LCOS LX 6.20

Addendum

09/2024

LANCOM SYSTEMS

Contents

Copyright

This product contains separate open-source software components. These are subject to their own licenses, in particular the General Public License (GPL). License information relating to the device firmware (LCOS LX) is available on the CLI by using the command `show 3rd-party-licenses`. If the respective license demands, the source files for the corresponding software components will be made available on request. Please contact us via e-mail under *gpl@lancom.de*.

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

Products from 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

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen, Germany

Germany

www.lancom-systems.com

1 Addendum to LCOS LX version 6.20

This document describes the changes and enhancements in LCOS LX version 6.20 since the previous version.

2 TACACS+

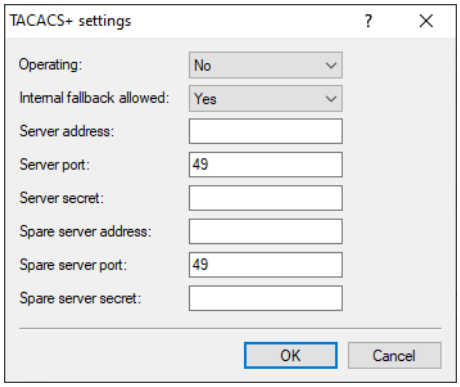
Configure authentication, authorization, and accounting (AAA) here using the TACACS+ protocol.

If this feature is active, admin logins are checked against the TACACS+ server and displayed and changed configuration items are transferred to the TACACS+ server for approval and/or logging.

The configuration points are transferred in OID representation.

When TACACS+ operation is active, the WEBconfig of the device is switched off.

The TACACS+ settings of the device can be found under **Management** > **Admin** > **TACACS+** > **TACACS+ settings**.



Operating

Switches the use of TACACS+ on or off.

Internal fallback allowed

If this option is activated, a login with local user data can be carried out if the TACACS+ server is not available.

Server address

The IP address of the primary TACACS+ server.

Server port

The port of the primary TACACS+ server.

Server secret

The key used for communication with the primary TACACS+ server.

Spare server address

The IP address of the backup TACACS+ server.

Spare server port

The port of the backup TACACS+ server.

Spare server secret

The key used for communication with the backup TACACS+ server.

2.1 Additions to the Setup menu

2.1.1 Tacacs-Plus

Configure authentication, authorization, and accounting (AAA) using the TACACS+ protocol here.

If this feature is active, admin logins are checked against the TACACS+ server and displayed and changed configuration items are transferred to the TACACS+ server for approval and/or logging.

The configuration points are transferred in OID representation.

When TACACS+ operation is active, the WEBconfig of the device is switched off.

SNMP ID:

2.11.51

Console path:

Setup > **Config**

2.1.1.1 Operating

Switches the use of TACACS+ on or off.

SNMP ID:

2.11.51.1

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

No

TACACS+ mode is switched off.

Yes

TACACS+ mode is switched on.

Default:

No

2.1.1.2 Internal-fallback-allowed

If this option is activated, a login with local user data can be carried out if the TACACS+ server is not available.

SNMP ID:

2.11.51.2

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

No

Authentication fallback is switched off.

Yes

Authentication fallback is switched on.

Default:

Yes

2.1.1.3 Server-Address

The IP address of the primary TACACS+ server.

SNMP ID:

2.11.51.10

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default:

empty

2.1.1.4 Server-Port

The port of the primary TACACS+ server.

SNMP ID:

2.11.51.11

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

0 … 65535

Default:

49

2.1.1.5 Server-Secret

The key used for communication with the primary TACACS+ server.

SNMP ID:

2.11.51.12

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default:

empty

2.1.1.6 Spare-Server-Address

The IP address of the backup TACACS+ server.

SNMP ID:

2.11.51.20

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

Default:

empty

2.1.1.7 Spare-Server-Port

The port of the backup TACACS+ server.

SNMP ID:

2.11.51.21

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

0 … 65535

Default:

49

2.1.1.8 Spare-Server-Secret

The key used for communication with the backup TACACS+ server.

SNMP ID:

2.11.51.22

Console path:

Setup > **Config** > **Tacacs-Plus**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

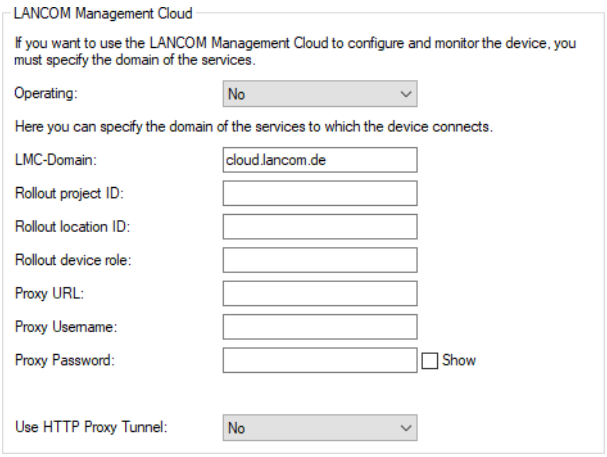
Default:

empty

3 Connect to the LMC via a proxy server

As of LCOS LX 6.20, you can connect to the LANCOM Management Cloud via a proxy server.

The settings can be found under **Management** > **LMC**.



Proxy URL

If the connection from the device to the LMC is to be established via an HTTP proxy server, this can be configured here. As soon as a proxy URL is entered, the LMC connection is always established via the proxy server.

Proxy Username

User name for use with an HTTP proxy server.

Proxy Password

Password for the user for use with an HTTP proxy server.

Repeat

Repeat the password for the user for use with an HTTP proxy server.

Use HTTP Proxy Tunnel

If a proxy URL has been specified and this switch is activated, a transparent tunnel is used via the proxy server using the HTTP CONNECT method. The proxy server must support this. If the switch is not activated, individual HTTP requests are forwarded via the proxy.

3.1 Additions to the Setup menu

3.1.1 Proxy

If the connection from the device to the LMC is to be established via an HTTP proxy server, this can be configured here. As soon as a proxy URL is entered, the LMC connection is always established via the proxy server.

If the switch *2.102.2.4 Tunnel* on page 12 is also activated, a transparent tunnel is used via the proxy server using the HTTP CONNECT method. The proxy server must support this. If the switch is not activated, individual HTTP requests are forwarded via the proxy.

SNMP ID:

2.102.2

Console path:

Setup > **LMC**

3.1.1.1 URL

If the connection from the device to the LMC is to be established via an HTTP proxy server, this can be configured here. As soon as a proxy URL is entered, the LMC connection is always established via the proxy server.

SNMP ID:

2.102.2.1

Console path:

Setup > **LMC** > **Proxy**

Possible values:

Max. 256 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

3.1.1.2 Username

User name for use with an HTTP proxy server.

SNMP ID:

2.102.2.2

Console path:

Setup > **LMC** > **Proxy**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

3.1.1.3 Password

Password for the user for use with an HTTP proxy server.

SNMP ID:

2.102.2.3

Console path:

Setup > **LMC** > **Proxy**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

3.1.1.4 Tunnel

If a proxy URL has been specified and this switch is activated, a transparent tunnel is used via the proxy server using the HTTP CONNECT method. The proxy server must support this. If the switch is not activated, individual HTTP requests are forwarded via the proxy.

SNMP ID:

2.102.2.4

Console path:

Setup > **LMC** > **Proxy**

Possible values:

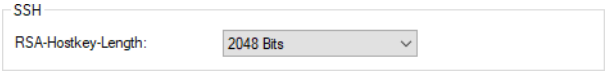
No
Yes

Default:

No

4 Adjustable SSH-RSA host key length

Under **Management** > **Extended** you will find the settings for the SSH functionality.



RSA-Hostkey-Length

The length of the SSH host key can be selected between 2048 bits and 4096 bits. After changing the setting, the hostkey is regenerated immediately.

4.1 Additions to the Setup menu

4.1.1 SSH

Configure SSH settings here.

SNMP ID:

2.11.52

Console path:

Setup > **Config**

4.1.1.1 RSA-Hostkey-Length

The length of the SSH host key can be selected between 2048 bits and 4096 bits. After changing the setting, the hostkey is regenerated immediately.

SNMP ID:

2.11.52.1

Console path:

Setup > **Config** > **SSH**

Possible values:

2048 Bits (2048)
4096 Bits (4096)

Default:

2048 Bits (2048)

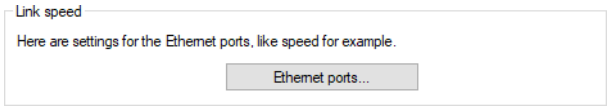
5 Energy-efficient Ethernet

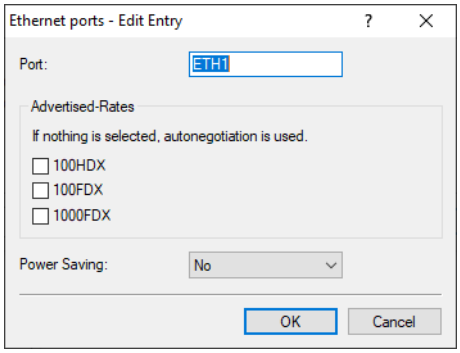
From LCOS LX 6.20 you can enable Energy Efficient Ethernet / IEEE 802.3az on the access points.

Supported LANCOM devices:

- LW-600
- LX-6200(E)
- LX-6500(E)
- OX-6400
- OX-6402
- OW-602

The settings can be found under **Interfaces** > **Port config** > **Link speed** > **Ethernet ports**.





Port

Configure the Ethernet port that these settings apply to.

Advertised rates

Configure the rates advertised for this Ethernet port here. With no value selected, auto-negotiation is used.

Power-Saving

Use this parameter to enable or disable Energy Efficient Ethernet/IEEE 802.3az for this Ethernet port.

5.1 Additions to the Setup menu

5.1.1 Ethernet ports

Settings for the Ethernet interfaces can be found here, such as for the speed or to activate Energy Efficient Ethernet/IEEE 802.3az.

SNMP ID:

2.62.2

Console path:

Setup > **LAN**

5.1.1.1 Port

Configure the Ethernet port that these settings apply to.

SNMP ID:

2.62.2.1

Console path:

Setup > **LAN** > **Ethernet-Ports**

Possible values:

Max. 10 characters from LAN port `ETHx|LANx`

5.1.1.2 Advertised-Rates

Configure the rates advertised for this Ethernet port here.

SNMP ID:

2.62.2.2

Console path:

Setup > **LAN** > **Ethernet-Ports**

Possible values:

Auto
100HDX
100FDX
1000FDX

Default:

Auto

5.1.1.3 Power-Saving

Use this parameter to enable or disable Energy Efficient Ethernet/IEEE 802.3az for this Ethernet port.

SNMP ID:

2.62.2.3

Console path:

Setup > **LAN** > **Ethernet-Ports**

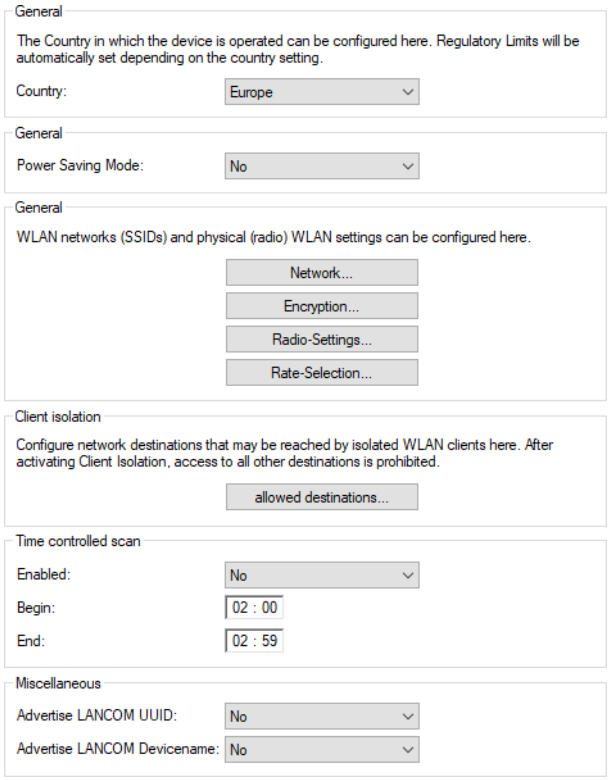
Possible values:

No
Yes

6 WLAN power-saving mode

As of LCOS LX 6.20 you can enable WLAN energy-efficiency mode on the access points.

The settings can be found under **Wireless-LAN** > **WLAN-Networks**.



Power-saving mode

If the WLAN power saving mode is activated and no client is logged in, the access point reduces the number of active WLAN streams to 1 per radio. As soon as at least one client is connected to the radio, the number of active streams is increased again to the maximum possible for this radio.

6.1 Additions to the Setup menu

6.1.1 Power-Saving-Mode

If the WLAN power-saving mode is activated and no client is logged in, the access point reduces the number of active WLAN streams to 1 per radio. As soon as at least one client is connected to the radio, the number of active streams is increased again to the maximum possible for this radio.

SNMP ID:

2.20.15

Console path:

Setup > **WLAN**

Possible values:

No

WLAN power-saving mode off.

Yes

WLAN power-saving mode on.

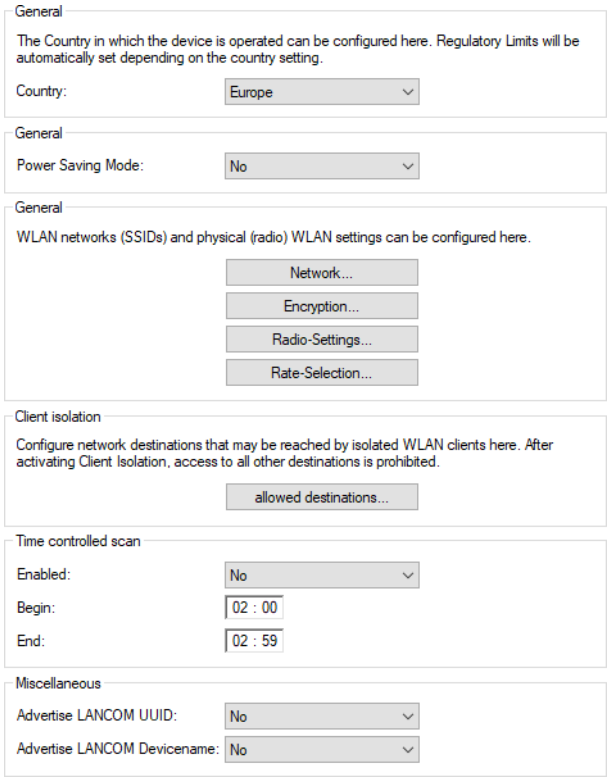
Default:

No

7 Announce access point device names in WLAN beacons

As of LCOS LX 6.20, you can announce the access point device names in WLAN beacons.

You can find the settings under **Wireless-LAN** > **WLAN-Networks**.



Advertise LANCOM device name

Configures whether an access point transmits its device name. To support WLAN site survey tools, the device name of the access point can be inserted into beacons. The name is identical for all radios of a multi-radio access point, so that the individual radios can be assigned to an access point by name.

The device name is coded as a vendor-specific info element as follows:

```
Tag: Vendor Specific: LANCOM Systems GmbH
  Tag Number: Vendor Specific (221)
    # 1 Byte (static value)
  Tag length: 13
    # 1 Byte (static length)
      # In this case: 3 Bytes OUI + 1 Byte LCS Subtype + 2 Bytes LCS Version + 7 Bytes LCS Devicename

  OUI: 00:a0:57 (LANCOM Systems GmbH)
    # 3 Bytes (static value)
  Vendor Specific OUI Type: 8
    # 1 Byte (static length)
      # LCS Subtype: 8 == Devicename
  Vendor Specific Data: 080100544553542d4150
    # Wireshark output comprising 1 Byte "Vendor Specific OUI Type" (0x08)
    # In this case: 9 Bytes
      # 2 Bytes (static value)
        # LCS Version: 1 (little-endian)
      # In this case: 7 Bytes
        # ASCII encoded String
          # In this case: 0x544553542d4150 == TEST-AP
```

7.1 Additions to the Setup menu

7.1.1 Include-Devicename

Configures whether an access point transmits its device name. To support WLAN site survey tools, the device name of the access point can be inserted into beacons. The name is identical for all radios of a multi-radio access point, so that the individual radios can be assigned to an access point by name.

The device name is coded as a vendor-specific info element as follows:

```
Tag: Vendor Specific: LANCOM Systems GmbH
  Tag Number: Vendor Specific (221)
    # 1 Byte (static value)
  Tag length: 13
    # 1 Byte (static length)
      # In this case: 3 Bytes OUI + 1 Byte LCS Subtype + 2 Bytes LCS Version + 7 Bytes LCS Devicename
  OUI: 00:a0:57 (LANCOM Systems GmbH)
    # 3 Bytes (static value)
  Vendor Specific OUI Type: 8
    # 1 Byte (static length)
      # LCS Subtype: 8 == Devicename
  Vendor Specific Data: 080100544553542d4150
    # Wireshark output comprising 1 Byte "Vendor Specific OUI Type" (0x08)
    # In this case: 9 Bytes
      # 2 Bytes (static value)
        # LCS Version: 1 (little-endian)
      # In this case: 7 Bytes
        # ASCII encoded String
          # In this case: 0x544553542d4150 == TEST-AP
```

SNMP ID:

2.20.16

Console path:

Setup > WLAN

Possible values:

No

Do not transfer device names.

Yes

Transfer device name.

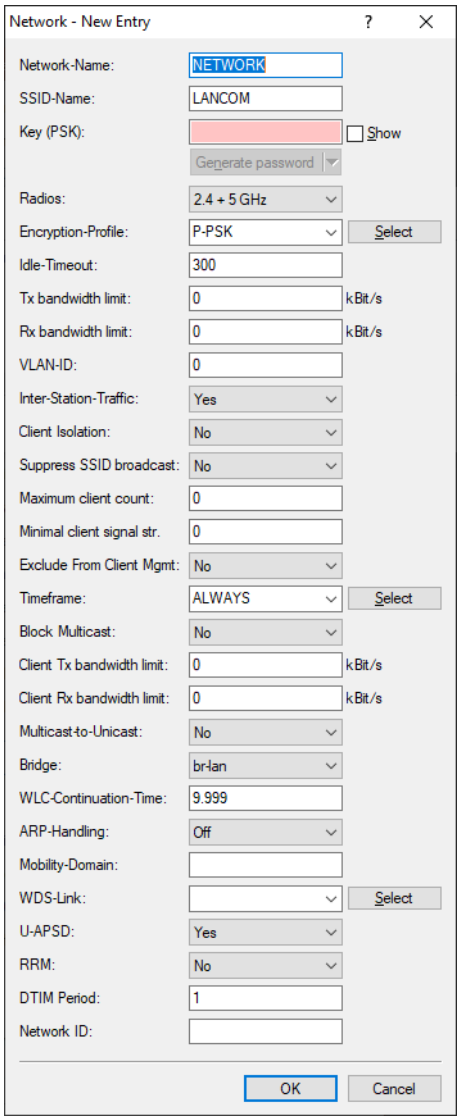
Default:

No

8 Configuring the DTIM period

As of LCOS LX 6.20, you can configure the DTIM period via SSID.

You can find the settings under **Wireless-LAN** > **WLAN-Networks** > **Network**.



DTIM Period

The DTIM period can be configured via SSID.

8.1 Additions to the Setup menu

8.1.1 DTIM-Period

The DTIM period can be configured via SSID.

SNMP ID:

2.20.1.36

Console path:

Setup > **WLAN** > **Network**

Possible values:

1 … 255

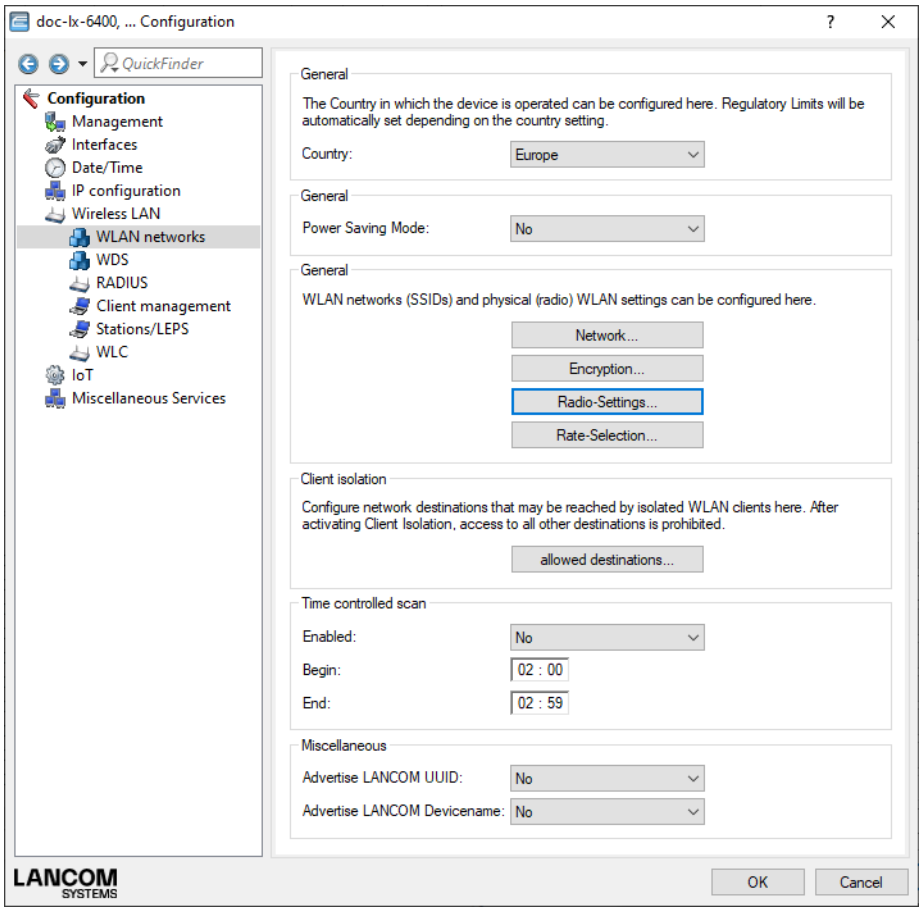
Default:

1

9 Random WLAN channel selection

As of LCOS LX 6.20 you can configure random WLAN channel selection.

The settings can be found under **Wireless-LAN** > **WLAN-Networks** > **Radio-Settings**.



Channel selection

Networks operating without manual WLAN channel planning or ARC 2.0 use automatic channel selection, which evaluates the WLAN channel based on quality criteria such as channel load, interference, and other SSIDs on that channel. If the access points in this type of network are all started at the same time, e.g. after a power failure, all of the access points will assess the channel quality and could well all come to the same result. In this case many access points will end up working on the same channel, which in some scenarios may be problematic. Random WLAN channel selection after restarting will ensure that the distribution is as even as possible in larger networks, with little multiple occupancy of any channels.

LANCOM recommends the use of LMC-supported channel planning via ARC 2.0, or to conduct manual planning based on a site survey.

9.1 Additions to the Setup menu

9.1.1 Channel-Selection

Networks operating without manual WLAN channel planning or ARC 2.0 use automatic channel selection, which evaluates the WLAN channel based on quality criteria such as channel load, interference, and other SSIDs on that channel. If the access points in this type of network are all started at the same time, e.g. after a power failure, all of the access points will assess the channel quality and could all come to the same result. In this case many access points will end up working on the same channel, which in some scenarios may be problematic. Random WLAN channel selection after restarting will ensure that the distribution is as even as possible in larger networks, with little multiple occupancy of any channels.

LANCOM recommends the use of LMC-supported channel planning via ARC 2.0, or to conduct manual planning based on a site survey.

SNMP ID:

2.20.8.37

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Auto

Automatic channel selection.

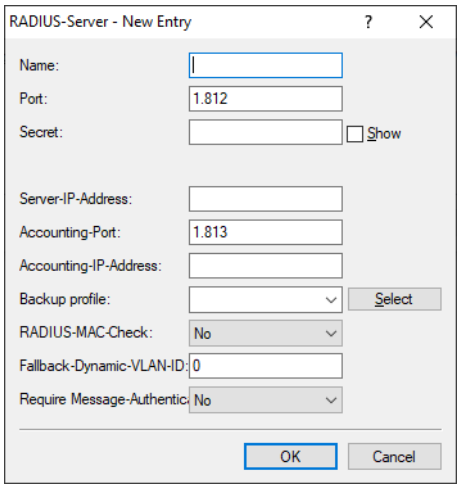
Random

Random WLAN channel selection.

10 Message authenticator required in RADIUS messages

As of LCOS LX 6.20 you can enforce the message authenticator in RADIUS messages.

The settings can be found under **Wireless-LAN** > **RADIUS**.



Require Message Authenticator

This option is used to specify whether a message authenticator is mandatory in RADIUS messages. If this is the case, messages without a message authenticator will not be processed and will be discarded.

10.1 Additions to the Setup menu

10.1.1 Require-Message-Authenticator

This option is used to specify whether a message authenticator is mandatory in RADIUS messages. If this is the case, messages without a message authenticator will not be processed and will be discarded.

SNMP ID:

2.30.3.17

Console path:

Setup > **RADIUS** > **RADIUS-Server**

Possible values:

No

Message authenticator not required in RADIUS messages.

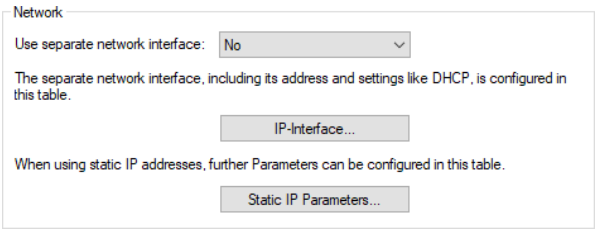
Yes

Message authenticator must be present in RADIUS messages.

11 Separate IP interface for Wireless ePaper

As of LCOS LX 6.20 you can configure a separate IP interface for Wireless ePaper.

Configure an optional separate network interface of the Wireless ePaper Server in LANconfig under **IoT** > **Wireless ePaper** > **Network**.This function allows you to specify a separate IP/VLAN interface for the access point's Wireless ePaper client. This means that the connection to the ePaper server or the Vusion Cloud can be established via a separate interface from the standard management IP/VLAN interface.

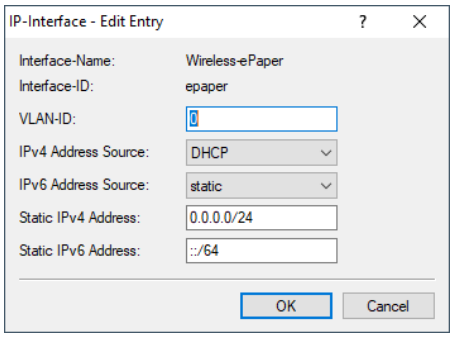


Use separate network interface

Activate a separate interface for the connection to the ePaper server or the Vusion Cloud.

IP interface

Configure the separate IP interface for the connection to the ePaper server or the Vusion Cloud.



Interface name

The interface is always "Wireless-ePaper". This is referred to by the other settings made here.

Interface-ID

The internal identifier for the interface.

VLAN-ID

Here you specify a VLAN ID for which the interface should be active and accessible. The default value "0" means that no VLAN is used.

IPv4 address source

Here you select how the IPv4 address of the interface is to be obtained.

DHCP

The IP address is retrieved via DHCP.

Static

The static IP address configured for the interface is used.

IPv6 address source

Here you select how the IPv6 address of the interface is to be obtained:

Router-Advertisement

The IPv6 address is derived from router advertisements that the device receives on the respective interface.

If the flag in the router advertisement is set to Other and/or Managed, additional configuration options are obtained via DHCPv6—even if the address source is set to **Router-Advertisement**.

DHCPv6

The IPv6 address is obtained via DHCPv6.

Static

The static IPv6 address configured for the interface is used.

Static IPv4 address

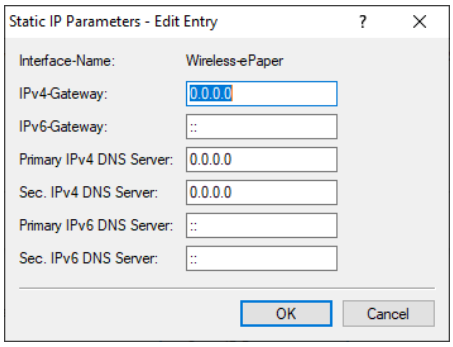
Here you configure the IP address to be used when the IPv4-Address-Source is set to **Static**. Add the subnet mask in CIDR notation (e.g. "/24") as a suffix.

Static IPv6 address

Here you configure the IP address to be used when the IPv6-Address-Source is set to **Static**. Add the subnet mask in CIDR notation (e.g. "/64") as a suffix.

Static IP Parameters

Here you configure the IP and network settings that apply when you use static IP addresses.



The settings made in this table only come into effect if the IPv4 or IPv6 address source for the IP interface is set to **static**. Otherwise all of the necessary information is retrieved via DHCP, for example, in which case no configuration is required here.

Interface name

The interface is always "Wireless-ePaper". This is referred to by the other settings made here.

IPv4-Gateway

Here you configure the IPv4 gateway for the referenced interface.

IPv6-Gateway

Here you configure the IPv6 gateway for the referenced interface.

Primary IPv4 DNS server

Here you configure the primary IPv4 DNS gateway for the referenced interface.

Secondary IPv4 DNS server

Here you configure the secondary IPv4 DNS gateway for the referenced interface.

Primary IPv6 DNS server

Here you configure the primary IPv6 DNS gateway for the referenced interface.

Secondary IPv6 DNS server

Here you configure the secondary IPv6 DNS gateway for the referenced interface.

11.1 Additions to the Setup menu

11.1.1 Use-Separate-IP-Interface

This function lets you specify a separate IP/VLAN interface for the access point's Wireless ePaper client. This means that the connection to the ePaper server or the Vusion Cloud can be established via a different interface to the standard management IP/VLAN interface.

SNMP ID:

2.111.88.10

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No

The separate IP interface for Wireless ePaper is not activated.

Yes

The separate IP interface for Wireless ePaper is activated. Configure these under *2.111.88.20 IP interface* on page 28 and *2.111.88.30 Static-IP-Parameters* on page 31.

Default:

No

11.1.2 IP interface

Configure the separate IP interface for connecting to the ePaper server or the Vusion Cloud.

SNMP ID:

2.111.88.20

Console path:

Setup > **IoT** > **Wireless-ePaper**

11.1.2.1 Interface name

The interface is always “Wireless-ePaper”. This is referred to by the other settings made here.

SNMP ID:

2.111.88.20.1

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Max. 64 characters from `INTRANET|Wireless-ePaper`

Default:

Wireless-ePaper

11.1.2.2 Interface-ID

The internal identifier for the interface. This cannot be modified.

SNMP ID:

2.111.88.20.2

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Max. 16 characters from `br-lan|epaper`

Default:

ePaper

11.1.2.3 VLAN-ID

Here you specify a VLAN ID for which the interface should be active and accessible.

SNMP ID:

2.111.88.20.3

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

2 … 4095

Special values:

0

The default value 0 means that no VLAN is used.

11.1.2.4 IPv4-Address-Source

Here you select how the IPv4 address of the interface is to be obtained.

SNMP ID:

2.111.88.20.4

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

DHCP

The IP address is retrieved via DHCP.

Static

The static IP address configured for the interface is used.

11.1.2.5 IPv6-Address-Source

Here you select how the IPv6 address of the interface is to be obtained.

SNMP ID:

2.111.88.20.5

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Router-Advertisement

The IPv6 address is derived from router advertisements that the device receives on the respective interface.

If the flag in the router advertisement is set to Other and/or Managed, additional configuration options are obtained via DHCPv6—even if the address source is set to **Router-Advertisement**.

DHCPv6

The IPv6 address is obtained via DHCPv6.

Static

The static IPv6 address configured for the interface is used.

11.1.2.6 Static-IPv4-Address

Here you configure the IP address to be used when the **IPv4-Address-Source** is set to **Static**. Add the subnet mask in CIDR notation (e.g. "/24") as a suffix.

SNMP ID:

2.111.88.20.6

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Max. 19 characters from `IPv4 address: a.b.c.d/xx`

11.1.2.7 Static-IPv6-Address

Here you configure the IP address to be used when the **IPv6-Address-Source** is set to **Static**. Add the subnet mask in CIDR notation (e.g. "/64") as a suffix.

SNMP ID:

2.111.88.20.7

Console path:

Setup > **IoT** > **Wireless-ePaper** > **IP-Interface**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d/64`

11.1.3 Static-IP-Parameters

Here you configure the IP and network settings that apply when you use static IP addresses.

SNMP ID:

2.111.88.30

Console path:

Setup > **IoT** > **Wireless-ePaper**

11.1.3.1 Interface name

The interface is always “Wireless-ePaper”. This is referred to by the other settings made here.

SNMP ID:

2.111.88.30.1

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 64 characters from `INTRANET|Wireless-ePaper`

Default:

Wireless-ePaper

11.1.3.2 IPv4-Gateway

Here you configure the IPv4 gateway for the referenced interface.

SNMP ID:

2.111.88.30.2

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

11.1.3.3 IPv6-Gateway

Here you configure the IPv6 gateway for the referenced interface.

SNMP ID:

2.111.88.30.3

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

11.1.3.4 Primary-IPv4-DNS

Here you configure the primary IPv4 DNS gateway for the referenced interface.

SNMP ID:

2.111.88.30.4

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

11.1.3.5 Secondary-IPv4-DNS

Here you configure the secondary IPv4 DNS gateway for the referenced interface.

SNMP ID:

2.111.88.30.5

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

11.1.3.6 Primary-IPv6-DNS

Here you configure the primary IPv6 DNS gateway for the referenced interface.

SNMP ID:

2.111.88.30.6

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

11.1.3.7 Secondary-IPv6-DNS

Here you configure the secondary IPv6 DNS gateway for the referenced interface.

SNMP ID:

2.111.88.30.7

Console path:

Setup > **IoT** > **Wireless-ePaper** > **Static-IP-Parameters**

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`