LCOS 10.70

Addendum

11/2022

LANCOM
SYSTEMS

Contents

Copyright

1 Addendum to LCOS version 10.70

This document describes the changes and enhancements in LCOS version 10.70 since the previous version.

2 Configuration

2.1 Extension of the LoadFirmware command

As of LCOS 10.70, the CLI command `loadfirmware` can be configured via the new -e option switch to first save the firmware file completely in the local file system before starting the firmware update. This does not apply to other files or configurations/scripts.

3 Routing and WAN connections

3.1 Selectable entries in the IPv6 routing table

As of LCOS 10.70 entries in the IPv6 routing table can be selected and deselected.

The option is configured in LANconfig under **IP Router** > **Routing** > **Routing table** > **IPv6 routing table**.

Active

> Activates or deactivates this entry in the routing table.

3.1.1 Additions to the Setup menu

Active

Activates or deactivates this entry in the routing table.

SNMP ID:

> 2.70.12.1.6

Console path:

> **Setup** > **IPv6** > **Router** > **Routing-Table**

Possible values:

> **Yes**
> **No**

Default:

> Yes

3.2 Comment fields in the action table

From LCOS 10.70 a comment can be added for each entry in the Action table.

In LANconfig, the option is configured under **Communication** > **General** > **Action table**.

Comment

Enter a descriptive comment for this entry.

3.2.1 Additions to the Setup menu

Comment

Enter a descriptive comment for this entry.

SNMP ID:

2.2.25.10

Console path:

Setup > **WAN** > **Action-Table**

Possible values:

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

Default:

empty

3.3 BGP large communities

As of LCOS 10.70 BGP large communities attributes are supported as per *RFC 8092*. This makes it possible to use 4-octet AS numbers in communities. Large communities are supported as a separate configuration parameter in the BGP policy.

3.3.1 Table: Routing-Protocols > BGP > BGP Policy > Matches

Large Communities

Contains the corresponding item in the list under **Large Communities** in the section "Prefix and attribute lists".

Table: Routing protocols > BGP > BGP Policy > Matches > Large Communities (Attributes list)

This table contains large-community lists in order to identify NLRIs by their community attributes.

Name

Contains the name of this entry.

Large Communities

Contains large communities that the large-community attribute of the NLRI must match with.

The communities are specified in a comma-separated list.

Structure of a large community: *<Global administrator or ASN>:<Local data part 1>:<Local data part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Comment

>   Comment on this entry.

3.3.2 Table: Routing-Protocols > BGP > BGP Policy > Actions

Large Communities

>   Contains the name of an override of large-community entries in the NLRI.

>   This entry refers to the entries in the override table under *Table: Routing protocols BGP BGP Policy Actions Large Communities (Overrides list)* on page 10.

Table: Routing protocols > BGP > BGP Policy > Actions > Large Communities (Overrides list)

This table contains overrides that manipulate the large community attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

1. **Clear**
2. **Add**
3. **Remove**

Name

>   Contains the name of this entry.

Clear

>   Determines whether the device deletes unknown large communities from the NLRI.

Add

>   Specifies which large communities the device adds to an NLRI. The large communities are specified in a comma-separated list.

Structure of a large community: *<Global administrator or ASN>:<Local data part 1>:<Local data part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Remove

Specifies which large communities the device removes from an NLRI. The large communities are specified in a comma-separated list.

Structure of a large community: *<Global administrator or ASN>:<Local data part 1>:<Local data part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

Comment

Comment on this entry.

3.3.3 Additions to the Setup menu

Large-Communities

This table contains overrides that manipulate the large community attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

1. **Clear**
2. **Add**
3. **Remove**

SNMP ID:

2.93.1.5.2.4

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides**

Name

Contains the name of this entry.

SNMP ID:

2.93.1.5.2.4.1

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

Clear

Determines whether the device deletes unknown large communities from the NLRI.

SNMP ID:

2.93.1.5.2.4.2

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Yes

The device deletes unknown large communities from the NLRI.

No

The device does not change the large communities of an NLRI.

Default:

No

Add alarm

Specifies which large communities the device adds to an NLRI. The large communities are specified in a comma-separated list.

Structure of a large community: `<Global Administrator or ASN>:<Local Data Part 1>:<Local Data Part 2>`

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

SNMP ID:

2.93.1.5.2.3.3

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Max. 62 characters from `[0-9],:`

Default:

empty

Remove

Specifies which large communities the device removes from an NLRI. The large communities are specified in a comma-separated list.

Structure of a large community: *<Global Administrator or ASN>*:*<Local Data Part 1>*:*<Local Data Part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

SNMP ID:

2.93.1.5.2.4.4

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Max. 62 characters from `[0-9],:`

Default:

empty

Comment

Comment on this entry.

SNMP ID:

2.93.1.5.2.4.5

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Large-Communities**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` `

Default:

empty

Large-Communities

Contains the name of an override of large-community entries in the NLRI.

This entry refers to the entries in the override table under

SNMP ID:

2.93.1.5.3.6

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Actions**

Possible values:

Max. 16 characters from `[A-z][a-z][0-9]-_`

Default:

empty

Large-Communities

This table contains large-community lists in order to identify NLRIs by their community attributes.

SNMP ID:

2.93.1.5.4.4

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists**

Name

Contains the name of this entry.

SNMP ID:

2.93.1.5.4.4.1

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Large-Communities**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

Large-Communities

Contains large communities that the large-community attribute of the NLRI must match with.

The communities are specified in a comma-separated list.

Structure of a large community: *<Global Administrator or ASN>:<Local Data Part 1>:<Local Data Part 2>*

Example of a single large community: `64496:4294967295:2`

Example as a comma-separated list: `64496:4294967295:2, 64496:0:0`

SNMP ID:

2.93.1.5.4.4.2

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Large-Communities**

Possible values:

Max. 62 characters from `[0-9],:`

Default:

empty

Comment

Comment on this entry.

SNMP ID:

2.93.1.5.4.4.3

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Large-Communities**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` `

Default:

empty

Large-Communities

Contains the corresponding item in the list under

SNMP ID:

2.93.1.5.5.6

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

Max. 80 characters from `[A-z][a-z][0-9],-_`

Default:

empty

3.4 BGP RPKI-RTR

LCOS 10.70 and later support Resource Public Key Infrastructure (RPKI) to Router Protocol (RTR) for BGP.

The Border Gateway Protocol (BGP) is susceptible to route hijacking, i.e. unauthorized routers can advertise routes and thus redirect data traffic from the actual destination to itself. This situation can be caused by erroneous configurations and by explicit attacks.

Resource Public Key Infrastructure (RPKI) is a cryptographic method for signing and validating routing data records, which consist of a prefix and an autonomous system (AS). This record is called the Route Origin Authorization (ROA). More information on RPKI can be found in *RFC 6480*.

LCOS supports the Resource Public Key Infrastructure to Router Protocol (RTR) as per *RFC 8210*, with which a validator or cache supplies the router with information about validated routes and the associated AS number. This information is used by the BGP process to check whether a prefix or route was sent from the correct origin AS. Also checked is whether the prefix length corresponds to the information from the ROA data set.

This cache either runs on its own server for its own prefixes, or a public validator is used.

Public RPKI caches contain a large number of ROA entries. The recommendation is to operate RPKI only on devices with sufficient main memory to meet requirements (i.e. more than 2 GB), meaning that central-site devices or the vRouter need a correspondingly large main memory.

3.4.1 Configuring RPKI

RPKI can be found in LANconfig under **Routing protocols** > **General** > **Resource Public Key Infrastructure (RPKI)**. With the help of RPKI, BGP prefixes can be validated against a cache. To do this, the **Matches** table of the BGP policy provides an option for selecting the RPKI state of the relevant prefix. See *Configuring RPKI under BGP* on page 18.

RPKI enabled

Activates or deactivates RPKI

Accepted prefix types

Specifies which ROA prefix types (IPv4 or IPv6) should be stored. To optimize the main memory, the prefix type is recommended to be restricted to the address family (IPv4, IPv6) that is actually operated.

Possible values:

Both

Both IPv4 and IPv6 RPKI records are stored on the device (default).

IPv4

Only IPv4 RPKI records are stored on the device.

IPv6

Only IPv6 RPKI records are stored on the device

RPKI caches

This table is used to configure the RPKI validator or RPKI cache. The supported transport protocol is TCP.

The settings for the RPKI caches in LANconfig are located under **Routing protocols** > **General** > **Resource Public Key Infrastructure (RPKI)** > **Caches**.

Cache

 IPv4, IPv6 address, or hostname where the RPKI cache is reached.

Preference

 Preferred cache where multiple caches are used. Lower values result in a higher preference. Default: 0

Loopback address

 You can optionally specify a source address that the RPKI client uses as the target address, instead of the one that would normally be selected automatically. If you have configured loopback addresses, you can specify them here as sender address.

Routing tag

 Enter the routing tag for setting the route to the cache. Default: 0

Port

 The port of the RPKI cache. Default: 323

Version

 Protocol version of the PRKI-RTR protocol operated. Possible values:

 Fallback

 Communication with the cache starts with version 1 and falls back to version 0 if necessary.

 Zero

 Protocol version 0 is used to communicate with the cache.

 One

 Protocol version 1 is used to communicate with the cache.

3.4.2 The CLI show commands

The available show commands are listed in the following:

> **show rpki-v4-cache**

 Displays all currently stored IPv4 ROAs received from the cache.

> **show rpki-v6-cache**

 Displays all currently stored IPv6 ROAs received from the cache.

> **show rpki-status**

Displays the current status of the RPKI clients.

> **show bgp-prefix <prefix>**

Along with the BGP prefix information, the show command also displays the RPKI state of the respective prefix (`Not found`, `Valid`, `Invalid`, `Not available`). The following RPKI state is possible for a BGP prefix:

> `Not found`: The validator did not return any information about this prefix and the associated AS. It cannot be determined whether the entry is valid or invalid.
> `Valid`: The validator returned information matching the prefix and AS in the BGP. The entry is therefore valid.
> `Not valid`: The validator returned information that does not match the prefix and AS. Either the origin AS is incorrect or the prefix length does not match the data in the validator.
> `Not available`: No data is available from the validator to perform a check. RPKI is either not enabled or the device has not yet retrieved data from the validator. The prefix is already in the BGP before information is available from the validator.

> **show bgp-v4-rib**

Added the ROA-AS column, which contains the AS used for the RPKI check. The same applies to the ROA flag column, which contains the result of the ROA check.

> **show bgp-v6-rib**

Added the ROA-AS column, which contains the AS used for the RPKI check. The same applies to the ROA flag column, which contains the result of the ROA check.

3.4.3 Configuring RPKI under BGP

The **Matches** table of the BGP policy provides a new option for selecting the PRKI state of the relevant prefix.

LANconfig: **Routing protocols** > **BGP** > **BGP Policy** > **Matches**

RPKI state

The Resource Public Key Infrastructure (RPKI) status of prefixes can be used in a BGP policy, so rules can apply it to a BGP prefix. The rejection of invalid prefixes is not recommended; instead, they should be given a lower preference. In this case, a BGP rule is defined that matches to the RPKI status "Invalid". The action sets the preference of this prefix to the value 10, for example. Once a prefix has been rejected, it is not saved and is no longer available unless the prefix is retransmitted and reevaluated by the BGP neighbor.

None

The RPKI state is not processed.

Not found

The entry matches if the PRKI state of the prefix is set to "Not-found".

Invalid

The entry matches if the PRKI state of the prefix is set to "Invalid".

Valid

The entry matches if the PRKI state of the prefix is set to "Valid".

3.4.4 Additions to the Setup menu

RPKI-State

The Resource Public Key Infrastructure (RPKI) status of prefixes can be used in a BGP policy, so rules can apply it to a BGP prefix. The rejection of invalid prefixes is not recommended; instead, they should be given a lower preference. In this case, a BGP rule is defined that matches to the RPKI status "Invalid". The action sets the preference of this prefix to the value 10, for example. Once a prefix has been rejected, it is not saved and is no longer available unless the prefix is retransmitted and reevaluated by the BGP neighbor.

SNMP ID:

2.93.1.5.5.7

Console path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Matches**

Possible values:

None

The RPKI state is not processed.

Not-found

The entry matches if the PRKI state of the prefix is set to "Not-found".

Valid

The entry matches if the PRKI state of the prefix is set to "Valid".

Invalid

The entry matches if the PRKI state of the prefix is set to "Invalid".

RPKI

The Border Gateway Protocol (BGP) is susceptible to route hijacking, i.e. unauthorized routers can advertise routes and thus redirect data traffic from the actual destination to itself. This situation can be caused by erroneous configurations and by explicit attacks.

Resource Public Key Infrastructure (RPKI) is a cryptographic method for signing and validating routing data records, which consist of a prefix and an autonomous system (AS). This record is called the Route Origin Authorization (ROA). More information on RPKI can be found in *RFC 6480*.

LCOS supports the Resource Public Key Infrastructure to Router Protocol (RTR) as per *RFC 8210*, with which a validator or cache supplies the router with information about validated routes and the associated AS number. This information is used by the BGP process to check whether a prefix or route was sent from the correct origin AS. Also checked is whether the prefix length corresponds to the information from the ROA data set.

This cache either runs on its own server for its own prefixes, or a public validator is used.

Public RPKI caches contain a large number of ROA entries. The recommendation is to operate RPKI only on devices with sufficient main memory to meet requirements (i.e. more than 2 GB), meaning that central-site devices or the vRouter need a correspondingly large main memory.

This directory contains the configuration for the RPKI.

SNMP ID:

2.93.7

Console path:

Setup > **Routing-Protocols**

Caches

The RPKI validator or RPKI cache used are configured in this table. The supported transport protocol is TCP.

SNMP ID:

2.93.7.1

Console path:

Setup > **Routing-Protocols** > **RPKI**

Cache

IPv4, IPv6 address, or hostname where the RPKI cache is reached.

SNMP ID:

2.93.7.1.1

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.``

Default:

empty

Preference

Preferred cache where multiple caches are used. Lower values result in a higher preference.

SNMP ID:

2.93.7.1.2

Console path:

> **Setup** > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

> Max. 10 characters from `[0-9]`

Default:

> 0

Loopback

You can optionally specify a source address that the RPKI client uses as the target address, instead of the one that would normally be selected automatically. If you have configured loopback addresses, you can specify them here as sender address.

SNMP ID:

> 2.93.7.1.3

Console path:

> **Setup** > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

> Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

> 0

Rtg-Tag

Enter the routing tag for setting the route to the cache.

SNMP ID:

> 2.93.7.1.4

Console path:

> **Setup** > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

> 0 … 65535

Default:

> 0

Port

The port of the RPKI cache.

SNMP ID:

2.93.7.1.5

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

Max. 5 characters from `[0-9]`

Default:

323

Version

Protocol version of the PRKI-RTR protocol operated.

SNMP ID:

2.93.7.1.6

Console path:

Setup > **Routing-Protocols** > **RPKI** > **Caches**

Possible values:

Null

Protocol version 0 is used to communicate with the cache.

One

Protocol version 1 is used to communicate with the cache.

Fallback

Communication with the cache starts with version 1 and falls back to version 0 if necessary.

Operating

Activates or deactivates RPKI

SNMP ID:

2.93.7.2

Console path:

Setup > **Routing-Protocols** > **RPKI**

Possible values:

> **No**
> **Yes**

Default:

> No

Accepted-Prefix-Type

Specifies which ROA prefix types (IPv4 or IPv6) should be stored. To optimize the main memory, the prefix type is recommended to be restricted to the address family (IPv4, IPv6) that is actually operated.

SNMP ID:

> 2.93.7.3

Console path:

> **Setup** > **Routing-Protocols** > **RPKI**

Possible values:

> **Both**
>> Both IPv4 and IPv6 RPKI records are stored on the device.
>
> **IPv4**
>> Only IPv4 RPKI records are stored on the device.
>
> **IPv6**
>> Only IPv6 RPKI records are stored on the device

Default:

> Both

3.5 BGP: Administrative shutdown communication

From LCOS 10.70 the command line command `do manual-stop <Name> [<Message>]` specifies the new optional parameter `<Message>`. This can be used to transmit a reason to the other BGP router as a message according to RFC 8203.

3.5.1 Additions to the Setup menu

Manual stop

With this action, you manually stop a BGP neighbor.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from `[A-Z][a-z][0-9]-_`).

If the arguments entered here match for several neighbors, the device terminates all of these connections.

(i)   If multiple connections are opened to a neighbor, the device terminates all of these connections.

Optionally, a reason can be posted to the other BGP router as a message according to *RFC 8203*. Enter this reason as an additional parameter.

SNMP ID:
> 2.93.1.10

Console path:
> **Setup** > **Routing-Protocols** > **BGP**

3.6 BGP: Graceful shutdown support

From LCOS 10.70 BGP supports the graceful shutdown community as per *RFC 8326*.

For this purpose, the known community `graceful shutdown` is supported in the configuration parameters of the communities.

4 IPv6

4.1 IPv6 neighbor discovery proxy (NDP)

From LCOS 10.70 the device supports an IPv6 neighbor discovery proxy (NDP). The ND proxy corresponds to the IPv4 counterpart ARP proxy. The ND proxy integrates remote IPv6 stations into your local network as if they were physically located within it. The router then responds to neighbor discovery packets on behalf of the remote station.

Scenarios:

> An upstream router does not support DHCPv6 prefix delegation. The downstream router enables the ND proxy and uses the same /64 prefix on its LAN and WAN interfaces. The LAN prefix is generated from the router advertisement of the upstream router of the WAN interface. This enables communication between LAN stations and WAN stations that use the same /64 prefix.

> A VPN gateway assigns dial-up clients an IPv6 address from the same prefix that is already configured on a local interface. This router must enable the ND proxy to allow communication between dial-in clients and stations on the local LAN with the same IPv6 prefix. This scenario is analogous to the ARP proxy for IPv4.

In LANconfig you configure the option under **IPv6** > **General** > **LAN interfaces** or **IPv6** > **General** > **WAN profiles**.

ND-Proxy

Enables or disables the IPv6 Neighbor Discovery proxy. The ND proxy corresponds to the IPv4 counterpart ARP proxy. The ND proxy integrates remote IPv6 stations into your local network as if they were physically located within it. The router then responds to neighbor discovery packets on behalf of the remote station.

4.1.1 Additions to the Setup menu

ND-Proxy

Enables or disables the IPv6 Neighbor Discovery proxy. The ND proxy corresponds to the IPv4 counterpart ARP proxy. The ND proxy integrates remote IPv6 stations into your local network as if they were physically located within it. The router then responds to neighbor discovery packets on behalf of the remote station.

SNMP ID:

2.70.6.14

Console path:

Setup > **IPv6** > **LAN-Interfaces**

Possible values:

No
Yes

Default:

No

ND-Proxy

Enables or disables the IPv6 Neighbor Discovery proxy. The ND proxy corresponds to the IPv4 counterpart ARP proxy. The ND proxy integrates remote IPv6 stations into your local network as if they were physically located within it. The router then responds to neighbor discovery packets on behalf of the remote station.

SNMP ID:

2.70.7.12

Console path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

No
Yes

Default:

No

4.2 PREF64 options

As of LCOS 10.70 the device supports the prefix option in router advertisements as per RFC 8781. This is configured in LANconfig under **IPv6** > **Router Advertisement** > **PREF64 options**.

This table configures the prefix option in router advertisements (PREF64 option as per *RFC 8781*) for NAT64 prefixes, which are announced to clients in the router advertisement. Clients adopt this prefix e.g. for 464XLAT.

Interface name

Specify the name of the interface to be used to advertise the PREF64 option.

Prefix

Defines the NAT64 prefix with prefix length, e.g. 64:ff9b::/96

Lifetime

Validity period of the NAT64 prefix in seconds. Default: 1800 seconds.

Comment

Enter a descriptive comment here.

4.2.1 Additions to the Setup menu

PREF64-Option

This table configures the prefix option (PREF64 option as per *RFC 8781*) for NAT64 prefixes, which are announced to clients in the router advertisement. Clients adopt this prefix e.g. for 464XLAT.

SNMP ID:

2.70.2.8

Console path:

Setup > **IPv6** > **Router-Advertisements**

Interface-Name

Specify the name of the interface to be used to advertise the PREF64 option.

SNMP ID:

2.70.2.8.1

Console path:

> **Setup** > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Possible values:

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

Default:

> *empty*

IPv6-Address-Prefixlength

Defines the NAT64 prefix with prefix length, e.g. 64:ff9b::/96

SNMP ID:

> 2.70.2.8.2

Console path:

> **Setup** > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Possible values:

> Max. 43 characters from `[A-F][a-f][0-9]:./`

Default:

> *empty*

Scaled-Lifetime

Validity period of the NAT64 prefix in seconds.

SNMP ID:

> 2.70.2.8.3

Console path:

> **Setup** > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Possible values:

> Max. 5 characters from `[0-9]`

Default:

> 1800

Comment

Enter a descriptive comment here.

SNMP ID:

> 2.70.2.8.4

Console path:

> **Setup** > **IPv6** > **Router-Advertisement** > **PREF64-Option**

Possible values:

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

Default:

> *empty*

4.3 IPv6 address table extension

As of LCOS 10.70 there are the new switch values **Delegated Auto Configuration** and **Delegated DHCPv6** in the IPv6 addresses table under **Address type**.

In LANconfig, the option is configured under **IPv6** > **General** > **IPv6 addresses**.

Address type

> Specify the type of IPv6 address.
>
> Options:
>
> › Delegated Auto Configuration
>
>   The IPv6 address is formed from the router advertisement prefix received on the selected interface (**Interface name** field) and the host identifier from the field **Address / Prefix length**. The field **Address / Prefix length** can be filled out e.g. with the value "::2/64" in combination with the prefix "2001:db8::/64" on the interface to form the address "2001:db8::2/64".
>
> › Delegated DHCPv6
>
>   The IPv6 address is formed from the delegated DHCPv6 prefix received on the selected interface (**Interface name** field) and the host identifier from the field **Address / Prefix length**. The field **Address / Prefix length** can be filled out e.g. with the value "::2/64" in combination with the prefix "2001:db8::/56" on the interface to form the address "2001:db8::2/64". Similarly, an address can be formed from any subnet of the delegated prefix, e.g "0:0:0:0001::1" and the prefix "2001:db8::/56" go to form the address "2001:db8:0:0001::1/64".

4.3.1 Additions to the Setup menu

Address type

Specify the type of IPv6 address.

SNMP ID:

> 2.70.4.1.3

Console path:

> **Setup** > **IPv6** > **Network** > **Addresses**

Possible values:

Unicast

> With the Unicast address type, you use the field *2.70.4.1.2 IPv6-Address-Prefixlength* to specify a full IPv6 address along with its interface identifier, e.g. "2001:db8::1234/64".

Anycast

> With the Anycast address type, you can also use the field *2.70.4.1.2 IPv6-Address-Prefixlength* to specify a full IPv6 address along with its interface identifier, e.g. "2001:db8::1234/64". Internally, the device handles this address as an anycast address.

EUI-64

> The IPv6 address is formed according to the IEEE standard "EUI-64". The MAC address of the interface thus forms a uniquely identifiable part of the IPv6 address. The correct input format for an IPv6 address including the prefix length as per EUI-64 would be: "2001:db8:1::/64".

> (!) EUI-64 ignores any value set as "interface identifier" in the corresponding IPv6 address and replaces it with an "interface identifier" as per EUI-64.

> (!) The prefix length for EUI-64 must be "/64".

Delegated-Auto-Configuration

> The IPv6 address is formed from the router advertisement prefix received on the selected interface (field *2.70.4.1.1 Interface name*) and the host identifier from the field *2.70.4.1.2 IPv6-Address-Prefixlength*. The field *2.70.4.1.2 IPv6-Address-Prefixlength* can be filled out e.g. with the value" ::2/64" in combination with the prefix "2001:db8::/64" on the interface to form the address "2001:db8::2/64".

Delegated-DHCPv6

> The IPv6 address is formed from the delegated DHCPv6 prefix received on the selected interface (field *2.70.4.1.1 Interface name*) and the host identifier from the field *2.70.4.1.2 IPv6-Address-Prefixlength*. The field *2.70.4.1.2 IPv6-Address-Prefixlength* can be filled out e.g. with the value "::2/64" in combination with the prefix "2001:db8::/56" on the interface to form the address "2001:db8::2/64". Similarly, an address can be formed from any subnet of the delegated prefix, e.g "0:0:0:0001::1" and the prefix "2001:db8::/56" go to form the address "2001:db8:0:0001::1/64".

Default:

> Unicast

4.4 IPv6 ND-cache limit

From LCOS 10.70 ND cache limits are enabled. This provides protection against flooding attacks. If necessary, you can adjust the global cache limit and the limit per interface using the command line.

4.4.1 Additions to the Setup menu

NDP

This menu allows you to find the settings for the ND cache.

SNMP ID:

> 2.70.16

Console path:

> **Setup** > **IPv6**

Global-Cache-Limit

Specifies the maximum allowed number of IPv6 neighbor cache entries per device.

SNMP ID:

> 2.70.16.1

Console path:

> **Setup** > **IPv6** > **NDP**

Possible values:

> Max. 10 characters from `[0-9]`

Default:

> 20000

Cache-Limit-Per-Interface

Specifies the maximum allowed number of IPv6 neighbor cache entries per interface.

SNMP ID:

> 2.70.16.2

Console path:

> **Setup** > **IPv6** > **NDP**

Possible values:

> Max. 10 characters from `[0-9]`

Default:

10000

5 Virtual Private Networks – VPN

5.1 LANCOM Advanced Mesh VPN (AMVPN)

Classic VPN scenarios in site connectivity are usually star-shaped (hub & spoke). The connected branches (spokes) set up VPN tunnels to one or more hubs. In such traditional scenarios, a hub & spoke network design is a logical topology decision, because data flows mainly between the branch and the headquarters, since central servers are located there, such as the ERP system, databases or web servers.
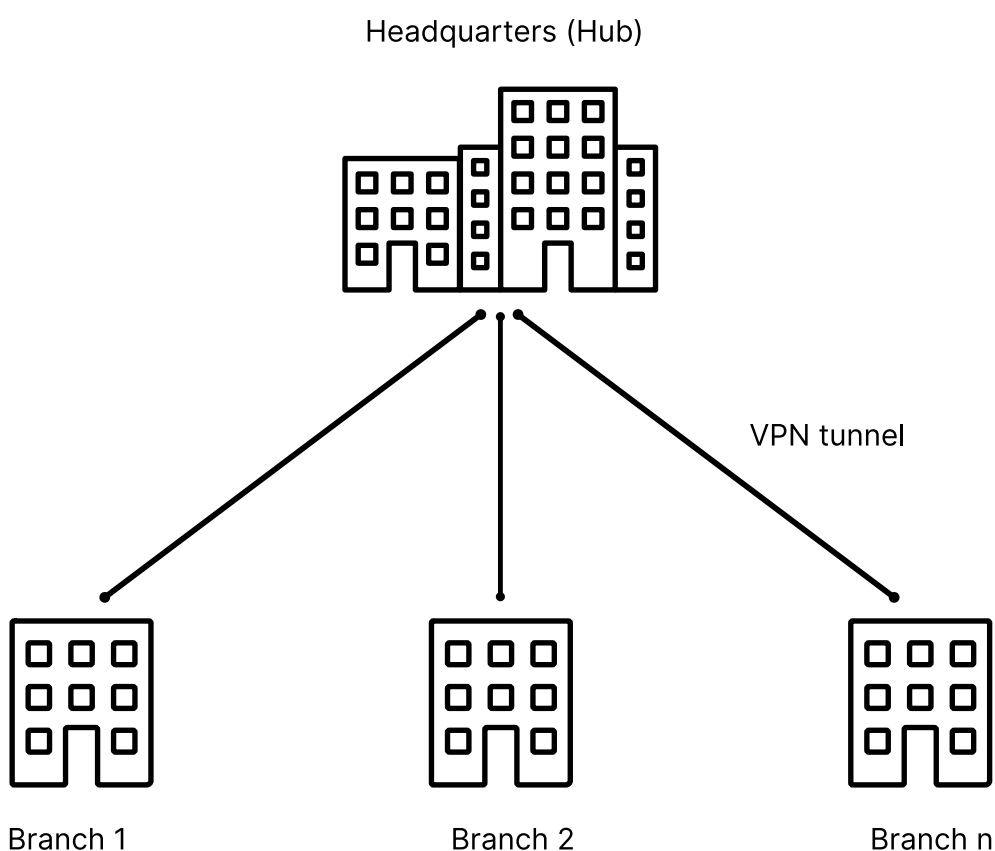
Headquarters (Hub)

Figure 1: Classic site networking (hub & spoke)

The advantages of this star-shaped network design are the simple structure and the central control in the headquarters. The disadvantage, however, is that all data traffic—including that between individual branches, such as telephony or file exchange via a file server—always takes place indirectly via the headquarters'. As a result, the headquarters Internet

connection is burdened with data traffic between the branches and thus becomes the bottleneck of the entire communication.

Headquarters (Hub)

Path of the
data packets

VPN tunnel

Branch 1   Branch 2   Branch n
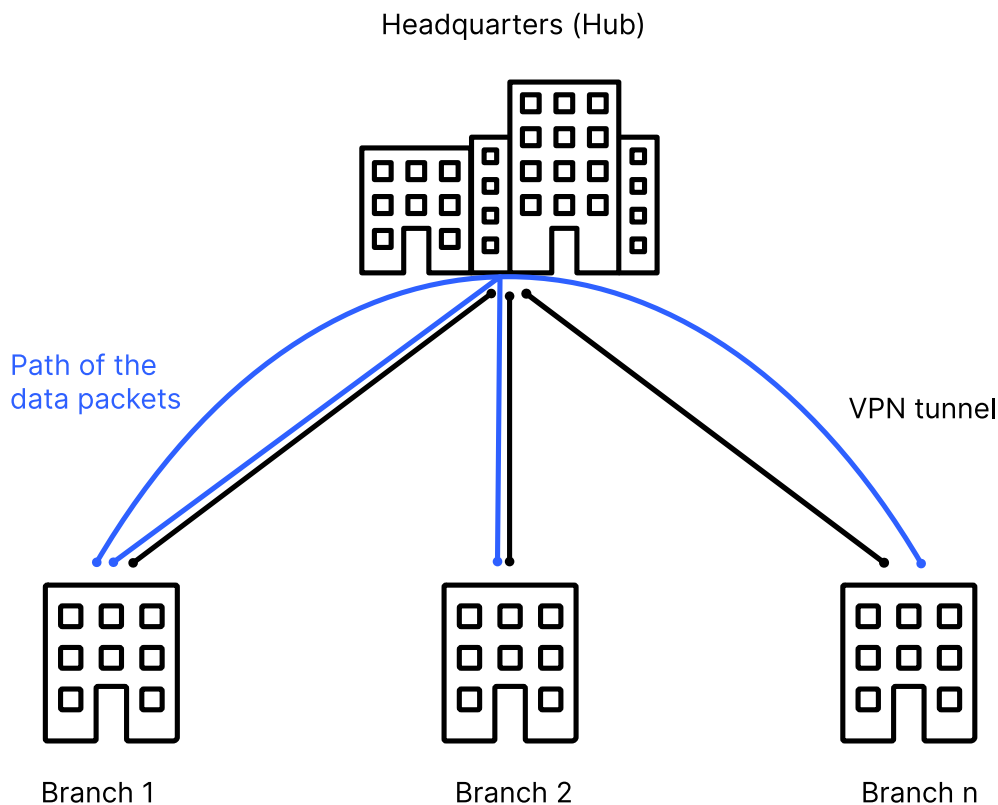
Figure 2: Data exchange between branches with classic site networking (hub & spoke)

If inter-branch traffic is the largest portion of the traffic relationship, a practical approach is to manually configure direct VPN tunnels between branches. This case is referred to as a VPN mesh scenario. In simple scenarios, the manual approach works well. However, if there are many branches and many possible VPN tunnels, this rigid, individual, and fixed configuration approach no longer scales.

LANCOM offers the "Advanced Mesh VPN" as a solution in this scenario. The starting point is a classic star-shaped VPN structure, where each of the branches connects to the headquarters via VPN tunnel. In the event of data traffic between two branches, a VPN tunnel is dynamically established directly between them. The data now flows directly through a VPN tunnel between the branches without the data going via the headquarters.

The initial data packets have to take the long route from branch A via the headquarters to the second branch B. Only when the first data packets are received at the target branch does the target branch initiate a dynamic VPN tunnel to the branch that was the origin of the initial data packet. If no data flows for a time, the tunnel is dynamically terminated again.

The advantage: Significantly less traffic in the headquarters and, as a result, higher performance throughout the entire corporate network.
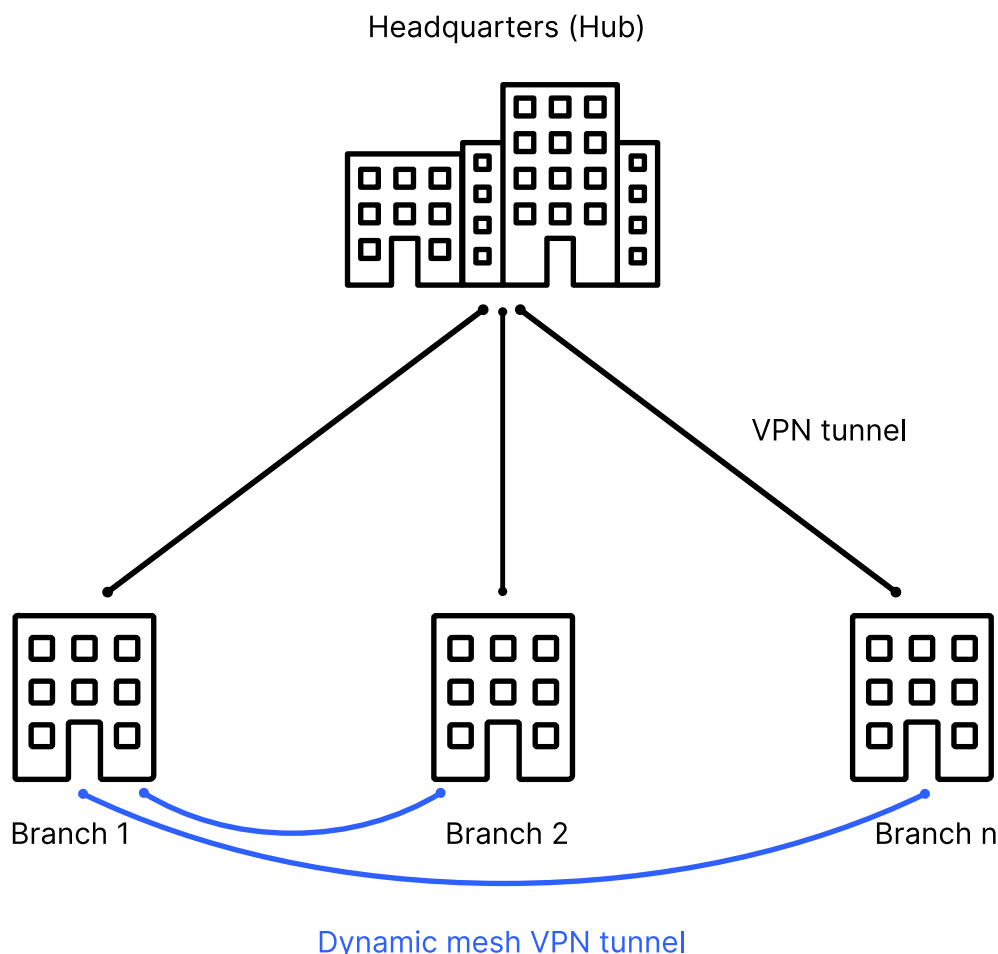
Headquarters (Hub)

Figure 3: Site networking via Advanced Mesh VPN

The following basic steps are necessary to configure Advanced Mesh VPN:

1. Configuring the VPN tunnel between the branch office and headquarters.
2. Creating a Mesh VPN tunnel template in the IKEv2 peer table that contains the shared VPN properties such as encryption method, PSK, or certificate for the dynamic Mesh VPN tunnel.
3. Activation of the Mesh VPN feature and configuration of the global mesh parameters on all relevant VPN routers.

How is the dynamic setup of a Mesh VPN done?

1. Branch A sends data packets over the existing static VPN tunnel via the main office to branch B.
2. The router at branch B detects a new session because data packets from an unknown subnet arrive via the VPN tunnel from the headquarters.
3. Branch B sends an encrypted manufacturer-specific IKEv2 message to the headquarters. The message contains the private subnets or IP addresses of the desired communication relationship and the public IP address of branch office B.
4. The headquarters receives the vendor specific IKEv2 message in the VPN tunnel from branch B and forwards it to branch A via the VPN tunnel to branch A.
5. Branch A receives the headquarters' vendor specific IKEv2 message.
6. Branch A creates a dynamic Mesh VPN tunnel and establishes it directly to the IP address of branch B. The router takes the necessary information from the vendor specific IKEv2 message (gateway IP address, subnet, etc.).

7. Branch B accepts the tunnel setup by branch A and updates its local routing table to include the subnet at branch A with the destination gateway that is the public IP address at branch A. The private subnet of branch A is used by IKEv2 routing as an IKEv2 message during VPN tunnel establishment and is more specific than the route to the headquarters.

8. Data now flows directly between branches A and B, since the routes at both ends now point to the dynamic VPN tunnel.

9. If no further data is transmitted after the timeout, the Mesh VPN tunnel is terminated.

> The first data packets initially flow via the tunnel to the main office and then trigger the establishment of a dynamic tunnel.

> A ping to the LAN IP address of the router at the peer does not trigger the establishment of a Mesh VPN tunnel. Only data packets to endpoints in the LAN will trigger tunnel establishment, as only these can be correctly identified by the router-firewall. However, a ping to a (possibly non-existent) IP address in the LAN does however trigger the establishment of a VPN mesh tunnel.

> Ongoing firewall sessions relating to the data packets first sent via the headquarters are moved to the newly established mesh tunnel after the Mesh VPN tunnel was set up successfully (session switchover).

> The branch that is to accept a dynamic Mesh VPN tunnel must have a public IP address (IPv4 or IPv6) and be reachable from the outside. Routers with a cellular connection usually do not have a public IP address.

> LANCOM Advanced Mesh VPN is a vendor-specific implementation based on IKEv2 and only works between LCOS-based LANCOM VPN routers. The LANCOM Advanced VPN Client does not support this.

> The security is based entirely on IKEv2/IPsec and can handle all settings such as PSK, certificates, encryption algorithms, or LANCOM HSVPN from IKEv2.

> All routers involved (branch office, main office) require LCOS 10.70 or higher.

Traces on LANCOM Advanced Mesh VPN have been facilitated by the parameter `VPN-Mesh`.

5.1.1 Licensing

Mesh VPN tunnels are counted separate from and in addition to normal VPN tunnels. If the licenses for Mesh VPN tunnels are exhausted, no mesh tunnel is set up and the data continues to travel the longer route via the main office. Central-site devices are limited to a maximum of 200 mesh tunnels, whatever their configuration.

The following Mesh VPN licenses apply (depending on the number of normal VPN tunnels):

Table 1: Mesh VPN tunnel licenses

Category	Devices	Number of licenses	
		VPN tunnel	Mesh VPN tunnel
CPE	R88x, 88x VoIP, 1640E	3	6
CPE	179x, 18xx	5	10
CPE	179x, 18xx with VPN 25	25	50
CPE	19xx	25	50
CPE	19xx with VPN 50	50	100
CPE	19xx with VPN 100	100	200
Central-site	ISG-1000	100	200
Central-site	ISG-4000	200	200
Central-site	ISG-5000	100	200
Central-site	ISG-8000	250	200

5.1.2 Configuring Advanced Mesh VPN

Now configure the Advanced Mesh VPN in LANconfig under **VPN** > **IKEv2/IPSec** > **Extended settings** > **Advanced Mesh VPN**.

Operation-Mode

This control affects the way the Mesh VPNs works and enables behavior as a spoke or hub, or even both roles at the same time. Possible values:

Deactivated

The Mesh VPN feature is disabled, Mesh VPN messages are not sent, forwarded, or processed. Mesh VPN tunnels are neither established nor accepted.

Hub

The device assumes the role of the central-site VPN gateway. Mesh VPN messages are forwarded between the tunnels. The device itself does not establish or accept any Mesh VPN tunnels.

Spoke

The device assumes the function of a branch office and establishes and accepts Mesh VPN tunnels.

Hub&Spoke

The device takes on the role of the central-site VPN gateway, and also establishes Mesh VPN tunnels to other spokes and accepts Mesh VPN tunnels.

VPN peer template

This parameter refers to an entry in the IKEv2 peer table. This entry is used as a configuration template for the Mesh VPN tunnels.

Detect on VPN peers

A comma-separated list of VPN peers that the (firewall) detector should react to. This entry is required for branches to detect incoming sessions. This can be left empty, e.g. for branches behind a NAT (without port forwarding) and therefore unable to act as responders for a mesh tunnel.

Group-ID

Each device can be assigned to a group that is used to send its requests. One option of this is to divide the mesh into smaller groups, e.g. regional mesh structures.

Accepted group IDs

A comma-separated list specifying the mesh group IDs that are accepted. A request from a group ID not listed here will be discarded.

Admin distance

The distance set in the IP router for routes received via the mesh tunnel. The special value "0" is equivalent to the internal default of "15".

Initial rate limit

Requested networks (addresses) are temporarily blocked in order to protect the network. The initial lockout period is specified here in seconds.

Max. rate limit

The lockout period from the **Initial rate limit** is doubled each time until the **Maximum rate limit** is reached.

Request validity

After the lockout period has expired, networks (addresses) that were previously requested will still be available. This validity always begins when the blocking expires and ends when the device sends or receives a request for this network (this address).

Forwarding filter

This filter list can be used to filter requests to specific networks on the hub. If the network request in a Mesh message does not match any row in the table, the request is allowed through (allow-all).

Prefix

Defines the prefix for which a rule should apply, e.g. 10.0.0.0/24 or 2001:db8::/32.

Day

Defines the routing tag or routing context associated with the filter rule.

Action

Defines the action for this filter entry. Possible values: Allow, Deny.

Comment

Enter a descriptive comment here.

5.1.3 Tutorial: Setting up Advanced Mesh VPN

Initial situation: The scenario consists of two branches (A and B) with public IPv4 addresses and a main office, also with a public IPv4 address. The two branches have already set up a static IKEv2 VPN tunnel to the main office, and this

is running. The VPN peer at the branches is called "MAIN". Branch A has the subnet 192.168.1.0/24 and branch B has the subnet 192.168.2.0/24 with the name "INTRANET".

Configuration at branch A

1. Create a new entry, e.g. "MESH-TEMPLATE", in the IKEv2 connection list under **VPN** > **IKEv2/IPSec** > **Connection list**.

   (i) This entry serves as a template used by the dynamic mesh tunnels take to read their parameters.

2. The **Short hold time** is the time of data inactivity after which Mesh VPN tunnels disconnect, e.g. 300 seconds.

   (!) Deactivating the short hold time by setting it to the value 0 is not recommended, otherwise dynamic Mesh VPN tunnels will never terminate after inactivity, and this will consume licenses.

3. Leave the remote **Gateway** blank as it is set dynamically.

4. The **Routing** parameter transmits the local network to the opposite branch, in this case the "INTRANET" network. To do this, create a new entry in the **IPv4 routing** table under **VPN** > **IKEv2 / IPSec** > **Extended settings**. For example, select "INTRANET-ROUTING" as the name and, in the **Network** field, select the local network to be used for Mesh VPN, e.g. "INTRANET".
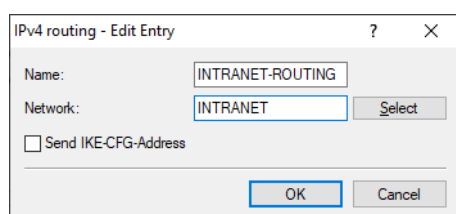
Figure 4: Example of the IPv4 routing entry

5. Under **Authentication**, set the option **Manage source**. Create a new entry, e.g. "MESH". Enter the **Local identifier** of the branch and the **PSK** used for all dynamic mesh tunnels. The PSK must be identical on all branches involved

in the mesh VPN tunnel. Leave the field **Remote identifier** blank and select the option "No identity" for **Remote identifier type**, so that all incoming identities with the correct PSK are accepted as mesh tunnels.

Figure 5: Example authentication settings

6. Set the **VPN rule** to "ANY" or select "RAS-WITH-NETWORK-SELECTION" for **IPv4 rules**. Thus uses 0.0.0.0/0 <=> 0.0.0.0/0.

7. Set **Rule creation** to "Manual".

Figure 6: Example of the Mesh VPN template in the connection list

8. Now configure the Mesh VPN parameters under **VPN** > **IKEv2/IPSec** > **Extended settings** > **Advanced Mesh VPN**.

9. Set **Operation mode** to "Spoke".

10. Under **VPN peer template** select the previously created IKEv2 peer as a template for the Mesh VPN tunnel.

11. Under **Detect on VPN peers**, select the name of the VPN peer that corresponds to the name of the tunnel to the main office.

Figure 7: Example of Advanced Mesh VPN settings in the branch office

Configuration at branch B

12. The configuration is performed similar to branch A. Change the **Local identifier** for the **Authentication** to the name of branch B.

Configuring the main office

13. Since the main office itself does not set up a dynamic mesh tunnel, there is no need to create a template for the peer. Set the **Operation mode** for the Advanced Mesh VPN to "Hub".

Figure 8: Example of Advanced Mesh VPN settings in the main office

If you now transfer data from branch A to branch B, the first packets take the detour via the main office. After that, the dynamic mesh tunnel is set up between the branches.

> (!) A ping to the router's IP address at the other end will not establish a mesh tunnel. A (possibly non-existent) station in the LAN at the other end must be used as the destination.

5.1.4 Additions to the Setup menu

Mesh

This item is used for the settings for the LANCOM Advanced Mesh VPN (AMVPN).

SNMP ID:

> 2.19.36.35

Console path:

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

Operation-Mode

This parameter affects the way the Mesh VPNs works and enables behavior as a spoke or hub, or even both roles at the same time.

SNMP ID:

> 2.19.36.35.1

Console path:

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

Possible values:

> **Inactive**
> **Spoke**
> **Hub**

Default:

> Inactive

Admin-Distance

The distance set in the IP router for routes received via the mesh tunnel.

SNMP ID:

> 2.19.36.35.2

Console path:

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

Possible values:

> 0 … 255

Special values:

0

Equivalent to the internal default of "15"

Default:

0

VPN-Peer-Template

This parameter refers to an entry in the IKEv2 peer table. This entry is used as a configuration template for the Mesh VPN tunnels.

SNMP ID:

2.19.36.35.3

Console path:

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

Possible values:

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

Default:

empty

Initial-Rate-Limit-Sec

Requested networks (addresses) are temporarily blocked in order to protect the network. The initial lockout period is specified here in seconds.

SNMP ID:

2.19.36.35.4

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Default:

5

Max-Rate-Limit-Sec

The blocking time from is doubled until the value set here is reached.

SNMP ID:

2.19.36.35.5

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Default:

320

Request-Validity-Sec

After the lockout period has expired, networks (addresses) that were previously requested will still be available. This validity always begins when the blocking expires and ends when the device sends or receives a request for this network (this address).

SNMP ID:

2.19.36.35.6

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Default:

3600

Group-ID

Each device can be assigned to a group that is used to send its requests. One option of this is to divide the mesh into smaller groups, e.g. regional mesh structures.

SNMP ID:

2.19.36.35.7

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Default:

1

Accepted-Group-IDs

A comma-separated list specifying the mesh group IDs that are accepted. A request from a group ID not listed here will be discarded.

SNMP ID:

2.19.36.35.8

Console path:

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

Possible values:

Max. 253 characters from `[0-9],`

Default:

1

Detect-on-VPN-Peers

A comma-separated list of VPN peers that the (firewall) detector should react to. This entry is required for branches to detect incoming sessions. This can be left empty, e.g. for branches behind a NAT (without port forwarding) and therefore unable to act as responders for a mesh tunnel.

SNMP ID:

2.19.36.35.9

Console path:

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

Possible values:

Max. 253 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Forwarding-Filter

This filter list can be used to filter requests to specific networks on the hub. If the requested network from a request via manufacturer-specific IKEv2 message does not match any table row, the request is allowed through (allow-all).

SNMP ID:

2.19.36.35.10

Console path:

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

IP-Address-Prefix

Defines the prefix for which a rule should apply, e.g. 10.0.0.0/24 or 2001:db8::/32.

SNMP ID:

2.19.36.35.10.1

Console path:

Setup > **VPN** > **IKEv2** > **Mesh** > **Forwarding-Filter**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Rtg-tag

Defines the routing tag or routing context associated with the filter rule.

SNMP ID:

2.19.36.35.10.2

Console path:

Setup > **VPN** > **IKEv2** > **Mesh** > **Forwarding-Filter**

Possible values:

0 … 65535

Default:

0

Filter-Action

Defines the action for this filter entry.

SNMP ID:

2.19.36.35.10.3

Console path:

Setup > **VPN** > **IKEv2** > **Mesh** > **Forwarding-Filter**

Possible values:

Allowed
Forbidden

Comment

Enter a descriptive comment here.

SNMP ID:

2.19.36.35.10.4

Console path:

Setup > **VPN** > **IKEv2** > **Mesh** > **Forwarding-Filter**

Possible values:

Max. 253 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` `

Default:

empty

5.2 Two-factor authentication in the VPN

As of LCOS 10.70, LCOS supports VPN two-factor authentication (EAP-OTP) with the LANCOM Advanced VPN Client. For this purpose, the internal RADIUS server can manage OTP users.

In addition to his normal VPN user name and password (EAP-MSCHAPv2), the VPN user has an authenticator app, e.g., on his smartphone, on which a second factor is generated and used in addition to the user name / password. Two-factor authentication is only possible with EAP in IKEv2 according to the RFC, so simple PSK or RSA signature methods cannot be used. LCOS supports a vendor-specific implementation together with the LANCOM Advanced VPN Client.

Any apps can be used as authenticators, e.g. from Google, Microsoft or NCP. You can find these apps in the app store of your mobile device.

The setup procedure is as follows: First, EAP-VPN with IKEv2 must be configured in the LANCOM device. The internal RADIUS server with its user accounts is used for this purpose. In addition to a RADIUS user account, an OTP user must be created. Subsequently, a QR code can be retrieved in WEBConfig under **Extras** > **EAP-OTP users** , which must be scanned by the Authenticator app. This QR code applies per user and must be used each time an Authenticator app is

to be set up. WEBconfig generates a QR code per user from the parameters of the **OTP user accounts** table that can be scanned by Authenticator apps. Alternatively, the key can be added manually in most apps.
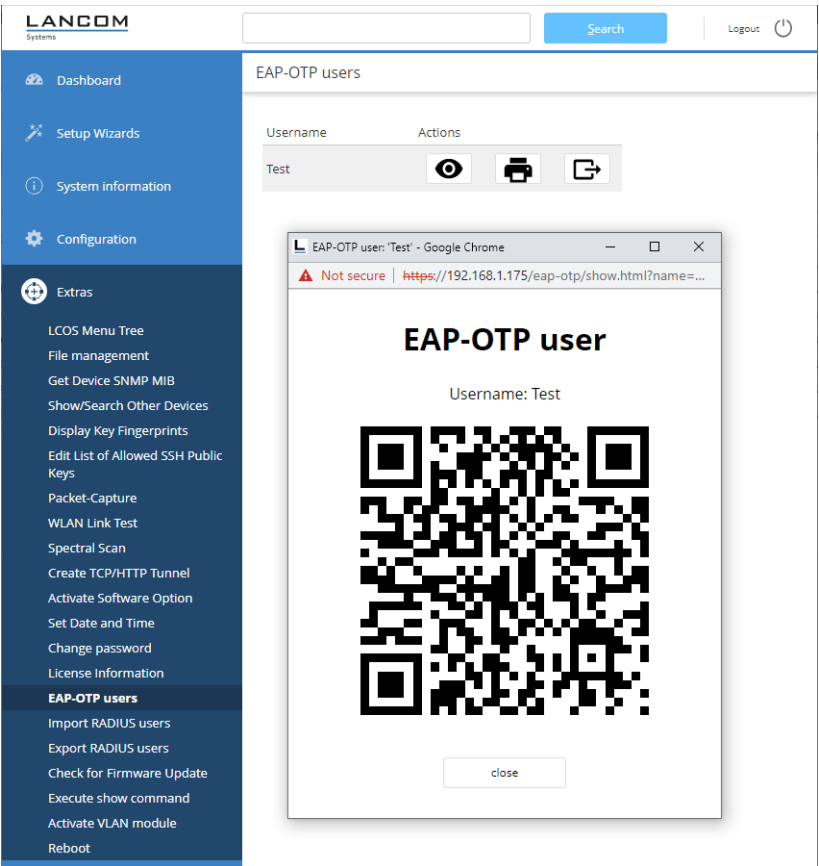
Figure 9: WEBconfig: Extras > EAP-OTP users

Instructions for setting up the entire scenario can be found in the *LANCOM Support Knowledge Base*.

ⓘ Please note that for correct time synchronization with the Authenticator, the router must have the current time. To do this, enable the NTP client in the router under **Date & Time** > **Synchronization** > **NTP client settings**.

5.2.1 Configuration with LANconfig

OTP user accounts

The OTP users are defined in the OTP user accounts table. For EAP-OTP, the user must be created with his normal password in the table of RADIUS user accounts, as well as additionally created in this table with the OTP secret.

The configuration of the OTP user accounts is done via **RADIUS** > **Server** > **User database** > **OTP user accounts**.

Username

Enter the name of the OTP user here. This must already be contained in the RADIUS user accounts table with the same name.

Hash algorithm

Defines the hash algorithm used.

> (i) Note that the Authenticator app supports the maximum possible hash algorithm. For example, Google Authenticator currently supports only SHA1 on certain Android platforms.

Time step

Defines the interval in seconds after which a new OTP is calculated. Default: 30 seconds

Network delay

Defines the maximum number of time steps by which the client's clock may deviate. The RADIUS server checks the OTP that is older or newer by this value.

Secret

Defines the actual shared secret that must be shared with the Authenticator app. The secret must be different for each user. There are currently three possible entries in the table:

Base32 (Default)

Prefix "base32:" followed by the base32 encoded secret. The prefix "base32:" may also be omitted.

Hexadezimal

Prefix "hex:" followed by an even number of hex digits.

Plain text passphrase

Prefix "ascii:" and then the characters.

> (i) For Google Authenticator, the secret must be 16 characters long (80 bit, Base32 encoded), e.g. E3U5IDWEE3KFCJ7G

Issuer

Freely definable text used in Authenticator to keep multiple keys apart when the same username is used. Must not contain a colon.

Number digits

Length of OTPs. Default: 6.

ⓘ For Google Authenticator, the value 6 should be used.

Calling station id mask

This mask restricts the validity of the entry to certain IDs transmitted by the calling station.

Called station id mask

This mask restricts the validity of the entry to certain IDs transmitted by the called station.

EAP-OTP

RADIUS > **Server** > **Extended configuration** > **EAP**

The **Default method** has been extended by the value OTP.

OTP

One Time Password. This value must be used with EAP-OTP for *two-factor authentication in the VPN*, because with the LANCOM Advanced VPN Client the EAP method is specified by the EAP server.

5.2.2 Additions to the Setup menu

Default-Method

This value specifies which method the RADIUS server should offer to the client outside of a possible TTLS/PEAP tunnel.

SNMP ID:

2.25.10.10.7

Console path:

Setup > **RADIUS** > **Server** > **EAP**

Possible values:

> **None**
> **MD5**
> **GTC**
> **MSCHAPv2**
> **TLS**
> **TTLS**
> **PEAP**
> **WFA-Unauth**
> **OTP**

Default:

> MD5

EAP-OTP

The parameters for EAP-OTP are set here.

SNMP ID:
> 2.25.10.10.20

Console path:
> **Setup** > **RADIUS** > **Server** > **EAP**

Users

In this table the OTP users are defined.

SNMP ID:
> 2.25.10.10.20.1

Console path:
> **Setup** > **RADIUS** > **Server** > **EAP** > **EAP-OTP**

User-Name

Enter the name of the OTP user here. This must already be contained in the RADIUS user accounts table with the same name.

SNMP ID:
> 2.25.10.10.20.1.1

Console path:
> **Setup** > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ```

Default:

empty

Calling-Station-Id-Mask

This mask restricts the validity of the entry to certain IDs transmitted by the calling station.

SNMP ID:

2.25.10.10.20.1.2

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

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

Default:

empty

Called-Station-Id-Mask

This mask restricts the validity of the entry to certain IDs transmitted by the called station.

SNMP ID:

2.25.10.10.20.1.3

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

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

Default:

empty

Hash-Algorithm

Defines the hash algorithm used.

(i) Note that the Authenticator app supports the maximum possible hash algorithm. For example, Google Authenticator currently supports only SHA1 on certain Android platforms.

SNMP ID:

2.25.10.10.20.1.4

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

SHA1
SHA256
SHA512

Default:

SHA1

Time-Step

Defines the interval in seconds after which a new OTP is calculated.

SNMP ID:

2.25.10.10.20.1.5

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 10 characters from `[0-9]`

Default:

30

Network-Delay

Defines the maximum number of time steps by which the client's clock may deviate. The RADIUS server checks the OTP that is older or newer by this value.

SNMP ID:

2.25.10.10.20.1.6

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 3 characters from `[0-9]`

Secret

Defines the maximum number of time steps by which the client's clock may deviate. The RADIUS server checks the OTP that is older or newer by this value.

Base32 (Default)

Prefix "base32:" followed by the base32 encoded secret. The prefix "base32:" may also be omitted.

Hexadecimal

Prefix "hex:" followed by an even number of hex digits.

Plain text passphrase

Prefix "ascii:" and then the characters.

(i) For Google Authenticator, the secret must be 16 characters long (80 bit, Base32 encoded), e.g. E3U5IDWEE3KFCJ7G

SNMP ID:

2.25.10.10.20.1.7

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` `

Default:

empty

Num-Digits

Length of the OTPs.

(i) For Google Authenticator, the value 6 should be used.

SNMP ID:

2.25.10.10.20.1.8

Console path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

Max. 3 characters from `[0-9]`

Default:

6

Issuer

Freely definable text used in Authenticator to keep multiple keys apart when the same username is used. Must not contain a colon.

SNMP ID:

> 2.25.10.10.20.1.9

Console path:

> **Setup** > **RADIUS** > **Server** > **EAP** > **EAP-OTP** > **Users**

Possible values:

> Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

> *empty*

6 WLAN management

6.1 Support for NTP server in WLAN controller

As of LCOS 10.70, the WLAN controller supports the specification of time servers (NTP) in the profiles of the WLAN controller.

The WLAN controller synchronizes the time with an access point when it accepts it. As a result, it is possible that an access point that has been managed for a long time without new time information may have larger deviations from the WLAN controller, possibly leading to certificate problems. By using a time server, this problem cannot occur.

Under **WLAN Controller** > **Profiles** > **WLAN profiles** there is a new parameter **Time server profile**:

Time server profile

The Time server profile selected here applies to the WLAN profile. You manage the Time server profiles under **WLAN Controller** > **Profiles** > **Advanced profiles** with the button **Time server profiles**.

Profile name

The name of this NTP profile.

Server name or IP addr.

The server name or IP address of the NTP server.

Authentication

Enables or disables MD5 authentication for the server.

Key ID

Identifies the key used for MD5 authentication for the server.

Key

The value of the key for authentication with the NTP server.

6.1.1 Additions to the Setup menu

NTP-Profile

The WLAN controller synchronizes the time with an access point when it accepts it. As a result, it is possible that an access point that has been managed for a long time without new time information may have greater deviations from the WLAN controller, possibly leading to certificate problems. By using a time server, this problem cannot occur.

From the list of NTP profiles under on page 57, select the profile that should apply in the WLAN profile.

SNMP ID:

> 2.37.1.3.12

Console path:

> **Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

> Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

> *empty*

NTP-Profiles

In this table you can find the NTP profiles of the defined time servers.

SNMP ID:

> 2.37.1.28

Console path:

> **Setup** > **WLAN-Management** > **AP-Configuration**

Name

The name of this NTP profile.

SNMP ID:

2.37.1.28.1

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

RQ-Address

The server name or IP address of the NTP server.

SNMP ID:

2.37.1.28.2

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

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

Default:

empty

Authentication-Enabled

Enables or disables MD5 authentication for the server.

SNMP ID:

2.37.1.28.3

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

No
   Disabled
Yes
   Enabled

Default:

No

Key-ID

Identifies the key used for MD5 authentication for the server.

SNMP ID:

2.37.1.28.4

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

1 … 65535

Key

The value of the key for authentication with the NTP server.

SNMP ID:

2.37.1.28.5

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **NTP-Profiles**

Possible values:

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

Default:

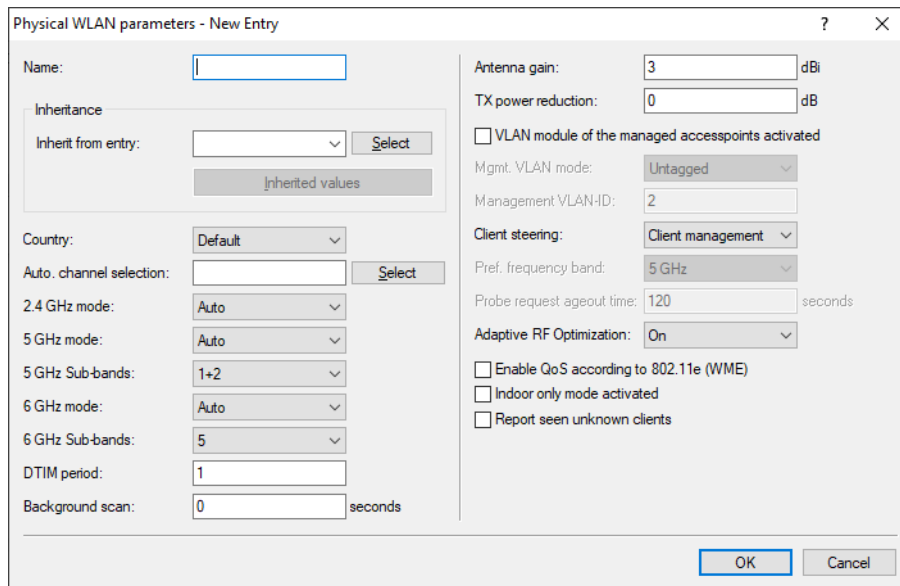*empty*

6.2 Support for three radio modules and 6 GHz in the WLAN controller

As of LCOS 10.70, the WLAN controller supports three radio modules and the 6 GHz band in the profiles of the WLAN controller.

Under **WLAN Controller** > **Profiles** > **Physical WLAN parameters**this mode and the sub-bands to be used are set.

Under **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)** select the 6 GHz band in the **Allowed frequency bands**.

6.2.1 Additions to the Setup menu

Radio-Band

Selecting the frequency band determines whether the wireless LAN adapter operates in the 2.4 GHz, 5 GHz or 6 GHz band, which in turn determines the available radio channels.

SNMP ID:

>   2.37.1.1.10

Console path:

>   **Setup** > **WLAN-Management** > **AP-Configuration** > **Networkprofiles**

Possible values:

>   **All**
>   **2.4GHz**
>   **5GHz**
>   **6GHz**

Default:

>   All

Subbands-6GHz

In the 6 GHz band, it is also possible to select a subband, which is linked to certain radio channels and maximum transmission powers.

SNMP ID:

>   2.37.1.2.26

Console path:

>   **Setup** > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

>   **Band-5**
>   **Band-7**
>   **Band-5+7**

6GHz-Mode

Specify which radio standards the physical WLAN interface you configured supports against a WLAN client in the 6 GHz frequency band.

SNMP ID:

>   2.37.1.2.27

Console path:

>   **Setup** > **WLAN-Management** > **AP-Configuration** > **Radioprofiles**

Possible values:

>   **Auto**
>   >   Automatic. Within the 6 GHz mode, the automatic leads to 802.11ax.

Default:

>   Auto

WLAN-Module-3

Frequency of the third WLAN module. This parameter can also be used to deactivate the WLAN module.

SNMP ID:

>   2.37.1.4.39

Console path:

>   **Setup** > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

>   **default**
>   >   Makes use of the encryption method defined in the "Options" area.
>   **2.4GHz**
>   **5GHz**
>   **6GHz**
>   **Off**
>   **Auto**

Default:

>   default

Module-3-Max.-Channel-Bandwidth

Enter how and to what extent the AP specifies the channel bandwidth for the 2nd physical WLAN interface.

SNMP ID:

>   2.37.1.4.40

Console path:

>   **Setup** > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Auto

The AP automatically detects the maximum channel bandwidth.

20MHz

The AP uses channels bundled at 20 MHz.

40MHz

The AP uses channels bundled at 40 MHz.

80MHz

The AP uses channels bundled at 80 MHz.

80+80MHz

The AP uses two channels bundled at 80 MHz.

160MHz

The AP uses channels bundled at 160 MHz.

Default:

Auto

Module-3-Channel-List

The radio channel selects a portion of the conceivable frequency band for data transfer.

SNMP ID:

2.37.1.4.41

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Module-3-Ant-Gain-Mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. In particular for outdoor access points with integrated high-gain antennas, this value had to be adjusted manually. As of LCOS 10.30 the standard antenna gain of a managed access point is automatically transmitted to and used by the WLAN controller. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.30. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

SNMP ID:

2.37.1.4.42

Console path:

> **Setup** > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

> **Standard**
>> The antenna gain value preset in the access point is used.
>
> **user-defined**
>> The value for **Module-3-Ant-Gain** is used.

Default:

> Standard

Module-3-Ant-Gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, and depending on the country where the system is operated and the frequency band, the base station calculates the maximum permitted transmission power.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4-GHz band or 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

Example:

AirLancer	Antenna gain	C a b l e attenuation:	Value to be entered
O-18a	18dBi	4dB	18dBi - 4dB = 14dBi

(i) The current transmission power is displayed by the device's web interface or by telnet under **Status** > **WLAN statistics** > **WLAN parameters** > **Transmission power** or with LANconfig under **System information** > **WLAN card** > **Transmission power**.

SNMP ID:

> 2.37.1.4.43

Console path:

> **Setup** > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

> 0 … 999 dBi

Default:

> *empty*

Module-3-TX-Reduct

If you use an antenna with a high amplification factor, you can use this entry to attenuate the transmission power of your base station to the transmission power permitted in your country in the frequency band in question.

If the field is left blank, the default setting defined in the configuration profile of relevant WLAN profile will be used.

Transmission power can be reduced to a minimum of 0.5 dBm in the 2.4-GHz band or 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band. Please ensure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

(i)   The current transmission power is displayed by the device's web interface or by telnet under **Status** > **WLAN statistics** > **WLAN parameters** > **Transmission power** or with LANconfig under **System information** > **WLAN card** > **Transmission power**.

SNMP ID:

2.37.1.4.44

Console path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

0 … 999 dBi

Default:

empty

WLAN-Modul-3-default

This setting allows you to configure the frequency band in which the AP operates the 3rd physical WLAN interface.

(i)   If a managed AP only has two ot less physical WLAN interfaces, the AP ignores the settings for the 3rd physical WLAN interface.

SNMP ID:

2.37.1.41

Console path:

Setup > **WLAN-Management** > **AP-Configuration**

Possible values:

Auto

The AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 6GHz band, if available.

2.4GHz

The AP operates the physical WLAN interface in the 2.4Ghz band.

5GHz

The AP operates the physical WLAN interface in the 5Ghz band.

6GHz

> The AP operates the physical WLAN interface in the 6Ghz band.

Off

> The AP disables the physical WLAN interface.

Default:

Auto

7 Voice over IP – VoIP

7.1 Support of NAPTR records by the Voice Call Manager

As of LCOS 10.70 the Voice Call Manager supports the DNS resolution of NAPTR (Naming Address Pointer) records. The telephony provider can use the NAPTR record to specify the transport protocol used, e.g. UDP, TCP, or TLS, that the VCM uses to resolve the SIP registrar. Priorities or weightings can also be assigned in case there are several NAPTR records for a request. By default, new configurations in the VCM use NAPTR records for DNS resolution.

For this purpose, the parameter **Signaling encryption** in LANconfig under **Voice Call Manager** > **Lines** > **SIP lines** > **Security** has been extended with the new default value **Automatic**.
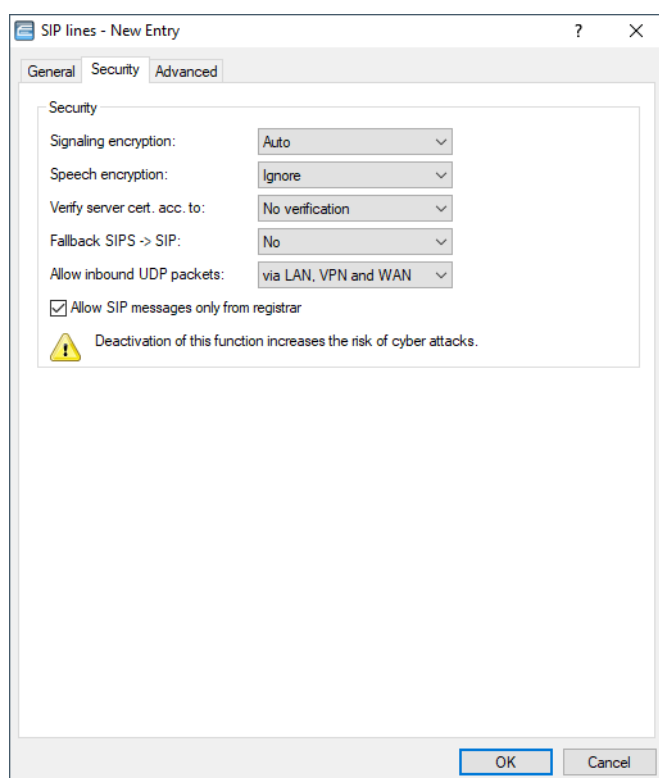
Signaling encryption

> This setting determines the protocol used for signaling encryption (SIP/SIPS) for communications with the provider.

> **Automatic**

> NAPTR (Naming Address Pointer) records are used for DNS resolution. In the DNS data, the provider specifies the use of transport protocols such as UDP, TCP or TLS. The provider can also specify weights or priorities.

> If TLS is specified as the transport protocol for signaling encryption by NAPTR, voice encryption is also used automatically, regardless of the explicit configuration setting of voice encryption.

7.1.1 Additions to the Setup menu

Transport

Use this entry to specify which protocol is used to encrypt the data streams.

SNMP ID:

> 2.33.4.1.1.28

Console path:

> **Setup** > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

> **Auto**
>
>> NAPTR (Naming Address Pointer) records are used for DNS resolution. In the DNS data, the provider specifies the use of transport protocols such as UDP, TCP or TLS. The provider can also specify weights or priorities.
>>
>> If TLS is specified as the transport protocol for signaling encryption by NAPTR, voice encryption is also used automatically, regardless of the explicit configuration setting of voice encryption.
>
> **UDP**
>
>> All SIP packets are transmitted connectionless. Most providers support this setting.
>
> **TCP**
>
>> All SIP packets are transmitted connection-oriented. The device establishes a TCP connection to the provider and maintains it for as long as it stays registered. Specialized providers, such as the providers of SIP trunks, support or force this setting.
>
> **TLSv1**
> **TLSv1.1**
> **TLSv1.2**
> **TLSv1.3**
>
>> Transmission is the same as with TCP, but all of the SIP packets are encrypted all the way to the provider. The TLS version selected in the configuration is taken as the minimum requirement for TLS encryption.

Default:

> Auto

8 Backup solutions

From LCOS 10.70 RU2, support for vRouter redundancy in Amazon AWS is available.

8.1 Support for vRouter redundancy in Amazon AWS

Cloud providers used for outsourcing virtual machines to the cloud, such as Amazon AWS, do not support layer-2 protocols such as VRRP. This means that common router redundancy concepts are not readily available and must be implemented differently. Amazon AWS offers an API that can be used to switch route entries to a secondary router in the event of a failover.

This scenario is structured as follows: One or more private virtual machines (EC2 instances) are available. Two redundant vRouters have a private subnet to the virtual machines and a public subnet to the Internet. Each vRouter has a VPN tunnel to the customer site, which thus provides access to the private machines. One vRouter is the primary router (active), the second router is secondary (passive). The latter is only involved in active routing in the event of a failover. An EC2 instance can only have one router as the next hop in the private subnet at a time. In case of failover, the AWS API uses the AWS routing table to switch from the primary vRouter to the secondary vRouter. If the primary vRouter is available again, it switches back to the primary router.

In order to access the AWS API, the vRouters require a role in the AWS Identity and Access Management (IAM).

A VPN tunnel is established between the two vRouters in order to detect the failure of the primary router. The action table in the secondary vRouter sends AWS API commands when it detects that the VPN tunnel to the primary vRouter is being established or shut down. The only purpose of the VPN tunnel is to detect the availability of the primary router. No data is transmitted via this VPN tunnel.

The vRouter needs access to the Internet in order to access the AWS API.

8.1.1 Configuration

Configure vRouter redundancy for AWS on the command line under **/Setup/Cloud-Provider/AWS/** in the table **HA-Redundancy**.

Profile-Name

Unique name of the profile. This name is used by the route-change command to reference the profile.

Route-Table

Name of the routing table to change in AWS, e.g. "rtb-099605ce6cb4ac319". This value can be taken from the AWS management interface.

CIDR-IP

Prefix in the routing table for which the next hop is to be changed, e.g. "0.0.0.0/0".

ENI

Name of the AWS network adapter (Elastic Network Interface) that the command is to set as the next hop, e.g. "eni-00c734d6da1fd8968". This value can be taken from the AWS management interface.

Region

Region where the AWS route table is located, e.g. "eu-central-1"

Network-name

Name of the interface or remote site used by the vRouter to reach the AWS API, e.g. "INTERNET".

Comment

Enter a descriptive comment for this entry.

8.1.2 Commands

Two commands are available under **/Setup/Cloud-Provider/AWS**:

> Switch-Route

```
do /Setup/Cloud-Provider/AWS/Switch-Route <Profile-Name>
```

This command uses the AWS API to switch the prefix in the AWS routing table to the new next hop as configured under <profile-name> in the table /Setup/Cloud-Provider/AWS/.

> Get-Remote-Route-Table

```
do /Setup/Cloud-Provider/AWS/Get-Remote-Route-Table <route-table-id>
    <region> <outgoing-network>
```

This command returns the current status of the AWS routing table <route-table-id> via the AWS API. Example:

```
do Get-Remote-Route-Table rtb-099605ce6cb4ac319 eu-central-1 INTERNET
```

Example: Using the commands in the action table

The backup vRouter has the following entries configured in the action table (**Communication** > **General** > **Action table**):

There are two profiles in the HA redundancy table that are referenced in the action table in the Switch-Route command. The first entry causes the backup vRouter to make itself the active router in the AWS routing table if the VPN tunnel (remote site AWS-VR1) to the primary router is disconnected or broken. If the VPN tunnel is reestablished, i. e. the primary router is available again, the primary router is reset as the next hop in the routing table.

8.1.3 Configuring the IAM role in AWS

In AWS, go to the IAM dashboard and click **Role** > **Create Role**.

The IAM role for the secondary vRouter requires the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateRouteTable",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:DisassociateRouteTable",
                "ec2:ReplaceRouteTableAssociation"
```

```
        ],
        "Resource": "*"
    }
    ]
}
```

Create a new policy and assign the policies to the secondary vRouter so that it has the correct permissions to invoke the API.

8.1.4 Additions to the Setup menu

Cloud-Provider

Configuration for special features of the vRouter if it is operated via a cloud provider such as Amazon AWS.

SNMP ID:

> 2.201

Console path:

> **Setup**

AWS

Entries on the vRouter for the cloud provider Amazon AWS.

SNMP ID:

> 2.201.1

Console path:

> **Setup** > **Cloud-Provider**

Switch-Route

`do /Setup/Cloud-Provider/AWS/Switch-Route <Profile-Name>`

This command uses the AWS API to switch the prefix in the AWS routing table to the new next hop as configured under

SNMP ID:

> 2.201.1.1

Console path:

> **Setup** > **Cloud-Provider** > **AWS**

Possible arguments:

> **<Profile-Name>**
>
> > Profile name from

HA-Redundancy

Table for the support of vRouter redundancy in AWS.

SNMP ID:

    2.201.1.2

Console path:

    Setup > **Cloud-Provider** > **AWS**

Profile name

Unique name of the profile. This name is used by the route-change command to reference the profile.

SNMP ID:

    2.201.1.2.1

Console path:

    Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

    Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

    empty

Route-Table

Name of the routing table to change in AWS, e.g. "rtb-099605ce6cb4ac319". This value can be taken from the AWS management interface.

SNMP ID:

    2.201.1.2.2

Console path:

    Setup > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

    Max. 50 characters from `[A-Z][a-z][0-9]-_`

Default:

    empty

CIDR-IP

Prefix in the routing table for which the next hop is to be changed, e.g. "0.0.0.0/0".

SNMP ID:

> 2.201.1.2.3

Console path:

> **Setup** > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

> Max. 18 characters from `[0-9]./`

Default:

> *empty*

ENI

Name of the AWS network adapter (Elastic Network Interface) that the command is to set as the next hop, e.g. "eni-00c734d6da1fd8968". This value can be taken from the AWS management interface.

SNMP ID:

> 2.201.1.2.4

Console path:

> **Setup** > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

> Max. 50 characters from `[A-Z][a-z][0-9]-_`

Default:

> *empty*

Region

Region where the AWS route table is located, e.g. "eu-central-1"

SNMP ID:

> 2.201.1.2.5

Console path:

> **Setup** > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

> Max. 30 characters from `[A-Z][a-z][0-9]-_`

Default:

> *empty*

Network name

Name of the interface or remote site used by the vRouter to reach the AWS API, e.g. "INTERNET".

SNMP ID:

> 2.201.1.2.6

Console path:

> **Setup** > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

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

Default:

> *empty*

Comment

Enter a descriptive comment for this entry.

SNMP ID:

> 2.201.1.2.7

Console path:

> **Setup** > **Cloud-Provider** > **AWS** > **HA-Redundancy**

Possible values:

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

Default:

> *empty*

Get-Remote-Route-Table

```
do /Setup/Cloud-Provider/AWS/Get-Remote-Route-Table <route-table-id>
   <region> <outgoing-network>
```

This command returns the current status of the AWS routing table <route-table-id> via the AWS API. Example:

```
do Get-Remote-Route-Table rtb-099605ce6cb4ac319 eu-central-1 INTERNET
```

SNMP ID:

> 2.201.1.3

Console path:

> **Setup** > **Cloud-Provider** > **AWS**

Possible arguments:

<route-table-id>

ID of an AWS route table.

<region>

<outgoing-network>

9 Other services

9.1 Stateless DHCP relay agent

From LCOS 10.70 the DHCP relay agent supports the "stateless relay" operating mode.

For this purpose, the parameter **DHCP server enabled** in LANconfig under **IPv4** > **DHCPv4** > **DHCP networks** has been extended with the new value **Stateless relay**.

DHCP server enabled

> The DHCP server can be configured to run in the following modes:

> **Stateless relay**

> The device accepts requests from DHCP clients in the local network. However, the device does not answer these requests itself, but forwards them to a central DHCP server in another network section (DHCP relay agent mode).

> The Stateless Relay Agent does not modify DHCP packets from the client to the server and back. In particular, unlike the Relay Agent, the DHCP server identifier is not modified.

9.1.1 Additions to the Setup menu

Operating

DHCP server operating mode in this network. Depending on the operating mode, the DHCP server can enable/disable itself. The DHCP statistics show whether the DHCP server is enabled.

ⓘ Only use the setting "Yes" if you are certain that no other DHCP server is active in the LAN.

Only use the "client mode" setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

SNMP ID:

2.10.20.11

Console path:

Setup > **DHCP** > **Network-List**

Possible values:

No

DHCP server is permanently switched off.

Yes

DHCP server is permanently switched on. When this value is entered the server configuration (validity of the address pool) is checked. If the configuration is correct then the device starts operating as a DHCP server in the network. Errors in the configuration (e.g. invalid pool limits) will cause the DHCP server to be deactivated. Only use this setting if you are certain that no other DHCP server is active in the LAN.

Auto

With this setting, the device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress. If another DHCP server is discovered the device switches its own DHCP server off. If the LANCOM is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. This prevents unconfigured devices introduced to the network from assigning addresses unintentionally. If no other DHCP server is discovered the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the device will be disabled.

Relay

The DHCP server is active and receives requests from DHCP clients in the LAN. The device does not respond to requests, but forwards them to a central DHCP server elsewhere in the network (DHCP relay agent mode).

Client

The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN. Only use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.

Stateless-relay

The device accepts requests from DHCP clients in the local network. However, the device does not answer these requests itself, but forwards them to a central DHCP server in another network section (DHCP relay agent mode).

The Stateless Relay Agent does not modify DHCP packets from the client to the server and back. In particular, unlike the Relay Agent, the DHCP server identifier is not modified.

Default:

No

9.2 BPjM module

As of LCOS 10.70, the BPjM module is supported. The BPjM module is issued by the German Federal Agency for the Protection of Children and Young People in the Media and blocks websites that may not be made accessible to children and young people in Germany. This function is particularly relevant for schools and educational institutions with underage students. This means that URLs whose content is officially classified as harmful to minors are inaccessible to the relevant target group in Germany. Automatic and regular updating and expansion of this listing is guaranteed. The BPJM module blocks URLs that are on the official website list of the Federal Review Board for Media Harmful to Young Persons (BPjM). Blocking by category or override (allow) is not possible.

The BPJM module is part of the LANCOM Content Filter Option or is available separately via the software option LANCOM BPjM Filter Option.

In the IPv4 or IPv6 firewall, there is a default firewall rule that can be activated and configured for each network. For example, it is possible to equip only the student network with this filter, but to exclude other networks from it.

In the IPv6 firewall, there is a new default rule BPJM that is disabled by default with the system object "BPJM" as the target station. In the IPv4 firewall there is an analogous rule. Define as source stations the networks that are to be protected by the BPjM module.

9.2.1 Recommendations for use

If content filters and BPJM filters are to be used together, both rules must be configured with different priorities so that they are run through one after the other.

Likewise, for the first rule, care must be taken to ensure that the item "Observe further rules, after this rule matches" is activated.

In rare cases, the BPJM module may block desired domains because only (DNS) domains and not URL directory levels can be checked due to TLS. In this case, these desired domains can be added to the "BPJM Allow list", e.g. *.example.com.

The LANCOM router must serve as DNS server or DNS forwarder in the network, i.e. clients in the local network must use the router as DNS server. In addition, the direct use of DNS-over-TLS and DNS-over-HTTPS (possibly browser-internal) with external DNS servers by clients must be prevented.

This can be achieved as follows:

> The DHCP server must distribute the router's IP address as the DNS server (set up by default by the Internet Wizard).
> Set up firewall rules that prevent direct use of external DNS servers, for example. by blocking outgoing port 53 (UDP) for clients from the corresponding source network.
> Setting up firewall rules that prevent direct use of external DNS servers supporting DNS-over-TLS, e.g. by blocking outgoing port 853 (TCP) for clients from the corresponding source network.
> Disabling DNS-over-HTTPS (DoH) in the browser.

(i) Notes on synchronizing the firewall's DNS database:

Because the firewall learns its information from client DNS requests, in certain situations the DNS database may not yet be complete. This can happen in the following situations:

> A new firewall rule is added, but the client still has a DNS record cached.
> Shortly after the router reboots and the client still has a DNS record cached.

In these cases, clearing the DNS cache on the client, rebooting the client, or timing out the DNS record on the client will help.

(i) If different DNS names resolve to the same IP address, then they cannot be distinguished. In this case, the first rule that references one of these DNS names always applies. This should not be a problem with large service providers. However, it could occur with small websites hosted by the same provider.

10 Enhancements in the menu system

10.1 Additions to the Setup menu

10.1.1 ARP-Bridge-Optimization

Switch for optimizing bridge negotiations for IPv4 and ARP.

SNMP ID:

> 2.7.33

Console path:

> **Setup** > **TCP-IP**

Possible values:

> **No**
>> For a packet received on a bridge link, the ARP stores the bridge information only. The switch port is set to 0. This forces the bridge to perform a MAC address lookup to find the actual link (and switch port).
>
> **Yes**
>> The ARP stores the LAN information and switch port of the received ARP request/replies in the ARP table, regardless of whether the packet was received on a bridge link.

Default:

> Yes

10.1.2 LAN-Client-ID-Typ

This switch controls how the Client ID is constructed in DHCPv4 client DHCPDISCOVER and DHCPREQUEST messages on the LAN.

SNMP ID:

> 2.10.31

Console path:

> **Setup** > **DHCP**

Possible values:

MAC

The Client ID contains only the MAC address of the device. Before LCOS 10.70, the MAC address was always used as the Client ID automatically without any configuration option of its own. This value is retained when the firmware is updated.

DUID

Compliant with *RFC 4361*, the Client ID is formed as a DUID (DHCP Unique IDentifier) from the IAID and the MAC address of the device. This is the default for new installations as of LCOS 10.70.

Default:

DUID

10.1.3 WAN-Client-ID-Typ

This switch controls how the Client ID is constructed in DHCPv4 client DHCPDISCOVER and DHCPREQUEST messages on the WAN.

SNMP ID:

2.10.32

Console path:

Setup > **DHCP**

Possible values:

MAC

The Client ID contains only the MAC address of the device. Before LCOS 10.70, the MAC address was always used as the Client ID automatically without any configuration option of its own. This value is retained when the firmware is updated.

DUID

Compliant with *RFC 4361*, the Client ID is formed as a DUID (DHCP Unique IDentifier) from the IAID and the MAC address of the device. This is the default for new installations as of LCOS 10.70.

Default:

DUID

10.1.4 MAC algorithms

As of LCOS version 10.70, SSH supports Encrypt-then-MAC HMAC-SHA algorithms.

The Message Authentication Code (MAC) algorithms are used to check the integrity of messages. Select one or more from the available Encrypt-and-MAC or Encrypt-then-MAC algorithms.

ⓘ   For SSH algorithms, client preference always applies. The client sets the algorithm and usually picks the first match from its list of available algorithms. If necessary, adjust the list of your clients.

SNMP ID:

2.11.28.2

Console path:

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

Possible values:

hmac-md5-96
hmac-md5
hmac-sha1-96
hmac-sha1
hmac-sha2-256-96
hmac-sha2-256
hmac-sha2-512-96
hmac-sha2-512
hmac-md5-96-etm
hmac-md5-etm
hmac-sha1-96-etm
hmac-sha1-etm
hmac-sha2-256-96-etm
hmac-sha2-256-etm
hmac-sha2-512-96-etm
hmac-sha2-512-etm
hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm,hmac-sha2-512-etm

Default:

hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm,hmac-sha2-512-etm

10.1.5 Key-Exchange-Algorithms

As of LCOS version 10.70, SSH supports Encrypt-then-MAC HMAC-SHA algorithms.

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-group16-sha512**

Default:

> diffie-hellman-group-exchange-sha256
>
> ecdh-sha2
>
> curve25519-sha256
>
> curve448-sha512
>
> sntrup761x25519-sha512
>
> diffie-hellman-group14-sha256
>
> diffie-hellman-group16-sha512

10.1.6 Frequency-Band

Here, the DECT frequency band of a Gigaset N670 or N870 base station can be set during provisioning.

SNMP ID:

> 2.33.10.1.6

Console path:

> **Setup** > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

> **Unchanged**
> > The frequency band configured in the base station is not changed.
>
> **Europe**
> > Setting for Europe.
>
> **Latin-America**
> > Setting for Latin-America.
>
> **Brazil**
> > Setting for Brazil.

Default:

Unchanged

10.1.7 Admin-Password

Here you can set the administrator password of a Gigaset N670 or N870 base station during provisioning.

SNMP ID:

2.33.10.1.7

Console path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

Min. 8 and max. 40 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopqrstuvwxyz`
`` ` ``

Special values:

empty

If the entry is empty, no password is transmitted in the XML. Thus, the password set so far remains unchanged.

Default:

empty

10.1.8 NDP-Bridge-Optimization

Switch for optimizing bridge negotiations for IPv6 and the Neighbor Discovery Protocol (NDP).

SNMP ID:

2.70.16.3

Console path:

Setup > **IPv6** > **NDP**

Possible values:

No

For a packet received on a bridge link, the Neighbor Discovery stores the bridge information only. The switch port is set to 0. This forces the bridge to perform a MAC address lookup to find the actual link (and switch port).

Yes

The Neighbor Discovery stores the LAN information and switch port of the received neighbor solicitation/advertisement in the neighbor cache, regardless of whether the packet was received on a bridge link.

Default:

Yes