

General Purpose Command Set



Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

[To the certification exam](#)

- [help](#)
- [system](#)
- [config](#)
- [set](#)
- [flashnet](#)
- [restart](#)
- [ping](#)
- [telnet](#)
- [tracert](#)
- [webcfg](#)
- [rshd](#)
- [ipstat](#)
- [sflowagent](#)
- [acl](#)
- [sntp](#)
- [date](#)
- [erp](#)
- [aaa \(access control using RADIUS server\)](#)
- [license](#)
- [dport](#)
- [mem](#)
- [grep](#)
- [gps](#)
- [tsync](#)
- [SSH protocol](#)
 - [sshd](#)
 - [sshc](#)
 - [sshtun](#)
- [nslookup](#)
- [DNSclient](#)
- [cron](#)

help

Displays system commands information. It is executed automatically, if the user types an unknown command.

Syntax:

```
help
```

system

The command is used to review and update system parameters.

Syntax:

```

sys [args...]
args are:
  user [Login]
  password [Password]
  [no]useAAA
  [no]useLocalAAA
  contact [String]
  guest [guest login]
  name [System Name]
  prompt [any_word]
  location [String]
  mgmtAccount [user:pass@host]
  gpsxy XX.XXXXX YY.YYYYY
  log {on|off} | {show [offset] | clear}| [no]filter | {ADDR | -}
  factorypassword {single|otp}
  search [seconds]
  [no]indicator
  [no]fastroute
  [no]mintgateway
  [no]authFailLog
  [no]sendredirects
  [no]dropredirects
  OfficialAddress X.X.X.X | 0
  icmplimit N [200]
  uptime
  cpu
  [no]pager
  [no]ipforwarding
  info [-f] [NAME]
  version

```

Parameter	Description
user [Login]	Assigns a name under which the system administrator enters the router from the console or remotely, using telnet/http.
password [Password]	Sets the system administrator's password. Use the "setpass" command to remove user name and password.
[no]useAAA	Enables/disables device access control using a RADIUS server. To use the authentication the AAA module should be running (see " AAA (access control using RADIUS server) "). Remember that the AAA authentication method has the highest priority and local login database is used only in case when the required account is not found on the RADIUS server. If there is no local user account the management interface will be accessible with any login and password even if the AAA authentication is turned on.
[no]useLocalAAA	Changes the authentication priority; the local account is checked first, in case it's not found, authentication is performed via RADIUS.
contact [String]	Contact details.
guest [guest login]	Specifies a login for entering a guest mode, any password may be used. In the guest mode the router's configuration parameters neither security-related parameters can't be modified. Use the "system noguest" command to remove guest access.
name [System Name]	The device name that will be displayed in the browser tab title while the web interface is used.
prompt [any_word]	Replaces the prompt on the screen with the given word of a maximum length of 16 characters.
location [String]	Describes the system location; for example in SNMP protocol.

mgmtAccount [user: pass@host]	Access details for the software update server via SNMP.
gpsxy XX.XXXXX YY.YYYYY	Sets the geographical coordinates of the device (longitude, latitude).
log {on off} / {show offset} / {clear} / {no} filter / {ADDR -}	<p>Manages the system log operation:</p> <ul style="list-style-type: none"> • "on" – display messages on the current console. • "off" – stop displaying messages on the console. • "show" – show the system log (time is expressed in seconds/milliseconds back from the current time). • "clear" – clear the system log. • "[no]filter" – removes neighboring identical lines from system log leaving only one copy of each message and counts their recurrence (enabled by default). • "ADDR" – IP address parameter specifies the UNIX host where the system log is located to which messages are directed under the standard "syslog" protocol. In the "syslogd" settings of the server set the "facility.level" equal to "user.notice" or just a numeric value 15 in order to registrate messages. • "-" – disable logging on the remote host.
factorypassword {single otp}	Sets the access mode on the device with the factory password. Each unit has its unique factory access password that can be obtained via the technical support. Once obtained this password stays the same for each factory login attempt (the "single" mode). Setting the unit to "otp" mode tells it to ask for a new password each time the factory login is given (the unit will provide different sequences, that should be submitted to the technical support in order to obtain a new password). Whenever the unit is set to "single" mode again, its unique factory access password is restored.
search [seconds]	Forces all indication to blink for searching the devices in a group of one type units. By default, this mode turns off after 10 seconds.
[no]indicator	Enables/disables LED indicators on the unit in order to hide the active device.
[no]fastroute	Enables/disables the fast routing mode. In this mode the router becomes invisible for traceroute network tracing procedures, while still performing all routing functions. It is not recommended to enable the fast routing mode simultaneously on several devices connected to the same cable Ethernet segment, because this may produce a IP packets storm.
[no]mintgateway	Позволяет использовать в качестве шлюза по умолчанию (default gateway) ближайший узел MINT, который сконфигурирован с опцией "mint extg", если такой имеется.
[no]authFailLog	Enables/disables the unsuccessful authentication attempts logging.
[no]sendredirects	Enables/disables sending "icmp redirect" messages for the packets source suppression if routing is incorrectly configured.
[no]dropredirects	Enables/disables receiving "icmp redirect" messages for routing tables updating if routing is incorrectly configured.
OfficialAddress X.X.X.X / 0	<p>Sets the IP address which will be used as a source IP address in all outgoing connections of the unit.</p> <p>The "0" value removes the current address.</p>
icmplimit N [200]	Sets the limit of the outgoing ICMP packets number per second (0 by default, no limitation applied). It helps to avoid the device reboot while network scanning programs are working. The "0" value removes all limitations.
uptime	Displays the time since the last system's reboot.
cpu	Indicates current CPU load (in percent).
[no]pager	Enables/disables page splits in the console output.
[no]ipforwarding	Enables/disables IP Forwarding.
info [-f] [NAME]	<p>Displays device information:</p> <ul style="list-style-type: none"> • "-f" – full information. • "NAME" – information about specified section.

version	Displays the software version.
----------------	--------------------------------

**NOTE**

Any parameter can be deleted by setting a "." value. Any changes in configuration can be saved by the "config save" command.

config

Allows to view, save, export, and import the device configuration..

Syntax:

```

config [show [KeyWords ...] | save | clear]
config {import | export} login:password@host/file
show - show current configuration
save - store current configuration to flash
clear - clear configuration in flash
import - import configuration from file
export - export configuration to file
-----
backup [list] - show list of backups
backup save N "Comment" - create configuration backup number N [1..8]
backup replace N "Text" - replace configuration backup number N
backup restore N - restore backup number N
backup del N - delete backup number N
backup show N - view text of backup number N
backup comment N "Comment" - change comment for backup N
backup {import | export} N ftp://login:password@host/file

```

Parameter	Description
show	<p>Displays the current configuration of the system. Any change of the system parameters may be immediately viewed using the config show command. The optional parameter may contain a selection of WANFlex commands (abbreviated to their initial letters), as shown in the following examples; only those system parameters will then be displayed which relate to the commands selected.</p> <p>Example:</p> <p>Display MINT and RIP protocols configuration:</p> <pre>co show mint rip</pre> <p>Display the configuration of all commands started with "r" , except "rip":</p> <pre>co show r !rip</pre>
diff	Displays all modifications made since the configuration was saved last time.
save	Saves the current system configuration in the router's flash memory for subsequent permanent use. All modifications to the system parameters, if not saved by this command, are valid only during the current session (until the system reset). After applying this command, the previous configuration is automatically saved as a backup with 0 number.
clear	Clears (resets to default) configuration in device flash. After entering device should be rebooted without saving the configuration.
import	Downloads the device configuration from the remote server. The information is performed using FTP . The file name shall be specified in full, in the format of the remote server's file system.
export	Saves the device configuration to the remote server. The information is performed using FTP. The file name shall be specified in full, in the format of the remote server's file system.

backup [list]	Displays backup configuration list.
backup save N "Comment"	Creates backup configuration N (1 ... 8).
backup replace N "Text"	Replace backup configuration.
backup restore N	Restore backup configuration N.
backup del N	Removes backup configuration N.
backup show N	Displays backup configuration N.
backup comment N "Comment"	Changes backup configuration N description.
backup {import export} N ftp://logi n:password@host /file	Imports/exports backup configuration from/to ftp server.

set

Sets time zone settings. Supports automatic summer/winter time switching.



NOTE

Timezone is determined on Master device and automatically distributed on all other devices, connected with it. Thus, if on Slave devices the timezone is set, then it will be redefined to the timezone of Master.

Syntax:

```
set TZ TIMEZONE
```

Parameter	Description
TIMEZONE	<p>Time zone in POSIX format:</p> <ul style="list-style-type: none"> "std offset" – time zone name and time offset, which must be added for a UTC time value. If only these parameters are specified, then the time zone will be applied without daylight saving time. <p>The following parameters are optional, must be used if automatic summer/winter time switching is needed.</p> <ul style="list-style-type: none"> "[dst] [offset]" – the name and offset for the corresponding Daylight Saving Time zone. start[/time],end[/time] – the day and time of the beginning and end of the period when summer time is applied. The "start" and "end" values are set in the "Mm.n.d" form: <ul style="list-style-type: none"> "Mm" – month, 1...12; "d" – day of week, 0...6, there 0 – is sunday; "n" – week in month, 1...5, there 1 – first week, 5 – last.

Example:

```
set TZ EST+5EDT,M4.1.0/2,M10.5.0/2
set TZ EKT+5
```



NOTE


For detailed information about TIMEZONE format: http://www.gnu.org/software/libc/manual/html_node/TZ-Variable.html

flashnet

Uploads a new software version.

Syntax:

```
flashnet get|put login:password@host/file [-S src_addr]
```

Parameter	Description
get	<p>Loads a new software version into the device from a remote server using FTP. The file name shall be specified in full, in the format of the remote server's file system.</p> <p>The download process has two phases:</p> <ul style="list-style-type: none"> • Reading a file from a remote server and checking its integrity. • Upload the system image to the device's memory. <p>The second phase is indicated with symbol ".".</p> <p>To update the firmware from InfiNet FTP server use command:</p> <pre>flashnet get ftp:ftp@ftp://92.168.100.34/firmware.H11S01v1.6.6.bin</pre> <p>where</p> <ul style="list-style-type: none"> • "H11" – hardware platform. • "1.6.6" – latest firmware version. • "ftp" – username. • "ftp" – password. <div>  NOTE After firmware updating, restart the unit with the command: <pre>restart yes</pre> </div>
put	Uploads current software from the device to a remote server.
-S	Any other IP address (SourceAddress) may be set as default.

restart

Full reset and re-initialization of a router. Equivalent to power off and on. May be used to restore initial configuration after a number of unsuccessful attempts to understand what exactly is done wrong, and after loading a new version of software.

Syntax:

```
restart [y] | [SECONDS] | [stop]
```

Parameter	Description
y	Restart is executed immediately, without asking for confirmation.

SECONDS	The time for which the device restart will be delayed, in seconds. This option can be useful in case of dangerous manipulations with device's configuration when there is a risk to lose control over the device. Repeated entering of this command will start the countdown from the beginning.
stop	Cancels a postponed restart.

ping

Sends test packets ("ICMP_ECHO_REQUEST") to the given IP-address. It allows estimating the attainability of a host and the destination response time.

Syntax:

```
ping IP [-s size_in_bytes] [-c count_packets] [-S IP] [-t sec] [-q] [-l]
```

Parameter	Description
-s size_in_bytes	The test packet length within the range of 10 to 8000 bytes (optional, 56 by default).
-c count_packets	Specifies the number of request messages sent, 5 by default.
-S IP	Sets different source IP address. By default, the sending interface's address is put in the "source address" field of the packets.
-t sec	Interval between sending each request, 1 second by default. Fractional values are possible.
-q	Quiet mode. Displays only summary information.
-l	Same as -q, but displays lost packets.

telnet

Sets up a connection with a remote host specified by the IP address in the terminal emulation mode. The "*telnet*" command uses transparent symbols stream without any intermediate interpretation; therefore, the terminal type is defined by the terminal from which the command has been executed. To interrupt the terminal emulation session, press "Ctrl/D".

Syntax:

```
telnet address [port] [-S source]
```

Parameter	Description
port	Telnet port.
-S source	Device's IP address.

tracert

Traces the packet transmission path up to the host, specified by the "*HostAddress*" parameter. The command sends packets to the specified host, assigning different values to the "*time to live*" field in their IP headers, and analyzes "*ICMP TIME_EXCEEDED*" indications coming from different routers along the path to that host. By default, the sending interface's address is put in the "*source address*" field of the packets. Using the "-s" option, any other IP address (SourceAddress) may be substituted for this default address.

Tracing is limited to a path with maximum 30 intermediate nodes. Trace packets are 36 bytes long. The trace procedure makes 3 attempts for every intermediate node. Every trace result contains the IP address of an intermediate node and the response time (in milliseconds) of every attempt.

Syntax:

```
tracert host [-S src_addr]
```

Parameter	Description
-S src_addr	Node IP address.

**NOTE**

In addition, it may contain some special symbols corresponding to specific reply codes of the ICMP protocol:

- "!" – port unattainable.
- "!N" – network unattainable.
- "!H" – node (host) unattainable.
- "!P" – inappropriate protocol.
- "!F" – too long packet.
- "!X" – access to a node is administratively restricted (filter, proxy etc.).
- "*" – no reply.

webcfg

Web-interface support module.

Syntax:

Available commands are:

```
sta[rt]           Start WEBCFG service
sto[p]           Stop WEBCFG service
cmd[s]           Show additional commands added by WEBCFG
clrc[md]         Clear additional commands added by WEBCFG
```

Available options are:

```
-http={on,off}    Off if Web interface access by HTTPS only
-help -h -?       Help
-lang={en|ru|fr|it|cn} Default language at service startup
```

Parameter	Description
sta[rt]	Enables web-interface support on the device. Web-interface allows easy graphical device configuration with the help of a web-browser.
sto[p]	Disables web-interface support on the device.
cmd[s]	Displays commands applied via web-interface.
clrc[md]	Removes commands applied via web-interface .
-http={on,off}	Enables/disables access to the web-interface via HTTPS.
-help -h -?	List all " webcfg " command arguments.
-lang={en ru fr it cn}	Sets web-interface localization: English, Russian, French, Italian and Chinese.

rshd

Remote Shell (RSH) Server is useful for periodic removal of accumulated statistics from the device (rsh -l mysecretuser [RWR.domain.ru](#) ipstat get). The built-in RSH server makes it possible remote command execution using the "rsh" program. Identification is based on using privileged TCP ports and a list of authorized hosts. By default RSH is disabled.

Syntax:

```
rshd {enable | ipstat | disable} RUSER RHOST LUSER
rshd start | stop | flush | [-]log
```


Parameter	Description
enable	Enters the system with three parameters: <ul style="list-style-type: none"> • "RUSER" – the remote user name (up to 16 symbols). • "RHOST" – remote host IP address. • "LUSER" – the local user name (up to 16 symbols).
ipstat	Allows specified user to use the "ipstat" command only.
disable	Disables an entry with defined parameters.
start	Starts server. When started, the server ignores requests for command execution until at least one valid system entry is enabled. A request for command execution is serviced only if for all three parameters it specifies the values corresponding to a valid entry. Up to 6 independent entries may be defined. The name of a local user is in no relation with the WANFlex main authorization system; it may be considered simply as a keyword.
stop	Stops server.
flush	Clears the RSH server configuration.
[-]log	Enables/disables logging attempts of RSH protocol command using.

Example:

```
rshd enable admin 195.38.44.1 mysecretuser
rshd enable root 195.38.45.123 mysecret2
rshd start
```

Remove the statistics from the device using RSH:

```
#!/usr/bin/perl -w
for(;;)
{
    my $stat;
    do
    {
        $stat = system("rsh -t 30 -n -l root IWR_IP
ips fixit >/dev/null");
        if(int($stat) != 0) { sleep(5); }
    } while (int($stat) != 0);
    do
    {
        $stat = system("rsh -t 30 -n -l root IWR_IP
ips fixget >stat.tmp");
        if(int($stat) != 0) { sleep(5); }
    } while (int($stat) != 0);
    do
    {
        $stat = system("rsh -t 30 -n -l root IWR_IP
ips fixclear >/dev/null");
        if(int($stat) != 0) { sleep(5); }
    } while (int($stat) != 0);

    system("cat stat.tmp >>stat.txt");


    sleep(300);
}
```

ipstat

The IP statistics gathering module provides for collecting information on data flows traversing the router, for further analysis and/or for accounting. Information is accumulated in the router's RAM memory as a series of records having three fields: source address, destination address, number of bytes transferred. By default, only outgoing packets are counted, at the moment they are sent to a physical interface.

Syntax:

```
ipstat enable [incoming|outgoing|full] [detail] [SLOTS] | disable
ipstat clear
ipstat traf [detail] [speed | total_bytes | pps] [reverse] [[if=IFNAME] [swg=N] -f "PCAP"]
ipstat fixit | fixget | fixclear
ipstat strict | -strict
ipstat add [intf] [swg=N] -f "PCAP"
ipstat del num
ipstat rearrange [N]
```

Parameter	Description
enable <i>[incoming outgoing full]</i> <i>[detail] [SLOTS] disable</i>	Enables/disables IP statistics gathering: <ul style="list-style-type: none"> "incoming/outgoing" – allows gathering only incoming/outgoing packets. "full" – gathering both incoming and outgoing packets. "detail" – detailed IP statistics gathering including ports and protocols information. "SLOTS" – allows to set the maximum number of records in the "ipstat" table. By default – 1000, this amount is usually enough for 15-20 minutes on a common subscriber terminal. One record takes 12 bytes.
clear	Clear accumulated statistical info.
traf <i>[detail] [speed total_bytes pps] [reverse]</i> <i>[[if=IFNAME] [swg=N] -f "PCAP"]</i>	Allows visually inspect statistics collection process in real time: <ul style="list-style-type: none"> "detail" – switches on detailed IP statistics gathering including ports and protocols information. "speed" – sorts the command output by transmission rate. "total_bytes" – sorts "ipstat" output according to the number of transmitted bytes for the whole period. "pps" – sorts the command output by the number of transmitted bytes in second. "reverse" – allows to sort by the specified criterium (speed total_bytes pps) in reverse order. "if=IFNAME" – the command output for the specified port. "swg=N" – the command output for the specified switch group. "-f "PCAP" – the command output for the specified pcap expression.
fixit	Dumps the statistic from the router's memory into an intermediate buffer. The memory is cleared, statistic accumulation starts from the begginig.
fixget	Shows the dump buffer content. This command may be executed any number of times, with no damage to the dumped statistical info.
fixclear	Clears the temporary dump buffer.
strict -strict	If the record table in the router memory overflows, or if there is not enough memory currently available, an appropriate warning is written into the system log, and further statistical data are discarded. If the "strict" option is enabled, then at the overflow condition the transit routing is disabled, but the router still responds to any protocol.
add <i>[intf] [swg=N] -f "PCAP"</i>	Limits the packets number to those that satisfy the added rule: <ul style="list-style-type: none"> "intf" – the interface name through which the packet enters the system. "swg=N" – accepts packets belonging to the switch group N. "-f "PCAP" – pcap expression filter. <div>  NOTE The syntax of the rules is equal to the "ipfw" command syntax. </div>
del num	Deletes the N-th rule from the list.

rearrange [N]	Renumbers all the ipstat rules with the given increment (default step is 1).
----------------------	--

sflowagent

Realization of a standard Sflow protocol. Sflow – is protocol for monitoring computer networks. It is commonly used by Internet Providers to capture traffic data in switched or routed networks.

Syntax:

```
Available commands are:
sta[rt]           Start Sflow agent
sto[p]           Stop Sflow agent
wi[pe]           Stop Sflow agent and clean all configuration
add[instance] 'name' Add instance (default 'ipstat')
del[instance] 'name' Delete instance (default 'ipstat')
stat 'name'       Show statistics for instance (default 'ipstat')
cl[earstat] 'name' Clear statistics for instance (default 'ipstat')

Available options are:
-collector=IPaddress[:port] Set collector address (default 0.0.0.0:6343 )
-agent=IPaddress           Set agent address (default 0.0.0.0)
-maxpacket=size            Set maximal datagram size (default 1472)
-interval=number           Set statistics receive interval, in seconds (default 15)
-datagrams=number          Set datagrams per statistics interval (default 100)
-rawheader={on|off}        Send packets raw header instead IPv4 data (default off)
-debug={on|off}            Display debug output (default off)
-version -v               Display Version
```

Parameter	Description
sta[rt]	Starts Sflow agent.
sto[p]	Stops Sflow agent.
wi[pe]	Stops Sflow agent and clears its configuration.
add [instance] 'name'	Adds statistics gathering component ("ipstat" by default).
del [instance] 'name'	Deletes statistics gathering component ("ipstat" by default).
stat 'name'	Shows statistics for a component ("ipstat" by default).
cl[earstat] 'name'	Clears component statistic ("ipstat" by default).
- collector=IP address[: port]	Sets address of a collector that process sflow-packets. Default port is 6343.
- agent=IP address	Sets agent's own address (device).
- maxpacket=size	Sets maximum size of a Sflow-packet in bytes. 1472 bytes by default. Upper bound is limited by hardware and operational system capabilities. In case of its exceeding packet size will be decreased to acceptable value.
- interval=number	Time in seconds equal to interval with which statistics is delivered from instance. Increasing of this parameter leads to increasing in overall system efficiency but in case of unexpected network activity splash data could be lost. 15 seconds by default.

- datagrams= number	Maximum number of datagrams between times of receiving statistics from instance. Increasing of this parameter leads to the decrease in datagram average size and increases in theoretical number of delivered statistics data. Reduces the load on the CPU but in the same time reduces overall system efficiency. However, reducing of system efficiency doesn't happen with low traffic. It is recommended to increase this parameter when decreasing maxpacket parameter and/or when increasing interval parameter. 100 by default. Maximum flow: sflow= datagrams /interval* maxpacket, (Bytes/sec)
-rawheader= {on off}	Sends original ip4v headers in spite of statistics data ("off" by default). Used for compliance with traffic monitoring programs.
-debug= {on off}	Adds debug output to the log.
-version -v	Shows current Sflow agent version.

Output parameter description.

Parameter	Description
Cycles	Overall number of gathering statistics success cycles.
Overflow records	Number of records in Instance for all cases when Instance overflowed earlier then interval period had ended.
Overflow count	Number of times when Instance overflowed earlier then interval period had ended.
Samples	Number of grouped records delivered from "flow records".
Datagrams	Overall number of sent datagrams.
Records	The number of statistics records.
Bytes	Overall number of transmitted data by Sflow protocol.
Unused datagrams	Number of datagrams that could be created in compliance with datagrams parameter but was not used.
Dropped records	Number of discarded datagrams.
Dropped samples	Number of discarded records delivered from "flow records".
Pending datagrams	The number of datagrams waiting to be sent.
Lost flow records	Number of "flow records" that were discarded because of "maxpacket", "interval" and "datagrams" parameters low values.
Lost overflow records	Number of times when Instance overflowed earlier then interval period had ended and data were lost.

Example:

```
ipstat enable full detail 3000
sflow add ipstat
sflow -collector=1.2.3.4 start
```

acl

While network planning it is often necessary to group similar parameters in lists which can be used for different filters (e.g. "ipfw", "qm", "ipstat"). Access control lists can effectively solve this problem.

Syntax:

```

acl add $NAME TYPE XXX ...
acl del $NAME [XXX ...]
acl ren $NAME1 $NAME2
acl flush
Possible TYPES: net num
Predefined ACL names:
  $ACLOCAL net    - Hosts (networks) permitted to access the device.
  $LOCAL  net     - all local IPv4 addresses (only for ipfw/qm).

```

Parameter	Description
add \$NAME TYPE XXX ...	Creates an access list with " <i>NAME</i> " title and " <i>TYPE</i> " type. Lists names must start with \$ symbol and can include up to 7 letters, digits and other symbols excluding spaces and semicolon. At the same time the command can contain several parameters of " <i>TYPE</i> " type which will be included in the list. If the list with this name has been already created listed parameters will be attached to this list.
del \$NAME [XXX ...]	Removes specified parameters from the " <i>NAME</i> " list. If none of parameters are mentioned all list will be deleted.
ren \$NAME1 \$NAME2	Changes list's name from " <i>NAME1</i> " to " <i>NAME2</i> ".
flush	Removes all lists
Accepted list types (TYPE)	
net	<p>Contains network addresses in dot format:</p> <ul style="list-style-type: none"> • xxx.xxx.xxx.xxx или xxx.xxx.xxx.xxx/MASKLEN or • xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx. <p>Lists of "<i>net</i>" type optimize their parameters by excluding duplicates and by having the feature that enables bigger networks include smaller networks. For example, if the list contained 1.1.1.1 parameter, when you include 1.1.1.0/24 parameter in the list 1.1.1.1 will be excluded.</p> <p>Example:</p> <pre> acl add \$LIST1 net 10.0.0.0/8 192.168.0.0/16 5.5.5.5 acl del \$LIST1 100.100.100.100/28 </pre>
Reserved access lists	
\$ACLOCAL net	<p>List of IP addresses for access limitation to the device via telnet, ssh, http/https, snmp protocols (ports 22, 23, 80, 162, 443).</p> <p>In case "\$ACLOCAL" access list is in the configuration all attempts to establish a connection with the device from addresses (networks) that are not in this list will be rejected. There is no need to create rules.</p> <p>Example:</p> <pre> acl add \$ACLOCAL net 10.0.0.0/8 192.168.0.0/16 </pre>
\$LOCAL net	All local IP addresses assigned to the device. It can be used to set filters to restrict/allow access to the device via telnet, ssh, http/https, snmp (ports 22, 23, 80, 162, 443). For detailed information about filters configuration see the ipfw command (IP Firewall) article.

**NOTE**

From the MINTv1.90.36 and TDMAv2.1.10 software versions, the \$ACLOCAL filter matching is not recorded in the system log, as it worked before. If you need to enable logging, use the "*td log*" command.

Allows the system to synchronize the time with configured NTP server using fourth version of SNTP protocol [RFC 2030](#). Client works in unicast server request mode in certain time range.

Since MINT provides both time and timezone synchronization it's not necessary to use SNTP protocol for host to host time synchronization. So the optimal synchronization scenario is as follows:

1. Master device
 - a. SNTP client is disabled and configured to receive time from corporate or public source.
 - b. SNTP server is disabled.
2. Slave device
 - a. SNTP client is disabled - synchronization is performed by MINT.



NOTE

Starting 1.90.29 software version SNTP transmit not only time data, but also timezone. Thus, there is no need to manually configure timezones on Slave devices. Their timezones will be automatically updated if they are synchronized with the Master via SNTP protocol.

Syntax:

```
sntp [options] [command]
where commands are:
  start - start service
  stop  - stop service
where options are:
  -server={ipaddr}    - set sntp server address
  -gps={on|off}       - enable/disable GPS time source
  -interval={seconds} - specify poll interval in seconds [1800]
  -supplier={on|off}  - enable/disable server mode
  -debug={on|off}     - enable/disable debug information
```

Parameter	Description
start	Starts time synchronization process.
stop	Stops process.
-server={ipaddr}	<p>Set SNTP server IP address.</p> <p>Example:</p> <pre>sntp -server=9.1.1.1</pre>
-gps={on off}	<p>Enable/disable GPS time source. In case the external synchronization unit AUX-OUT-SYNC is connected to the device, the built-in GNSS receiver can be used as a precise time source (if there are signals from satellites constellation). It is not necessary to set the external SMTP server address.</p> <p>Example:</p> <pre>sntp -server='ip-external-sntp-server' -gps=on</pre> <p>In this case, the device will use both the satellite and the external SNTP server as the source of the precise time, and the satellite source will be the priority.</p>
-interval={seconds}	<p>Specifies poll interval in seconds, by default is 1800.</p> <p>Example:</p> <pre>sntp -interval=5000</pre>

-supplier= {on off}	Enables/disables server mode support.
-debug= {on off}	Enables/disables debug information logging. Example: <div>sntp -debug=on sntp -debug=off</div>

date

Date and time management. Shows or sets the date and time in WANFlex system. While setting the date and time not only kernel clock is being changed but hardware clock changes its value either (if the device supports this feature).

Syntax:

```
date [[[[cc]yy]mm]dd][HH]MM[.ss]]
```

Parameter	Description
cc	Century, 20 or 21.
yy	Year in abbreviated form (i.e. 89 for 1989, 05 for 2005).
mm	Month in numeric form (1 to 12).
dd	Day (1 to 31).
HH	Hour (0 to 23).
MM	Minute (0 to 59).
ss	Second (0 to 61 - 59 plus maximum two leap seconds).

Examples:

```
date 20040210053004
Tue Feb 1005:30:042004
```

```
date
Tue Feb 1005:30:102004
```

erp

Emergency Repair Procedure utility allows restoring lost system password to the device.

Syntax:

```

erp [options] [command]
[options]:
  -serial <n>      - device serial number
  -code <c>        - ERP code (Factory password)
  -ip <address>    - interface IP address
  -mask <mask>     - interface IP address mask

[command]:
  boot            - force continuing boot on device(s).
                   Device serial number may be unspecified
                   and means 'any device'.
  reset           - resets device's configuration.
                   Serial number and ERP code must be specified
  ifup            - turns up device's interface and adds IP address
                   and mask alias to it. Serial number, IP address
                   and IP address mask should be specified
  If command is not specified, then it's assumed the 'boot' command.

```

Parameter	Description
-serial <n>	Device serial number.
-code <c>	Special ERP code (factory password).
-ip <address>	IP address of device's Ethernet interface.
-mask <mask>	Network mask.
boot	Device reboot.
reset	Resets device configuration including system user name and password. Serial number and special ERP code must be specified.
ifup	Turns up device's Ethernet interface (eth0) and adds IP address and net mask alias to it. Serial number, IP address and net mask should be specified.

Two InfiNet Wireless devices are required to perform Emergency Repair Procedure. First device is a device which should be repaired, second – device on which ERP utility will be run to repair the first device. Both of the devices should be connected to the same Ethernet segment via their Ethernet interfaces. The second device should have no "*switch local tag <x>*" option configured on its Ethernet interface.

Password restore procedure:

- Run the ERP utility with "*serial*" option and specify a repairing device serial number. ERP will go to standby mode waiting for a first device to reboot.

```
erp -serial <SERIAL>
```

- Reboot device which should be repaired by power off and on.
- After device is rebooted ERP will show "*Sequence*" parameter value and serial number of device. Please contact InfiNet Wireless tech support and provide these values.
- The tech support write back an ERP code.
- Run the following ERP command:

```
erp -serial <SERIAL> -code <ERP code> reset
```

- Reboot a repairing device again.
- The utility will reset login, password and configuration on device to default.
- Login to a repairing device with any non-blank username and password and enter the following command:

```
config save
```

To change IP address on Ethernet interface of a repairing device from a second device without login use the following command:


```
erp -serial <SERIAL> -ip <address> -mask <mask> ifup
```

aaa (access control using RADIUS server)

The "aaa" module allows access control configuration on the device using remote RADIUS server.

Syntax:

```
aaa [options] [command]
  where commands are:
    start - start service
    stop  - stop service
  where options are:
    -auth=ip[:port],secret[,identifier] - RADIUS server parameters,
                                          address      - Server IP Address
                                          secret       - shared secret
                                          identifier  - NAS Identifier
                                          this option can be repeated.
    -remove=ip[:port]                  - Remove RADIUS server.
```

Parameter	Description
start	Starts "aaa" utility.
stop	Stops "aaa" utility.
-auth=ip[:port],secret[,identifier]	Sets parameters to access remote RADIUS server: <ul style="list-style-type: none"> "ip[:port]" – IP address and port of a RADIUS server. "secret" – password to access the server. "identifier" – Network Access Server ID.
-remove=ip[:port]	Removes information about a RADIUS server from the configuration.

Whenever the debug mode is activated on a device that uses "aaa" access authentication via the remote RADIUS server, the authentication debug info is displayed on the local console to verify the settings.

Parameter	Description
Request id	Internal unique id of the request.
Type	Request type, i.e. "Access-Request".

The RADIUS attributes for Access-Request and Access-Accept requests are shown in the tables below.

Access-Request

Attribute	Description
1 - User-Name	The user name
2 - User-Password	The password
4 - NAS-IP-Address	IP address of the remote access server
6 - Service-Type	The Login (1) value is sent
31 - Calling-Station-Id	IP address of the connecting device
32 - NAS-Identifier	Base station symbolic name

Title

61 - NAS-Port-Type	The Virtual (5) value is sent
---------------------------	-------------------------------

Simplified, extended support of the RADIUS server for the wireless connections identification is provided:

Attribute=Value	Description
1 - User-Name = "00-00-00-00-00-00"	Connecting device MAC address
2 - User-Password = "dummy"	Dummy predefined value
6 - Service-Type = Framed (2)	The Framed (2) value is sent
31 - Calling-Station-Id = "00-00-00-00-00-00"	MAC address of the connecting device
2 - NAS-Identifier = "Infinet Base 1"	Base station symbolic name
61 - NAS-Port-Type = Wireless-802.16 (27)	Value Wireless-802.16 (27)

Access-Accept

Attribute	Description
Session-Timeout	If the response from the RADIUS server contains the Session-Timeout parameter, then after a specified time (sec.), a new authentication request will be sent to extend or break the existing link. Value: 3600 seconds

license

The "license" command manages operations with a license file on the device.

Syntax:

```
license [options]
options are:
--install=<url> - install new license
--export=<url>  - export current license to external server
--show         - show license info
<url> = ftp://[login[:password]@]host/file
```

Parameter	Description
-install=<url>	Uploads license file into the device from a remote server using FTP.
-export=<url>	Downloads license file from the device to a remote server using FTP.
-show	Displays license information on the screen.

Example:

```
li --export=ftp://ftp_login:ftp_password@192.168.145.1/license_file
li --show
```

dport

This command sets a console port bitrate. Available values are: 9600, 19200, 38400, 57600, 115200 Bit/sec. Default value is 38400 Bit/sec.

Syntax:

```
dport BAUD
```

mem

This command show statistics for allocated device memory, network buffers, queues and drops on interfaces. Command output is described in the picture below.

Syntax:

mem

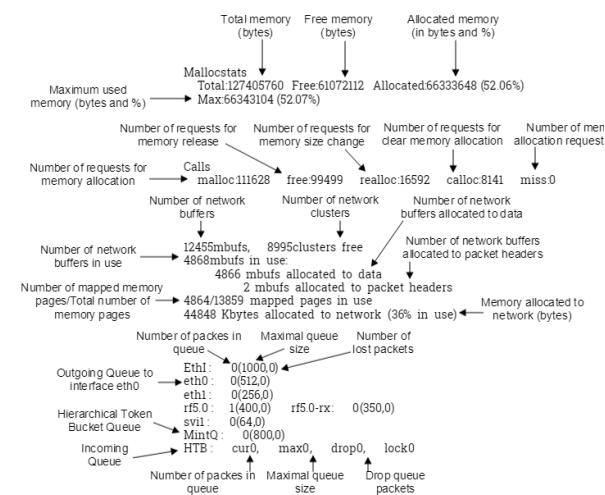


Figure- "mem" command output

grep

The "grep" command searches the output of the given command for lines matching the given PATTERN and displays the result.



CAUTION

This command is not available on the H01/H02 platforms.

Syntax:

```
grep [OPTIONS] [-e]PATTERN "command"
or
command | grep [OPTIONS] [-e]PATTERN
```

OPTIONS:

```
-e PATTERN, --regexp=PATTERN
    Use search PATTERN possibly beginning with (-)
-i, --ignore-case
    Ignore case distinctions in PATTERN
-v, --invert-match
    Invert the sense of matching, to select non-matching lines
-w, --word-regexp
    Select only those lines containing matches that form whole words
-x, --line-regexp
    Select only those matches that exactly match the whole line
-c, --count
    Suppress normal output; instead print a count of matching lines
    With the -v, --invert-match option, count non-matching lines
-m NUM, --max-count=NUM
    Stop parsing after NUM matching lines
-n, --line-number
    Prefix each line of output with the 1-based line number
-A NUM, --after-context=NUM
    Print NUM lines of trailing context after matching lines
    Places a group separator line (--) between contiguous groups of matches
-B NUM, --before-context=NUM
    Print NUM lines of leading context before matching lines
    Places a group separator line (--) between contiguous groups of matches
-C NUM, --context=NUM
    Print output context NUM lines before and NUM lines after matching lines
    Places a group separator line (--) between contiguous groups of matches
```

Parameter	Description
-e PATTERN, --regexp=PATTERN	Uses a searching PATTERN that starts with "-" sign.
-i, --ignore-case	Ignore case distinction between capital and lowercase letters.
-v, --invert-match	Perform the invert filtering.
-w, --word-regexp	Display only those lines that matches the whole word.
-x, --line-regexp	Display only those lines that matches the whole line.
-c, --count	Does not display output, but number of lines matched, in combine with "-v, --invert-match" option - number of non-matching lines.
-m NUM, --max-count=NUM	Stops searching after the specified number of matching lines
-n, --line-number	All the command output lines are index numbered starting from 1.
-A NUM, --after-context=NUM	Prints the specified number "NUM" of lines, situated after "A" lines, matching given PATTERNS. Resulting output is separated from other matching entries with a special line (--).
-B NUM, --before-context=NUM	Prints the specified number " NUM" of lines, situated after "B" lines, matching given PATTERNS. Resulting output is separated from other matching entries with a special line (--).
-C NUM, --context=NUM	Prints the specified number " NUM" of lines, situated after "C" lines, matching given PATTERNS. Resulting output is separated from other matching entries with a special line (--).


gps

Manages GPS/GLONASS module.

Syntax:

```
gps [options] [command]
Options:
  -t=<level> - turn trace level (1, 2 or 0 - turn trace off)
  -i=<int>   - set integrator time constant in seconds
  -a[=(0:1)] - turn the power on the antenna amplifier
  -r[=(0:1)] - set reset signal
  -p=<port>  - set TCP port for service (2323 by default)
  -s=<baudrate|0> - set baud rate for GPS NMEA port (0 - set 115200)
Command:
  start      - start GPS service
  stop       - stop  GPS service
  coordinates - show  GPS coordinates
  console     - map GPS NMEA port to stdin/stdout
  tcp        - map GPS NMEA port to TCP service
  stat       - show GPS statistics
  clear      - clear GPS statistics
```

Parameter	Description
-t=<level>	Service messages logging level: <ul style="list-style-type: none"> • "2" – logging all NMEA messages received from GPS/GLONASS module. • "1" – logging information about connection/disconnection to GPS/GLONASS, changing the number of visible satellites or a significant change in coordinates. • "0" – no logging is performed.
-a[=(0:1)]	Turn on/off the power supply to the antenna amplifier (if any): <ul style="list-style-type: none"> • "1" – turn on (by default, if value is not specified). • "2" – turn off.
start	Starts GPS/GLONASS module.
stop	Stops GPS/GLONASS module.

coordinates	Displays information about current GPS/GLONASS receiver state.
Command output:	
<pre>#l> gps coordinates Satellites: 8 LAT/LONG: 56.811911/60.547041 Altitude: 275.89 HDOP: 0.92 FIX: 3D, GLONASS Total GPS time: 17:43:19 Total nonvalid time: 00:00:01(0%) Number of losses: 0 Now coordinates are valid last 17:43:18 Satellites histogram: ^ 2.0 + 3.0 + 4.0 + 5.0 + <1% 6.0 + 1% 7.0 + 99% v SATmin= 5 SATmax= 10</pre>	
<ul style="list-style-type: none"> "<i>Satellites</i>" – current number of visible satellites. "<i>LAT/LONG</i>" – receiver geographic coordinates in degrees: <ul style="list-style-type: none"> "<i>LAT</i>" – latitude -90.000000° ... +90.000000°. "<i>LONG</i>" – longitude -180.000000° ... +180.00000°. "<i>Altitude</i>" – height above sea level in meters. "<i>HDOP</i>" – horizontal plane coordinates accuracy reduction coefficient. 	
<div>  CAUTION <p>For reliable time synchronization, it is recommended to use less than 1,5 the "<i>HDOP</i>" parameter values.</p> </div>	
The GNSS system can have following values:	
<ul style="list-style-type: none"> GPS. GLONASS. GPS+GLONASS. 	
Statistic data (can also be displayed by " <i>gps stat</i> " command):	
<ul style="list-style-type: none"> "<i>Total GPS time</i>" – total time of GPS service operation. "<i>Total nonvalid time</i>" – total time during which the coordinates were nonvalid. "<i>Number of losses</i>" – coordinates losses number. "<i>Now coordinates are valid last ...</i>" – time of GPS service operation since coordinates become valid. "<i>Satellites histogram</i>" – visible satellites histogram. "<i>SATmin</i>" and "<i>SATmax</i>" – the minimum and maximum number of visible satellites recorded since the last statistics reset. "<i>FIX - NO FIX 2D 3D</i>" – coordinate determination current state. Following values are available: <ul style="list-style-type: none"> "<i>NO FIX</i>" – coordinates are not defined. "<i>2D</i>" – latitude and longitude are defined. "<i>3D</i>" – latitude, longitude and height above sea level are defined. 	
stat	Displays statistic about GPS/GLONASS module operation (without current receiver state).

clear	Clears statistic.
--------------	-------------------

**CAUTION**

Note, that "*tcp*", "*console*", "*-i*", "*-r*", "*-p*" and "*-s*" parameters are used for diagnostics and debugging in case of emergency and only by specialists.

**NOTE**

The "*gps*" command is available in software version with the TDMA technology support.

tsync

Manages external synchronization source.

Syntax:

```
tsync [command]
Command:
  enable [BAUDRATE] - enable external synchronization sources
  disable           - disable external synchronization sources
  [no]trace         - turn trace (debug) messages output to syslog
  [show]            - show statistics
  clear             - clear statistics
```

Parameter	Description
<i>enable [BAUDRATE]</i>	Enable synchronization by using external source.
<i>disable</i>	Disable external source.
<i>[no]trace</i>	Enable message output tracing (debugging) in the syslog.
<i>[show]</i>	Displays statistic.
<i>clear</i>	Clears statistic.

**NOTE**

The "*tsync*" command is available in software version with the TDMA technology support.

SSH protocol

SSH (Secure Shell) protocol allows secure remote management of network devices. Its functionality is similar to Telnet protocol but, as opposed to Telnet, SSH encodes all protocol messages/datagrams including transmitted passwords. For using SSH protocol SSH Server and SSH Client is needed. SSH Server accepts connections from client hosts (SSH Clients), performs their authentication and start serving the authorized clients.

InfNet Wireless devices has built-in SSH Server and SSH Client functionality.

sshd

Built-in SSH Server (SSH daemon) configuration is performed using "*sshd*" command. By default, the SSH Server is disabled.

Access to the device via SSH protocol may be limited by using "*\$ACLOCAL*" access control list. When "*\$ACLOCAL*" list is configured on the device SSH Server rejects all connection attempts from SSH Clients with IP address or networks that are not present in the list.


Syntax:

```

sshd -help, -h
sshd -port=PORT
sshd -window=SIZE
sshd -keepalive=TIME
sshd -banner=on | off
sshd -log-level={emerg|alert|crit|error|warning|notice|info|debug|LEVEL} [notice]
sshd -algo-list
sshd -kex-algos[=ALGO-LIST]
sshd -hostkey-algos[=ALGO-LIST]
sshd -cipher-algos[=ALGO-LIST]
sshd -hash-algos[=ALGO-LIST]
sshd -comp-algos[=ALGO-LIST]
sshd -auth-methods[=AUTH-METHODS-LIST]
sshd -none-cipher=on | off
sshd start
sshd stop
sshd newkeys
sshd pub[key] {sh[ow] | cl[ear] | de[lete] N}
sshd pub[key] {in[stall] | im[port] [LOGIN[:PASSWORD]@]HOST/FILE} [COMMENT]
sshd tun[nel] add LOGIN PASSWORD IFNAME
sshd tun[nel] del LOGIN | clear

```

Parameter	Description
-help, -h	Displays the command syntax.
-port=PORT	SSH Server TCP port number, which is used to receive connections SSH, by default is 22.
-window=SIZE	Allows changing SSH Server internal receiving window size in bytes. SSH Server window size defines maximum allowed bandwidth for "SSH Client - SSH Server" data channel. By default, SSH Server window size is 24576 bytes.
-keepalive=TIME	Sets session activity check duration period in seconds. By default server doesn't make activity check ("0" value).
-banner=on off	Shows/hide IW WANFlex SSH information banner after login.
-log-level={emerg alert crit error warning notice info debug LEVEL} [notice]	<p>Allows choosing logging levels of the SSH Server service information that will be written into the system log, to manage system log please use "sys log" command.</p> <p>Different levels of logging can be chosen by "emerg", "alert", "error", "warning", "notice", "info", "debug" parameters or specified by the number of the needed level (from 0 to 7) using numeric "LEVEL" parameter. By default, "info" (6th level) is chosen.</p>
-algo-list	Shows a list of all available SSH algorithms for key exchange (<i>kex</i>), authentication (<i>host key</i>), data encoding (cipher), data verification (<i>hash</i>) and data compression (<i>compress</i>).
-kex-algos[=ALGO-LIST]	Choosing kex algorithms from the list of algorithms (ALGO-LIST), to be used in SSH key exchange process.
-hostkey-algos[=ALGO-LIST]	Choosing host key algorithms from the list of algorithms (ALGO-LIST), to be used in SSH Server-Client authentication process.
-cipher-algos[=ALGO-LIST]	Choosing cipher algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data encoding.
-hash-algos[=ALGO-LIST]	Choosing hash algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data verification.
-comp-algos[=ALGO-LIST]	Choosing compression algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data compression.
-auth-methods[=AUTH-METHODS-LIST]	<p>Choosing an available authentication method from the (AUTH-METHODS-LIST) list.</p> <p>An "all" value enables all authentication methods (set by default).</p>
-none-cipher=on off	Enable/disable encoding usage. Used when the simple TCP tunnel is needed, that significantly reduces the CPU load.
start	Starts SSH Server.
stop	Stops SSH Server.

<i>newkeys</i>	Host Keys re-generation. <div>  NOTE When first-time started SSH Server generates DSS and RSA Host Keys to be used for public key based SSH Server authentication. </div>
<i>pub[key] {sh[ow] cl[ear] de[lete] N}</i>	<ul style="list-style-type: none"> • "show" – shows SSH Client's public keys that are registered in the SSH Server list. • "clear" – deletes all the SSH Client's public keys from the SSH Server. • "delete" – deletes a certain SSH Client's public key from the SSH Server list. Parameter "N" – is an index of the key in the list.
<i>pub[key] {in[stall] im[port] [LOGIN[:PASSWORD]@]HOST /FILE} [COMMENT]</i>	Allows enabling public key based authentication of SSH Clients. In the Public key authentication mode SSH Server authorize SSH Client bypassing password login procedure. This mode is enabled automatically once a public key of the SSH Client is cached in SSH Server's registry: <ul style="list-style-type: none"> • "install" – sets the SSH client public key in the SSH server registry. • "import" – imports an SSH client's public key into the SSH server registry from a remote FTP server: <ul style="list-style-type: none"> • "HOST" – remote FTP server IP address. • "FILE" – file containing SSH Client's RSA/DSS public key in OpenSSH or SSH2 format. If login and password are set on the remote FTP server they should be specified as "LOGIN" and "PASSWORD" parameters. • "COMMENT" – allows adding a comment to the public key entry in the SSH Server list of clients public keys. By default, a comment with clients IP address or FTP IP address from where the key was obtained is added.
<i>tun[nel] add LOGIN PASSWORD IFNAME</i>	Sets separate authentication parameters for each tap interface: <ul style="list-style-type: none"> • "LOGIN" – username. • "PASSWORD" – password. • "IFNAME" – tap interface name. <p>If the values above are not specified, default authentication parameters will be used.</p>
<i>tun[nel] del LOGIN clear</i>	<ul style="list-style-type: none"> • "del LOGIN" – deletes specified username from the SSH Tunnel configuration. • "clear" – deletes all SSH Tunnel users from SSH Server configuration.

**NOTE**

By default SSH Server applies only password authentication. However, this may not be enough to provide the necessary security level. InfiNet Wireless devices have several built-in SSH authentication methods, which are managed by "*sshd pubkey*" and "*sshd -auth-methods*" command. At the same time, an SSH Server will keep the connected SSH client public key.

sshc

Built-in SSH Client configuration is performed using "*sshc*" command.

Syntax:

```
ssh [options] [LOGIN@]HOST[:PORT] [REMOTE-COMMAND]
options:
  -help, -h
  -window=SIZE
  -keepalive=TIME
  -compress, -C
  -bind-addr=ADDR, -b ADDR
  -pubkey-show
  -pubkey-new[=BITS]
  -pubkey-clear
  -pubkey-export=[LOGIN[:PASSWORD]@]HOST/FILE
  -algo-list
  -kex-algos[=ALGO-LIST]
  -hostkey-algos[=ALGO-LIST]
  -cipher-algos[=ALGO-LIST], -c ALGO-LIST
  -hash-algos[=ALGO-LIST], -m ALGO-LIST
  -comp-algos[=ALGO-LIST]
```

Parameter	Description
[options] [LOGIN@]HOST[:PORT] [REMOTE-COMMAND]	Connect to the remote SSH Server: <ul style="list-style-type: none"> • "LOGIN" – username (maybe omitted when default logging name is used on the remote device). • "HOST" – a remote device IP address. • "REMOTE-COMAND" – defines a command that should be executed on the SSH Server after successful login.
-help, -h	Displays the command syntax.
-window=SIZE	Allows changing SSH Server internal receiving window size in bytes. SSH Server window size defines maximum allowed bandwidth for "SSH Client - SSH Server" data channel. By default, SSH Server window size is 24576 bytes.
-keepalive=TIME	Sets a frequency of sending compulsory session activity confirmations to the server. This allows not to loose the session to the server when SSH Client leaved unused for a long time period. By default, SSH Client doesn't send any special activity confirmations ("0" value). Measured in seconds.
-compress, -C	Enables data compression.
-bind-addr=ADDR, -b ADDR	Sets SSH packets source IP address. This source IP address substitutes the default sending interface's IP address field of the SSH packets.
-pubkey-show	Displays generated public keys.
-pubkey-new[=BITS]	Generates new DSS and RSA SSH Client's public keys. "BITS" parameter should be specified as a key size in bits, possible values: 512-4096.
-pubkey-clear	Deletes public keys on SSH Client.
-pubkey-export=[LOGIN[:PASSWORD]@]HOST/FILE	Exports public keys from SSH Client to a file on the remote FTP server: <ul style="list-style-type: none"> • "HOST" – remote FTP Server IP address. • "FILE" – a file name that will contain SSH Client's RSA/DSS public keys. If login and password are set on the remote FTP server they should be specified as "LOGIN" and "PASSWORD" parameters.
-algo-list	Shows a list of all available SSH algorithms for key exchange (<i>kex</i>), authentication (<i>host key</i>), data encoding (<i>cipher</i>), data verification (<i>hash</i>) and data compression (<i>compress</i>).
-kex-algos[=ALGO-LIST]	Choosing kex algorithms from the list of algorithms (ALGO-LIST), to be used in SSH key exchange process.
-hostkey-algos[=ALGO-LIST]	Choosing host key algorithms from the list of algorithms (ALGO-LIST), to be used in SSH Server-Client authentication process.
-cipher-algos[=ALGO-LIST], -c ALGO-LIST	Choosing cipher algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data encoding.

-hash-algos[=ALGO-LIST], -m ALGO-LIST	Choosing hash algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data verification.
-comp-algos[=ALGO-LIST]	Choosing compression algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data compression.

**NOTE**

For compulsory SSH Client's session interruption (for example, if SSH Server is not responding to SSH Client's requests) please use the following key sequence: "Enter~." (on the keyboard, firstly, press "Enter" key, then "~" key, then "." key).

sshtun

The "sshtun" command allows to create upto 16 independent L2 [tunnels](#) via SSH connection.


In order to create tunnel, it is necessary to create tap interfaces on the both sides by using "ifconfig tapX up" command. The tap interface can have an IP address and be used as independent network interface, e.g. for routing, as well as a part of switch group. In addition, the tap interface can be used as the parent interface for the vlan, lag and prf interfaces, also as MINT network part.

The client SSH Tunnel module automatically re-establishes the connection to the remote server when the device is rebooted or the connection is broken. It can work with NAT, including addresses that are obtained dynamically via DHCP.

Syntax:

```
sshtun -help, -h
sshtun -log-level={emerg|alert|crit|error|warning|notice|info|debug|LEVEL}
sshtun -algo-list
sshtun start | stop | clear
sshtun IFNAME [options] [LOGIN[:PASSWORD]@HOST[:PORT]] [start | stop | del[ete]]
options:
  -window=SIZE
  -keepalive=TIME
  -compress=on | off, -C on | off
  -bind-addr=ADDR, -b ADDR
  -remote-if=REMOTE_TAP_NUM
  -reconnect-delay=TIME
  -kex-algos[=ALGO-LIST]
  -hostkey-algos[=ALGO-LIST]
  -cipher-algos[=ALGO-LIST], -c ALGO-LIST
  -hash-algos[=ALGO-LIST], -m ALGO-LIST
  -comp-algos[=ALGO-LIST]
  -auth-methods[=AUTH-METHODS-LIST]
  -none-cipher=on | off
```

Parameter	Description
-help, -h	Displays the command syntax.
-log-level={emerg alert crit error warning notice info debug LEVEL}	Allows choosing logging levels of the SSH Server service information that will be written into the system log, to manage system log please use "sys log" command. Different levels of logging can be chosen by "emerg", "alert", "error", "warning", "notice", "info", "debug" parameters or specified by the number of the needed level (from 0 to 7) using numeric "LEVEL" parameter. By default, "info" (6th level) is chosen.
-algo-list	Shows a list of all available SSH algorithms for key exchange (kex), authentication (host key), data encoding (cipher), data verification (hash) and data compression (compress).
start stop clear	Starts/stops/clears SSH Tunnel configuration.

<i>IFNAME [options] [LOGIN[:PASSWORD]@HOST[:PORT]] [start stop del[ete]]</i>	<p>Starts/stops/removes specified SSH tunnel.</p> <p>Parameters for an SSH tunnel establishing:</p> <ul style="list-style-type: none"> • "<i>IFNAME</i>" – remote SSH server tap interface name. • "<i>LOGIN</i>" – remote SSH server username . • "<i>PASSWORD</i>" – remote SSH server password. • "<i>HOST</i>" – remote SSH server IP address. • "<i>PORT</i>" – remote SSH server port number.
<i>-window=SIZE</i>	<p>Allows changing SSH Server internal receiving window size in bytes. SSH Server window size defines maximum allowed bandwidth for "SSH Client - SSH Server" data channel. By default, SSH Server window size is 24576 bytes.</p> <div>  NOTE For maximum performance, the "<i>-window</i>" parameter value should be not less than 128000 on the both tunnel sides. </div>
<i>-keepalive=TIME</i>	Sets a frequency of sending compulsory session activity confirmations to the server. This allows not to loose the session to the server when SSH Client leaved unused for a long time period. By default, SSH Client doesn't send any special activity confirmations ("0" value). Measured in seconds.
<i>-compress=on off, -C on off</i>	Enables/disables data compression.
<i>-bind-addr=ADDR, -b ADDR</i>	Sets SSH packets source IP address. This source IP address substitutes the default sending interface's IP address field of the SSH packets.
<i>-remote-if=REMOTE_TAP_NUM</i>	The tap interface number on the remote site.
<i>-reconnect-delay=TIME</i>	Timeout for reconnection in case the connection is broken.
<i>-kex-algos[=ALGO-LIST]</i>	Choosing kex algorithms from the list of algorithms (ALGO-LIST), to be used in SSH key exchange process.
<i>-hostkey-algos[=ALGO-LIST]</i>	Choosing host key algorithms from the list of algorithms (ALGO-LIST), to be used in SSH Server-Client authentication process.
<i>-cipher-algos[=ALGO-LIST], -c ALGO-LIST</i>	Choosing cipher algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data encoding.
<i>-hash-algos[=ALGO-LIST], -m ALGO-LIST</i>	Choosing hash algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data verification.
<i>-comp-algos[=ALGO-LIST]</i>	Choosing compression algorithms from the list of algorithms (ALGO-LIST), to be used in SSH data compression.
<i>-auth-methods[=AUTH-METHODS-LIST]</i>	<p>Choosing an available authentication method from the (AUTH-METHODS-LIST) list.</p> <p>An "<i>all</i>" value enables all authentication methods (set by default).</p>
<i>-none-cipher=on off</i>	Enable/disable encoding usage. Used when the simple TCP tunnel is needed, that significantly reduces the CPU load.

nslookup

Nslookup utility sends requests to the DNS server for direct and reverse domain names exchange.

Syntax:

```
nslookup {name|ip}
```

Parameter	Description
<i>name</i>	Domain name is used to get an IP address.


ip	IP address is used to get a domain name .
-----------	---

DNSclient

DNS module provides the node address definition by its full name.

Syntax:

```
dnsclient [options] [command]
where commands are:
    start - start service
    stop  - stop service
where options are:
    -domain={name}    - set local domain name.
    -server={address} - set Internet address (in dot notation) of a name server,
                        this option can be repeated.
```

Parameter	Description
start	Starts DNS client service.
stop	Stops DNS client service.
-domain={name}	Sets a local domain name.
-server={address}	Sets a server IP address. This parameter can be set several times.
get	<p>Loads a new software version to the device. Loading is performed via FTP. The file name shall be specified in full, in the format of the file system.</p> <p>The download process has two phases:</p> <ul style="list-style-type: none"> • Reading a file from a remote server and checking its integrity. • Upload the system image to the device's memory. <p>The second phase is indicated with symbol ".".</p> <p>To update firmware from InfiNet FTP server use command:</p> <pre>flashnet get ftp:ftp@ftp://92.168.100.34/firmware.H11S01v1.6.6.bin</pre> <p>where</p> <ul style="list-style-type: none"> • "H11" – hardware platform. • "1.6.6" – latest firmware version. • "ftp" – username. • "ftp" – password. <div>  NOTE After firmware updating, restart the unit with the command: <pre>restart yes</pre> </div>
put	Downloads current software from the device.
-S	Any other IP address (SourceAddress) may be set as default.

cron

The WANFlex firmware allows to set execution of some commands at a specified time or periodically with a certain frequency. Thus, is possible to perform regular configuration backup without the participation of the system administrator.

Syntax:

```
cron start
cron stop
cron clear
cron add commandID "command" [from][-to][\interval]
cron del commandID
cron dump
```

Examples from or to:

```
31/12/2016 12:00:00
31/12/2016 12:00
12:00:00
12:00
```


Any field can be set as '.' - don't care.

Examples of intervals

```
DD HH:MM:SS
\ 2 12:33:15
\ 2 12:33
\ 12:33:15
\ 12:33
\ 2
```

Don't care not allowed.

Parameter	Description
start	Starts the Cron service.
stop	Stops the Cron service.
clear	Clears all records in the table.

add commandID "command" [from][-to] [interval]	<p>Adds new record to the Cron table:</p> <ul style="list-style-type: none"> • "commandID" – arbitrary name of the record. • "command" – command to be executed. • "from" and "-to" – allow to set the exact date and/or time of the command execution. Valid formats (any character can be replaced with "." to set "don't care" value) are: <ul style="list-style-type: none"> • 31/12/2016 12:00:00 • 31/12/2016 12:00 • 12:00:00 • 12:00 • "interval" – allows to adjust the frequency of the command application. Valid formats (the "." character is not allowed) are: <ul style="list-style-type: none"> • \ 2 12:33:15 • \ 2 12:33 • \ 12:33:15 • \ 12:33 • \ 2 <div data-bbox="371 797 1453 965">  NOTE Records that contain the exact date and/or time will be valid only if the system date and time are set by sntp or gps. Otherwise, only records with execution frequency will be executed, every 7 days for example (since the device last reboot). </div>
del commandID	Removes the record from the Cron table.
dump	Displays the Cron table.

Example:

Set the configuration backup every 6 days.

```
#1> cron add TEST "co export test:admin@11.12.13.14/testserver/1111" \6
cron: ID 'TEST' replaced
#1> cron start
#1> cron dump
id='TEST' range=' \ 6' command='co export test:admin@11.12.13.14/testserver/1111' next='23/07/2019 10:40:29'
```