

LCOS 10.72

Addendum

01/2023

Contents

1 Addendum to LCOS version 10.72.....	4
2 IPv6.....	5
2.1 Multiple DHCPv6 relay destinations.....	5
2.1.1 Additions to the Setup menu.....	5
3 Virtual LANs (VLAN).....	10
3.1 Q-in-Q VLAN.....	10
3.1.1 Additions to the Setup menu.....	11
4 Backup solutions.....	12
4.1 Master holddown time in VRRP.....	12
4.1.1 Additions to the Setup menu.....	12
5 Other services.....	14
5.1 BPjM module with loopback address.....	14
5.1.1 Additions to the Setup menu.....	14
5.2 Menu action to delete the BPjM signature definition.....	15

Copyright

© 2023 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components which are subject to their own licenses, in particular the General Public License (GPL). The license information for the device firmware (LCOS) is available on the device's WEBconfig interface under "Extras > License information". If the respective license demands, the source files for the corresponding software components will be made available on a download server upon request.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (www.openssl.org).

Products from LANCOM Systems include cryptographic software written by Eric Young (ey@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Germany

www.lancom-systems.com

1 Addendum to LCOS version 10.72

This document describes the changes and enhancements in LCOS version 10.72 since the previous version.

2 IPv6

2.1 Multiple DHCPv6 relay destinations


As of LCOS 10.72 RU1, multiple server targets can be configured in the DHCPv6 relay agent to which the relay agent sends the requests. The requests are always sent to all configured servers simultaneously.


In addition, an optional IPv6 sender address can be specified, which the relay agent uses for packets towards the DHCPv6 server.

2.1.1 Additions to the Setup menu

Dest-Address

Define the IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

 You can define additional server targets via [2.70.3.3.1.6 Dest-Address-2](#) on page 6, [2.70.3.3.1.8 Dest-Address-3](#) on page 7 and [2.70.3.3.1.10 Dest-Address-4](#) on page 8.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.4

Console path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Possible values:


Max. 39 characters from `[A-Z][a-z][0-9]`:

Default:

ff02::1:2

Dest-Interface

Here you specify the destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 You can define additional server targets via [2.70.3.3.1.7 Dest-Interface-2](#) on page 6, [2.70.3.3.1.9 Dest-Interface-3](#) on page 7 and [2.70.3.3.1.11 Dest-Interface-4](#) on page 8.


 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.


SNMP ID:

2.70.3.3.1.5

Console path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default:***empty***Dest-Address-2**

Define a second IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

 You can define additional server targets via [2.70.3.3.1.4 Dest-Address](#) on page 5, [2.70.3.3.1.8 Dest-Address-3](#) on page 7 and [2.70.3.3.1.10 Dest-Address-4](#) on page 8.


 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.


SNMP ID:

2.70.3.3.1.6

Console path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List****Possible values:**Max. 39 characters from `[A-Z][a-z][0-9]:`**Default:***empty***Dest-Interface-2**

Here you specify a second destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 You can define additional server targets via [2.70.3.3.1.5 Dest-Interface](#) on page 5, [2.70.3.3.1.9 Dest-Interface-3](#) on page 7 and [2.70.3.3.1.11 Dest-Interface-4](#) on page 8.


 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.7

Console path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default:***empty***Dest-Address-3**

Define a third IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

 You can define additional server targets via [2.70.3.3.1.4 Dest-Address](#) on page 5, [2.70.3.3.1.6 Dest-Address-2](#) on page 6 and [2.70.3.3.1.10 Dest-Address-4](#) on page 8.


 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.8

Console path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List****Possible values:**Max. 39 characters from `[A-Z][a-z][0-9]:`**Default:***empty***Dest-Interface-3**

Here you specify a third destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 You can define additional server targets via [2.70.3.3.1.5 Dest-Interface](#) on page 5, [2.70.3.3.1.7 Dest-Interface-2](#) on page 6 and [2.70.3.3.1.11 Dest-Interface-4](#) on page 8.


 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.9

Console path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default:***empty***Dest-Address-4**

Define a fourth IPv6 address of a (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

 You can define additional server targets via [2.70.3.3.1.4 Dest-Address](#) on page 5, [2.70.3.3.1.6 Dest-Address-2](#) on page 6 and [2.70.3.3.1.8 Dest-Address-3](#) on page 7.


 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.10

Console path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List****Possible values:**Max. 39 characters from `[A-Z][a-z][0-9]:`**Default:***empty***Dest-Interface-4**

Here you specify a fourth destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

 You can define additional server targets via [2.70.3.3.1.5 Dest-Interface](#) on page 5, [2.70.3.3.1.7 Dest-Interface-2](#) on page 6 and [2.70.3.3.1.9 Dest-Interface-3](#) on page 7.

 In case of multiple configured server targets, the requests are always sent to all configured servers simultaneously.

SNMP ID:

2.70.3.3.1.11

Console path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]#{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default:***empty***Dest-Loopback**

Specify here an optional sender address that the relay agent uses for packets towards the DHCPv6 server.

SNMP ID:

2.70.3.3.1.12

Console path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]#{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default:***empty*

3 Virtual LANs (VLAN)

3.1 Q-in-Q VLAN

As of LCOS 10.72 the router supports WAN connections with VLAN double tagging (“stacked VLAN”) or Q-in-Q VLAN according to IEEE 802.1ad. With Q-in-Q VLAN, service providers support layer-2 Ethernet connections between customer sites and so that the customer’s own VLAN can be transmitted unmodified. The inner VLAN (C-VLAN) is used by the customer, the outer VLAN (S-VLAN) by the service provider.

LANconfig: **Communication > Remote sites > Remote sites (DSL)**

S-VLAN ID

Here you configure the S-VLAN for VLAN double tagging (Q-in-Q VLAN connections according to IEEE 802.1ad). The VLAN is also referred to as the outer VLAN. The S-VLAN protocol ID that is used can be configured under **Interfaces > VLAN**.

LANconfig: **Interfaces > VLAN**

S-VLAN protocol ID

Defines the VLAN tagging ID for Q-in-Q VLAN tagging. The Ethernet2 type of the VLAN tag is a "tag value" configured as a 16-bit hexadecimal value. The default according to IEEE 802.1ad is "88a8", and another common value for VLAN tagging would be "8100", for example.

3.1.1 Additions to the Setup menu

S-VLAN-ID

Here you configure the S-VLAN for VLAN double tagging (Q-in-Q VLAN connections according to IEEE 802.1ad). The VLAN is also referred to as the outer VLAN. The S-VLAN protocol ID that is used can be configured under [2.32.6 S-Tag-Value](#) on page 11.

SNMP ID:

2.2.19.21

Console path:

Setup > WAN > DSL-Broadband-Peers

Possible values:

0 ... 4096

Default:

0

S-Tag-Value

Defines the VLAN tagging ID for Q-in-Q VLAN tagging. The Ethernet2 type of the VLAN tag is a "tag value" configured as a 16-bit hexadecimal value. The default according to IEEE 802.1ad is "88a8", and another common value for VLAN tagging would be "8100", for example.

SNMP ID:

2.32.6

Console path:

Setup > VLAN

Possible values:

Max. 4 characters from `[0-9][a-f]`

Default:

88a8

4 Backup solutions

4.1 Master holddown time in VRRP

As of LCOS 10.72 a new switch for a master holddown time is supported in VRRP. To this end, in LANconfig under **IP Router > VRRP** the parameter **Master holddown time** was added.

VRRP

VRRP activate

Within the VRRP list you can define virtual routers.

VRRP list...

Reconnect delay: 30 minutes

Advert. interval: 1 seconds

Master holddown time: 0 minutes

Propose internal services on the virtual IPs

Master holddown time

If a time is configured here, the virtual router changes to the “Hold-Down” state as soon as the monitored WAN connection is terminated with an error and the backup delay expires (i.e. switches to backup state). In the “Hold-Down” state, the monitored WAN connection can no longer be established. Also, no further VRRP advertisements will be sent.

As soon as the “Master-Holddown-Time” expires, the virtual router transitions to the “Standby” state, in which the monitored WAN connection can be reestablished.

The “Master-Holddown-Time” is a string with a maximum of 6 characters, which may include the digits 0-9 and a colon. This allows the entry of times of up to 999 minutes 59 seconds (999:59).

If there is no colon (e.g. “30”) then the specification is interpreted as minutes. In this case the maximum is “999”.

If a colon is present, the colon must be followed by two characters that are interpreted as seconds. The maximum possible value here is “59”.

Correct time specifications are, for example “5” (5 minutes), “5:30” (5 minutes, 30 seconds) or “0:30” (30 seconds).

A value of “0” or “0:00” disables the Master-Holddown.

4.1.1 Additions to the Setup menu

Master-Holddown-Time

If a time is configured here, the virtual router changes to the “Hold-Down” state as soon as the monitored WAN connection is terminated with an error and the backup delay expires (i.e. switches to backup state). In the “Hold-Down” state, the monitored WAN connection can no longer be established. Also, no further VRRP advertisements will be sent.

As soon as the “Master-Holddown-Time” expires, the virtual router transitions to the “Standby” state, in which the monitored WAN connection can be reestablished.

The “Master-Holddown-Time” is a string with a maximum of 6 characters, which can include the digits 0-9 and a colon. This allows times of up to 999 minutes 59 seconds (999:59) to be entered.

If there is no colon (e.g. "30") then the specification is interpreted as minutes. In this case the maximum is "999".

If a colon is present, the colon must be followed by two characters which are interpreted as seconds. The maximum possible value here is "59".

Correct time specifications are, for example "5" (5 minutes), "5:30" (5 minutes, 30 seconds) or "0:30" (30 seconds).

A value of "0" or "0:00" disables the Master-Holddown.

SNMP ID:

2.8.21.6

Console path:

Setup > IP-Router > VRRP

Possible values:

Max. 6 characters from [0-9] :

Default:

0

5 Other services

5.1 BPjM module with loopback address

As of LCOS 10.72 the BPjM module includes the option of specifying a loopback address. To this end, in LANconfig under **Miscellaneous Services > Services > BPjM filter** the parameter **Source address** was added.

The screenshot shows a configuration window titled "BPjM filter". Inside, there is a label "Source address (opt.):" followed by a text input field and a "Select" button.

Source address

Source address used by the BPjM module to access the server for BPjM signature updates.

5.1.1 Additions to the Setup menu

BPJM

Settings of the BPjM module.

SNMP ID:

2.110.5

Console path:

Setup > Firewall

BPJM-Loopback-Address

Loopback address used by the BPjM module to access the server for BPjM signature updates.

SNMP ID:

2.110.5.1

Console path:

Setup > Firewall > BPJM

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/;<=>?[\]^_.`

Default:

empty

5.2 Menu action to delete the BPjM signature definition

You can use the CLI to delete the BPjM signature definition from the router's file system. To do this, execute the command `do /Status/Firewall/BPJM/Delete-Values`.