the specified tag.

Table 68: logger options

Examples:

Send the message `System rebooted` to the syslog daemon.

```
logger "System rebooted"
```

Send the message `System going down immediately!!!` to the syslog daemon at the emerg level and user facility.

```
logger -p user.emerg "System going down immediately!!!"
```


2.3.20 losetup

This command sets up and controls loop devices.

Synopsis:

`losetup [-rP] [-o OFS] -f|LOOPDEV FILE` : associate loop devices

`losetup -c LOOPDEV` : reread file size

`losetup -d LOOPDEV` : disassociate

`losetup -a` : show status

`losetup -f` : show next free loop device

Options:

Option	Description
-o OFS	Start OFS bytes into FILE
-P	Scan for partitions
-r	Read-only
-f	Show/use next free loop device

Table 69: losetup options

Examples:

Show all active loop device associations:

```
losetup -a
```

Associate the next free loop device with an image file:

```
losetup -f /tmp/image.img
```

Detach the loop device `/dev/loop0`:

```
losetup -d /dev/loop0
```

2.3.21 mount

This command mounts a file system.

Synopsis:

```
mount [-a] [-o] [-r] [-t] [-w] <DEVICE> <NODE> [ -o <option>, ...]
```

Options:

Flag	Description
-a	Mount all filesystems in fstab
-o	One of many filesystem options, listed below
-r	Mount the filesystem read-only
-t	Specify the filesystem type
-w	Mount for reading and writing (default)

Table 70: mount flags

Option	Description
async/sync	Writes are asynchronous / synchronous
atime/noatime	Enable / disable updates to inode access times
dev/nodev	Allow use of special device files / disallow them
exec/noexec	Allow use of executable files / disallow them
suid/nosuid	Allow set-user-id-root programs / disallow them
remount	Re-mount a mounted filesystem, changing its flags
ro/rw	Mount for read-only / read-write
bind	Bind a directory to an additional location
move	Relocate an existing mount point

Table 71: mount options

Info

For a detailed description of this command, refer to the Linux manual pages.

Examples:

Mount a USB flash drive to the directory `/mnt`:

```
mount -t vfat /dev/sda1 /mnt
```

Connect the contents of a USB flash drive formatted with the exFAT file system (e.g., in Microsoft Windows) to the directory `/mnt`:

```
mount -t exfat /dev/sda1 /mnt
```

Mount a filesystem as read-only:

```
mount -r -t ext4 /dev/sda1 /mnt
```

2.3.22 openssl

The `openssl` program is a command-line tool for using the various cryptography functions of the OpenSSL library. It can be used for:

- Creation of RSA, DH, and DSA key parameters
- Creation of X.509 certificates, CSRs, and CRLs
- Calculation of message digests
- Encryption and decryption with ciphers
- SSL/TLS client and server tests
- Handling of S/MIME signed or encrypted mail

Synopsis:

```
openssl [<option> ...]
```

Options:

Info

For a detailed description of this command, refer to the Linux manual pages.

Examples:

Generate a new RSA key for the SSH server:

```
openssl genrsa -out /etc/certs/ssh_rsa_key 512
```

Generate a new self-signed certificate for the HTTPS server:

```
openssl req -new -out /tmp/csr -newkey rsa:1024 -nodes -keyout /etc/certs/https_key  
openssl x509 -req -setstart 700101000000Z -setend 400101000000Z \  
-in /tmp/csr -signkey /etc/certs/https_key -out /etc/certs/https_cert
```

2.3.23 passwd

This command changes user passwords. A user with the *User* role can change only their own password; a user with the *root* role can change passwords for all users.

Synopsis:

```
passwd [options] [LOGIN]
```

Options:

Option	Description
-a, -all	Report password status on all accounts
-d, -delete	Delete the password for the named account
-e, -expire	Force expire the password for the named account
-h, -help	Display this help message and exit
-k, -keep-tokens	Change password only if expired
-i, -inactive INACTIVE	Set password inactive after expiration to INACTIVE
-l, -lock	Lock the password of the named account
-n, -mindays MIN_DAYS	Set minimum number of days before password change to MIN_DAYS
-q, -quiet	Quiet mode
-r, -repository REPOSITORY	Change password in REPOSITORY repository
-R, -root CHROOT_DIR	Directory to chroot into
-P, -prefix PREFIX_DIR	Directory prefix
-S, -status	Report password status on the named account
-u, -unlock	Unlock the password of the named account
-w, -warndays WARN_DAYS	Set expiration warning days to WARN_DAYS
-x, -maxdays MAX_DAYS	Set maximum number of days before password change to MAX_DAYS
-s, -stdin	Read new token from stdin

Table 72: passwd options

Examples:

Change the password for the currently logged-in user `john`:

```
passwd
```

```
Changing password for john.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

Administrator changes the password for user `john` (requires *root* role):

```
passwd john
```

```
New password:
Retype new password:
passwd: password updated successfully
```

2.3.24 pidof

This command lists the PIDs of all processes whose names match those specified on the command line.

Synopsis:

```
pidof <process-name> [<option>] [<process-name> ...]
```

Options:

Option	Description
-s	Display only a single PID.

Table 73: pidof options

Examples:

Find the PID of the `sshd` process:

```
pidof sshd
```

Find a single PID of the `dnsmasq` process:

```
pidof -s dnsmasq
```

2.3.25 ps

This command displays information about currently running processes on the system.

Synopsis:

```
ps [w] [l]
```

Options:

Option	Description
w	Wide output.
l	Long output.

Table 74: ps options

Examples:

Display all running processes:

```
ps
```

Display processes with wide, long output:

```
ps w l
```

2.3.26 restore

This program restores a previously created router configuration from a backup file generated by the `backup` command; see Chapter 2.3.2 [backup](#). The backup file may be either plain text or encrypted.

During restoration, the configuration is validated, optionally decrypted, and then applied to the device.

Synopsis:

```
restore [-p <password>] <filename>
```

Options:

Option	Description
-p <password>	Decrypt the backup file before restoration (required if the backup was created with <code>backup -p</code>).

Table 75: restore options

Notes:

- The `<filename>` must be provided as a normal command argument (unlike `backup`, which uses output redirection).
- If the backup is encrypted, the same password used during backup must be supplied with the `-p` option.
- When the configuration is changed, the system generates an internal *configuration changed* event.

Examples:

Restore a plain-text backup:

```
restore /tmp/my.cfg
```

Restore an encrypted backup:

```
restore -p MySecretPass /tmp/backup.enc
```

Typical output messages returned by `restore`:

- Configuration remains unchanged.
- File not found.
- Decryption of configuration failed.
- Configuration successfully updated.

2.3.27 rlog

This command prints emergency log messages.

Synopsis:

```
rlog
```

Examples:

Display the emergency log:

```
rlog
```

2.3.28 slog

This command prints the system log (file `/var/log/messages`).

Synopsis:

```
slog [-n <number>] [-f]
```

Options:

Option	Description
-n <number>	Print the last N lines instead of the default 10.
-f	Follow the log output as new entries are added.

Table 76: slog options

Examples:

Follow the system log in real time:

```
slog -f
```

Display the last 50 lines of the system log:

```
slog -n 50
```

2.3.29 service

This command starts, stops, or restarts a specified system service.

Synopsis:

```
service <service_name> [start | stop | restart]
```

Info

To list the available services, run: `ls /etc/init.d/`

Examples:

Start the `cron` service:

```
service cron start
```

Restart the `syslog` service:

```
service syslog restart
```

Stop the `ppp` service:

```
service ppp stop
```


2.3.30 sudo

This command is no longer supported by ICR-OS as of version 6.2.8. For compatibility reasons, `sudo` is just a symlink to the `doas` command; see the [2.3.11 doas](#) command.

2.3.31 sysctl

This command lists and modifies kernel parameters at runtime. The available parameters are those listed under `/proc/sys/`.

Synopsis:

```
sysctl -p [-enq] [FILE...] / [-enqaw] [KEY[=VALUE]]...
```

Options:

Option	Description
-p	Set values from FILES (default /etc/sysctl.conf).
-e	Ignore errors about unknown keys.
-n	Disable printing of the key name when printing values.
-q	Quiet mode, don't display the values set to stdout.
-a	Display all values currently available.
-w	Use this option when all arguments prescribe a key to be set.

Table 77: sysctl options

Examples:

Return the value of the `kernel.hostname` parameter without printing the key name:

```
sysctl -n kernel.hostname
```

Output:

Router

Set the value of the `kernel.domainname` parameter:

```
sysctl -w kernel.domainname="example.com"
```

Output:

kernel.domainname = example.com

2.3.32 taskset

Info

This command is available only on the ICR-4xxx routers.

This command sets or retrieves the CPU affinity of a process — the set of CPU cores the process is allowed to run on. It can either launch a new program with the given affinity or change the affinity of an already running process. Pinning a demanding process to specific cores can help balance the system load.

Synopsis:

```
taskset [-ap] [HEXMASK | -c LIST] { PID | PROG ARGS }
```

Options:

Option	Description
-p	Operate on an existing process specified by its PID instead of launching a new program.
-a	Operate on all threads of the process.
-c	Specify the affinity as a list of CPU cores (e.g., 0,2) instead of a hexadecimal mask.

Table 78: taskset options

Examples:

Retrieve the CPU affinity of the process with PID 1234:

```
taskset -p 1234
```

Restrict the process with PID 1234 to CPU cores 0 and 1:

```
taskset -cp 0,1 1234
```

Launch a program restricted to the first CPU core (mask 0x1):

```
taskset 0x1 tcpdump -n -i eth0
```

2.3.33 times

This shell built-in command displays the accumulated user and system times for the current shell and all its child processes. It is useful for evaluating the performance and resource usage of scripts.

Synopsis:

```
times
```

Examples:

Display accumulated shell and child process times:

```
times Output:
```

```
0m0.020s 0m0.070s
```

```
0m0.130s 0m0.260s
```

2.3.34 top

Warning

This command displays only free memory, not available memory. For more information, refer to Chapter [2.3.13 free](#).

This program provides a dynamic real-time view of a running system. It can display system summary information, as well as a list of processes or threads currently being managed by the kernel.

Synopsis:

```
top [-b] [-nCOUNT] [-dSECONDS]
```

Options:

Option	Description
-b	Batch mode - could be useful for sending output from <i>top</i> to other programs or to a file. In this mode, <i>top</i> will not accept input and runs until the iterations limit you've set with the '-n' command-line option, or until killed.
-nCOUNT	Exit after N iterations.
-dSECONDS	Delay between updates in <i>secs</i> format.

Table 79: top options

Keys:

Key	Description
n/m/p/t	Sort by PID / memory / CPU / time.
r	Reverse sort.
q, ^C	Exit.

Table 80: top keys

Examples:

Run `top` in batch mode and exit after 5 iterations:

```
top -b -n5
```

Run `top` and update the output every 10 seconds:

```
top -d10
```

2.3.35 umask

This shell built-in command sets or displays the default file permission creation mask. The umask determines which permissions are *not* set on newly created files and directories.

Synopsis:

```
umask [OPTION]... [MODE]
```

Options:

Option	Description
-S	Display the current umask in symbolic format.
-p	Display the output in a format reusable as input.

Table 81: umask options

Examples:

Display the current umask value:

```
umask
```

Set a new umask so that new files are accessible only by the owner:

```
umask 077
```

Display the current umask in symbolic format:

```
umask -S
```

2.3.36 umount

This command unmounts file systems.

Synopsis:

```
umount [-a] [-r] [-l] [-f] <file system> | <directory>
```

Options:

Option	Description
-a	Unmount all file systems
-r	Try to remount devices as read-only if mount is busy
-l	Lazy unmount (detach filesystem)
-f	Force unmount (i.e. unreachable NFS server)

Table 82: umount options

Examples:

Unmount the filesystem mounted at `/mnt`:

```
umount /mnt
```

Unmount a device by its device path:

```
umount /dev/sda1
```

2.3.37 umupdate

This command installs, updates, or removes a Router App from the command line.

Synopsis:

```
umupdate [-a <filename>] [-d <n>]
```

Options:

Option	Description
-a	Install or update a Router App. Specify the path to the installation file.
-d	Remove an installed Router App with the specified name. The list of installed apps can be obtained with <code>service module list</code> .

Table 83: umupdate options

Examples:

Install a *Python 3* Router App from an installation file:

```
umupdate -a /var/tmp/python3.v3.tgz
```

Remove an installed *Python 3* Router App:

```
~ # ls /opt
fota          log_temp.csv  python3       usrled_mgmt   zabbix_agent
iperf3        pinger        sleepmode     webTerm
~ # umupdate -d python3
```

2.4 Network Commands

Networking commands facilitate the configuration and troubleshooting of network settings. These tools are essential for managing connections, analyzing traffic, and ensuring secure communication over the network.

2.4.1 arp

This program displays and modifies the Internet-to-Ethernet address translation tables used by the address resolution protocol.

Synopsis:

```
arp [-a <hostname>] [-s <hostname> <hw_addr>] [-d <hostname>] [-v] [-n] [-i <if>]
[-D <hostname>] [-A ] [-f <filename>]
```

Options:

Option	Description
-a	The entries will be displayed in alternate (BSD) style.
-s	Manually create an ARP address mapping entry for host hostname with hardware address set to hw_addr.
-d	Remove any entry for the specified host.
-v	Tell the user what is going on by being verbose.
-n	Shows numerical addresses instead of trying to determine symbolic host, port or user names.
-i	Select an interface.
-D	Use the interface ifa’s hardware address.
-f	Similar to the -s option, only this time the address info is taken from the file filename set up. The name of the data file is very often /etc/ethers, but this is not official. If no filename is specified, /etc/ethers is used as default. The format of the file is simple; it only contains ASCII text lines with a hardware address and a hostname separated by whitespace. Additionally, the pub, temp, and netmask flags can be used.

Table 84: arp options

With no flags, the program displays the current ARP entry for hostname. The host may be specified by name or by number, using Internet dot notation. For a detailed description of this command, visit the Linux manual pages.

Examples:

View the ARP table without resolving IP addresses to domain names:

```
arp -n
```

Add a static ARP entry:

```
arp -s 192.168.1.100 00:11:22:33:44:55
```

2.4.2 brctl

Info

The `brctl` command is a legacy utility for managing Ethernet bridges. While retained for backward compatibility, it is considered deprecated. For new configurations, especially those involving VLANs or Distributed Switch Architecture (DSA), it is strongly recommended to use the modern `ip` and `bridge` commands. `brctl` does not support advanced features like VLAN filtering.

This command sets up, maintains, and inspects the Ethernet bridge configuration in the Linux kernel. An Ethernet bridge connects different Ethernet networks, making them appear as a single unified network to all connected devices.

Each connected network segment corresponds to a physical interface added to the bridge. These individual interfaces are bundled into one larger logical network, which corresponds to the bridge network interface itself.

Synopsis:

```
brctl [<command>]
```

Commands:

Command	Parameters	Description
addbr	<bridge>	Creates a new bridge instance.
delbr	<bridge>	Deletes an existing bridge.
addif	<bridge> <device>	Adds a network interface (port) to a bridge.
delif	<bridge> <device>	Removes a network interface from a bridge.
setageing	<bridge> <time>	Sets the Ethernet address ageing time (in seconds).
setbridgepri	<bridge> <priority>	Sets the bridge's priority for STP (Spanning Tree Protocol).
setfd	<bridge> <time>	Sets the bridge's forward delay (in seconds).
sethello	<bridge> <time>	Sets the time between hello packets for STP.
setmaxage	<bridge> <time>	Sets the maximum message age for STP.
setpathcost	<bridge> <port> <cost>	Sets the STP cost of a path via a specific port.
setportprio	<bridge> <port> <priority>	Sets the STP priority for a specific port.
show		Displays a list of all current bridge instances.
showmacs	<bridge>	Displays a list of MAC addresses learned by the bridge.
showstp	<bridge>	Displays the STP status for a bridge.
stp	<bridge> {on off}	Enables or disables the Spanning Tree Protocol on a bridge.

Table 85: brctl commands

Examples:

Create a bridge named `br0` and add interfaces `eth0` and `eth1` to it:

```
brctl addbr br0
```

```
brctl addif br0 eth0
```

```
brctl addif br0 eth1
```

Display the status of all configured bridges:

```
brctl show
```

2.4.3 bridge

Info

The `bridge` command is the modern, feature-rich utility for managing Ethernet bridges and their advanced features, such as VLAN filtering. It is part of the `iproute2` suite and serves as the replacement for the legacy `brctl` command. For all new configurations, the use of `ip` and `bridge` is strongly recommended.

The `bridge` command allows for the configuration and inspection of bridge devices, ports, and VLAN settings. It works in conjunction with the `ip` command, which is used for creating the bridge device itself and for assigning interfaces to it.

Synopsis:

```
bridge [ OPTIONS ] OBJECT { COMMAND | help }
```

Global Options:

Option	Description
-V, -Version	Displays the version of the <code>bridge</code> utility.
-s, -stats	Displays more detailed statistics.
-d, -details	Provides more detailed information in the output.
-j, -json	Displays output in JSON format.
-p, -pretty	Makes JSON output more human-readable.
-o, -oneline	Formats output on a single line, which is useful for scripting.

Table 86: global bridge options

The `bridge` utility operates on several objects. The most common objects are `link`, `mdb`, and `vlan`.

Object: link

The `link` object is used to inspect and configure bridge ports.

Command	Description
show	Displays the status and configuration of all bridge ports.
set dev <port> <args>	Sets various parameters for a specific port. Common arguments include: <code>cost <value></code>: Sets the STP path cost. <code>priority <value></code>: Sets the STP port priority. <code>state <state></code>: Sets the port state (e.g., <code>forwarding</code>). <code>vlan_filtering <0 1></code>: Disables or enables VLAN filtering on the bridge device. Must be set on the bridge interface (e.g., <code>br0</code>), not a port.

Table 87: bridge link commands

Object: fdb

The `fdb` object manages the Forwarding Database, which contains the MAC address table for the bridge.

Command	Description
<code>show [dev <bridge>]</code>	Displays the FDB entries (MAC table) for a given bridge.
<code>add <MAC> dev <port></code>	Adds a permanent (static) MAC address entry to the FDB, associating it with a specific port.
<code>delete <MAC> dev <port></code>	Removes a MAC address entry from the FDB.
<code>append <MAC> dev <port></code>	Appends a static FDB entry that is externally learned.

Table 88: bridge fdb commands

Object: vlan

The `vlan` object is used to configure VLAN filtering on bridge ports, which is a key feature not available in `brctl`. VLAN filtering must first be enabled on the bridge device itself using

```
bridge link set dev <bridge> vlan_filtering 1
```

Command	Description
<code>show [dev <port>]</code>	Displays the VLAN configuration for all ports or for a specific port.
<code>add vid <ID> dev <port> [pvid] [untagged]</code>	Adds a VLAN to a port. <code>vid <ID></code>: The VLAN ID to add. <code>pvid</code>: Marks this VLAN as the Port VLAN ID (native VLAN). Ingress untagged traffic is assigned to this VLAN. <code>untagged</code>: Egress traffic for this VLAN will be sent untagged.
<code>delete vid <ID> dev <port></code>	Removes a VLAN from a port.

Table 89: bridge vlan commands

Examples:

Create a bridge, add ports, and bring it up. This uses the `ip` command, which is standard practice.

```
ip link add name br0 type bridge Create a bridge device named br0
ip link set dev eth0 master br0 Add eth0 to the bridge
ip link set dev eth1 master br0 Add eth1 to the bridge
ip link set dev br0 up Bring the bridge interface up
```

Enable VLAN filtering on the bridge and configure VLANs on its ports.

```
bridge link set dev br0 vlan_filtering 1 Enable VLAN awareness
bridge vlan add vid 100 dev eth1 Allow tagged VLAN 100 on eth1
bridge vlan add vid 200 dev eth2 pvid untagged Allow untagged VLAN 200 on eth2 (native VLAN)
```

Display the VLAN configuration for the bridge.

```
bridge vlan show
```

2.4.4 conntrack

This program is the user interface to the netfilter connection tracking system.

Synopsis:

```
conntrack [commands] [option]
```

Options:

Command	Description
-L [table] [option]	List conntrack or expectation table
-G [table]	Get conntrack or expectation
-D [table]	Delete conntrack or expectation
-I [table]	Create a conntrack or expectation
-U [table]	Update a conntrack
-E [table]	Show events
-F [table]	Flush table

Table 90: conntrack commands

Table	Description
conntrack	This is the default table. It contains a list of all currently tracked connections through the system.
expect	This is the table of expectations. Connection tracking expectations are the mechanism used to "expect" RELATED connections to existing ones.

Table 91: conntrack tables

Option	Description
-n <ip>	Source NAT ip
-g <ip>	Destination NAT ip
-m <mark>	Set mark
-e <eventmask>	Event mask, eg. NEW,DESTROY
-z	Zero counters while listing
-o <type[...]>	Output format, eg. xml

Table 92: conntrack options

Option	Description
--tuple-src <ip>	Source address in expect tuple
--tuple-dst <ip>	Destination address in expect tuple
--mask-src <ip>	Source mask address
--mask-dst <ip>	Destination mask address

Table 93: expectation options

Option	Description
-s <ip>	Source address from original direction
-d <ip>	Destination address from original direction
-r <ip>	Source address from reply direction
-q <ip>	Destination address from reply direction
-p <proto>	Layer 4 Protocol, eg. 'tcp'
-f <proto>	Layer 3 Protocol, eg. 'ipv6'
-t <timeout>	Set timeout
-u <status>	Set status, eg. ASSURED

Table 94: conntrack and expectation options

Examples:

Display the content of the conntrack table:

```
conntrack -L
```

Flush (delete) all entries from the conntrack table:

```
conntrack -F
```

2.4.5 curl

`curl` (Client URL) is a versatile tool for transferring data to or from a server. It supports HTTP, HTTPS, and FTP/FTPS. It is often used as a more feature-rich alternative to `wget` (see Chapter 2.4.40).

Curl is an extremely powerful tool with hundreds of options. For complete documentation, type `curl --help` or visit the online manual: [curl.1 the man page](#)

Synopsis:

```
curl [options...] <url>
```

Common Options:

Option	Description
<code>-o <file></code>	Write the output to a specified file instead of stdout.
<code>-O</code>	Write output to a local file named like the remote file we get.
<code>-I</code>	Fetch the HTTP-header only. Useful for checking if a link is alive or seeing server information.
<code>-L</code>	If the server reports that the requested page has moved to a different location (3xx error), this option will make curl redo the request on the new place.
<code>-k</code>	Allow insecure connections (ignore SSL certificate issues). Common on local networks with self-signed certificates.
<code>-u <user:pwd></code>	Specify the user name and password to use for server authentication.

Table 95: curl options

Examples:

Download a file, keeping the remote filename:

```
curl -O https://downloads.example.com/firmware.bin
```

Check HTTP response headers without downloading the page:

```
curl -I https://www.google.com
```

Output:

```
HTTP/2 200 OK
```

```
Content-Type: text/html; charset=ISO-8859-1
```

Call a web API with authentication (e.g., for Dynamic DNS update):

```
curl -u "admin:password123" "https://api.service.com/update?ip=1.2.3.4"
```

2.4.6 dig

This command is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers returned by the queried servers in a human-readable format. The output includes the question section, answer section, authority section, and additional section as appropriate.

The `dig` utility supports both IPv4 and IPv6 queries, various query types (A, AAAA, MX, NS, TXT, etc.), and advanced DNS features like DNSSEC validation, EDNS options, and encrypted transports (DoH/DoT).

For complete documentation of all options including extensive debug flags (+d-opt), query classes, and advanced features, see: [dig\(1\) — Arch Linux manual page](#)

Info

The `dig` tool was added in firmware version 6.6.1.

Synopsis:

```
dig [@global-server] [domain] [q-type] [q-class] {q-opt}
    {global-d-opt} host [@local-server] {local-d-opt}
    [ host [@local-server] {local-d-opt} [...] ]
```

Note: Global debug options (before hostname) affect all queries. Local debug options (after hostname) apply only to that specific lookup. Default query class is `in` and type is `a`.

Options:

Option	Description
-4	Use IPv4 query transport only.
-6	Use IPv6 query transport only.
-b address[#port]	Bind to source address/port.
-c class	Specify query class (in,hs,ch,...).
-f filename	Batch mode - read queries from filename.
-h	Print help and exit.
-k keyfile	Specify TSIG key file.
-m	Enable memory usage debugging.
-p port	Specify port number.
-q name	Specify query name.
-r	Do not read ~/.digrc.
-t type	Specify query type (a,mx,ns,soa,...).
-u	Display times in microseconds instead of milliseconds.
-v	Print version and exit.
-x dot-notation	Shortcut for reverse lookups (PTR queries).
-y [hmac:]name:key	Specify named base64 TSIG key.

Table 96: dig options

Examples:

Basic domain lookup (A record):

```
dig example.com
```

Specify nameserver and query type:

```
dig @8.8.8.8 example.com MX
```

IPv6-only AAAA query

```
dig -6 example.com AAAA
```

Reverse DNS lookup using shortcut

```
dig -x 93.184.216.34
```

Custom port and query class

```
dig -p 5353 chaos.example.com CH TXT
```

DNSSEC validation with trace

```
dig +trace +dnssec example.com
```

Multiple queries with different options

```
dig google.com +short A
```

DNS over HTTPS

```
dig +https example.com
```

Show statistics and memory usage

```
dig -m example.com +stats +multiline
```

2.4.7 dhcrelay

The Dynamic Host Configuration Protocol (DHCP) Relay Agent, `dhcrelay`, provides a means for relaying DHCP and BOOTP requests from a subnet to which no DHCP server is directly connected to one or more DHCP servers on other subnets. It supports both DHCPv4/BOOTP and DHCPv6 protocols (v3 routers only).

Synopsis:

```
dhcrelay [-4] [-d] [-q] [-a] [-D] [-A <length>] [-c <hops>] [-p <port>]
[-pf <pid-file>] [--no-pid] [-m append|replace|forward|discard]
[-i interface0 [ ... -i interfaceN] server0 [ ... serverN]
dhcrelay -6 [-d] [-q] [-I] [-c <hops>] [-p <port>] [-pf <pid-file>] [--no-pid]
-l lower0 [ ... -l lowerN] -u upper0 [ ... -u upperN]
```

Options:

Option	Description
-a	Append an agent option field to each request before forwarding it to the server. Agent option fields in responses sent from servers to clients will be stripped before forwarding such responses back to the client.
-A <length>	Specify the maximum packet size to send to a DHCPv4/BOOTP server. This might be done to allow sufficient space for addition of relay agent options while still fitting into the Ethernet MTU size.
-D	Drop packets from upstream servers if they contain Relay Agent Information options that indicate they were generated in response to a query that came via a different relay agent.
-i <ifname>	Listen for DHCPv4/BOOTP queries on interface ifname. Multiple interfaces may be specified by using more than one -i option. If no interfaces are specified on the command line, <code>dhcrelay</code> will identify all network interfaces, eliminating non-broadcast interfaces if possible, and attempt to listen on all of them.
-m <option>	Control the handling of incoming DHCPv4 packets which already contain relay agent options.

Table 97: `dhcrelay` options available in DHCPv4 mode only

Option	Description
-c <hops>	Maximum hop count. When forwarding packets, <code>dhcrelay</code> discards packets which have reached a hop count of <hops>. Default is 10. Maximum is 255.
-d	Force <code>dhcrelay</code> to run as a foreground process.
-p <port>	Listen and transmit on port <port>. Default is port 67 for DHCPv4, or port 547 for DHCPv6.
-q	Quiet mode.

Table 98: `dhcrelay` options available for both DHCPv4 and DHCPv6

Option	Description
-I	Force use of the DHCPv6 Interface-ID option. This option is automatically sent when there are two or more downstream interfaces in use, to disambiguate between them.
-l	Specifies the "lower" network interface for DHCPv6 relay mode: the interface on which queries will be received from clients or from other relay agents.
-u	Specifies the "upper" network interface for DHCPv6 relay mode: the interface to which queries from clients and other relay agents should be forwarded.

Table 99: `dhcrelay` options available in DHCPv6 mode only:

For help in command line type `dhcrelay -h`. For more information on this command, look up the man page on the Internet.

Warning

It is necessary to set at least **two interfaces** for sending/listening – see an Example below.

Examples:

Relay DHCP requests from interfaces `eth0` and `eth1` to a DHCP server: "upstream" server `<server ip>`. When a reply is received from upstream, it is multicast or unicast back downstream to the source of the original request.

```
dhcrelay -i eth1 -i eth0 <server ip>
```


2.4.8 ebtables

This program can be used as an administration tool for firewall IP packets filtering. It enables transparent filtering of network traffic passing through a Linux bridge. The filtering possibilities are limited to link layer filtering and some basic filtering on higher network layers. Advanced logging, MAC DNAT/SNAT and router facilities are also included.

The `ebtables` tool can be combined with the other filtering tools (`iptables` and `ip6tables`) to make a bridging firewall that is also capable of filtering these higher network layers.

Synopsis:

```
ebtables -[ADI] chain rule-specification [options]
```

```
ebtables -P chain target
```

```
ebtables -[LFZ] [chain]
```

```
ebtables -[NX] [chain]
```

```
ebtables -E old-chain-name new-chain-name
```

Commands:

Option	Description
<code>-append -A chain</code>	append to chain
<code>-delete -D chain</code>	delete matching rule from chain
<code>-delete -D chain rulenum</code>	delete rule at position rulenum from chain
<code>-change-counters -C chain [rulenum] pcnt bcnt</code>	change counters of existing rule
<code>-insert -I chain rulenum</code>	insert rule at position rulenum in chain
<code>-list -L [chain]</code>	list the rules in a chain or in all chains
<code>-flush -F [chain]</code>	delete all rules in chain or in all chains
<code>-init-table</code>	replace the kernel table with the initial table
<code>-zero -Z [chain]</code>	put counters on zero in chain or in all chains
<code>-policy -P chain target</code>	change policy on chain to target
<code>-new-chain -N chain</code>	create a user defined chain
<code>-rename-chain -E old new</code>	rename a chain
<code>-delete-chain -X [chain]</code>	delete a user defined chain
<code>-atomic-commit</code>	update the kernel w/t table contained in <FILE>
<code>-atomic-init</code>	put the initial kernel table into <FILE>
<code>-atomic-save</code>	put the current kernel table into <FILE>
<code>-atomic-file file</code>	set <FILE> to file

Table 100: ebtables commands

Options:

Option	Description
<code>-proto -p [!] proto</code>	protocol hexadecimal, by name or LENGTH
<code>-src -s [!] address[/mask]</code>	source mac address
<code>-dst -d [!] address[/mask]</code>	destination mac address
<code>-in-if -i [!] name[+]</code>	network input interface name
<code>-out-if -o [!] name[+]</code>	network output interface name

Table 101: ebtables options

Option	Description
-logical-in [!] name[+]	logical bridge input interface name
-logical-out [!] name[+]	logical bridge output interface name
-set-counters -c chain pcnt bcnt	set the counters of the to be added rule
-modprobe -M program	try to insert modules using this program
-concurrent	use a file lock to support concurrent scripts
-version -V	print package version

Table 101: ebtables options (continued)

Environment variable:

EBTABLES_ATOMIC_FILE – if set <FILE> (see above) will equal its value

Standard targets: DROP, ACCEPT, RETURN or CONTINUE;

The target can also be a user defined chain.

Supported chains for the filter table:

INPUT FORWARD OUTPUT

2.4.9 email

The program can be used for sending email.

Warning

To work properly, this command requires the SMTP service to be configured correctly. Refer to the *Configuration Manual* of your router, chapter *Configuration* → *Services* → *SMTP*.

Synopsis:

```
email -t <to> [-s <subject>] [-m <message>] [-a <attachment>] [-r <retries>]
```

Options:

Option	Description
-t	E-mail address of the recipient
-s	Subject, enter the subject in quotation marks
-m	Message, enter the message in quotation marks
-a	Attachment file of the email
-r	Number of attempts to send the e-mail (default value: 2)

Table 102: email options

Examples:

Send the system log as an email attachment:

```
email -t john.doe@email.com -s "System Log" -a /var/log/messages
```

2.4.10 ether-wake

This command sends a Wake-on-LAN (WoL) Magic Packet to a network interface, which can wake up sleeping machines that support this feature. The target machine is identified by its MAC address.

Synopsis:

```
ether-wake [-b] [-i IFACE] [-p aa:bb:cc:dd[:ee:ff]] MAC
```

Options:

Option	Description
MAC	The MAC address of the network card of the machine to be woken up. The address must be specified in the format <code>00:11:22:33:44:55</code> .
-b	Broadcasts the Magic Packet to all devices on the network segment.
-i IFACE	Specifies the network interface through which the Magic Packet will be sent. If not specified, the default interface is <code>eth0</code> .
-p PASSWORD	Appends a four or six-byte password to the Magic Packet for systems that require a SecureON password. The password should be specified in a MAC-like hex format, separated by colons.

Table 103: ether-wake options

Examples:

Wake up a machine using the default `eth0` interface:

```
ether-wake 00:11:22:33:44:55
```

Wake up a machine, sending the packet through the `eth1` interface.

```
ether-wake -i eth1 00:11:22:33:44:55
```

Broadcast a Magic Packet to wake up a machine with a specific MAC address.

```
ether-wake -b 00:11:22:33:44:55
```

Wake up a machine that requires a six-byte SecureON password.

```
ether-wake -p 11:22:33:44:55:66 00:11:22:33:44:55
```

2.4.11 ethtool

This command displays or modifies Ethernet interface settings.

Synopsis:

```
ethtool [<option> ...] <devname> [<commands>]
```

Options:

For a detailed description of this command, refer to the Linux manual pages.

Examples:

View the status of the interface `eth0`:

```
ethtool eth0
```

Set interface `eth0` to 10 Mbit/s half duplex:

```
ethtool -s eth0 speed 10 duplex half autoneg off
```

Enable autonegotiation on interface `eth0`:

```
ethtool -s eth0 autoneg on
```

2.4.12 **ftpput**

This command facilitates uploading files to an FTP server. It is designed for simplicity and embedded environments, offering essential functionality for transferring files over FTP.

Synopsis:

```
ftpput [OPTIONS] HOST [REMOTE_FILE] LOCAL_FILE
```

Description:

This command uploads LOCAL_FILE from the local system to the specified HOST. The file on the host can be specified with [REMOTE_FILE]; if not provided, the name of the LOCAL_FILE is used on the remote server.

Options:

Option	Description
-v	Enables verbose output, providing additional details during the file transfer process.
-u USER	Specifies the username for authentication with the FTP server.
-p PASS	Specifies the password for authentication with the FTP server.
-P PORT	Specifies the port on which to connect to the FTP server. If not provided, the standard FTP port (21) is used.

Table 104: ftpput options

Examples:

Upload a file to an FTP server:

```
ftpput -u username -p password ftp.example.com /remote/path/file.txt
```

Upload a file with verbose output:

```
ftpput -v -u username -p password -P 21 ftp.example.com /remote/file.txt
```

For more detailed information about using ftpput, refer to the official BusyBox documentation or the built-in help by executing ftpput --help in the terminal.

2.4.13 hostname

Info

Go to *Configuration* → *System* → *Identification* in the router GUI if you want to change the hostname.

The `hostname` command is used to display the system's network name. In a network environment, this name helps to identify the router among other devices.

On this system, the `hostname` command is used solely for viewing the name. It finishes execution immediately and returns you to the shell prompt.

Synopsis:

```
hostname [-b]
```

Options:

Option	Description
<code>-b</code>	Set hostname to 'localhost' if it is otherwise unset/empty (boot default).

Table 105: hostname options

Examples:

Display the current hostname:

```
hostname
```

Output:

```
Router
```

2.4.14 ifconfig

The `ifconfig` (interface configurator) utility is used to display or configure network interfaces. It allows you to assign IP addresses, enable or disable interfaces, and manage settings like MTU or promiscuous mode.

Note: Changes made with `ifconfig` are immediate but temporary. They will be lost after a system reboot unless they are also updated in the router's permanent configuration files or via the GUI.

Synopsis:

```
ifconfig [-a] <interface> [<option> ...]
```

Options:

Option	Description
up	Activate the specified interface.
down	Shut down the driver for the specified interface.
netmask <addr>	Set the IP network mask for this interface.
broadcast <addr>	Set the protocol broadcast address for this interface.
mtu <NN>	Set the Maximum Transfer Unit (MTU) of an interface.
promisc	Enable or disable (-promisc) promiscuous mode. If enabled, all packets on the network will be received by the interface.
txqueuelen <NN>	Set the length of the transmit queue of the device.

Table 106: ifconfig options

Examples:

View the status of all active interfaces:

```
ifconfig
```

Output:

```
eth0  Link encap:Ethernet  HWaddr 00:11:22:33:44:55
      inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      ...
```

Set an IP address and bring up the interface:

```
ifconfig eth1 10.0.0.1 netmask 255.255.255.0 up
```

Create a virtual interface alias with a second IP address:

```
ifconfig eth0:0 192.168.2.1 netmask 255.255.255.0 up
```

Disable the `eth1` interface:

```
ifconfig eth1 down
```


2.4.15 ip

The `ip` command is a powerful tool for network interface configuration, routing, and tunnel management. It serves as a modern replacement for the older `ifconfig`, `route`, and `arp` utilities.

For complete documentation of all sub-commands and advanced networking features (tunnels, xfrm, policy routing), see [ip-address\(8\) — Arch Linux manual page](#).

Synopsis:

```
ip [options] <object> command | help
```

Common Options:

Option	Description
-s	Statistics. Output more information (e.g., packet counts). Repeat for more detail.
-o	Oneline. Output each record on a single line for easier parsing with <code>grep</code> or <code>awk</code> .
-4 / -6	Shortcut for IPv4 or IPv6 protocol family.

Table 107: ip common options

Common Objects:

Object	Description
link	Network device (e.g., <code>eth0</code> , <code>wlan0</code>). Used to bring interfaces up or down.
addr	IP addresses assigned to devices.
route	Routing table entries.
neigh	ARP or NDISC cache entries (neighbor management).

Table 108: ip common objects

Examples:

Display all interfaces and their IP addresses:

```
ip addr show
```

Display the routing table:

```
ip route list
```

Add a static route via a gateway:

```
ip route add 192.168.3.0/24 via 192.168.1.2
```

Bring the `eth1` interface down:

```
ip link set eth1 down
```

2.4.16 ipcalc

The `ipcalc` utility is used to calculate and display network settings based on an IP address and a netmask or prefix length. It is an essential tool for verifying subnetting and determining broadcast or network addresses.

Synopsis:

```
ipcalc [-bnmphps] ADDRESS[/PREFIX] [NETMASK]
```

Description:

`ipcalc` takes an IP address, and optionally a slash notation prefix or a netmask, and calculates the resulting broadcast, network, netmask, and IP prefix. It simplifies network configuration and planning tasks.

Options:

Option	Description
-b	Display the broadcast address for the given network.
-n	Calculate and display the network address.
-m	Display the netmask for the provided IP address/prefix.
-p	Show the prefix length (e.g., /24).
-h	Display the hostname (via reverse DNS lookup).
-s	Silent mode. Suppress error messages.

Table 109: ipcalc options

Examples:

Calculate the broadcast address, network address, and netmask for a /24 subnet:

```
ipcalc -bnm 192.168.1.100/24
```

Output:

```
NETMASK=255.255.255.0
BROADCAST=192.168.1.255
NETWORK=192.168.1.0
```

Example #2: Determine prefix length from a netmask
If you have a traditional netmask and need the CIDR prefix notation.

```
ipcalc -p 192.168.1.100 255.255.255.0
```

Output:

```
PREFIX=24
```

Example #3: Get only the netmask
Useful for scripts that need to extract a specific value.

```
ipcalc -m 192.168.1.100/26
```

Output:

```
NETMASK=255.255.255.192
```

2.4.17 iptables

The `iptables` utility is the administration tool for IPv4 packet filtering and NAT (Network Address Translation). It allows you to configure tables, chains, and rules that manage how the router handles incoming, outgoing, and forwarded traffic.

Iptables is a vast subject. For a detailed description of all commands, targets, and match extensions, refer to the official manual pages: [iptables\(8\) — Linux manual page](#)

Synopsis:

```
iptables [-t table] [command] [chain] [match] [target]
```

Key Features & Supported Modules:

- **DSCP & QoS:** Supports `DSCP` target and `dscp` match for Quality of Service (QoS) configurations based on packet marking.
- **CONNMARK:** Allows marking entire connections rather than just individual packets. This is useful for complex routing and traffic shaping where only the first packet of a session needs to be inspected.
- **String Match:** Supports searching for specific text patterns within packets using the `string` extension.
- **U32 Match:** An advanced module for matching arbitrary bytes at any offset within a packet.
- **Statistic Module:** Matches packets based on statistical conditions (e.g., matching every *n*-th packet or using a random probability).

To see which modules are currently available on your system, check the proc filesystem:

```
cat /proc/net/ip_tables_matches
```

Examples:

Port forwarding (DNAT) — redirect TCP port 8080 to an internal server:

Redirect incoming TCP traffic from port 8080 to an internal server at 192.168.1.11 on port 80.

Add DNAT rule

```
iptables -t nat -A pre_nat -p tcp --dport 8080 -j DNAT --to-destination 192.168.1.11:80
```

Allow traffic in mangle table

```
iptables -t mangle -A pre_nat -p tcp --dport 8080 -j ACCEPT
```

Example #2: Quality of Service (DSCP marking)

Mark outgoing traffic on port 81 with a specific DSCP value and then apply a firewall mark for routing.

Set DSCP value

```
iptables -t mangle -I POSTROUTING -p tcp --dport 81 -j DSCP --set-dscp 0x0a
```

Match DSCP and set MARK

```
iptables -t mangle -I POSTROUTING -m dscp --dscp 0x0a -j MARK --set-mark 81
```

Example #3: Drop every second Ping (ICMP) packet

A demonstration of the `statistic` module using the `nth` mode.

```
iptables -I INPUT -p icmp -m statistic --mode nth --every 2 --packet 0 -j DROP
```

2.4.18 iw

This program is used for displaying and manipulating wireless devices and their configuration.

Synopsis:

```
iw [options] command
```

Options:

For more details see [iw](#) manual page.

Command	Description
-debug	enable netlink debugging
-version	show version

Table 110: iw options

Commands:

For more details see [iw](#) manual page.

Command	Description
dev	List all devices or specify a device to manipulate.
link	Display the status of the current link.
scan	Trigger a scan and dump the results.
station dump	Show information about all stations.
interface add	Add a new virtual interface.
phy	Show information about physical devices.

Table 111: iw commands

Examples:

Scan for available wireless networks on `wlan0`:

```
iw dev wlan0 scan
```

Display the status of the current wireless link on `wlan0`:

```
iw dev wlan0 link
```

Show detailed information about all connected stations:

```
iw dev wlan0 station dump
```

Show capabilities of the physical device `phy0`:

```
iw phy phy0 info
```

Add a virtual monitor interface:

```
iw dev wlan0 interface add wlan1 type monitor
```

2.4.19 nc

The `nc` (`netcat`) program can be used to open a pipe to IP:port.

Synopsis:

```
nc [OPTIONS] HOST PORT : connect
```

```
nc [OPTIONS] -l -p PORT [HOST] [PORT] : listen
```

Options:

Option	Description
-e	PROG Run PROG after connect (must be last)
-l	Listen mode, for inbound connects
-lk	With -e, provides persistent server
-p PORT	Local port number
-s ADDR	Local address
-w SEC	Timeout for connects and final net reads
-i SEC	Delay interval for lines sent
-n	Don't do DNS resolution
-u	UDP mode
-b	Allow broadcasts
-v	Verbose
-o FILE	Hex dump traffic
-z	Zero-I/O mode (scanning)

Table 112: nc options

Examples:

Open a TCP connection to port 42 of 192.168.3.1 using port 31337 as the source port with a 5-second timeout:

```
nc -p 31337 -w 5 192.168.3.1 42
```

Listen on port 8080 and print received data:

```
nc -l -p 8080
```

2.4.20 net-snmpinform

This command is designed to send SNMP INFORM messages to a management entity. It supports SNMP versions 1, 2c, and 3, offering a reliable way to notify management systems of significant events.

Synopsis:

```
net-snmpinform [OPTIONS] AGENT TRAP-PARAMETERS
```

Options:

For more details, see the [snmpinform\(1\) - Linux man page](#).

Option	Description
-v 1 2c 3	SNMP version to use.
-c COMMUNITY	SNMP community string (for SNMP v1 and v2c).
-a PROTOCOL	Authentication protocol (MD5 or SHA, for SNMPv3).
-A PASSPHRASE	Authentication passphrase (for SNMPv3).
-l LEVEL	Security level: noAuthNoPriv, authNoPriv, or authPriv (for SNMPv3).
-u USER-NAME	Security name (for SNMPv3).

Table 113: net-snmpinform options

Examples:

```
net-snmpinform -v 2c -c public AGENT " 0 .1.3.6.1.6.3.1.1.5.2
```

Sends an INFORM message to the SNMP manager specified by AGENT using SNMP version 2c and the community string "public".

```
net-snmpinform -v 3 -u myUser -l authPriv -a SHA -A myAuthPass -x DES -X myPrivPass AGENT
" 0 .1.3.6.1.6.3.1.1.5.3
```

Sends an SNMPv3 INFORM message with authentication (SHA) and encryption (DES), using the specified usernames and passphrases.

```
net-snmpinform -v 1 -c public AGENT .1.3.6.1.4.1.8072.2.3.2.1 0 .1.3.6.1.4.1.8072.2.3.2.2
6
```

Uses SNMP version 1 to send an INFORM message with specified enterprise OID and trap parameters.

2.4.21 net-snmptrap

This command is used to send SNMP trap messages to a management entity. It supports SNMP versions 1, 2c, and 3.

Synopsis:

```
net-snmptrap [OPTIONS] AGENT TRAP-PARAMETERS
```

Options:

For more details see the [*snmptrap\(1\) - Linux man page*](#).

Option	Description
-v 1 2c 3	Specifies SNMP version to use.
-c COMMUNITY	Set the community string (for SNMP v1 and v2c).
-a PROTOCOL	Set authentication protocol (for SNMP v3).
-A PASSPHRASE	Set authentication protocol pass phrase (for SNMP v3).
-l LEVEL	Set security level (for SNMP v3).
-u USER-NAME	Set security name (for SNMP v3).
-C i	Send an INFORM instead of a TRAP.

Table 114: net-snmptrap options

Examples:

```
net-snmptrap -v 2c -c public AGENT " 0 .1.3.6.1.4.1.8072.2.3.0.1 0 0 "
```

Sends a test trap to the SNMP manager specified by AGENT using SNMP version 2c and the community string "public".

```
net-snmptrap -v 3 -u myUser -l authPriv -a SHA -A myAuthPass -x DES -X myPrivPass AGENT  
" 0 .1.3.6.1.6.3.1.1.5.1
```

Sends an SNMPv3 trap with authentication (SHA) and encryption (DES), using the specified usernames and passphrases.

```
net-snmptrap -v 2c -c public -C i AGENT " 0 .1.3.6.1.4.1.8072.2.3.0.2 0 0 "
```

Uses the `-C i` option to send an INFORM message instead of a TRAP using SNMP version 2c.

2.4.22 netstat

The `netstat` (network statistics) command is a valuable troubleshooting tool used to display active network connections (sockets), routing tables, and network interface statistics.

Synopsis:

```
netstat [options]
```

Options:

Option	Description
-l	Display only listening server sockets (wait for incoming connections).
-a	Display all sockets (both listening and connected).
-e	Display extended information.
-n	Do not resolve names. Show IP addresses and port numbers numerically (this significantly speeds up the output).
-r	Display the kernel routing table.
-t	Filter for TCP sockets.
-u	Filter for UDP sockets.
-w	Filter for RAW sockets.
-x	Filter for UNIX domain sockets.

Table 115: netstat options

Examples:

List all listening TCP and UDP ports numerically:

```
netstat -tuln
```

Combining the `-t`, `-u`, `-l`, and `-n` flags is the most common way to see which services are currently waiting for connections on the router, without resolving DNS names.

```
netstat -tuln
```

Output:

Active Internet connections (only servers)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN
udp	0	0	0.0.0.0:53	0.0.0.0:*	

Example #2: Print the routing table

Use the `-r` flag to show the routing table. Adding `-n` prevents delays caused by DNS lookups on the gateway IP addresses.

```
netstat -rn
```

Output:

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
0.0.0.0	192.168.1.1	0.0.0.0	UG	0	0	0	eth0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

2.4.23 nsupdate

The `nsupdate` command is a DNS update utility that allows dynamic updates to a zone using the DNS UPDATE protocol (RFC 2136). It reads commands from files or standard input to add, delete, or modify DNS resource records on a nameserver that supports dynamic updates.

Synopsis:

```
nsupdate [-CdDi] [-L level] [-l] [-g | -o | -y keyname:secret | -k keyfile] [-p port]
          [-v] [-V] [-P] [-T] [-4 | -6] [filename]
```

Options:

Option	Description
-C	Check names processing.
-d	Debug mode.
-D	Debug level.
-i	Interactive mode.
-L level	Set logging level.
-l	Localhost mode (default server/zone).
-g	GSS-TSIG authentication.
-o	GSS-TSIG ownername mode.
-y keyname:secret	Direct TSIG key specification.
-k keyfile	Specify TSIG key file for authentication.
-p port	Specify destination port.
-v	Verbose output.
-V	Print version.
-P	Primary server only.
-T	Use TCP transport.
-4	Use IPv4 transport only.
-6	Use IPv6 transport only.
[filename]	Read update commands from specified file (or stdin).

Table 116: nsupdate options

Examples:

Update a DNS A record using a TSIG key (the `send` command is required):

```
nsupdate -k ddns-key.txt «EOF
update delete routerX.example.com A
update add routerX.example.com 200 A 1.2.3.4
send
EOF
```

Example #2: Interactive mode with verbose output

Start an interactive session to type commands manually.

```
nsupdate -v
```

Example #3: Update from a command file

Read a list of update commands from a text file. Ensure the file contains the `send` command at the very end.

```
nsupdate -4 updates.txt
```

Example #4: Localhost zone updates

Update the zone on the local server without specifying credentials.

```
nsupdate -l
```

2.4.24 ntpdate

This command synchronizes the system time from an NTP server.

Synopsis:

```
ntpdate [-p <probes>] [-t <timeout>] <server>
```

Options:

Option	Description
-p	Specify the number of samples to be acquired from each server as the integer samples, with values from 1 to 8 inclusive.
-t	Specify the maximum time waiting for a server response as the value timeout, in seconds and fraction.

Table 117: ntpdate options

Examples:

Synchronize the system time with an NTP server:

```
ntpdate time.windows.com
```

2.4.25 ping

This command sends ICMP echo requests to a network host to test connectivity.

Synopsis:

```
ping [OPTIONS] HOST
```

Options:

Option	Description
-4, -6	Force IP or IPv6 name resolution.
-c CNT	Send only CNT pings.
-s SIZE	Send SIZE data bytes in packets (default = 56).
-i SECS	Interval.
-A	Ping as soon as reply is received.
-t TTL	Set TTL.
-I IFACE/IP	Source interface or IP address.
-W SEC	Seconds to wait for the first response (default 10). After all -c CNT packets are sent.
-w SEC	Seconds until ping exits (default:infinite). Can exit earlier with -c CNT.
-q	Quiet mode, only displays output at start and when finished.
-p HEXBYTE	Payload pattern.

Table 118: ping options

Examples:

Send a single ICMP echo request with a 500-byte payload to 10.0.0.1:

```
ping -c 1 -s 500 10.0.0.1
```

Continuously ping a host to check connectivity:

```
ping 192.168.1.1
```

2.4.26 ping6

This command is designed for diagnosing IPv6 network connections by sending ICMP ECHO_REQUEST packets to a specified host. It is a useful tool for testing the reachability of hosts on an IPv6 network and measuring the round-trip time for messages sent from the originating host to a destination computer.

Usage:

```
ping6 [OPTIONS] HOST
```

Description:

Sends ICMP ECHO_REQUEST packets to the HOST specified as an argument. By default, *ping6* sends packets until interrupted. If the host is reachable and responding, *ping6* displays the time taken for the round-trip.

Options:

Option	Description
-c CNT	Stop after sending CNT pings.
-s SIZE	Specifies the number of data bytes to be sent.
-i SECS	Wait SECS seconds between sending each packet.
-A	Ping the host as soon as the reply is received.
-I IFACE/IP	Use the specified interface or IP address as the source.
-W SEC	Time to wait for the first response before timing out.
-w SEC	Timeout before <i>ping6</i> exits, regardless of how many packets have been sent or received.
-q	Operate in quiet mode, only displaying summary lines at startup and completion.
-p HEXBYTE	Pattern to use for payload data.

Table 119: ping6 options

Examples:

Ping an IPv6 host 4 times:

```
ping6 -c 4 fe80::1
```

Ping with a 2-second interval and 120-byte packets:

```
ping6 -i 2 -s 120 fe80::1
```

The `ping6` command is essential for network administrators and users who need to verify IPv6 connectivity or diagnose IPv6 network problems.

2.4.27 route

This command displays and manipulates the IP routing table.

Synopsis:

```
route [ -n ] [ -e ] [ -A ] [ add | del | delete ]
```

Options:

Option	Description
-n	Don't resolve names
-e	Display other/more information
-A	Select address family

Table 120: route options

Info

For a detailed description of this command, refer to the Linux manual pages.

Examples:

Display the routing table without resolving IP addresses:

```
route -n
```

Add a route for the network 192.168.3.0/24 through `eth0`:

```
route add -net 192.168.3.0/24 dev eth0
```

Add a route for a specific host via a gateway:

```
route add -host 192.168.3.1 gw 192.168.1.2
```

Set the default gateway:

```
route add default gw 192.168.1.2
```

2.4.28 scp

This program can be used for secure file transferring between hosts on a network. It uses the `ssh` protocol for data transfer with the same authentication and security.

Synopsis:

```
scp [-12346BCpqr] [-c cipher] [-F ssh_config] [-i identity_file]
[-l limit] [-o ssh_option] [-P port] [-S program]
[[user@]host1:]file1 ... [[user@]host2:]file2
```

Options:

Option	Description
-1	Forces scp to use protocol 1.
-2	Forces scp to use protocol 2.
-4	Forces scp to use IPv4 addresses only.
-6	Forces scp to use IPv6 addresses only.
-B	Selects batch mode (prevents asking for passwords or passphrases).
-C	Compression enable. Passes the -C flag to ssh to enable compression.
-c cipher	Selects the cipher to use for encrypting the data transfer. This option is directly passed to ssh.
-F ssh_config	Specifies an alternative per-user configuration file for ssh. This option is directly passed to ssh.
-i identity_file	Selects the file from which the identity (private key) for public key authentication is read. This option is directly passed to ssh.
-l limit	Limits the used bandwidth, specified in Kbit/s.
-o ssh_option	Can be used to pass options to ssh in the format used in ssh_config.
-P port	Specifies the port to connect to on the remote host.
-p	Preserves modification times, access times, and modes from the original file.
-q	Quiet mode: disables the progress meter as well as warning and diagnostic messages from ssh.
-r	Recursively copy entire directories. Note that scp follows symbolic links encountered in the tree traversal.
-S program	Name of program to use for the encrypted connection. The program must understand ssh options.
-v	Verbose mode. Causes scp and ssh to print debugging messages about their progress.

Table 121: scp options

Info

The scp utility exits 0 on success, and >0 if an error occurs.

Examples:

Copy a file from a remote host to the local machine:

```
scp root@remotehost.edu:/etc/version/myFolder
```

Copy a file from the local machine to a remote host:

```
scp /etc/version root@remotehost.edu:/
```

Copy a directory recursively to a remote host:

```
scp -r /home/user root@remotehost.edu:/tmp/bar
```

2.4.29 sipcalc

This command is an advanced console-based IP subnet calculator. It is capable of handling both IPv4 and IPv6 addressing schemes. It provides detailed information about network addresses, subnet masks, and more, making it a valuable tool for network administrators and IT professionals.

Usage:

```
sipcalc [OPTIONS]... <[ADDRESS]... [INTERFACE]... | [-]>
```

Global options

Option	Description
-a, -all	Display all possible information.
-d, -resolve	Enable name resolution for addresses.
-h, -help	Show help message and exit.
-I, -addr-int=INT	Specify an interface to add.
-n, -subnets=NUM	Display NUM extra subnets starting from the current subnet.
-u, -split-verbose	Enable verbose output for subnet splitting.
-v, -version	Show version information and exit.
-4, -addr-ipv4=ADDR	Specify an IPv4 address to add.
-6, -addr-ipv6=ADDR	Specify an IPv6 address to add.

Table 122: sipcalc – global options

IPv4 options

Option	Description
-b, -cidr-bitmap	Show CIDR bitmap.
-c, -classful-addr	Display classful address information.
-i, -cidr-addr	Display CIDR address information (default).
-s, -v4split=MASK	Split the current network into subnets of MASK size.
-w, -wildcard	Display information for a wildcard (inverse mask).
-x, -classful-bitmap	Show classful bitmap.

Table 123: sipcalc – IPv4 options

IPv6 Options

Option	Description
-e, -v4inv6	Show IPv4 compatible IPv6 information.
-r, -v6rev	Generate IPv6 reverse DNS output.
-S, -v6split=MASK	Split the current IPv6 network into subnets of MASK size.
-t, -v6-standard	Show standard IPv6 address information (default).

Table 124: sipcalc – IPv6 options

Examples:

Calculate and display all information for an IPv4 address:

```
sipcalc -a 192.168.1.1/24
```


Split an IPv6 network into smaller subnets:

```
sipcalc -S 64 2001:db8::/32
```

Address and netmask formats are flexible, supporting dotted quad, number of bits, and hex formats. The tool also supports reading arguments from stdin if `-` is used in place of an address or interface name.

For detailed usage and options, refer to the `sipcalc` manual or the help option `-h`.

2.4.30 `snmpget`

This is an SNMP application that uses the SNMP GET request to query for information on a network entity. One or more object identifiers (OIDs) may be given as arguments on the command line.

Synopsis:

```
snmpget [OPTIONS] [-Cf] OID [OID]...
```

Options:

Option	Description
-h, -help	Display the help.
-H	Display configuration file directives understood.
-v 1 2c 3	Specifies SNMP version to use.
-V, -version	Display package version number.
-Cf	If -Cf is not specified, some applications (<i>snmpdelta</i> , <i>snmpget</i> , <i>snmpgetnext</i> and <i>snmp-status</i>) will try to fix errors returned by the agent that you were talking to and resend the request. The only time this is really useful is if you specified a OID that didn't exist in your request and you're using SNMPv1 which requires "all or nothing" kinds of requests.
other	<i>For other options see the command help.</i>

Table 125: `snmpget` options

Examples:

Retrieve the `sysDescr.0` variable from a host using the community string `public`:

```
snmpget -c public zeus system.sysDescr.0
```

2.4.31 snmpset

This is an SNMP application that uses the SNMP SET request to set information on a network entity. One or more object identifiers (OIDs) must be given as arguments on the command line. A type and a value to be set must accompany each object identifier.

Synopsis:

```
snmpset [OPTIONS] OID TYPE VALUE [OID TYPE VALUE]...
```

Options:

Option	Description
-h, -help	Display the help.
-H	Display configuration file directives understood.
-v 1 2c 3	Specifies SNMP version to use.
-V, -version	Display package version number.
other	<i>For other options see the command help.</i>

Table 126: snmpset options

The TYPE is a single character, one of:

Character	Description
i	integer
u	unsigned
s	string
x	hex string
d	decimal string
n	nullobj
o	objid
t	timeticks
a	ipaddress
b	bits

Table 127: type options

Examples:

Set `sysContact.0` and `ipForwarding.0`:

```
snmpset -c private -v 1 test-hub \  
system.sysContact.0 s dpz@noc.rutgers.edu \  
ip.ipForwarding.0 i 2
```

2.4.32 snmptrap

Info

See similar programs `snmpinform` (Chapter 2.4.20) and `snmptrap` (Chapter 2.4.21).

This command sends an SNMP trap.

Synopsis:

```
snmptrap [-c <community>] [-g <generic>] [-s <specific>] [-R] <hostname>  
[<oid> <type> <value>]
```

Options:

Option	Description
-c	Community
-g	Specifies generic trap types: 0 – coldStart 1 – warmStart 2 – linkDown 3 – linkUp 4 – authenticationFailure 5 – egpNeighborLoss 6 – enterpriseSpecific
-R	Sends MAC address of eth0 interface
-s	Specifies user definition trap types in the enterpriseSpecific

Table 128: snmptrap options

Examples:

Send a trap with the state of digital input BIN0 to 192.168.1.2:

```
snmptrap 192.168.1.2 1.3.6.1.4.1.30140.2.3.1.0 u 'io get bin0'
```

Send a warm-start trap to 192.168.1.2:

```
snmptrap -g 1 192.168.1.2
```

2.4.33 ssh

This is a program for logging into a remote machine and for executing commands on a remote machine.

Synopsis:

```
ssh [-4AaCfGgKkMMNnqsTtVvXxYy] [-B bind_interface] [-b bind_address]
    [-c cipher_spec] [-D [bind_address:]port] [-E log_file]
    [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
    [-J destination] [-L address] [-l login_name] [-m mac_spec]
    [-O ctl_cmd] [-o option] [-P tag] [-p port] [-Q query_option]
    [-R address] [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
    destination [command [argument ...]]
```

Options:

For more details see [ssh\(1\) — Linux manual page](#).

Option	Description
-4	Forces to use IPv4 addresses only.
-6	Forces to use IPv6 addresses only.
-i identity_file	Specifies the file from which the identity (private key) for public key authentication is read.
-l login_name	Specifies the user to log in as on the remote machine.
-p port	Specifies the port to connect to on the remote host.
-v	Verbose mode. Causes ssh to print debugging messages about its progress. This is helpful in diagnosing connection, authentication, and configuration problems.
-A and -a	These options control the use of SSH agent forwarding, a mechanism for single sign-on.
-X and -x	These manage X11 forwarding, enabling the secure transmission of X11 windows from the remote machine to the local machine.
-L address	Specifies that connections to the given TCP port or Unix socket on the local (client) host are to be forwarded to the given host and port, or Unix socket, on the remote side.
-C	Requests compression of all data. This can speed up transfers over slow networks.
-F configfile	Specifies an alternative per-user configuration file.

Table 129: ssh options

Examples:

Log in to a remote server:

```
ssh root@192.168.1.1
```

Connect to a non-standard SSH port:

```
ssh -p 2222 username@remote_host
```

Use a specific private key for authentication:

```
ssh -i /path/to/private_key username@remote_host
```

Execute a single command on the remote server:

```
ssh user@server 'ls -l /var/www'
```

Set up SSH local port forwarding:

```
ssh -L local_port:remote_host:remote_port username@ssh_server
```

2.4.34 tc

The `tc` (traffic control) command in Linux is a powerful tool utilized for managing network bandwidth and handling Quality of Service (QoS). It allows administrators to control the flow of network traffic by defining policies for traffic classification, prioritization, and rate limiting, among other functionalities. This command is essential for optimizing network performance and ensuring that critical network services remain highly available and responsive.

Synopsis:

```
tc [OPTIONS] OBJECT COMMAND | help
```

Description:

Tc operates on several objects such as qdiscs (queuing disciplines), classes, and filters, each of which plays a vital role in defining traffic control policies. By manipulating these objects, administrators can tailor the network traffic behavior to suit the specific needs of their environment. This includes creating traffic queues, setting up bandwidth limits for different types of traffic, and applying traffic filters to categorize network packets into various classes.

Options:

Option	Description
-s	Show detailed information. When used, <i>tc</i> displays more detailed information about the specified object.
-d	Show raw data. This option is useful for debugging purposes.
-p	Pretty print. Formats the output in a more readable form.
-b	Batch mode. Allows <i>tc</i> to read a series of commands from a file.

Table 130: tc options

Examples:

Show all current qdiscs:

```
tc -s qdisc show
```

Limit outbound traffic on `eth0` to 1 Mbit/s:

```
tc qdisc add dev eth0 root tbf rate 1mbit burst 32kbit latency 400ms
```

For a comprehensive guide on QoS configuration, see the [Quality of Service \(QoS\) Application Note](#).

2.4.35 tcpdump

This command captures and displays network traffic.

Synopsis:

```
tcpdump [-AdDeflLnNOpqRStuUvxX] [-c <count>] [-C <file size>] [-E algo:secret]
[-F <file>] [-i <interface>] [-r <file>] [-s <snaplen>] [-T type] [-w <file>]
[-y <datalinktype>] [expression]
```

Options:

For a detailed description of this command, refer to the Linux manual pages.

Examples:

Capture traffic on interface `ppp0`:

```
tcpdump -n -i ppp0
```

View traffic on interface `eth0` except protocol Telnet.

```
tcpdump -n not tcp port 23
```

View UDP traffic on interface `eth0`.

```
tcpdump -n udp
```

View HTTP traffic on interface `eth0`.

```
tcpdump -n tcp port 80
```

View all traffic from/to IP address `192.168.1.2`.

```
tcpdump -n host 192.168.1.2
```

View traffic from/to IP address `192.168.1.2` except protocol Telnet.

```
tcpdump -n host 192.168.1.2 and not tcp port 23
```

2.4.36 telnet

This command establishes an interactive session with a remote host using the Telnet protocol.

Synopsis:

```
telnet <host> [<port>]
```

Examples:

Connect to a host using Telnet:

```
telnet 192.168.1.2
```

2.4.37 traceroute

This command traces the network route to a remote host.

Synopsis:

```
traceroute, [-Flnrv], [-f, <1st_ttl>], [-m, <max_ttl>], [-p, <port#>], [-q, <nqueries>]
[-s, <src_addr>], [-t, <tos>], [-w, <wait>], [-i, <iface>], [-z, <pausesecs>]
host, [data size]
```

Options:

Item	Description
-4, -6	Force IP or IPv6 name resolution
-F	Set the don't fragment bit
-l	Display the TTL value of the returned packet
-n	Print hop addresses numerically rather than symbolically
-r	Bypass the normal routing tables and send directly to a host
-f N	First number of hops (default 1)
-m N	Set the max time-to-live (max number of hops)
-q N	Set the number of probes per hop (default is 3)
-p N	Set the base UDP port number used in probes (default is 33434)
-s IP	Use the following IP address as the source address
-i IFACE	Source interface
-t N	Set the type-of-service in probe packets to the following value (default 0)
-w SEC	Set the time (in seconds) to wait for a response to a probe (default 3 sec)
-z MSEC	Wait before each send
-v	Verbose output

Table 131: traceroute options

Examples:

Trace the route to a remote host:

```
traceroute 8.8.8.8
```

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 46 byte packets
 1  192.168.1.1 (192.168.1.1)  1.014 ms  0.921 ms  0.878 ms
 2  10.0.0.1 (10.0.0.1)  8.342 ms  8.251 ms  8.198 ms
 3  * * *
 4  72.14.194.34 (72.14.194.34)  19.443 ms  19.381 ms  19.302 ms
 5  8.8.8.8 (8.8.8.8)  19.451 ms  19.367 ms  19.289 ms
```

Trace the route without resolving hostnames (faster output):

```
traceroute -n 8.8.8.8
```

Limit the trace to a maximum of 15 hops:

```
traceroute -m 15 192.168.100.1
```

Specify a source interface and send only 1 probe per hop:

```
traceroute -i eth0 -q 1 10.0.0.1
```

2.4.38 traceroute6

This command is a network diagnostic tool included with BusyBox that is designed to trace the path packets take to reach an IPv6 host. By sending packets with incrementally increasing hop limits (TTL, Time-To-Live), *traceroute6* determines the route packets follow to reach the target host. This command is essential for identifying network bottlenecks and routing issues in IPv6 networks.

Synopsis:

```
traceroute6 [-nrv] [-f 1ST_TTL] [-m MAXTTL] [-q PROBES] [-p PORT]
[-t TOS] [-w WAIT_SEC] [-s SRC_IP] [-i IFACE] [-z PAUSE_MSEC] HOST [BYTES]
```

Description:

traceroute6 utilizes IPv6 packets to trace the network route from the source to the specified HOST. It provides various options to customize the trace, including setting the first and maximum number of hops, the number of probes per hop, and the source IP address or interface.

Options:

Option	Description
-n	Do not resolve IP addresses to their domain names, display numeric addresses.
-r	Bypass the normal routing tables and send directly to the host.
-f N	Set the initial time-to-live (hop limit) to N.
-m N	Specify the maximum number of hops (TTL) traceroute6 will probe.
-q N	Set the number of probe packets per hop.
-p N	Use N as the base UDP port number for probes.
-s IP	Use IP as the source address for the outgoing probe packets.
-i IFACE	Specify the interface through which traceroute should send packets.
-t N	Set the type-of-service in probe packets to N.
-w SEC	Set the time to wait for a response to a probe.
-z MSEC	Wait MSEC milliseconds between sending each packet.

Table 132: traceroute6 options

Examples:

Trace the route to an IPv6 host without resolving names:

```
traceroute6 -n HOST
```

Trace the route with a specific number of probes per hop:

```
traceroute6 -q 1 HOST
```

Specify a source address and maximum number of hops:

```
traceroute6 -s SRC_IP -m 15 HOST
```

traceroute6 offers valuable insights into the network path and performance characteristics between the source and an IPv6 destination, aiding in network troubleshooting and analysis.

2.4.39 vconfig

This command creates and removes virtual Ethernet devices.

Synopsis:

```
vconfig command [OPTIONS]
```

Options:

Command [OPTIONS]	Description
add IFACE VLAN_ID	Creates a vlan-device on IFACE. The resulting vlan-device will be called according to the naming convention set.
rem VLAN_NAME	Removes the named VLAN_NAME.
set_flag IFACE 0 1 VLAN_QOS	When 1, ethernet header reorders are turned on. Dumping the device will appear as a common ethernet device without vlans. When 0(default) however, ethernet headers are not reordered, which results in vlan tagged packets when dumping the device. Usually the default gives no problems, but some packet filtering programs might have problems with it.
set_egress_map VLAN_NAME SKB_PRIO VLAN_QOS	This flags that outbound packets with a particular skb-priority should be tagged with the particular vlan priority vlan-qos. The default vlan priority is 0.
set_ingress_map VLAN_NAME SKB_PRIO VLAN_QOS	This flags that inbound packets with the particular vlan priority vlan-qos should be queued with a particular skb-priority. The default skb-priority is 0.
set_name_type NAME_TYPE	Sets the way vlan-device names are created. Use vconfig without arguments to see the different formats.

Table 133: vconfig commands and options

Info

Vlan ID 4091 and 4092 are reserved for the system

Examples:

Create VLAN ID 1 on the `eth0` interface:

```
vconfig add eth0 1
```

Remove a VLAN interface:

```
vconfig rem eth0.1
```

2.4.40 wget

The `wget` utility is a non-interactive network downloader used to retrieve files from the web using HTTP, HTTPS, or FTP protocols. Because it is non-interactive, it is highly suitable for use in background scripts, cron jobs, or automated provisioning.

Synopsis:

```
wget [options] <URL>
```

Options:

Option	Description
-spider	Only check if the URL exists (do not download the file). The exit status (\$?) is 0 if the file exists.
-c	Continue retrieving a partially downloaded file (resume an aborted transfer).
-q	Quiet mode. Turn off all output, including error messages.
-P <DIR>	Save the downloaded file to the specified directory <DIR> instead of the current working directory.
-S	Print the HTTP or FTP server response headers.
-T <SEC>	Set the network read timeout to <SEC> seconds.
-O <FILE>	Save the downloaded document as <FILE>. Use - to write to standard output (stdout).
-o <FILE>	Log all messages and output to <FILE> instead of the terminal.
-U <STR>	Identify as <STR> in the User-Agent HTTP header.
-Y on/off	Explicitly turn the use of a proxy server on or off.

Table 134: wget options

Examples:

Download a file from a local HTTP server:

```
wget http://10.0.0.1/my.cfg
```

Save a downloaded file under a different name:

```
wget -O /tmp/new_config.cfg http://10.0.0.1/my.cfg
```

Check whether a file exists on a server without downloading it:

```
wget --spider http://10.0.0.1/my.cfg
```

Output:

```
0
```

2.5 Scripting/Shell Commands

This section covers commands integral to shell scripting and command-line manipulation. These commands are foundational for automating tasks, managing files, and configuring system behavior through scripts.

2.5.1 `awk`

This program scans each input file for lines that match any of a set of patterns specified literally in program-text or in one or more files specified as `-f progfile`.

Synopsis:

```
awk [-v var=val] [-F FS] [-f progfile] [<program-text>] [<file> ...]
```

Note: Program can be inline or from file (`-f`). Multiple `-f` options allowed.

Options:

Option	Description
<code>-v var=val</code>	Set variable before program execution (BEGIN block).
<code>-F FS</code>	Set input field separator (FS variable).
<code>-f progfile</code>	Read program from file (multiple allowed).

Table 135: `awk` options

Examples:

Show IP address of Gateway

```
route -n | awk '/^0.0.0.0/ { print $2 }'
```

Output:

192.168.1.1

2.5.2 break

This command is used within looping constructs in Bash/Shell scripting to exit from the loop prematurely. It breaks out of the nearest enclosing loop, skipping the remaining iterations of the loop.

Synopsis:

```
break [n]
```

Note: Optional argument `n` specifies which enclosing loop to break (default: 1 = innermost loop).

Options:

Option	Description
[n]	Exit from the nth enclosing loop (default: 1).

Table 136: break options

2.5.3 clear

This command clears the terminal screen/console, moving the cursor to the home position (top-left corner). It is equivalent to pressing `Ctrl+L` in most terminals. The screen content is not deleted from memory - only the display is refreshed.

Synopsis:

```
clear
```

2.5.4 continue

The `continue` command is used within loops in Bash/Shell scripting to skip the rest of the current loop iteration and continue with the next iteration. This command is particularly useful when a condition is met that requires prematurely proceeding to the next cycle of the loop without executing the remaining commands in the current iteration.

Synopsis:

```
continue [n]
```

Note: Optional argument `n` specifies which enclosing loop to continue (default: 1 = innermost loop).

Options:

Option	Description
[n]	Continue at the nth enclosing loop (default: 1).

Table 137: continue options

2.5.5 echo

This command prints strings to standard output. It supports basic escape sequence interpretation and newline control.

Synopsis:

```
echo [-n] [-e] [-E] [<string> ...]
```

Note: Multiple strings are concatenated with spaces. Backslash escapes are processed only with `-e`.

Options:

Option	Description
-n	Do not output the trailing newline.
-e	Enable interpretation of backslash escapes.
-E	Disable interpretation of backslash escapes (default).

Table 138: echo options

Examples:

Switch profile to "Standard".

```
echo "PROFILE=" > /etc/settings
```

```
reboot
```

Switch profile to "Alternative 1".

```
echo "PROFILE=alt1" > /etc/settings
```

```
reboot
```

Send a sequence of bytes 0x41,0x54,0x0D,0x0A to serial line (write data in octal).

```
echo -n -e "\101\124\015\012" > /dev/ttyS0
```

2.5.6 eval

This command is a built-in utility in Bash/Shell scripting environments used to concatenate its arguments into a single command, which is then executed by the shell. This command is particularly useful for constructing commands based on variables or processing complex expressions where commands depend on other commands’ outputs or file contents.

Synopsis:

```
eval [arg ...]
```

Note: All arguments are concatenated (separated by spaces) into a single string, then parsed and executed as shell commands.

Options:

Option	Description
[arg ...]	Arguments to be concatenated and executed as shell command(s).

Table 139: eval options

Examples:

Execute a dynamically constructed command:

```
CMD="echo Hello"
eval $CMD
```

Parse output from previous command

```
read var1 var2 < <(date); eval echo "Year: $var2"
```

Create function from variable content

```
FUNC="echo Hello"; eval $FUNC
```

2.5.7 exec

This command is used in shell scripting to replace the current shell process with a specified program. Unlike running a program normally, *exec* does not return to the shell once the program completes. Instead, the new program takes over the current process space, maintaining the same process ID (PID).

Synopsis:

```
exec command [arguments]
```

Note: Without arguments, *exec* reopens stdin/stdout/stderr from the shell's current redirections.

Options:

Option	Description
command [arguments]	Replace shell with specified command (no return).
(no arguments)	Reopen stdin/stdout/stderr using current redirections.
-a name	Set argv[0] of executed program to name.
-l	Place a dash at start of argv[0] (login shell).

Table 140: exec options

Examples:

Replace the shell with the vi editor:

```
exec vi /etc/settings.ppp
```

Replace the shell with a new shell instance:

```
exec /bin/sh
```

Redirect all output of the script to a log file:

```
exec > /tmp/script.log 2>&1
```

```
echo "This goes to the log"
```

Exec with a custom argv[0]:

```
exec -a mysh /bin/sh
```

2.5.8 exit

This command terminates the current shell session or script execution. It allows the script or shell to exit with an optional exit status, which can be used to indicate the success or failure of the script's execution to the calling environment.

Synopsis:

```
exit [n]
```

Note: Exit status *n* should be 0-255. 0 indicates success, non-zero values indicate various errors.

Options:

Option	Description
[n]	Exit status code (0-255, default: last command status).

Table 141: exit options

Examples:

Exit shell with success status

```
exit 0
```

Exit script with error status

```
exit 1
```

Exit with status of last command

```
false; echo $?; exit
```


2.5.9 export

This command in shell scripting is utilized to set or export environment variables and functions to the current shell and all processes started from it. By marking an environment variable or function to be exported, it becomes available to subprocesses spawned from the shell, allowing those processes to use the variable or function.

Synopsis:

```
export [NAME[=VALUE] ...]
```

Note: Without arguments, displays all exported variables. NAME=VALUE sets and exports; NAME only exports existing variable.

Options:

Option	Description
[NAME[=VALUE]]	Set and/or export environment variable(s).
(no arguments)	List all currently exported variables.
-p	List in portable format (export NAME=VALUE).
-n	Remove NAME from exported list.

Table 142: export options

Examples:

Display all exported variables

```
export
```

Set the HOME environment variable:

```
export HOME='/root'
```

Export the PATH environment variable, appending a new directory:

```
export PATH=$PATH:/usr/local/bin
```

List all exported names in portable format:

```
export -p
```

Remove a variable from the exported list:

```
export -n MYVAR
```

2.5.10 hash

This command in shell scripting is utilized to handle the hash table of commands in memory, which tracks the full path of previously executed commands. This optimizes the shell's performance by avoiding the need to search the `$PATH` environment variable for command locations on subsequent executions.

Synopsis:

```
hash [options] [name ...]
```

Note: Without arguments, displays current hash table contents. With name only, adds command to hash table.

Options:

Option	Description
-r	Reset/clear the entire hash table.
-l	List hash table in portable format.
-p pathname name	Probe specific pathname for command name.
-d name	Remove specified name from hash table.
-t name	Show path for specific command only.
[name]	Add command name to hash table.
(no arguments)	Display all hashed commands and paths.

Table 143: hash options

Examples:

Display current hash table

```
hash
```

Add command to hash table

```
hash myscript
```

Reset hash table

```
hash -r
```

Remove specific command

```
hash -d myscript
```

Direct pathname mapping

```
hash -p /usr/local/bin/myscript myscript
```

2.5.11 inc

This command is a specialized, proprietary tool designed to output a number that is incremented by one from the given value. This utility can be particularly useful in scripting and automation tasks where numerical adjustments and calculations are required.

Synopsis:

```
inc <value>
```

Note: Accepts only numeric input. Outputs result to stdout.

Options:

Option	Description
<value>	Numeric value to increment by 1.

Table 144: inc options

Examples:

Increment value 5 to 6

```
inc 5
```

Output:

6

Use in arithmetic sequence

```
val=10; next=$(inc $val); echo $next
```

Output:

11

Increment a variable step by step:

```
x=20; x=$(inc $x); echo $x
```

Output:

21

2.5.12 let

This command is a built-in shell command primarily used for evaluating arithmetic expressions. It provides a straightforward method for performing numerical calculations within shell scripts, supporting operators like addition, subtraction, multiplication, division, and bitwise operations.

Synopsis:

```
let "expression"
```

Note: Variables in expressions don't need \$ prefix. Expressions must be quoted to prevent shell expansion.

Options:

Option	Description
"expression"	Arithmetic expression to evaluate (quoted).

Table 145: let options

Examples:

Increment counter

```
count=5; let "count += 1"; echo $count
```

Output:

6

Basic arithmetic

```
a=10; b=3; let "c = a * b"; echo $c
```

Output:

30

Compare and assign

```
x=15; y=25; let "z = (x > y) ? x : y"; echo $z
```

Output:

25

2.5.13 local

This command is a shell built-in that is used within functions to declare variables as having a function-local scope. It prevents variable names from conflicting with variables outside the function, making shell scripts more reliable and modular.

Synopsis:

```
local [name[=value] ...]
```

Note: Can only be used inside functions. Variables remain local to function scope.

Options:

Option	Description
name[=value]	Declare local variable with optional initial value.
-	Restore local variables from stack (advanced usage).

Table 146: local options

Examples:

Local variable in function

```
myfunc() { local temp=10; echo $temp; }; myfunc
```

Output:

10

Local variable in function

```
f() { local x=5 y=10; echo $((x+y)); }
```

```
f
```

Output:

15

Prevent global namespace pollution:

```
foo() { local counter=1; counter=$((counter+1)); echo $counter; }
```

```
foo
```

Output:

2

2.5.14 nohup

`nohup` is short for “No Hang-up”. This command runs a program immune to hangups, with output redirected to `nohup.out` by default. The program continues running even after the user logs out.

Synopsis:

```
nohup <program> [<arguments>]
```

Note: Output is redirected to `nohup.out` unless redirected elsewhere. Exit status is returned when program completes.

Options:

Option	Description
program [arguments]	Program to run immune to hangups and logout.

Table 147: nohup options

Examples:

Run ping in background, immune to logout:

```
nohup ping -c 10 google.com &
```

Output:

```
nohup: appending output to nohup.out
```

Redirect nohup output to a custom log file:

```
nohup ./myscript.sh > mylog.txt 2>&1 &
```

2.5.15 printf

This command formats and prints ARGUMENT(s) according to FORMAT (C printf syntax). It provides precise control over output formatting including numbers, strings, and escape sequences.

Synopsis:

```
printf FORMAT [ARGUMENT...]
```

Note: FORMAT string uses C-style conversion specifiers. Unlike echo, no automatic newline is added.

Format Options:

Specifier	Description
%d, %i	Signed decimal integer
%u	Unsigned decimal integer
%o	Unsigned octal
%x, %X	Unsigned hexadecimal (lower/upper)
%f	Decimal floating point
%e, %E	Scientific notation (lower/upper)
%g, %G	Shortest of %e/%f or %E/%F
%a, %A	Hexadecimal floating point (lower/upper)
%c	Character
%s	String
%p	Pointer address
%n	Store number of characters printed
%%	Literal percent sign

Table 148: printf format specifiers

Examples:

Print number 10 in unsigned hexadecimal integer (uppercase) format:

```
printf "Output: %X \n" 10
```

Output:

A

Example of printing system variables:

```
printf "User '%s' in directory '%s'.\n" "$USER" "$PWD"
```

Output:

User 'root' in directory '/home/httpd'.

Right-aligned decimal:

```
printf "Value: %8d\n" 42
```

Output:

Value: 42

2.5.16 read

This command reads one line from standard input (stdin) and assigns values to shell variables.

Synopsis:

```
read [-r] [-t TIMEOUT] [-p PROMPT] [VARIABLE ...]
```

Options:

Option	Description
-r	Raw mode — do not interpret backslash escapes.
-t TIMEOUT	Time out and return failure if no input is received within TIMEOUT seconds.
-p PROMPT	Display PROMPT on stderr before reading.

Table 149: read options

Examples:

Read single line into variable

```
read line;
```

Input:

Hello World

```
echo "You entered: $line"
```

Output:

You entered: Hello World

Read into multiple variables

```
read user host;
```

Input:

john server1

```
echo "$user@$host"
```

Output:

john@server1

Read with a timeout:

```
read -t 5 -p "Enter value: " VAL || echo "Timed out"
```

Raw mode (preserve backslashes)

```
read -r line;
```

Input:

path to config.ini

```
echo "$line"
```

Output:

path to config.ini

2.5.17 readonly

This command in shell scripting is used to mark variables and functions as immutable. Once a variable or a function is set to read-only, its value or function body cannot be changed or unset. Attempting to modify a read-only variable or function will result in an error.

Synopsis:

```
readonly [-p] [name[=value] ...]
```

Examples:

Declare a read-only variable:

```
readonly VERSION="1.0"
```

```
VERSION="2.0"    # Error: VERSION: is read only
```

2.5.18 return

This command is used within shell functions to terminate the function execution and optionally return an exit status to the calling environment. This command is similar in behavior to the `exit` command but is specifically designed for use within functions.

Synopsis:

```
return [n]
```

Options:

Option	Description
n	Exit status (0-255, default 0)

Table 150: return options

Examples:

Return success from function

```
check_file() { [ -f /etc/passwd ] && return 0; };
check_file && echo "OK"
```

Output:
OK

Return success status

```
divide() { [ $2 -eq 0 ] && return 1; return 0; };
```

Output:
(nothing)

Return error status

```
divide 10 0 && echo "OK" || echo "Error: $?"
```

Output:
Error: 1

Return error/success message

```
divide 10 1 && echo "OK" || echo "Error: $?"
```

Output:
OK

2.5.19 shlock

This command locks a specified file during script execution using `flock(LOCK_EX)`. Ensures only one script instance accesses the file at a time. If already locked, waits until released.

Synopsis:

```
shlock <filename>
```

Description:

Creates exclusive lock on specified file, preventing concurrent script execution. Other shlock instances block until the locking script terminates. Manual file access (`vi/cat`) remains possible. Lock automatically released when script exits.

Examples:

Multi-script coordination:

Script 1: `shlock /tmp/config.txt; sleep 10; echo "Done"`

Script 2: `shlock /tmp/config.txt` (waits 10s until Script 1 finishes)

Lock released automatically when script process terminates.

2.5.20 set

Shell built-in to set/unset options and positional parameters (\$1, \$2...).

Synopsis:

```
set [--] [arg1 arg2 ...]  
set -e, set -x, set +e, set +x
```

Examples:

Set positional parameters

```
set -- file1 file2 file3  
echo $1 $2 $3
```

Output:

```
file1 file2 file3
```

Enable exit-on-error in a script

```
set -e; false; echo "This won't print"
```

(script exits immediately, echo is not printed)

Enable command tracing

```
set -x  
ls /tmp
```

```
+ ls /tmp
```

Output:

```
+ ls /tmp
```

(shows each command as executed)

Disable tracing

```
set +x
```

Output:

```
+ set +x
```

2.5.21 shift

The `shift` command shifts the positional parameters to the left. It renames the positional parameters `$N+1`, `$N+2`, ... to `$1`, `$2`, ... and so on. If `n` is specified, the parameters are shifted by `n` positions.

Synopsis:

```
shift [n]
```

Examples:

Example #1: Process all script arguments using a loop

`script.sh` code:

```
#!/bin/sh
# Process arguments one by one
while [ "$#" -gt 0 ]; do
    echo "Processing: $1"
    shift
done
```

Execute script:

```
./script.sh apple banana cherry
```

Output:

```
Processing: apple
Processing: banana
Processing: cherry
```

Example #2: Shift by 2 positions

```
set -- a b c d e; echo $1 $2 $3; shift 2; echo $1 $2 $3
```

Output:

```
a b c
c d e
```

Example #3: Check the number of remaining arguments

The `$#` variable holds the count of current positional parameters. Continuing from Example #2 (where 3 arguments remained):

```
echo "Arguments remaining: $#"
```

Output:

```
Arguments remaining: 3
```

2.5.22 sleep

The `sleep` command pauses the execution of a script or process for a specified amount of time. The time must be specified as an integer number of seconds.

Synopsis:

```
sleep <seconds>
```

Examples:

Example #1: Sleep for 30 seconds

```
sleep 30
```

Example #2: Sleep for 5 minutes (300 seconds)

```
sleep 300
```

Example #3: Practical usage in a script

This script checks for an internet connection every 10 seconds.

```
#!/bin/sh
while ! ping -c 1 8.8.8.8 > /dev/null; do
    echo "Waiting for internet connection..."
    sleep 10
done
echo "Connected!"
```

2.5.23 source

The `source` command reads and executes commands from a specified file within the **current** shell environment.

Unlike executing a script directly (which launches a new subshell process), `source` runs the commands in the existing process. This means that any variables set, functions defined, or environment changes made by the script will persist in the current shell after the script finishes.

Note: The `.` (dot) command is a synonym for `source` in POSIX shells.

Synopsis:

```
source <filename> [arguments]
```

or

```
. <filename> [arguments]
```

Examples:

Example #1: Load system-wide environment variables

It is common to use `source` to reload configuration files without rebooting or logging out.

```
source /etc/profile
```

Example #2: Persisting variables (The difference between execution and sourcing)

Create a file named `config.sh` with content of:

```
MY_VAR="12345"
```

Scenario A: Executing the script

If you run the script as an executable, the variable is set in a subshell and disappears when the script ends:

```
chmod +x config.sh
```

```
./config.sh
```

```
echo "Value: $MY_VAR"
```

Output:

Value:

Scenario B: Sourcing the script

If you use `source`, the variable is set in your current shell. Note that if the file is in the current directory, you should prefix it with `./` to ensure it is found.

```
source ./config.sh
```

```
echo "Value: $MY_VAR"
```

Output:

Value: 12345

2.5.24 test

The `test` command checks file types and compares values. It returns an exit status of 0 (true) or 1 (false). This command is most commonly used as `[ EXPRESSION ]` in `if` statements or combined with logical operators `&&` and `||`. The `[` command is a synonym for `test`, but it requires a closing `]` as its last argument.

Synopsis:

```
test <expression> | [ <expression> ]
```

Common Operators:

Option	Description
<code>-f <file></code>	Returns true if the file exists and is a regular file.
<code>-d <file></code>	Returns true if the file exists and is a directory.
<code>-e <file></code>	Returns true if the file exists (regardless of type).
<code>-z <string></code>	Returns true if the length of the string is zero.
<code>-n <string></code>	Returns true if the length of the string is non-zero.
<code>s1 = s2</code>	Returns true if the strings are equal.
<code>s1 != s2</code>	Returns true if the strings are not equal.
<code>n1 -eq n2</code>	Returns true if integers are equal.
<code>n1 -ne n2</code>	Returns true if integers are not equal.
<code>n1 -gt n2</code>	Returns true if <i>n1</i> is greater than <i>n2</i> .
<code>n1 -ge n2</code>	Returns true if <i>n1</i> is greater than or equal to <i>n2</i> .
<code>n1 -lt n2</code>	Returns true if <i>n1</i> is less than <i>n2</i> .
<code>n1 -le n2</code>	Returns true if <i>n1</i> is less than or equal to <i>n2</i> .
<code>! <expr></code>	Returns true if the expression is false (negation).

Table 151: commonly used tests

Examples:

Example #1: Check if a file exists

Using the `[ ]` syntax within an if-statement:

```
if [ -f "/etc/config/network" ]; then
    echo "Network configuration found."
else
    echo "Configuration missing."
fi
```

Example #2: Compare two strings

Note the spaces around the brackets and the equals sign.

```
STATUS="active"
if [ "$STATUS" = "active" ]; then
    echo "The service is running."
fi
```


Example #3: Integer comparison

Check if a counter is greater than 5.

```
COUNT=10
if [ "$COUNT" -gt 5 ]; then
    echo "Count is greater than 5."
fi
```

2.5.25 trap

The `trap` command allows you to catch signals and execute code when they occur. This is useful for cleaning up temporary files, ignoring specific signals, or executing custom commands when a script finishes.

Synopsis:

```
trap [action] [signal...]
```

To list currently defined traps:

```
trap
```

Common Signals:

Option	Description
SIGINT (2)	Interrupt signal (typically sent by pressing Ctrl+C).
SIGTERM (15)	Termination signal. Requests the program to end gracefully.
SIGHUP (1)	Hangup signal. Often sent when a terminal window is closed.
EXIT (0)	A pseudo-signal used to execute commands when the shell exits (regardless of the reason).

Table 152: common signals

Examples:

Example #1: Ensure cleanup on exit
This script creates a temporary file and ensures it is deleted even if the user presses Ctrl+C. Note that we trap `EXIT`, `SIGINT`, and `SIGTERM` to ensure the cleanup runs in all cases.

```
#!/bin/sh
TEMP_FILE="/tmp/data.tmp"

# Define cleanup function
cleanup() {
    echo "Cleaning up temporary files..."
    rm -f "$TEMP_FILE"
    exit
}

# Register the trap for EXIT and signals
trap cleanup EXIT SIGINT SIGTERM

touch "$TEMP_FILE"
echo "Working... (Press Ctrl+C to test cleanup)"
sleep 10
```

Example #2: Ignore a signal
To ignore a signal (e.g., to prevent a script from stopping if the terminal closes), use an empty string as the action.

```
trap '' SIGHUP
```

Example #3: Reset signal to default
To revert the signal handling back to the system default, use a hyphen (`-`).

```
trap - SIGINT
```

2.5.26 type

The `type` command indicates how the shell interprets a specific command name. It reveals whether a command is a shell builtin, an external executable file, a function, or if it does not exist at all.

This is particularly useful for debugging scripts to ensure that you are executing the specific version of a command you expect (e.g., a system binary versus a user-defined function).

Synopsis:

```
type <command_name>
```

Examples:

Example #1: Check a shell builtin

Commands like `cd` or `echo` are built directly into the shell.

```
type cd
```

Output:

```
cd is a shell builtin
```

Example #2: Check an executable

Commands like `cat` or `vi` are typically external binaries (or applets in BusyBox).

```
type cat
```

Output:

```
cat is /bin/cat
```

Example #3: Check if a command exists (Scripting)

You can use `type` in a script to verify that a required program is installed before trying to run it. This example checks for `cat` and displays the hosts file.

```
CHECK_CMD="cat"

if type "$CHECK_CMD" > /dev/null; then
    echo "Command '$CHECK_CMD' found. Reading /etc/hosts:"
    $CHECK_CMD /etc/hosts
else
    echo "Error: $CHECK_CMD is not installed."
    exit 1
fi
```

Output:

```
Command 'cat' found. Reading /etc/hosts:
```

```
127.0.0.1 localhost
```

2.5.27 unset

The `unset` command removes variables and functions from the current shell execution environment. Once unset, the variable or function is no longer accessible.

By default, `unset` tries to unset a variable. If you want to explicitly unset a function, use the `-f` option.

Synopsis:

```
unset [-v] [-f] <name>
```

Examples:

Example #1: Delete a variable

Define a variable, display it, then remove it.

```
CITY="Prague"
```

```
echo "City is: $CITY"
```

Output:

```
City is: Prague
```

```
unset CITY
```

```
echo "City is: $CITY"
```

Output:

```
City is:
```

Example #2: Delete a function

Define a function and then remove it using the `-f` flag.

```
# Define function
```

```
hello() {
```

```
echo "Hello World"
```

```
}
```

Run function

```
hello
```

Output:

```
Hello World
```

Unset function

```
unset -f hello
```

Try to run it again

```
hello
```

Output:

```
-sh: hello: not found
```

2.5.28 wait

The `wait` command pauses the script execution until a background process finishes. You can specify a Process ID (PID) to wait for a specific process. If no argument is provided, the shell waits for **all** currently active background child processes to complete.

This is essential for scripts that launch parallel tasks and need to ensure they are all finished before proceeding.

Synopsis:

```
wait [PID]
```

Examples:

Example #1: Wait for a specific process

Start a process in the background using `&`, capture its PID using the `$_` variable, and then wait for it to finish.

Start background process

```
sleep 30 &
```

Capture PID

```
PID=$_
```

Wait for the PID

```
echo "Waiting for PID $PID..."
```

```
wait $PID
```

```
echo "Done."
```

Output:

```
Waiting for PID 1045...
```

```
Done.
```

Example #2: Wait for all background processes

If you do not specify a PID, `wait` pauses until all child processes are finished. This is useful for parallel execution.

Start first job

```
sleep 30 &
```

Start second job

```
sleep 30 &
```

Wait for both

```
echo "Waiting for jobs..."
```

```
wait
```

```
echo "All finished."
```

Output:

```
Waiting for jobs...
```

```
All finished.
```

2.5.29 watch

The `watch` command is used to run a specified program periodically, showing its output in real-time. This is useful for monitoring status changes, such as network connections, process lists, or file sizes, without manually re-running the command.

Synopsis:

```
watch [-n SEC] [-t] PROG [ARGS]
```

Options:

Option	Description
-n <SEC>	Specify the update period in seconds (the default is 2 seconds).
-t	Do not print the header (which normally shows the interval, command name, and current time).

Table 153: watch options

Examples:

Example #1: Monitor active network connections

Every 5 seconds, display the current listening ports and active connections using `netstat`.

Run watch with 5-second interval (exit the command by pressing *Ctrl + c*):

```
watch -n 5 netstat -tupln
```

Output (Header included):

```
Every 5.0s: netstat -tupln          2026-02-12 12:45:01
(netstat output follows...)
```

Example #2: Monitor system memory without header

Use the `-t` option to display only the raw output of the `free` command, updated every 2 seconds.

Run watch without header (exit the command by pressing *Ctrl + c*):

```
watch -t free
```

Output:

```
          total          used          free          shared          buff/cache          available
Mem:    1008460      149408      802824           372           56228           845280
Swap:
```

2.5.30 xargs

The `xargs` command reads items from standard input (delimited by blanks or newlines) and executes a specified command using those items as arguments.

It is commonly used in pipelines to process lists of files generated by commands like `find` or `ls`.

Synopsis:

```
xargs [options] [command [initial-arguments]]
```

Options:

Option	Description
-o	Reopen stdin as /dev/tty. This is necessary if you want to run interactive applications (like a text editor) via xargs.
-r	Do not run the command if the standard input is empty (no input).
-t	Print the command line to standard error (stderr) before executing it (verbose mode).
-n <n>	Pass at most <i>n</i> arguments per command line. The command will be executed repeatedly until all input is processed.
-s <n>	Pass a command line of no more than <i>n</i> bytes.
-E <str>	Stop processing input when the string <i>str</i> is encountered.
-e[<str>]	Synonym for -E. If <i>str</i> is omitted, the end-of-file string feature is disabled.

Table 154: xargs options

Examples:

Example #1: Limit arguments per command

Use the `-n` option to process items in groups. In this example, we echo two numbers at a time.

Pipe numbers to xargs

```
printf "1 2 3 4 5 6" | xargs -n 2 echo "Pair:"
```

Output:

Pair: 1 2

Pair: 3 4

Pair: 5 6

Example #2: Delete files found by `find`

Find files named `core` in `/tmp` and delete them. The `-r` option ensures `rm` is not run if no files are found.

Note: This method may fail if filenames contain spaces or newlines.

```
find /tmp -name core -type f -print | xargs -r rm -f
```

3. Related Resources

You can obtain all product-related documents, software updates, and supplementary materials on the Advantech *Engineering Portal* at icr.advantech.com.

For easy access to specific resources, please refer to the following sections of the portal:

- **Router Support Materials:** To access your router's supporting documents (such as the *Hardware Manual* and *Configuration Manual*), the latest firmware, or other technical resources, navigate to *Support* → [Router Models](#). Locate your specific model and select the appropriate tab under the *Documents to download* section. Available tabs include *Brochures*, *Manuals*, *Certificates*, *Firmware*, *Images/3D Models*, *PCN/SA*, and *Others*.
- **Router Apps:** To extend your router's functionality, installation packages and comprehensive manuals for various extension modules are available by navigating to *Download* → [Router Apps](#).
- **Application Notes:** For detailed guides, configuration examples, and step-by-step instructions for implementing specific networking features and use cases, navigate to *Download* → [Application Notes](#).
- **Development Documents:** If you are interested in custom scripting, programming your own applications, or compiling custom modules, navigate to [Development](#) page.

Appendix: Command Index

A

adduser	57
arp	84
awk	129

B

backup	58
basename	30
brctl	85
break	130
bridge	86

C

cat	30
cd	31
cdmaat	4
cdmapwr	5
chdir	31
chmod	59
chown	59
chpasswd	60
clear	130
clog	61
cmp	32
conntrack	88
continue	130
cp	33
curl	90
cut	34

D

date	61
dd	35
decode	35
deluser	62
df	63
dhcrelay	93
dig	91
dirname	36
dmesg	63
doas	64

E

ebtables	95
----------------	----

echo	131
email	97
esim	6
ether-wake	98
ethtool	99
eval	132
exec	133
exit	134
export	135

F

faillock	65
find	36
free	66
ftpput	100
fwupdate	67

G

grep	37
gsmat	9
gsmat2	9
gsminfo	7
gsmpwr	10
gsmpwr2	11
gsmsms	11
gunzip	38
gzip	38

H

halt	11
hash	136
head	39
hostname	101
hwclock	12

I

id	68
ifconfig	102
inc	137
io	13
ip	103
ipcalc	104
iptables	105
iw	106

J

jq 40

K

kill 69

killall 69

klog 70

L

led 14

less 41

let 138

ln 42

local 139

logger 70

losetup 71

lpm 15

ls 43

M

mac 16

mkdir 44

mount 72

mv 44

N

nc 107

net-snmpinform 108

net-snmptrap 109

netstat 110

nohup 140

nsupdate 111

ntpdate 112

O

openssl 73

P

passwd 74

pidof 75

ping 113

ping6 114

port1 16

port2 17

portd 18

printf 141

ps 75

pse 20

pwd 45

R

read 142

readlink 45

readonly 143

realpath 46

reboot 21

report 22

restore 76

return 144

rlog 77

rm 46

rmdir 47

route 115

S

scp 116

sed 48

service 78

set 146

shift 147

shlock 145

shred 49

sipcalc 118

sleep 148

slog 77

sms 23

snmpget 119

snmpset 120

snmptrap 121

source 149

split 50

ssh 122

status 24

stty 27

sudo 79

sync 50

sysctl 79

T

tail 51

tar 52

taskset 80

tc	123
tcpdump	124
telnet	124
test	150
times	80
top	81
touch	53
tpm2	28
tracert	125
tracert6	126
trap	152
type	153

U

umask	82
umount	83
umupdate	83
unset	154

V

vconfig	127
vi	54

W

wait	155
watch	156
wc	54
wget	128

X

xargs	157
xbus	29
xxd	55

Z

zcat	56
------------	----