

# Miure Duo 5 Command Reference

Note: available settings and their allowed values may differ depending on configuration and additional device options.

## 1. Basic

### 1.1. *hostname* - Host name

**Description.** This setting configures a DNS name for your device. It is used for quick identification of the machine that you are on. If in doubt, leave the default value.

**Value type.** *text* (value required)

**Default value.** *duo.lan*

**Examples.**

- *rpt1.isp.com*
- *p2p-duo.lan*

### 1.2. *sysdescr* - System description

**Description.** Here you can describe how (or what for) the device is used. It may be helpful for other administrators to understand the purpose of the system. If in doubt, leave it blank.

**Value type.** *text*

**Default value.** *Miure Duo*

**Examples.**

- *Bridge to the management building*
- *To TheISP Inc.*

### 1.3. *country* - Country

**Value type.** *select*

**Allowed values.**

- *40* (Austria)
- *56* (Belgium)
- *100* (Bulgaria)
- *196* (Cyprus)

- 203 (Czech Republic)
- 208 (Denmark)
- 233 (Estonia)
- 246 (Finland)
- 250 (France)
- 276 (Germany)
- 348 (Hungary)
- 372 (Ireland)
- 380 (Italy)
- 440 (Lithuania)
- 442 (Luxembourg)
- 528 (Netherlands)
- 554 (New Zealand)
- 616 (Poland)
- 620 (Portugal)
- 703 (Slovak Republic)
- 705 (Slovenia)
- 724 (Spain)
- 752 (Sweden)
- 826 (United Kingdom)
- 1000 (Extended channels: level 0)
- 1001 (Extended channels: level 1) (\*)
- 1002 (Extended channels: level 2) (\*)
- 1003 (Extended channels: level 3) (\*)
- 1004 (Extended channels: level 4) (\*)

**Default value.** *616*

## **1.4. *syslocation* - System location**

**Description.** This option allows describing physical location of the device. It will appear e.g. when browsing the MIB tree through the SNMP agent of the device.

**Value type.** *text*

**Examples.**

- *NY, Some Street 11, rooftop*

## 1.5. *syscontact* - Administrator e-mail address

**Description.** This option allows setting the e-mail address that will appear as the administrator e-mail when browsing the MIB tree through the SNMP agent of the device.

**Value type.** *text*

**Examples.**

- *admin@isp.com*
- *root@hell.com*

## 1.6. *ipaddr* - IP address

**Hint.** IP address in CIDR form under which the device will be available

**Description.** This option configures the IPv4 address of this device. The care should be taken that the only IP format accepted is the CIDR form (Classless Inter-Domain Routing), e.g. 192.168.1.1/24.

**Value type.** *text* (value required)

**Default value.** *192.168.1.1/24*

**Examples.**

- *192.168.1.1/24*
- *10.1.20.5/30*
- *80.40.2.12/27*

## 1.7. *gw* - Gateway IP address

**Description.** This option lets you set the IP address of router to use to access the Internet. Make sure that the IP address that you are setting is directly attached to the subnetwork configured in the "IP address" option above, i.e. check if the gateway is within the configured IP range.

**Value type.** *text*

**Examples.**

- *192.168.0.1*
- *142.51.23.52*

## 1.8. *dns* - DNS server

**Description.** DNS is a system for changing host names (e.g. www.miure.pl) into IP addresses. This option lets you set the IP address of your DNS server, i.e. this server will be asked to resolve a domain name into IP address. You may use your internal DNS caching server as well as any external, globally

available DNS server allowing recursive queries, provided that you give this device access to the Internet (see the "Gateway IP address" option above).

**Value type.** *text*

**Default value.** *208.67.222.222*

**Examples.**

- *192.168.0.1*
- *208.67.222.222* (OpenDNS #1)
- *208.67.220.220* (OpenDNS #2)

## 2. Radio parameters

### 2.1. *magic* - Unique link name

**Hint.** Enter the same string on both peers

**Description.** Link name is used to identify the traffic belonging to given radio. The same name should be set on the remote link peer. Otherwise, both incoming and outgoing data would be discarded, disrupting any means of radio communication through this link. This also includes signal level indication, so it is important also for antenna alignment. Additionally, link name is used to generate cryptographic key for traffic confidentiality and authentication. Security provided relies on uniqueness of this parameter. Therefore, it is important not only to make it unique across devices used at certain area, but also to put an effort to make it globally unique and hard to guess by third party. Think of it as a "password" or a "pre-shared key". NOTE: Examples are provided only to show how a good link name would look like, but exactly them, being published here, are no longer secure. Do not use any one of them as that would effectively compromise any security provided by this device.

**Value type.** *text*

**Default value.** *duo*

**Examples.**

- *link-1-XYZZY31337*
- *f7858e6d95d8dbad*

### 2.2. *side* - Link side

**Hint.** Choose different values on both peers

**Description.** This setting is needed to properly setup antenna polarity. It does not set any of the devices in "master", "client" or similar modes.

**Value type.** *select*

**Allowed values.**

- *A*
- *B*

**Default value.** *A*

## 2.3. *mode* - Operating mode

**Hint.** Chooses the way that radio devices are used

**Description.** The Full-Duplex mode uses one radio only for receiving, and one only for transmitting the data. Thanks to such approach the link latency is minimized and the bandwidth is maximized in case the traffic being transmitted is symmetric. The Half-Duplex mode can dynamically use both radios for transmitting and receiving, thus maximizing the bandwidth in case the traffic is asymmetric, ie. the traffic being transmitted is much greater than the one being received, or opposite.

**Value type.** *select***Allowed values.**

- *fdx* (Full-Duplex (1 TX, 1 RX))
- *hdx* (Half-Duplex (2 TX/RX))

**Default value.** *fdx*

## 2.4. *strict* - Strict Ethernet frames order

**Description.** Turn this option on in order to strictly preserve the order in which Ethernet frames are received from other network devices, thus conforming to IEEE 802.3 standards. Generally it is not required as many protocols can cope with Ethernet frames received in different order. Turning this option off should increase the overall performance and decrease link latency.

**Value type.** *bool***Default value.** *0*

## 2.5. *freq* - Main frequency (MHz)

**Description.** This option configures the frequency that the first radio operates on. Be sure to select only these frequencies that you are allowed to transmit on.

**Value type.** *select*

## 2.6. *freq2* - Secondary frequency (MHz)

**Description.** This option configures the frequency that the second radio operates on. In automatic mode the second frequency will be chosen basing on the main frequency so separation between them is maximal. Be sure to select only these frequencies that you are allowed to transmit on.

**Value type.** *select*

## 2.7. *width* - Channel width (MHz)

**Description.** This option configures the width of the channel that radio operates on. Be sure to select only the channel width that you are allowed to transmit with.

**Value type.** *select*

**Allowed values.**

- 5
- 10
- 20
- 40 (\*)

**Default value.** 20

## 2.8. *power* - Transmit power

**Value type.** *select*

**Allowed values.**

- *auto* (automatic)
- 100% (18dBm)
- 90% (16dBm)
- 80% (14dBm)
- 70% (13dBm)
- 60% (11dBm)
- 50% (9dBm)
- 40% (7dBm)
- 30% (5dBm)
- 20% (4dBm)
- 10% (2dBm)
- 0% (0dBm)

## 2.9. *maxpower* - Maximum transmit power

Value type. *select*

Allowed values.

- *100%* (18dBm)
- *90%* (16dBm)
- *80%* (14dBm)
- *70%* (13dBm)
- *60%* (11dBm)
- *50%* (9dBm)
- *40%* (7dBm)
- *30%* (5dBm)
- *20%* (4dBm)
- *10%* (2dBm)
- *0%* (0dBm)

## 2.10. *modulation* - Modulation

Value type. *select*

Allowed values.

- *auto* (automatic)
- *0* (BPSK, r=1/2)
- *1* (BPSK, r=3/4)
- *2* (QPSK, r=1/2)
- *3* (QPSK, r=3/4)
- *4* (16-QAM, r=1/2)
- *5* (16-QAM, r=3/4)
- *6* (64-QAM, r=2/3)
- *7* (64-QAM, r=3/4)

## 2.11. *framesize* - Radio frame size

Value type. *select*

Allowed values.

- *auto* (automatic)
- *500*
- *900*
- *1400*
- *1800*
- *2300*
- *2700*
- *3100*
- *3600*
- *4000*

## 2.12. *txcont* - Continuous transmission

**Hint.** Radio transmits regardless of the actual payload. Useful for medium reservation.

**Description.** Continuous transmission forces the radio to transmit frames as fast as possible, what leads to full utilization of the medium regardless of the actual payload. It delivers a functionality of reporting link capabilities without a need to generate any traffic externally. Also, it contributes to faster adaptation of transmission parameters. This feature is available only in Full-Duplex mode.

**Value type.** *bool*

**Default value.** *0*

## 2.13. *shortifs* - Short inter-frame spaces

**Description.** Enabling short inter-frame spaces increases the maximum achievable throughput and link stability at the expense of disabling cooperation with other devices operating on the same frequency. This feature is available only in Full-Duplex mode.

**Value type.** *bool*

**Default value.** *0*

## 2.14. *sampling* - Sampling intensity

**Description.** Algorithm performing optimization of transmission parameters requires continuous sampling in order to follow changing conditions. Sampling is realized by sending frames with suboptimal parameters, which causes decrease of resultant throughput. This parameter specifies maximum fraction of the radio throughput that can be sacrificed for the purpose of sampling. Higher value can result in faster and more precise reaction to changes of transmission conditions.

**Value type.** *select*

**Allowed values.**

- 1%
- 2%
- 5%
- 10%
- 20%
- 30%
- 40%
- 50%

## 3. Advanced

### 3.1. *ping1* - Ping watchdog: IP address

**Description.** This option lets setting an IP address the availability of which to check periodically using ICMP Echo-Requests (so-called pings). In case the host does not respond, the device is rebooted. The requests are sent each ~1 second, with ~15-second timeout. Maximal number of unreplied requests is 5. In case the tested IP address is unavailable for a longer period of time, the device will not be rebooted more frequently than each ~6 minutes.

**Value type.** *text*

**Examples.**

- 192.168.1.2
- 212.77.100.101
- 213.180.130.200

### 3.2. *ping2* - Ping watchdog: second IP address

**Description.** This option lets setting a second IP address for the ping watchdog. If any of IP addresses are not responding, the device is rebooted. For more information, see the help for the primary ping watchdog IP address.

**Value type.** *text*

### 3.3. *stp* - Enable STP

**Description.** This option lets you to control the Spanning Tree Protocol (IEEE 802.1D), which can automatically prevent loops in a LAN segment. It periodically broadcasts special messages (BPDUs), thus discovering the network topology. After a loop is detected, some links are disabled, and they remain

is such state until they are needed due to failure of other links. Note that enabling this option will cause the device to NOT transfer any data during 30 seconds after device start.

**Value type.** *bool*

**Default value.** *0*

### 3.4. *sshkey* - Public RSA key for SSH

**Description.** A public key that is permitted for logging in as admin without providing the password

**Value type.** *text*

### 3.5. *snmpcom* - SNMP: community

**Value type.** *text* (value required)

**Default value.** *public*

### 3.6. *snmpsrc* - SNMP: source network

**Description.** This option sets the only source IP network that is allowed to access the SNMP agent

**Value type.** *text*

**Default value.**

**Examples.**

- *192.168.10.0/24*

### 3.7. *txlimit* - Ethernet transfer limit (kbps)

**Description.** This option lets you to limit the maximal bandwidth that the device is allowed to send using the Ethernet interface. Note that in order to limit the bandwidth in the other direction, you need to use the same option on the second device.

**Value type.** *int*

### 3.8. *txhash* - TX limit: hashing algorithm

**Description.** This option tells which IP packet addresses to use in order to identify a single data flow. Each such data flow is then assigned the same, fair amount of the available bandwidth.

**Value type.** *select*

**Allowed values.**

- *classic* (source and destination)

- *src* (source)
- *dst* (destination)

**Default value.** *classic*

### 3.9. *filter* - Enable filter

**Description.** After enabling this option the device will not transmit any data using the radio interface (ie. the data received on the Ethernet interface) except for traffic types which have been allowed. The filter will also disable STP (ie. drop BPDUs) and VLAN frames on the Ethernet interface.

**Value type.** *bool*

**Default value.** *0*

### 3.10. *allowip* - Allow IP and ARP traffic

**Hint.** DHCP and SMB traffic should be enabled separately

**Value type.** *bool*

**Default value.** *1*

### 3.11. *allowdhcp* - Allow DHCP traffic

**Value type.** *bool*

**Default value.** *1*

### 3.12. *allowsmb* - Allow SMB traffic

**Hint.** Including NetBIOS; required for Microsoft Windows Networks

**Value type.** *bool*

**Default value.** *0*

### 3.13. *allowpppoe* - Allow PPPoE traffic

**Value type.** *bool*

**Default value.** *1*

### 3.14. *macdnat* - Network Access Server MAC

**Description.** After enabling this option, the destination MAC addresses of frames leaving the radio interfaces will be changed to the specified value. In the opposite direction, only frames having the specified address as source address will be transmitted. This option may be used to increase the security

of access networks by limiting the range of MAC addresses that the hosts behind the Ethernet interface of the device have access to to one, single address. It also lets to force the users behind the device to use the specified Network Access Server, like IP router, PPPoE concentrator, etc.

**Value type.** *text*