SECURE. NETWORKS.

LCOS 10.72

Addendum

05/2024

LANCOM
Systems

Contents

Copyright

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.

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 (*eay@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 Wuerselen

Germany

www.lancom-systems.com

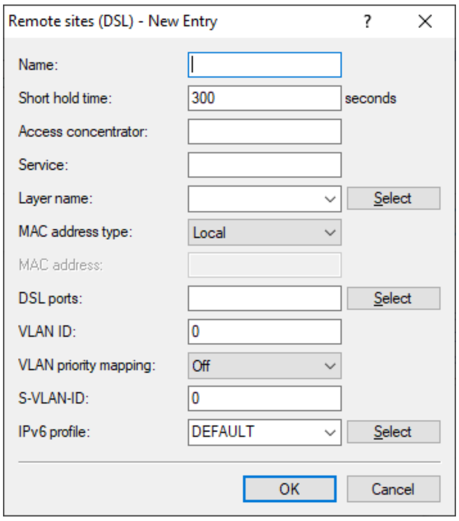
1 Addendum to LCOS version 10.72

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

2 Virtual LANs (VLAN)

2.1 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.



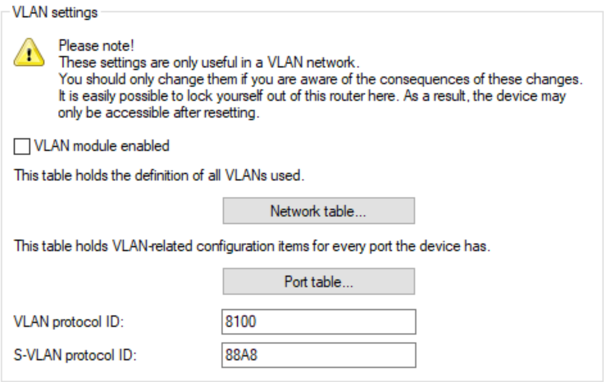
Remote sites (DSL) - New Entry

Name:
Short hold time: 300 seconds
Access concentrator:
Service:
Layer name:
MAC address type: Local
MAC address:
DSL ports:
VLAN ID: 0
VLAN priority mapping: Off
S-VLAN-ID: 0
IPv6 profile: DEFAULT

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**.



VLAN settings

Please note!
These settings are only useful in a VLAN network.
You should only change them if you are aware of the consequences of these changes.
It is easily possible to lock yourself out of this router here. As a result, the device may only be accessible after resetting.

□ VLAN module enabled

This table holds the definition of all VLANs used.

This table holds VLAN-related configuration items for every port the device has.

VLAN protocol ID: 8100
S-VLAN protocol ID: 88A8

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.

2.1.1 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 6.

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]`

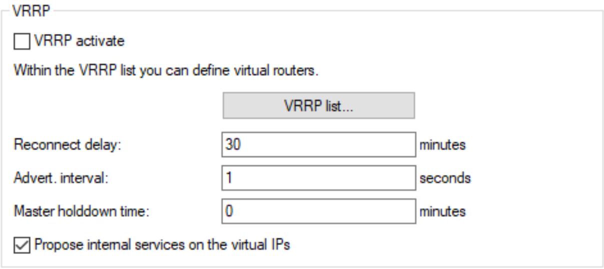
Default:

88a8

3 Backup solutions

3.1 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.

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.

3.1.1 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]:`

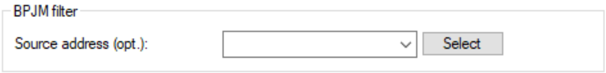
Default:

0

4 Other services

4.1 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.



Source address

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

4.1.1 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 Enhancements in the menu system

5.1 Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.2.22.28

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

5.2 L2TP-Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.2.22.29

Console path:

Setup > **WAN** > **RADIUS**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

5.3 Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.11.81.1.10

Console path:

Setup > **Config** > **RADIUS** > **Server**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

5.4 Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.12.29.21

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

5.5 Backup-Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.12.29.22

Console path:

Setup > **WLAN** > **RADIUS-Access-Check**

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

5.6 Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.19.36.9.1.1.11

Console path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

No
: Access requests do not have to contain a message authenticator.

Yes
: Access requests must always contain a message authenticator.

Default:

No

5.7 Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.2.6

Console path:

Setup > **RADIUS** > **Server** > **Clients**

Possible values:

No
: Access requests do not have to contain a message authenticator.

Yes
: Access requests must always contain a message authenticator.

Proxy-Only
: If an access request contains a proxy state attribute, a message authenticator must be included.

Default:

No

5.8 Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.3.18

Console path:

Setup > **RADIUS** > **Server** > **Forward-Servers**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Default:

No

5.9 Require-Msg-Authenticator

New switch as of LCOS 10.72 RU8. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.16.6

Console path:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Possible values:

No
Access requests do not have to contain a message authenticator.

Yes
Access requests must always contain a message authenticator.

Proxy-Only
If an access request contains a proxy state attribute, a message authenticator must be included.

Default:

No