LCOS 11.00

Addendum

11/2026

ROHDE&SCHWARZ
Make ideas real

Contents

1 Addendum to LCOS version 11.00....4
2 Configuration....5
2.1 **IPv6 support for TCP- / HTTP tunnels**....5
2.2 File download from a USB flash drive....5
3 Virtual Private Networks – VPN....6
3.1 Post-quantum methods in IKEv2 key exchange....6
3.1.1 Support for ML-KEM in IKEv2....6
3.1.2 Why multiple key exchange methods?....6
3.1.3 Effects on performance....7
3.1.4 Deployment recommendations....8
3.1.5 Configuration with LANconfig....8
3.1.6 Additions to the Setup menu....11
3.2 IKEv2: Support for RADIUS Accounting-On....19
4 Voice over IP – VoIP....20
4.1 Voice backup using VRRP....20
4.2 Additions to the Setup menu....21
4.2.1 Vrrp-Interface....21
4.2.2 Vrrp-Interface....21
5 RADIUS....22
5.1 Transfer DHCPv6 options in the RADIUS Auth VSA....22
6 Enhancements in the menu system....24
6.1 Additions to the Setup menu....24
6.1.1 CHAP-Reauth-Minutes....24
6.1.2 Key-Exchange-Algorithms....24
6.1.3 Access-Type....25
6.1.4 Authentication-Type....26

Copyright

© 2026 Rohde & Schwarz Networks and Cybersecurity GmbH, Würselen (Germany). All rights reserved.

Notice on the company name: Since July 1, 2026, LANCOM Systems has been named **Rohde & Schwarz Networks and Cybersecurity**. Product information and communication materials are accordingly issued under the new company name.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Rohde & Schwarz Networks and Cybersecurity 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 Rohde & Schwarz Networks and Cybersecurity. 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.

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies 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 Rohde & Schwarz Networks and Cybersecurity include software developed by the “OpenSSL Project” for use in the “OpenSSL Toolkit” (*www.openssl.org*).

Products from Rohde & Schwarz Networks and Cybersecurity include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from Rohde & Schwarz Networks and Cybersecurity include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from Rohde & Schwarz Networks and Cybersecurity contain the LZMA SDK developed by Igor Pavlov.

Rohde & Schwarz Networks and Cybersecurity GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.rohde-schwarz.com/networks-and-cybersecurity

1 Addendum to LCOS version 11.00

This document describes the changes and enhancements in LCOS version 11.00 since the previous version.

2 Configuration

2.1 IPv6 support for TCP- / HTTP tunnels

As of LCOS 11.00, IPv6 addresses can also be specified and used for TCP- / HTTP tunnels.

2.2 File download from a USB flash drive

As of LCOS 11.00, a firmware file or a configuration script can be loaded from a connected USB flash drive. Examples:

1. Loading an LCOS firmware from the USB flash drive from the “Firmware” directory on the USB flash drive:

```
loadfirmware file://usb/Firmware/LC-1800EF-4G-10.94.0327-RU4.upx
```

2. Loading a WWAN firmware from the USB flash drive from the “Firmware” directory on the USB flash drive:

```
loadfirmware file://usb/Firmware/LC-1800EF-4G-EM060KEAAAR01A05M2G-A0.301.A0.301-RU2.upx
```

3. Loading a script configuration from the USB flash drive from the “Config” directory on the USB flash drive:

```
LoadScript file://usb/Config/Initital-Provisioning-V1.1.lcs
```

3 Virtual Private Networks – VPN

3.1 Post-quantum methods in IKEv2 key exchange

As of LCOS 11.00, LCOS Intermediate Exchange in IKEv2 according to *RFC 9242* as well as Multiple Key Exchanges according to *RFC 9370*. These methods serve as the basis for the use of post-quantum methods in key exchange.

Intermediate Exchange enables the exchange of additional key material even with large messages without having to transfer it completely in the initial IKE_AUTH message. Multiple Key Exchanges allow multiple independent key exchange methods to be combined, for example a traditional Diffie-Hellman method with a post-quantum-resistant method such as ML-KEM. This creates a hybrid key exchange that provides both the proven security of traditional methods and protection against future attacks by powerful quantum computers. Additional support for ML-KEM as a new post-quantum-resistant KEM group makes it possible to prepare IKEv2 connections today for a future post-quantum security strategy.

Both methods cannot be explicitly configured in LCOS, but are used automatically when required, e.g. when using additional rounds in key exchange as well as large DH groups such as ML-KEM.

LCOS supports the ML-KEM groups DH37 (ml-kem-1024), DH36 (ml-kem-768), and DH35 (ml-kem-512). These groups can be used natively as well as in hybrid key exchange with other additional DH groups.

3.1.1 Support for ML-KEM in IKEv2

ML-KEM is a standardized post-quantum-resistant key encapsulation mechanism method and is based on lattice-based cryptographic problems. It is frequently used to protect against so-called “store now, decrypt later” attacks.

In such an attack, an attacker records encrypted communication today in order to decrypt it later using powerful quantum computers. By incorporating a post-quantum-resistant method such as ML-KEM, the IKEv2 key exchange can already be secured today against this future scenario.

It is fundamentally important to distinguish between:

- **Key exchange:** Generation of the shared secret, for example using DH or ML-KEM.
- **Authentication:** Verification of the identity of the communication partners, for example using certificates or digital signatures.
- **Encryption:** Protection of the IPsec data transmitted later.

The use of ML-KEM primarily protects the key exchange. For a fully post-quantum-resistant overall solution, it must also be verified whether the signature and authentication methods used are suitable against quantum attacks.

3.1.2 Why multiple key exchange methods?

A hybrid key exchange is intended to maintain security even if one of the methods used is weakened or broken in the future. Example:

- The traditional Diffie-Hellman method is well established today.
- A future quantum computer could compromise certain traditional methods, especially those based on the discrete logarithm, using Shor’s algorithm.

- ML-KEM is based on a different mathematical problem and is intended for use against quantum computers.
- If both methods are combined (hybrid), an attacker must fundamentally compromise both secrets in order to reconstruct the resulting IKE key material.

A hybrid exchange can therefore provide transitional protection: Existing traditional cryptography remains usable while at the same time a post-quantum-resistant component is added.

3.1.3 Effects on performance

The use of post-quantum methods in key exchange affects the performance or speeds when establishing IKEv2 VPN tunnels. IPSec data throughput is not affected.

The following consequences arise in practical use:

- **Additional latency**

  With RFC 9242 and RFC 9370, an additional exchange may be added. This results in at least one additional request/response step. The actual delay therefore depends heavily on network latency. For connections with high latency – for example via satellite, cellular, or long-distance WAN links – this additional round trip can be clearly measurable.

- **Additional computational effort**

  In a hybrid key exchange, multiple cryptographic methods must be executed. In addition to the traditional Diffie-Hellman method, ML-KEM in particular adds the following operations:

  - Generation or processing of ML-KEM key material,
  - encapsulation on the initiating side,
  - decapsulation on the responding side,
  - additional processing during derivation of the shared IKE key material.

  The computational effort is typically higher than with a traditional DH exchange alone. Especially on devices with limited CPU performance, this can affect the time required to establish new VPN tunnels.

  The following distinction is important:

  - The establishment of new IKE SAs may take longer.
  - The subsequent data transmission within an existing CHILD_SA is generally not significantly slowed down by the additional key exchange.
  - However, the additional effort can become relevant with frequent rekey operations or when many tunnels are established simultaneously.

- **Effects on the size of IKEv2 messages**

  RFC 9242 does not automatically reduce the total amount of transmitted data. The extension merely distributes additional information across multiple IKE messages.

  The total size of all messages may even increase slightly due to additional payloads, since each message requires its own IKE headers and payload structures. The main advantage is that individual messages become smaller and easier to transport.

  This can reduce problems with the following network characteristics:

  - limited MTU,
  - UDP fragmentation,
  - firewalls and NAT devices,
  - VPN gateways with size limitations,
  - unreliable transmission of large UDP datagrams.

3.1.4 Deployment recommendations

In general, the use of a hybrid IKEv2 key exchange is currently recommended. For this purpose, a traditional method is combined, for example, with a post-quantum-resistant ML-KEM method. For a security level of approximately 128 bits, the combination of ECP256 (DH group 19) or X25519 (DH group 31) with ML-KEM-768 is suitable. For higher security requirements, ECP384 (group 20) can be used together with ML-KEM-1024. Older MODP groups (e.g. DH14) should only be used for compatibility reasons. The specific selection should be based on current BSI recommendations, protection requirements, and the methods supported by the remote endpoint.

The combination of traditional DH and ML-KEM initially protects the key exchange. It does not automatically make the entire IKEv2 authentication quantum-resistant. For example, if traditional RSA or ECDSA signatures are used for certificates, they may still be vulnerable to quantum computers in the long term. Newer methods, e.g. for certificate-based authentication, are currently in the standardization phase at the IETF.

It is generally possible to combine key exchange with post-quantum preshared keys according to *RFC 8784*.

3.1.5 Configuration with LANconfig

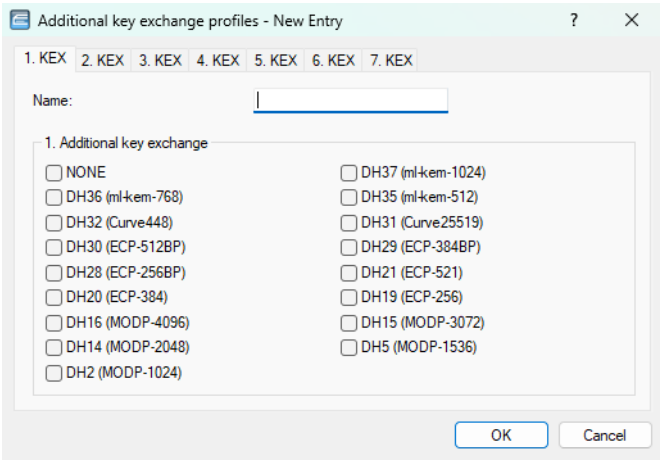
Select a profile for the additional key exchange in the **VPN** > **IKEv2 / IPSec** > **Encryption** > **Encryption** section.

Additional key exchange

Profile

Name of the profile for the additional key exchange. If the parameter is left empty, no additional key exchange is performed, and only the negotiated DH group of the normal encryption profile is used. Define the profiles under **VPN** > **IKEv2 / IPSec** > **Encryption** > **Additional key exchange profiles**.

You can configure up to seven additional key exchanges. The key exchanges are optional in principle, and, for example, only the first round can be used. A proposal, that is, a selection of options negotiated between the connection partners, is created in each key exchange. As with regular IKE proposals and DH groups, the communication partners must have a common subset. If they do not match, the IKEv2 negotiation fails.



Name

Contains the unique name of this key exchange profile. Assign this name as an additional optional key exchange profile in the **Encryption Table**. You can define up to seven additional key exchange profiles.

Additional key exchange

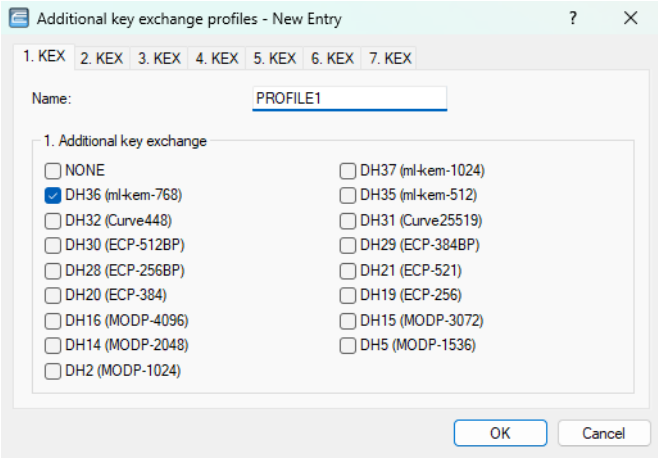
Contains the selection of Diffie-Hellman groups on the basis of which the VPN partners generate a key for data exchange. The higher the selected DH group, the more complex the generated key. The following groups are currently supported:

- DH-2 (1024-bit modulus)
- DH-5 (1536-bit modulus)
- DH-14 (2048-bit modulus)
- DH-15 (3072-bit modulus)
- DH-16 (4096-bit modulus)
- DH-19 (256-bit random ECP group)
- DH-20 (384-bit random ECP group)
- DH-21 (521-bit random ECP group)
- DH-28 (brainpoolP256r1)
- DH-29 (brainpoolP384r1)
- DH-30 (brainpoolP512r1)
- DH-31 (Curve25519)
- DH-32 (Curve448)
- DH-35 (ml-kem-512)
- DH-36 (ml-kem-768)
- DH-37 (ml-kem-1024)

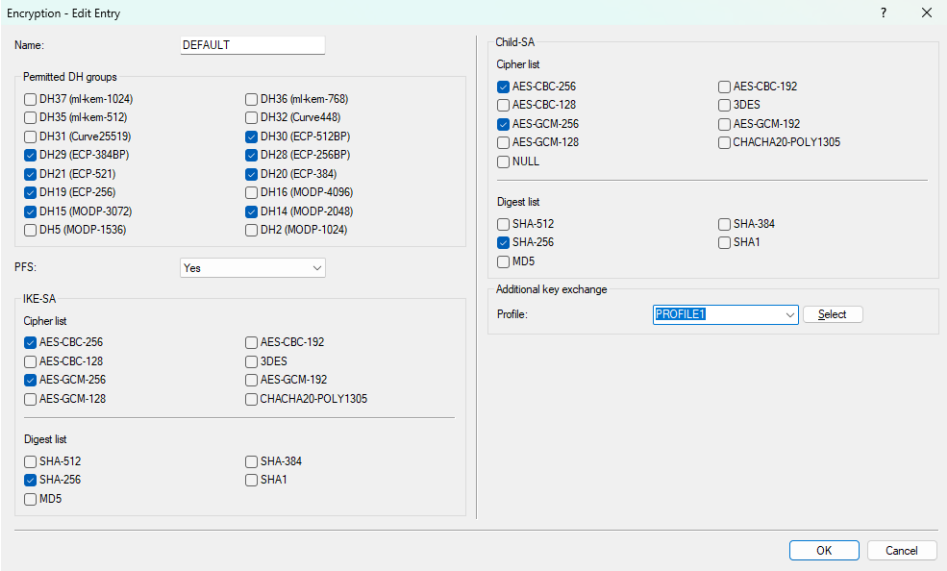
3.1.5.1 Example 1

An existing IKEv2 connection with ML-KEM 768 (DH36) is to be made post-quantum secure through a hybrid method using an additional key exchange (round 1).

1. Open the table **VPN** > **IKEv2 / IPSec** > **Encryption** > **Additional key exchange profiles**. Assign a name for the profile, e.g. “PROFILE1”, and enable DH36.



2. Open the table **VPN** > **IKEv2 / IPSec** > **Encryption** > **Encryption** of the DEFAULT profile and, if applicable, in the next step also the profile of an IKEv2 connection:

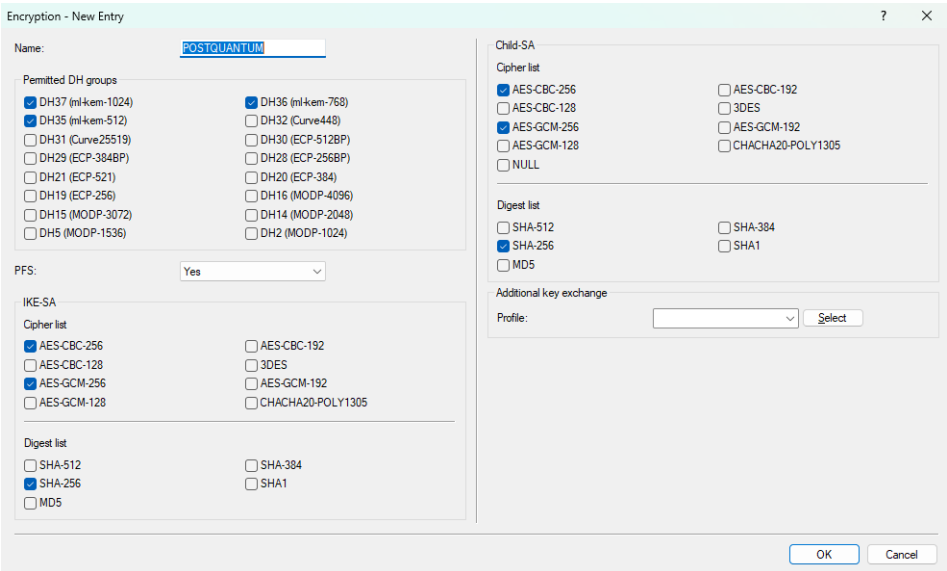


Under Profile at **Additional key exchange**, enter the name of the profile from step 1). In the traditional IKEv2 key exchange, the DH groups configured under **Permitted DH groups** are used. ML-KEM 768 (DH36) is used in the additional key exchange profile. This configuration sets up a hybrid post-quantum method.

3.1.5.2 Example 2

An IKEv2 connection is to be used only with ML-KEM groups, i.e. a pure post-quantum key exchange. A hybrid method is not to be used. Therefore, the use of additional key exchange rounds is not required.

1. Open the table **VPN** > **IKEv2 / IPSec** > **Encryption** > **Additional key exchange profiles** of the profile for an IKEv2 connection. In the traditional IKEv2 key exchange, only post-quantum groups based on ML-KEM are permitted under **Permitted DH groups**, e.g. DH37, DH36, DH35.



3.1.6 Additions to the Setup menu

3.1.6.1 DH-Groups

Contains the selection of Diffie-Hellman groups.

SNMP ID:

2.19.36.2.2

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

DH37
ml-kem-1024 (as of LCOS version 11.00)
DH36
ml-kem-768 (as of LCOS version 11.00)
DH35
ml-kem-512 (as of LCOS version 11.00)
DH32
Curve448
DH31
Curve25519
DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2

3.1.6.2 Add.-Key-Exchange-Profile

Name of the profile for the additional key exchange. If the parameter is left empty, no additional key exchange is performed and only the negotiated DH group of the normal encryption profile is used.

SNMP ID:

2.19.36.2.8

Console path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

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

Default:

empty

3.1.6.3 Add.-Key-Exchange-Profiles

You can configure up to seven additional key exchanges. The key exchanges are optional in principle, and, for example, only the first round can be used. A proposal, that is, a selection of options negotiated between the connection partners, is created in each key exchange. As with regular IKE proposals and DH groups, the communication partners must have a common subset. If they do not match, the IKEv2 negotiation fails.

SNMP ID:

2.19.36.36

Console path:

Setup > **VPN** > **IKEv2**

3.1.6.3.1 Name

Contains the unique name of this key exchange profile. Assign this name as an additional optional key exchange profile in the **Encryption Table**. You can define up to seven additional key exchange profiles.

SNMP ID:

2.19.36.36.1

Console path:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Possible values:

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

Default:

empty

3.1.6.3.2 ADDKE1

Contains the selection of Diffie-Hellman groups on whose basis the VPN peers create a key for data exchange. The higher the selected DH group, the more complex the generated key.

SNMP ID:

2.19.36.36.3

Console path:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Possible values:

DH37
ml-kem-1024 (as of LCOS version 11.00)
DH36
ml-kem-768 (as of LCOS version 11.00)
DH35
ml-kem-512 (as of LCOS version 11.00)
DH32
Curve448
DH31
Curve25519
DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE
When configuring “NONE”, it is permitted that no proposal or an empty proposal for this round is also accepted from the remote endpoint.

3.1.6.3.3 ADDKE2

Contains the selection of Diffie-Hellman groups on whose basis the VPN peers create a key for data exchange. The higher the selected DH group, the more complex the generated key.

SNMP ID:

2.19.36.36.4

Console path:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Possible values:

DH37
ml-kem-1024 (as of LCOS version 11.00)
DH36
ml-kem-768 (as of LCOS version 11.00)
DH35
ml-kem-512 (as of LCOS version 11.00)

DH32
Curve448
DH31
Curve25519
DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE
When configuring “NONE”, it is permitted that no proposal or an empty proposal for this round is also accepted from the remote endpoint.

3.1.6.3.4 ADDKE3

Contains the selection of Diffie-Hellman groups on whose basis the VPN peers create a key for data exchange. The higher the selected DH group, the more complex the generated key.

SNMP ID:
2.19.36.36.5

Console path:
Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Possible values:

DH37
ml-kem-1024 (as of LCOS version 11.00)
DH36
ml-kem-768 (as of LCOS version 11.00)
DH35
ml-kem-512 (as of LCOS version 11.00)
DH32
Curve448
DH31
Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

When configuring “NONE”, it is permitted that no proposal or an empty proposal for this round is also accepted from the remote endpoint.

3.1.6.3.5 ADDKE4

Contains the selection of Diffie-Hellman groups on whose basis the VPN peers create a key for data exchange. The higher the selected DH group, the more complex the generated key.

SNMP ID:

2.19.36.36.6

Console path:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Possible values:

DH37
ml-kem-1024 (as of LCOS version 11.00)
DH36
ml-kem-768 (as of LCOS version 11.00)
DH35
ml-kem-512 (as of LCOS version 11.00)
DH32
Curve448
DH31
Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

When configuring “NONE”, it is permitted that no proposal or an empty proposal for this round is also accepted from the remote endpoint.

3.1.6.3.6 ADDKE5

Contains the selection of Diffie-Hellman groups on whose basis the VPN peers create a key for data exchange. The higher the selected DH group, the more complex the generated key.

SNMP ID:

2.19.36.36.7

Console path:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Possible values:

DH37

ml-kem-1024 (as of LCOS version 11.00)

DH36

ml-kem-768 (as of LCOS version 11.00)

DH35

ml-kem-512 (as of LCOS version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

When configuring “NONE”, it is permitted that no proposal or an empty proposal for this round is also accepted from the remote endpoint.

3.1.6.3.7 ADDKE6

Contains the selection of Diffie-Hellman groups on whose basis the VPN peers create a key for data exchange. The higher the selected DH group, the more complex the generated key.

SNMP ID:

2.19.36.36.8

Console path:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Possible values:

DH37

ml-kem-1024 (as of LCOS version 11.00)

DH36

ml-kem-768 (as of LCOS version 11.00)

DH35

ml-kem-512 (as of LCOS version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

When configuring “NONE”, it is permitted that no proposal or an empty proposal for this round is also accepted from the remote endpoint.

3.1.6.3.8 ADDKE7

Contains the selection of Diffie-Hellman groups on whose basis the VPN peers create a key for data exchange. The higher the selected DH group, the more complex the generated key.

SNMP ID:

2.19.36.36.9

Console path:

Setup > **VPN** > **IKEv2** > **Add.-Key-Exchange-Profiles**

Possible values:

DH37

ml-kem-1024 (as of LCOS version 11.00)

DH36

ml-kem-768 (as of LCOS version 11.00)

DH35

ml-kem-512 (as of LCOS version 11.00)

DH32

Curve448

DH31

Curve25519

DH30
DH29
DH28
DH21
DH20
DH19
DH16
DH15
DH14
DH5
DH2
NONE

When configuring “NONE”, it is permitted that no proposal or an empty proposal for this round is also accepted from the remote endpoint.

3.2 IKEv2: Support for RADIUS Accounting-On

As of LCOS 11.00, RADIUS Accounting-On and Off are supported.

In IKEv2, the RADIUS messages “Accounting-On” and “Accounting-Off” are supported when using RADIUS accounting. At startup, the device sends “Accounting-On” to the active RADIUS accounting servers. During shutdown, the device sends “Accounting-Off” to the active RADIUS accounting servers. This function is automatically active when RADIUS accounting is used. RADIUS servers can use these messages to receive the operational status of the NAS.

4 Voice over IP – VoIP

4.1 Voice backup using VRRP

The Virtual Router Redundancy Protocol (VRRP) is a network protocol that combines multiple physical routers into a single virtual router in order to increase fail safety. The Voice Call Manager can also be operated on this virtual interface.

If multiple virtual networks are used, the Voice Call Manager must be bound to one of these networks. To do this, the virtual ID (VRRP ID) and the interface name of the virtual router (VRRP interface) must be specified in the Voice Call Manager. These two values refer to the “Interface” and “Router ID” entries in the “Virtual Routers” table in the VRRP settings. If “0” is specified as the VRRP ID, the VRRP function in the Voice Call Manager is disabled.

To register the SIP telephones, the corresponding virtual IP address of the router is stored in the telephone as the registrar. Alternatively, the VoIP domain can also be used here, provided it differs from the DNS domain. It should be noted, however, that the SIP endpoints only register with the new master router after the re-registration timeout has expired.

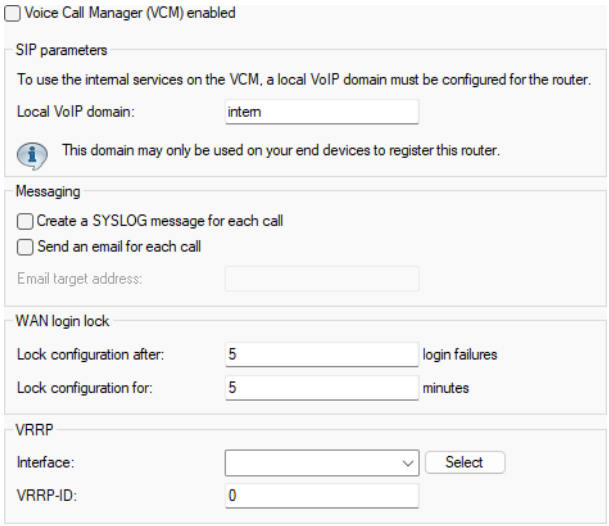
If a standby device takes over network communication, the SIP endpoints are unavailable until they register again.

Mixed operation in which telephones register using both the virtual and physical IP address is not intended.

ISDN and analog telephones cannot continue to be used in the event of a backup scenario.

Configuration in LANconfig

Configure the settings for voice backup using VRRP under **Voice Call Manager** > **General**.



VRRP Interface

Interface name of the virtual router.

VRRP ID

Virtual router ID.

4.2 Additions to the Setup menu

4.2.1 Vrrp-Interface

Interface name of the virtual router.

SNMP ID:

2.33.2.27

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

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

4.2.2 Vrrp-Interface

Virtual router ID.

SNMP ID:

2.33.2.28

Console path:

Setup > **Voice-Call-Manager** > **General**

Possible values:

1 … 255

5 RADIUS

5.1 Transfer DHCPv6 options in the RADIUS Auth VSA

As of LCOS 11.00, a new vendor-specific RADIUS attribute LCS-DHCPv6-Option with number 35 under the vendor LCS (2356) is supported. It is a RADIUS text attribute that only appears in Access-Accept messages (i.e. the response packets from the RADIUS server for RADIUS authorization) and may occur multiple times in the same message. In order for LCOS to process this option, the text must have the form specified below.

The attribute can be used for RADIUS authorization when the device is a RADIUS client and either a PPPoE server or an IKEv2 responder (VPN). Each instance of the attribute defines a DHCPv6 option that the DHCPv6 server in LCOS is to send to the DHCPv6 client on the PPPoE or VPN connection, provided that the DHCPv6 client requests it in its Option Request Option. This feature therefore fulfills the same purpose as the static table **Setup** > **IPv6** > **DHCPv6** > **Server** > **Additional-Options** [2.70.3.1.8].

The attribute text must consist of the three parts Option-Number, Option-Type, and Option-Value, each separated by a comma without spaces or other separators. Option-Value may be empty, but the second comma is still required. The three parts correspond to the columns of the same name in the setup table mentioned above and are formatted as follows:

- Option-Number specifies the option number (the DHCPv6 option code) as a number, either decimal, octal with a “0” prefix, or hexadecimal with a “0x” prefix. The number must be in the range from 1 to 65535.
- Option-Type is either a number in the range from 0 to 6, otherwise encoded like Option-Number, or one of the strings “Integer8”, “Integer16”, “Integer32”, “IPv6-Addresses”, “Domain-List”, “String”, or “Hexdump”, where the capitalization specified here must be observed.
- Option-Value is formatted exactly like the Option-Value column of the setup table mentioned above, where the format here, just as there, depends on the Option-Type. I quote the description from the current menu reference here, which applies equally to the RADIUS attribute. All types except String are comma- and space-separated lists, where empty list elements are ignored and an empty list is also permitted and results in an option of length 0.
  - “Integer8” or number 0: 8-bit integer from -128 to 127, optionally decimal, octal with prefix “0”, or hexadecimal with prefix “0x”.
  - “Integer16” or number 1: 16-bit integer from -32768 to 32767, optionally decimal, octal with prefix “0”, or hexadecimal with prefix “0x”.
  - “Integer32” or number 2: 32-bit integer from -2147483648 to 2147483647, optionally decimal, octal with prefix “0”, or hexadecimal with prefix “0x”.
  - “IPv6-Addresses” or number 3: IPv6 addresses without regard to capitalization in all permitted representations, including the mixed IPv4/IPv6 representation of mapped v4 addresses such as ::ffff:1.2.3.4.
  - “Domain-List” or number 4: Domain names in normal notation as strings separated into labels by dots, each label being at most 63 characters long. Empty labels are permitted but ignored. The DHCPv6 option is encoded as a sequence of labels with leading length bytes, as specified in *RFC 3315*, section 8 and *RFC 1035*, section 3.1. A domain always ends with the empty label 0.
  - “String” or number 5: The characters are taken over as a string. The string begins immediately after the second comma and may also contain additional commas, spaces, or quotation

marks, which are then interpreted as part of the string. If there is a space immediately after the second comma, this space is already considered part of the string.

- “Hexdump” or number 6: Expects only hexadecimal digits in each block without a “0x” prefix and pads each block with a leading 0 if necessary to achieve an even length. The block is interpreted as big-endian.

The Option-Number must be unique, i.e. the RADIUS response must not contain multiple LCS-DHCPv6-Option attributes with the same Option-Number, just as DHCPv6 must not contain multiple options with the same option code in the same message.

Examples of valid LCS-DHCPv6-Option attributes:

```
2356,0,0,-128,255,+13,-0200,0377,+0xD,0xff,-0x80,0X12
200,1,0,-32768,65535,+13,-0100000,0177777,+0xD,0xffff,-0x8000,0X12d
201,02,0,-2147483648,4294967295,+13,-020000000000,037777777777,+0xDEF,0xffffffff,-0x80000000,0X12d
202,03,::,2001:db87::beef,2001:004:00:0:56::,::ffff:192.168.0.4,fe80::02:a0:57:ff:fe:12:45:82,FE80::BDE
203,0x4,www.lancom.de,fully.qualified.,ThisIsAVeryLongLabelNamelyExactly63CharactersLongWhichIsMaximum.de
204, 5, alskdflaweiurqtow34875qor87aef<ynbxcv  4365o  7q64@!$&(/==%=?(
205,6,0123456789,abcdef,ABCDEF,8,123
0x2356,Integer8,,,,0, -128, 255, +13, -0200, 0377, +0xD, 0xff, -0x80, 0X12
0x200,Integer16,,,,0, -32768, 65535, +13, -0100000, 0177777, +0xD, 0xffff, -0x8000, 0X12d
0x201,Integer32,,,,0, -2147483648,4294967295,+13,-020000000000,037777777777,+0xDEF,0xffffffff,-0x80000000,0X12d
0x202,IPv6-Addresses,,,,::,2001:db87::beef,2001:004:00:0:56::,::ffff:192.168.0.4,fe80::02:a0:57:ff:fe:12:45:82,FE80::BDE
0x203,Domain-List,,,, www.lancom.de, fully.qualified., ThisIsAVeryLongLabelNamelyExactly63Characters.de
0x204,String,,,, alskdflaweiurqtow34875qor87aef<ynbxcv  4365o  7q64@!$&(/==%=?(
0x205,Hexdump,,,, 0123456789, abcdef, ABCDEF, 8, 123
```

Examples of invalid LCS-DHCPv6-Option attributes:

```
666,666,666
777,Integer64,12345
65536,0,1,2,3
144,4
```

6 Enhancements in the menu system

6.1 Additions to the Setup menu

6.1.1 CHAP-Reauth-Minutes

The CHAP rechallenge or CHAP reauthentication in the PPP server (PPTP, L2TP, PPPoE) can be configured here. Enter the time until CHAP reauthentication in minutes here.

The default is 0, which disables CHAP reauthentication.

If a CHAP packet is not answered, there are 4 additional retries at intervals of 5 seconds (a total of 5 attempts) before the connection is terminated with a timeout.

SNMP ID:

2.2.80

Console path:

Setup > **WAN** > **QoS**

Possible values:

Max. 2 characters from `[0-9]`

Default:

0

6.1.2 Key-Exchange-Algorithms

As of LCOS version 11.00, SSH supports two additional new hybrid post-quantum algorithms: “mlkem768nistp256-sha256” and “mlkem1024nistp384-sha384”.

The MAC key exchange algorithms are used to negotiate the key algorithm. Select one or more of the available algorithms.

SNMP ID:

2.11.28.3

Console path:

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

Possible values:

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2
curve25519-sha256
curve448-sha512
sntrup761x25519-sha512
diffie-hellman-group14-sha256
diffie-hellman-group15-sha512
diffie-hellman-group16-sha512
diffie-hellman-group17-sha512
diffie-hellman-group18-sha512
sntrup4591761x25519-sha512
mlkem768x25519-sha256

Hybrid post-quantum algorithm mlkem768x25519. In this case, the post-quantum algorithm ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) is combined with the well-known classical method Curve25519.

mlkem768nistp256-sha256

ybrid post-quantum algorithm mlkem768nistp256-sha256.

mlkem1024nistp384-sha384

ybrid post-quantum algorithm mlkem1024nistp384-sha384.

Default:

diffie-hellman-group-exchange-sha256

ecdh-sha2

curve25519-sha256

curve448-sha512

sntrup761x25519-sha512

diffie-hellman-group14-sha256

diffie-hellman-group15-sha512

diffie-hellman-group16-sha512

mlkem768x25519-sha256

6.1.3 Access-Type

As of LCOS 11.00, you can downgrade the access rights of a WireGuard tunnel to WAN. Configure the access type of the WireGuard tunnel per peer here.

SNMP ID:

2.19.70.3.17

Console path:

Setup > **VPN** > **WireGuard** > **Peers**

Possible values:

VPN
WAN

Default:

VPN

6.1.4 Authentication-Type

As of LCOS 11.00, additional algorithms according to RFC 5709 are supported for cryptographic authentication in OSPFv2. New additional methods are SHA1, SHA256, SHA384, and SHA512.

Authentication method used for this interface.

SNMP ID:

2.93.3.4.11

Console path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

Null
Simple-Password
Cryptographic-MD5
Cryptographic-SHA1
Cryptographic-SHA256
Cryptographic-SHA384
Cryptographic-SHA512

Default:

Null