



Addendum LCOS 8.63 Public Beta 1

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Contents

- 1 Addendum to LCOS version 8.63 Public Beta.....3
 - 1.1 IPv6.....3
 - 1.1.1 IPv6 basics.....3
 - 1.1.2 IPv6 tunneling technologies.....4
 - 1.1.3 DHCPv6.....6
 - 1.1.4 IPv4 VPN tunnel via IPv6.....6
 - 1.2 Additional command-line commands.....8
 - 1.2.1 IPv6 addresses.....8
 - 1.2.2 IPv6 prefixes.....9
 - 1.2.3 IPv6 interfaces.....9
 - 1.2.4 IPv6 neighbor cache.....9
 - 1.2.5 IPv6 DHCP server.....10
 - 1.2.6 IPv6 DHCP client.....10
 - 1.2.7 IPv6 route.....10
 - 1.3 Enhancements to LANconfig.....11
 - 1.3.1 IPv6 configuration menu.....11
 - 1.3.2 Settings in the PPP list.....17
 - 1.3.3 IP routing tables.....18
 - 1.4 Additions to the menu system.....20
 - 1.4.1 Tunnel.....20
 - 1.4.2 Router advertisement.....30
 - 1.4.3 DHCPv6.....39
 - 1.4.4 Network.....51
 - 1.4.5 Firewall.....54
 - 1.4.6 LAN interfaces.....55
 - 1.4.7 WAN interfaces.....58
 - 1.4.8 Operating.....62
 - 1.4.9 Forwarding.....62
 - 1.4.10 Router.....62
 - 1.5 Tutorials.....64
 - 1.5.1 Setting up IPv6 Internet access.....64
 - 1.5.2 Setting up a 6to4 tunnel.....73

1 Addendum to LCOS version 8.63 Public Beta

The addendum describes the changes and additions to LCOS version 8.63 Public Beta over the previous version.

1.1 IPv6

1.1.1 IPv6 basics

IPv4 (Internet Protocol version 4) is a protocol for unique addressing of nodes in a network and, at the time of writing, it has defined all of the IP addresses assigned globally. The limited availability of address space required the development of IPv6 (Internet Protocol version 6), which is to replace the former standard. With a different IP-address structure, IPv6 provides for a greater range of IP addresses and thus increases the possible number of participants in networks worldwide.

Why use IPv6-standard IP addresses?

The new IPv6 standard was developed for the following reasons:

- IPv4 address space allows for approximately four billion IP addresses for unique identities in networks. When the IPv4 standard was implemented in the '80s this address space was considered to be sufficient. Due to the enormous growth of the World Wide Web and the unexpectedly large number of computers and network devices, an address shortage has arisen that the IPv6 standard is intended to bridge.
- The increase in address space with IPv6 hampers the scanning of IP addresses by viruses and Trojans. The broader spectrum provides greater protection against attacks.
- IPv6 has been implemented with a view to the security requirements. For this reason it uses the security protocol IPSec (IP Security). This provides secure network communications on layer 3, whereas many of IPv4 security mechanisms only operate on higher layers.
- Simplified, fixed descriptors for data packets save on router processing power and thus accelerate the available throughput.
- IPv6 allows for easier and faster transmission of data in real time, making it suitable for multimedia applications such as Internet telephony and Internet TV.
- So-called mobile IPs allow you to use a fixed IP address to login to different networks. This allows you to log on with your laptop using the same IP address, whether you are in your home network, in a café or at work.

IP address structure according to the IPv6 standard

The new IPv6 addresses are 128 bits long and the range of possible addresses can cater for about 340 sextillion network participants. IPv6 addresses consist of eight blocks of 16 bits and are written as hexadecimal numbers. The following is an example of a possible IPv6 address:

2001:0db8:0000:0000:0000:54f3:dd6b:0001/64

To improve the legibility of these IP addresses, zeros at the beginning of a block of numbers are omitted. It is also possible to omit one group of blocks that consist entirely of zeros. For the above example, one possible representation would be as follows:

2001:db8::54f3:dd6b:1/64

An IPv6 address consists of two parts; a prefix and an interface identifier. The prefix denotes the membership of the IP address to a network, while the interface identifier (e.g. in the case of auto-configuration) is generated from a link-layer address, and thus belongs to a particular network card. The device can also generate interface identifiers from random numbers. This improves security. In this way, multiple IPv6 addresses can be assigned to a single component.

The prefix describes the first part of the IP address. The length of the prefix is shown as a decimal number after a slash. For the example given here the prefix is:

2001:db8::/64

The remainder of the IP address is the interface identifier. In our example, this is:

::54f3:ddb6:1

Compared with the IP addresses for the IPv4 standard, a number of changes have resulted in the structure of the new IPv6 addresses:

- While IPv4 addresses cater for an address space of 32 bits, the new length of 128 bits results in a significantly larger address space with IPv6. IPv6 addresses are four times longer than IPv4 addresses.
- An interface can have multiple IPv6 addresses due to the potential assignment of multiple prefixes to a single interface identifier. With the IPv4 standard, an interface has only one IP address.
- IPv4 addresses must be assigned by a central server. This is usually a DHCP server. However, IPv6 can operate an auto-configuration, which makes the use of a DHCP server unnecessary. However, you the option of using a DHCP server is still open to you.

Stages of migration

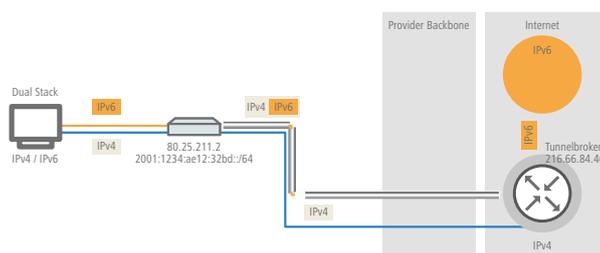
IPv6 is available to networks in a variety of ways. We make a distinction between environments with native IPv6 and those which provide IPv6 through a tunnel.

- **Pure (or native) IPv6:** Pure IPv6 describes a network that communicates to the outside only via IPv6. Users with IPv4 addresses can only access this network by communicating through a gateway that mediates between IPv6 and IPv4 networks.
- **IPv6 via dual stack:** Dual stack refers to the parallel operation of IPv4 and IPv6 in a network. A router mediates between devices that "speak" only IPv4 or IPv6. The clients select the protocol they need.
- **IPv6 tunneling:** If a router does not have IPv6 Internet access, it can still access IPv6 networks by means of a tunnel.

1.1.2 IPv6 tunneling technologies

6in4 tunneling

6in4 tunnels are used to connect two hosts, routers, or to interconnect a host and router. This means that 6in4 tunnels can connect two IPv6 networks via an IPv4 network. The diagram shows a static 6in4 tunnel between the local router and a 6in4 gateway belonging to a tunnel broker.



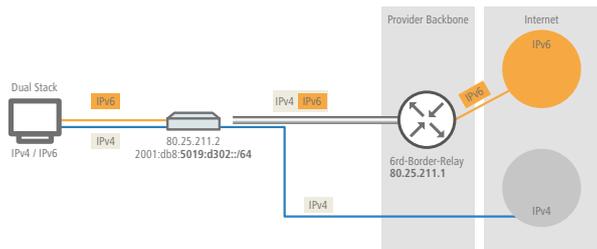
Unlike 6to4, these are dedicated services operated by a known provider. The end-points are fixed and the tunnel broker assigns a static prefix. The advantages of a 6in4 solution are that the gateways are fixed and the operator is known. The fixed prefix from the tunnel broker also determines the number of possible subnets that can be used. A 64-bit prefix (e.g. 2001:db8::/64) allows one subnet to be used. If a 48-bit prefix is used, 16 bits of the 64-bit prefix are available for use. This allows the implementation of up to 65,536 subnets.

The disadvantage of the 6in4 technology is the higher administrative effort. You must be registered with and login to the tunnel broker. In addition, the tunnel endpoints must be statically configured. Where a dynamic IPv4 address is used, the relevant data must be updated regularly. This can be automated by running a script on a router.

6in4 is a relatively secure and stable technology for providing IPv6 Internet access. This technology is thus suitable for operating web servers that are to be accessed over IPv6. The only drawback is the increased effort in administration. This technology is also suitable for professional use.

6rd tunneling

6rd (rapid deployment) is a development of 6to4. The underlying function is identical. The difference is that just one particular relay is used, as operated by a provider. This solves the two basic problems of the 6to4 technology—the lack of security and stability. The prefix with 6rd is either configured manually or sent via DHCP (IPv4), which further reduces the effort involved with configuration. The diagram is a schematic representation of a 6rd scenario.

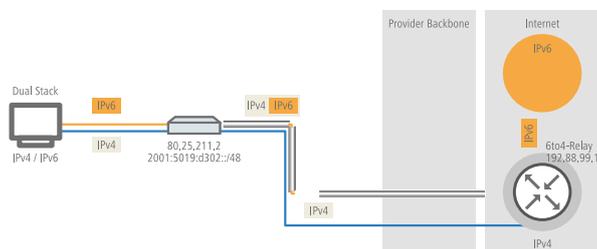


The provider assigns the router with a prefix (2001:db8::/32), which the router then supplements with its own IPv4 address. The IPv6 address generated in this way has the form: 2001:db8:5019:d302::/64. This makes 6rd interesting from two perspectives. The provider has a simple way to give its customers access to the IPv6 Internet. In addition, customers benefit from greatly simplified usage. They do not have to accept the security risks of 6to4, nor do they have to handle the complicated configuration of 6in4.

6to4 tunneling

6to4 tunneling offers you an easy way to set up a connection between two IPv6 networks via an IPv4 network. To this end, what is known as a 6to4 tunnel is set up:

- A router between the local IPv6 network and an IPv4 network serves to mediate between the networks.
- The router has both a public IPv4 address and an IPv6 address. The IPv6 address consists of an IPv6 prefix and the IPv4 address in hexadecimal notation. If a router such as this has the IPv4 address 80.25.211.2, this will first be converted into hexadecimal notation: 5019:d302. Supplementing this is an IPv6 prefix (e.g. 2002::/16), so that the IPv6 address for the router appears as follows: 2002:5019:d302::/48.
- If a device in the IPv6 network sends data packets via the router to a destination address in the IPv4 network, then the router first of all repacks the IPv6 packets and encapsulates them into a package with an IPv4 header. The router then forwards the encapsulated package to a 6to4 relay. The 6to4 relay unpacks the packet and forwards it to the desired destination. The following illustration shows the operating principle of 6to4 tunneling:



6to4 tunnels establish a dynamic connection between IPv6 and IPv4 networks: the response packets may be routed back via a different 6to4 relay. 6to4 tunnels are not a point-to-point connection. For every new connection, the router always looks for the "nearest" public 6to4 relay. This is done using the anycast address 192.88.99.1. This aspect is an advantage of 6to4 tunneling on the one hand, but it also presents a disadvantage on the other. Public 6to4 relays do not require registration and are freely accessible. What's more, the dynamic connection is easily configured. In this way it is possible for any user to create a 6to4 tunnel over a public relay, quickly and easily.

On the other hand, the dynamic connection means that the user has no influence on the choice of the 6to4 relay. The provider of the relay is able to intercept or manipulate data.

1.1.3 DHCPv6

Compared to IPv4, clients in an IPv6 network do not require automatic address assignment from a DHCP server because they use auto-configuration. However, because certain information such as DNS server addresses are not transmitted during auto-configuration, certain application scenarios can benefit from a DHCP service on the IPv6 network.

DHCPv6 server

The use of a DHCPv6 server is optional for IPv6. In principle, a DHCPv6 server supports two modes:

- **Stateless:** The DHCPv6 server does not distribute addresses but only information, such as DNS server addresses. Using this method, clients generate their own IPv6 addresses by 'stateless address auto-configuration (SLAAC)'. This method is particularly attractive for example for small networks in order to keep administration efforts to a minimum.
- **Stateful:** The DHCPv6 server distributes IPv6 addresses, similar to IPv4. This method is more complicated, since a DHCPv6 server has to assign and manage the addresses.

A DHCPv6 server distributes only the options that are explicitly requested by an IPv6 client, i. e. the server only assigns an address to a client if it explicitly requests one.

Additionally, the DHCPv6 server can pass on prefixes to routers for further distribution. This method is referred to as 'prefix delegation'. A DHCPv6 client must have explicitly requested this prefix, however.

DHCPv6 client

The auto-configuration available with IPv6 networks makes it very easy and convenient to configure the clients.

However, in order for a client to receive additional information, such as a DNS server address, you must configure the device so that it can activate the DHCPv6 client when necessary.

The settings for the DHCPv6 client ensure that a device receiving certain flags in the router advertisement will start the DHCPv6 client, which can then send requests to the DHCPv6 server:

- **M flag:** If an appropriately configured device receives a router advertisement with the 'M flag' set, the DHCPv6 client will request an IPv6 address from the DHCPv6 server along with other information such as DNS server, SIP server and NTP server.
- **O flag:** With an 'O flag', the DHCPv6 client requests the DHCPv6 server for information such as a DNS server, SIP server and NTP server only, but not an IPv6 address.

 If the 'M-flag' is set, the 'O-flag' does not necessarily have to be set as well.

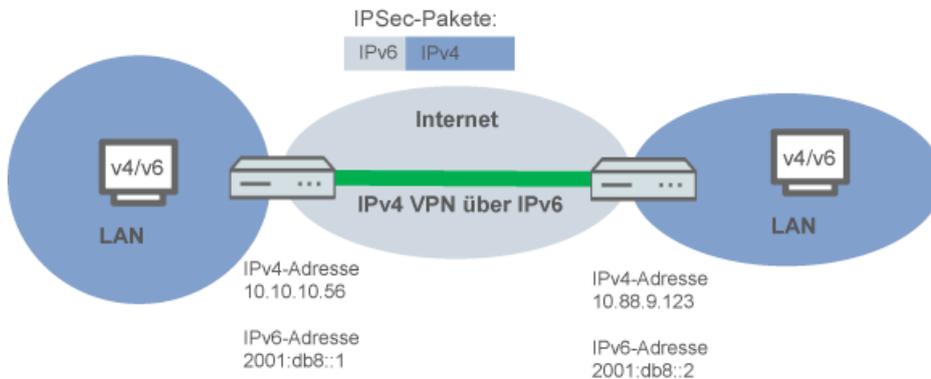
 With IPv6, the default route is distributed via router advertisements and not via DHCPv6.

1.1.4 IPv4 VPN tunnel via IPv6

Until now it was not possible to connect remote sites via VPN, if the gateways were using private IP addresses for Internet access (e.g. in cellular networks).

IPv6 overcomes these restrictions, since each IPv6 device has its own public IP address. Therefore an IPv4 tunnel can be established over IPv6. The IPv4 tunnel connects IPv4 remote networks, independent from the WAN IPv4 addresses used by the corresponding remote sites.

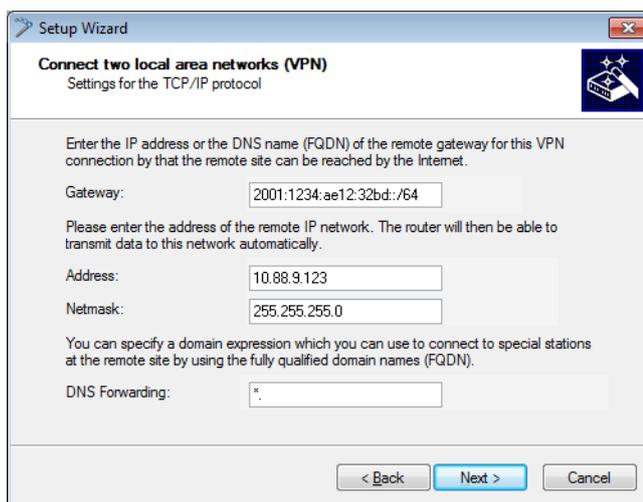
The following example shows how to connect two local IPv4 networks via IPv4 tunnel, which is build on a IPv6 Internet connection. The IPv4 packets are send with IPv6 header to the remote gateway using the IPv6 Internet connection (native or via tunnel broker).



Setup Wizard – Setting up an IPv4 VPN connection via IPv6

The Setup Wizard option "Connect two local area networks" helps you to set up a VPN connection.

1. Start LANconfig, for example from the Windows start menu with **Start > Programs > LANCOM > LANconfig**. LANconfig now automatically searches the local network for devices. As soon as LANconfig has completed its search, it presents a list of all the devices it found, if possible with a brief description, the IP address and the status.
2. Choose your device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu under **Tools > Setup Wizard**. LANconfig first reads out the device configuration and then displays the selection window with the optional applications.
3. Launch the action **Connect two local area networks**.
4. Follow the Wizard's instructions and enter the necessary data.
5. As the gateway address, enter the IPv6 address of the gateway.



6. You can then close the Wizard with **Finish**. The Setup Wizard writes the configuration to the device.

1.2 Additional command-line commands

Various IPv6 functions can be queried at the command line. The following command-line functions are available:

- *IPv6 addresses*: `show ipv6-addresses`
- *IPv6 prefixes*: `show ipv6-prefixes`
- *IPv6 interfaces*: `show ipv6-interfaces`
- *IPv6 neighbor cache*: `show ipv6-neighbor-cache`
- *IPv6 DHCP*: `show dhcpv6-server`
- *IPv6 DHCP*: `show dhcpv6-client`
- *IPv6 route*: `show ipv6-route`

1.2.1 IPv6 addresses

The command `show ipv6-addresses` shows a list of IPv6 addresses that are currently being used. This is sorted by interface. Note that an interface can have multiple IPv6 addresses. One of these addresses is always the link-local address, which starts with `fe80` .

The output is formatted as follows:

<Interface> :

<IPv6 address>, <status>, <attribute>, (<type>)

Table 1: Components of the command-line output `show ipv6-addresses`:

Output	Comment
Interface	The name of the interface
IPv6 address	The IPv6 address
Status	<p>The status field can contain the following values:</p> <ul style="list-style-type: none"> ■ TENTATIVE Duplicate Address Detection (DAD) is currently checking the address. It is not yet available for unicast. ■ PREFERRED The address is valid ■ DEPRECATED The address is still valid, but it is being discontinued. The optimal status for communication is PREFERRED. ■ INVALID The address is invalid and cannot be used for communication. An address given this status after its lifetime has expired.
Attribute	<p>Shows an attribute of the IPv6 address. Possible attributes are:</p> <ul style="list-style-type: none"> ■ None No special attributes ■ (ANYCAST) This is an anycast address ■ (AUTO CONFIG)

Output	Comment
	The address was retrieved by auto-configuration <ul style="list-style-type: none"> ■ (NO DAD PERFORMED) No DAD is performed
Type	The type of IP address

1.2.2 IPv6 prefixes

The command `show ipv6-prefixes` displays all known prefixes. These are sorted according to the following criteria:

- **Delegated prefixes:** All prefixes that the router has obtained by delegation.
- **Advertised prefixes:** All prefixes that the router announces in its router advertisements.
- **Deprecated prefixes:** All prefixes that are being discontinued. These may still be functional, but they will be deleted after a certain time.

1.2.3 IPv6 interfaces

The command `show ipv6-interfaces` displays a list of IPv6 interfaces and their status.

The output is formatted as follows:

<Interface> : <Status>, <Forwarding>, <Firewall>

Table 2: Components of the command-line output `show ipv6-interfaces`:

Output	Comment
Interface	The name of the interface
Status	The status of the interface Possible entries are: <ul style="list-style-type: none"> ■ oper status is up ■ oper status is down
Forwarding	The forwarding status of the interface. Possible entries are: <ul style="list-style-type: none"> ■ forwarding is enabled ■ forwarding is disabled
Firewall	The status of the firewall. Possible entries are: <ul style="list-style-type: none"> ■ forwarding is enabled ■ firewall is disabled

1.2.4 IPv6 neighbor cache

The command `show ipv6-neighbor-cache` displays the current neighbor cache.

The output is formatted as follows:

<IPv6 address> iface <interface> lladdr <MAC address> (<switch port>) <device type> <status> src <source>

Table 3: Components of the command-line output `show ipv6-neighbor-cache`:

Output	Comment
IPv6 address	The IPv6 address of the neighboring device
Interface	The interface where the neighbor is accessed
MAC address	The MAC address of the neighbor
Switch port	The switch port on which the neighbor was found
Device type	Neighbor's device type (host or router)
Status	<p>The status of the connection to neighboring devices. Possible entries are:</p> <ul style="list-style-type: none"> ■ INCOMPLETE Resolution of the address was still in progress and the link-layer address of the neighbor was not yet determined. ■ REACHABLE The neighbor was reached in the last ten seconds. ■ STALE The neighbor is no longer qualified as REACHABLE, but an update will only be performed when an attempt is made to reach it. ■ DELAY The neighbor is no longer qualified as REACHABLE, but data was recently sent to it; waiting for verification by other protocols. ■ PROBE The neighbor is no longer qualified as REACHABLE. Neighbor solicitation probes are sent to it to confirm availability.
Source	The IPv6 address at which the neighbor was detected.

1.2.5 IPv6 DHCP server

The command `show dhcpv6-server` displays the current status of the DHCP server. The display includes information about the interface on which the server is active, which DNS server and prefixes it has, and what client preferences it has.

1.2.6 IPv6 DHCP client

The command `show dhcpv6-client` displays the current status of the DHCP client. The display includes information about the interface being used by the client and the prefixes and DNS server that it is using.

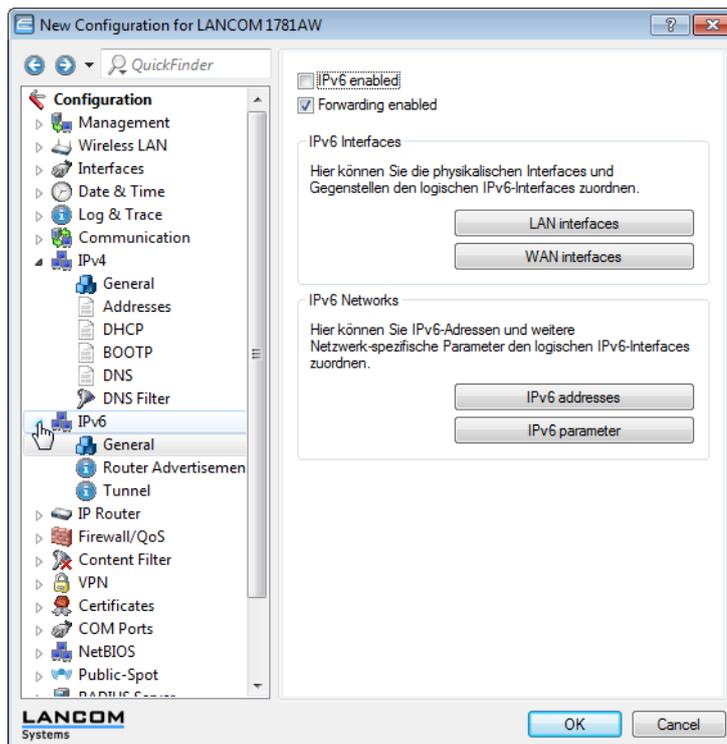
1.2.7 IPv6 route

The command `show ipv6-route` displays the complete IPv6 routing table. Routers with fixed entered routes are displayed with the suffix [static] and the dynamically obtained routes have the suffix [connected]. The loopback address is marked [loopback]. Other automatically generated addresses have the suffix [local].

1.3 Enhancements to LANconfig

1.3.1 IPv6 configuration menu

Where previous versions provided configuration menus for TCP/IP for IPv4, you now find the options **IPv4** and **IPv6**.



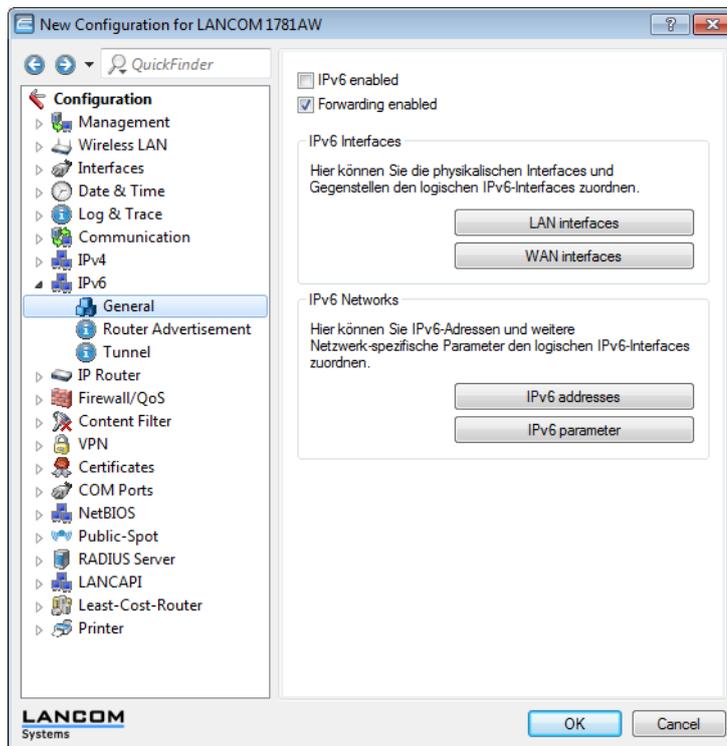
Click on **IPv6** to adjust the settings for this protocol. The configuration dialog **IPv6** is divided into the options **General**, **Router advertisement** and **Tunnel**. By default a click on **IPv6** takes you straight to the *General* options.

General

This is where you make the basic settings.

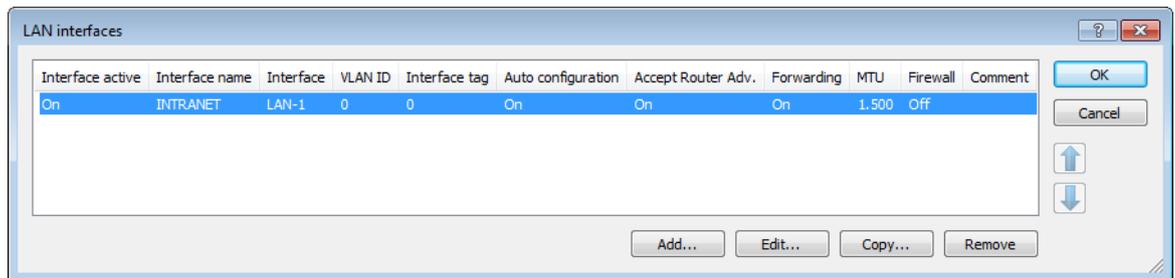
- **IPv6 enabled:** This is where you can enable or disable IPv6 for the device.

- **Forwarding enabled:** Forwarding is used for packet forwarding between IPv6 interfaces. This option is activated by default.



- The buttons **LAN interfaces** and **WAN interfaces** access the tables where you can add new interfaces, configure existing interfaces, or delete them.

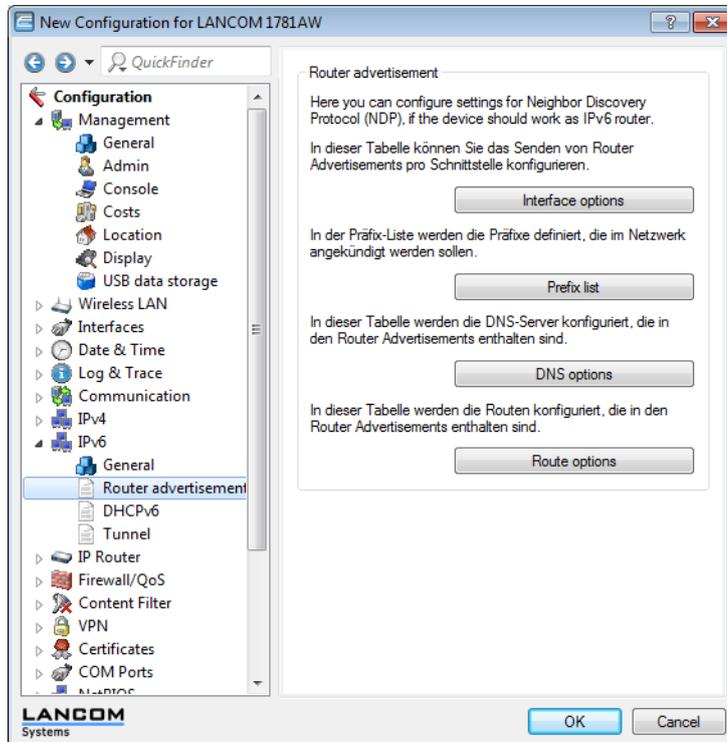
This shows the table with a LAN interface:



- The buttons **IPv6 addresses** and **IPv6 parameters** are used to assign IPv6 addresses to interfaces and to configure the interface parameters (gateway address, primary and secondary DNS).

Router advertisement

The **Router advertisement** configuration provides you with four buttons for setting up the Neighbor Discovery Protocol (NDP) if the device is to operate as an IPv6 router:



Each button opens a table with the settings for the corresponding function:

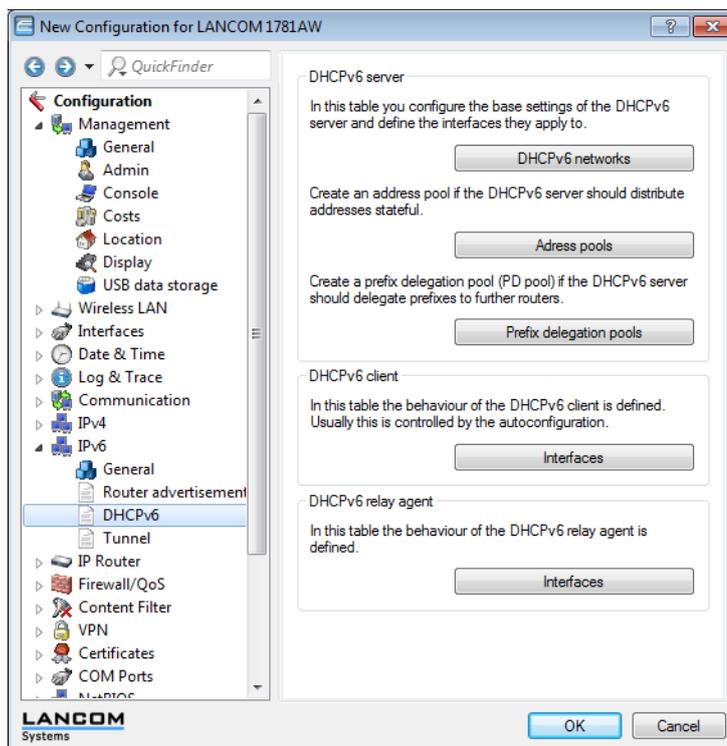
- **Interface options:** Enable or disable the following interface features:
 - **Send router advertisements:** Regulates the periodic transmission of router advertisements and the response to router solicitations.
 - **Managed address configuration flag:** With this function enabled, clients receiving this router advertisement will configure their addresses with Stateful Autoconfiguration (DHCPv6). Clients then automatically retrieve other information, such as the DNS server.
 - **Other configuration flag:** When this function is enabled, clients that receive this router advertisement use autoconfiguration to form their addresses and they use DHCPv6 to retrieve other information such as the DNS server address.
 - **Default router:** Defines how the device advertises itself as the default gateway or router.
 - **Router priority:** Defines the preference of this router. Clients enter this preference into their local routing tables.
- **Prefix list:** Set the prefix options for the interfaces that are being used. The following settings are possible:
 - **Prefix:** Enter a prefix that is announced in the router advertisements, e. g. "2001:db8::/64". The prefix length must always be exactly "/64", otherwise it will be impossible for clients to generate their addresses by adding their interface identifiers (with a length of 64 bits). If a prefix delegated by the provider is to be propagated automatically, set "::/64" here and enter the name of the corresponding WAN interface as the parameter **Prefix delegation from**.
 - **Subnet ID:** Here you enter the subnet ID that is to be combined with the prefix delegated by the provider. If the provider assigns the prefix "2001:db8:a::/48", for example, and the subnet ID is "0001" (or "1" for short), then the router advertisement on this interface is given the prefix "2001:db8:a:0001::/64". The maximum subnet length with a 48-bit long delegated prefix is 16 bits (i.e. 65,536 subnets), with available subnet IDs ranging from "0000" to "FFFF". With a delegated prefix of "/56", the maximum subnet length is 8 bits (i.e. 256 subnets) with

subnet IDs ranging from "00" to "FF". In general, the subnet ID "0" is used when the WAN IPv6 address is formed automatically. This is why subnet IDs for LANs start at "1". The default setting is '1'.

- **Stateless address configuration:** Specifies whether the prefix is to be used for a stateless address autoconfiguration (SLAAC). The default setting is 'Yes'.
 - **Prefix delegation from:** Defines the name of the interface used to receive a prefix via DHCPv6 prefix delegation or via a tunnel. This prefix can be used to derive and propagate a subnet for each interface.
- **DNS options :** Sets the DNS server for the interfaces.
 - **Route options:** Sets the route preferences ("high", "medium" or "low").

DHCPv6

This is where you configure the DHCPv6 server, the DHCPv6 client and the DHCPv6 relay agent.



DHCPv6 server

Use the following buttons to access the tables and adjust the respective functions:

- **DHCPv6 networks:** This table is used to configure the basic settings of the DHCPv6 server, and to define which interfaces they apply to
 - **Interface-name-or-relay:** Name of the interface on which the DHCPv6 server is working, for example "INTRANET"
 - **Entry active:** Activates or deactivates the entry.
 - **Primary DNS:** IPv6 address of the primary DNS server. The default value is "::".
 - **Secondary DNS:** IPv6 address of the secondary DNS server.
 - **Address pool:** Name of the address pool used for this interface.
-
- ! If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the **Address pools** table.
- **Prefix delegation pool:** Name of prefix pools to be used by the DHCPv6 server.

 If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table **Prefix delegation pools**.

- **Rapid commit:** With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.

 The client must explicitly include the rapid commit option in its solicit message.

- **Address pools:** If distribution of the DHCPv6 server is to be stateful, this table defines an address pool:
 - **Address pool name:** Name of the address pool
 - **First address:** First address in the pool, e. g. "2001:db8::1"
 - **Last address:** Last address in the pool, e. g. "2001:db8::9"
- **Prefix delegation pools:** In this table, you specify the prefixes that the DHCPv6 server delegates to other routers:
 - **PD pool name:** Name of the PD pool
 - **First prefix:** First prefix for delegation in the PD pool, e. g. "2001:db8:1100::"
 - **Last prefix:** Last prefix for delegation in the PD pool, e. g. "2001:db8:FF00::"
 - **Prefix length:** Length of the prefixes in the PD pool, e. g. "56" or "60"

DHCPv6 client

Use the following buttons to access the tables and adjust the respective functions:

- **Interfaces:** This table determines the behavior of the DHCPv6 client.

 Normally client behavior is controlled by the auto-configuration.

- **Interface name:** Name of the interface on which the DHCPv6 client is working. These can be LAN interfaces or WAN interfaces (remote sites), e. g. "INTRANET" or "INTERNET".
- **Operating:** Determines if and how the device enables the client. Possible values are:
 - ▶ **Autoconf:** The device waits for router advertisements, and then starts the DHCPv6 client. This option is the default setting.
 - ▶ **Yes:** The device starts the DHCPv6 client as soon as the interface is active, without waiting for router advertisements.
 - ▶ **No:** The DHCPv6 client is disabled on this interface. Even if the device receives router advertisements, it will not start the client.
- **Request DNS server:** Specifies whether the client queries the DHCPv6 server for DNS servers.

 You must enable this option in order for the device to obtain information about a DNS server.

- **Request address:** Determines whether the client should request the DHCPv6 server for an IPv6 address.

 Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i. e. not distributed by 'SLAAC'.

- **Request prefix:** Determines whether the client should request the DHCPv6 server for an IPv6 prefix. Activating this option is only required when the device itself functions as a router and redistributes the prefixes. This option is enabled by default on WAN interfaces in order for the DHCPv6 client to request a prefix from the provider for use in its local network. This option is disabled by default on LAN interfaces because devices in a local network are more likely to function as clients rather than as routers.
- **Rapid commit:** When rapid commit is activated, the client attempts to obtain an IPv6 address from the DHCPv6 server with just two messages. If the DHCPv6 server is configured correspondingly, it immediately responds to this solicit message with a reply message.

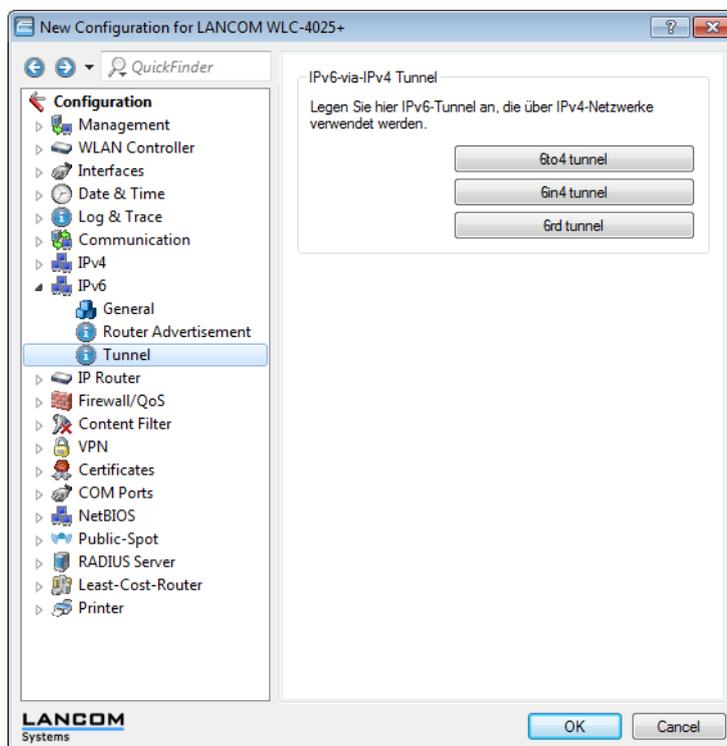
DHCPv6 relay agent

Use the following buttons to access the tables and adjust the respective functions:

- **Interfaces:** A DHCPv6 relay agent forwards DHCP messages between DHCPv6 clients and DHCPv6 servers, which are located in different networks. This table determines the behavior of the DHCPv6 relay agent.
 - **Interface name:** The name of the interface on which the relay agent receives requests from DHCPv6 clients, e. g. "INTRANET".
 - **Relay agent enabled:** Determines if and how the device enables the relay agent. Possible values are:
 - ▶ **Yes:** Relay agent is enabled. This option is the default setting.
 - ▶ **No:** Relay agent is not enabled.
 - **Interface address:** The relay agent's own IPv6 address at the interface that is configured under Interface Name. This IPv6 address is used as a sender address in DHCP messages that are forwarded. This sender address enables DHCPv6 clients to uniquely identify a relay agent. An explicit specification of the interface address is necessary because an IPv6 host can have multiple IPv6 addresses for each interface.
 - **Destination address:** The IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.
 - **Destination interface:** The destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

Tunnel

The **Tunnel** configuration offers you 3 buttons to create IPv6 tunnels that can be used over IPv4 networks. Use these options to gain access to the IPv6 Internet using an IPv4 connection.



- **6to4 tunnel:** This button opens the 6to4 tunnel settings.

 Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the selected relay can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

- **6in4 tunnel:** This button opens the 6in4 tunnel settings.

 6in4 tunnels require more administrative effort, but they represent a secure and stable technology for IPv6 Internet access. This option is also suitable for professional use.

- **6rd tunnel:** This button opens the 6rd tunnel settings.

 6rd tunneling is suitable for end users and for professional applications because configuration is less complex than with 6in4 tunneling and the technology avoids the security risks of 6to4 tunneling.

1.3.2 Settings in the PPP list

In the PPP list, you are able to specify your own definition of PPP negotiation for every remote site contacting your network.

You can also specify whether communications should use an IPv4 or an IPv6 connection.

The authentication of point-to-point connections in the WAN commonly relies on one of the protocols PAP, CHAP, MSCHAP or MSCHAPv2. The protocols here have a "hierarchy" amongst themselves, i.e. MSCHAPv2 is a "higher-level" protocol than MSCHAP, CHAP and PAP (higher protocols provide higher security). Many dial-in routers at Internet providers allow up-front authentication using a higher-level protocol such as CHAP, but only support the use of PAP further down the line. If the setting for the protocol for authentication is fixed in the LANCOM, the connection may fail because no common authentication protocol can be negotiated.

 In principle authentication can be repeated while the connection is being negotiated. Another protocol can be selected if, for example, it can only be recognized from the username at the earliest. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, the device must explicitly refuse the provider's request for CHAP to be able to provide PAP user data for requests to be forwarded by the provider.

A flexible setting for the authentication protocols in the device ensures that the PPP connection is established as required. In addition, one or more protocols can be defined that are accepted for authentication of remote sites in the device (inbound connections) and on login of the device into other remote sites (outbound connections).

- When establishing inbound connections, the device requires the lowest of the permitted protocols, but where possible it also permits the remote site to use one of the higher-level protocols (enabled in the device).
- When establishing outbound connections, the device offers all enabled protocols, but only permits a selection from precisely these protocols. It is not possible to negotiate one of the disabled, possibly higher-level, protocols.

The PPP authentication protocols are set in the PPP list.

LANconfig: **Communication > Protocols > PPP list**

The screenshot shows the 'PPP list - New Entry' dialog box. It includes the following elements:

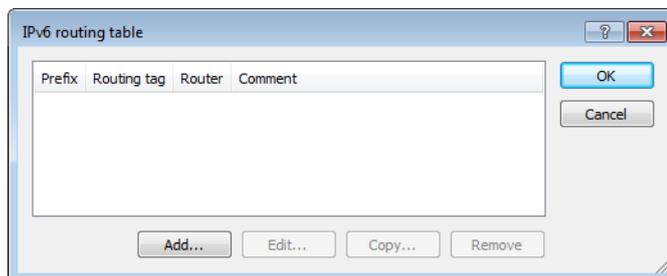
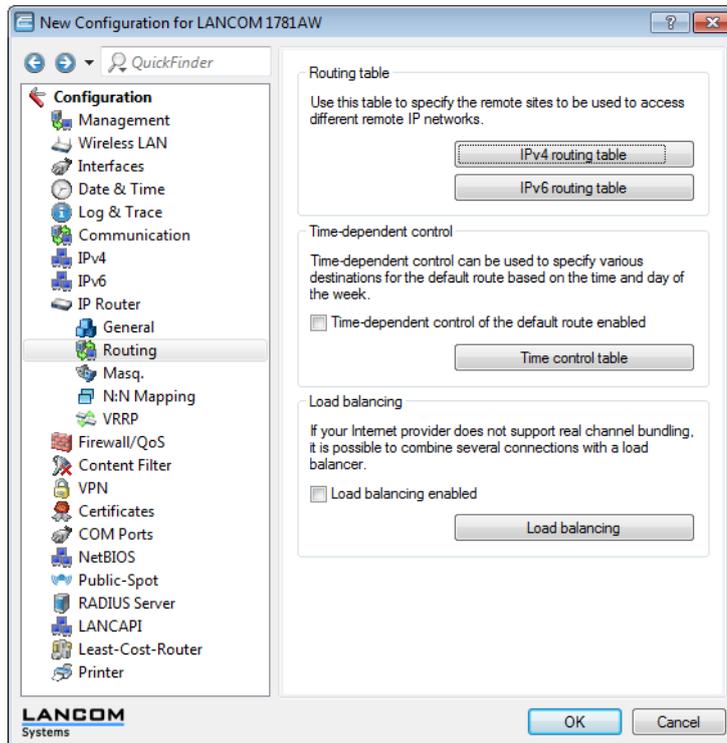
- Remote site:** A dropdown menu.
- User name:** A text input field.
- Password:** A text input field with a 'Show' checkbox and a 'Generate password' dropdown.
- Routing options:**
 - Activate IPv4 routing
 - Activate NetBIOS over IP
 - Activate IPv6 routing
- Authentication of the remote site (request):**
 - MS-CHAPv2
 - MS-CHAP
 - CHAP
 - PAP
- Authentication by the remote site (response):**
 - MS-CHAPv2
 - MS-CHAP
 - CHAP
 - PAP
- Time:** Input field with value 0.
- Retries:** Input field with value 5.
- Conf:** Input field with value 10.
- Fail:** Input field with value 5.
- Term:** Input field with value 2.

1.3.3 IP routing tables

Unlike previous versions where the configuration menu contained just a single IP routing table, this item now offers the configuration of separate routing tables for IPv4 and IPv6 connections.

You will find the new table under **IP router > Routing > IPv6 routing table**

The IPv4 settings that were previously in the table **IP routing table** are now located in the **IPv4 routing table** .



The table contains the entries to be used for routing packets with IPv6 addresses.

Prefix

Specify the prefix of the network area for which the data is to be routed to the given remote station.

Routing tag

Specify the routing tag for this route. This route is active only for packets with the same tag. The data packets receive the routing tag either from the firewall or depending on the LAN or WAN interface used.

Router

This is where you specify the remote site for this route.

Comment

Enter a descriptive comment for this entry.

 Entering a comment is optional.

1.4 Additions to the menu system

1.4.1 Tunnel

Use this setting to manage the tunneling protocols to provide access to the IPv6 Internet via an IPv4 Internet connection.

SNMP ID:

2.70.1

Telnet path:

Setup > IPv6 > Tunnel

6in4

The table contains the settings for the 6in4 tunnel.

SNMP ID:

2.70.1.1

Telnet path:

Setup > IPv6 > Tunnel > 6in4

Peer name

Contains the name of the 6in4 tunnel.

SNMP ID:

2.70.1.1.1

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Peer-Name

Possible values:

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.1.1.2

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Rtg-Tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

Gateway address

Contains the IPv4 address of the remote 6in4 gateway.

 The 6in4 tunnel is only set up if the gateway can be reached by ping at this address.

SNMP ID:

2.70.1.1.3

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Gateway-Address

Possible values:

IP address in IPv4 notation, max. 64 characters

Default:

Blank

IPv4 routing tag

Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4 anycast address
- 6in4 gateway address
- 6rd border relay address

SNMP ID:

2.70.1.1.4

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > IPv4-Rtg-tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

Gateway IPv6 address

Contains the IPv6 address of the remote tunnel endpoint on the intermediate network, for example, "2001:db8::1".

SNMP ID:

2.70.1.1.5

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Gateway-IPv6-Address

Possible values:

IPv6 address with max. 43 characters

Default:

Blank

Local-IPv6-Address

Contains the local IPv6 address of the device on the intermediate network, for example "2001:db8::2/64".

SNMP ID:

2.70.1.1.6

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Local-IPv6-Address

Possible values:

Max. 43 characters

Default:

Blank

Routed IPv6 prefix

Contains the prefix that is routed from the remote gateway to the local device and that is to be used in LAN, e.g. "2001:db8:1:1::/64" or "2001:db8:1::/48".

SNMP ID:

2.70.1.1.7

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Routed-IPv6-Prefix

Possible values:

Max. 43 characters

Default:

Blank

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.

.

 Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

SNMP ID:

2.70.1.1.8

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Firewall

Possible values:

Yes

No

Default:

Yes

6rd border relay

.

SNMP ID:

2.70.1.2

Telnet path:**Setup > IPv6 > Tunnel > 6rd-Border-Relay****Peer name**

Contains the name of the 6rd border relay tunnel.

SNMP ID:

2.70.1.2.1

Telnet path:**Setup > IPv6 > Tunnel > 6rd-Border-Relay > Peer-Name****Possible values:**

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.1.2.2

Telnet path:**Setup > IPv6 > Tunnel > 6rd-Border-Relay > Rtg-Tag****Possible values:**

Max. 5 characters in the range 0 – 65534

Default:

0

IPv4 loopback address

Set the IPv4 loopback address

SNMP ID:

2.70.1.2.3

Telnet path:**Setup > IPv6 > Tunnel > 6rd-Border-Relay > IPv4-Loopback-Address****Possible values:**

Max. 16 characters

Default:

Blank

6rd prefix

Contains the prefix used by the provider for 6rd services, e.g. 2001:db8::/32.

SNMP ID:

2.70.1.2.4

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > 6rd-Prefix

Possible values:

Max. 24 characters as a prefix of an IPv6 address with up to four blocks of four hexadecimal digits each

Default:

Blank

IPv4 mask length

Defines the number of significant bits of IPv4 addresses that are identical within a 6rd domain. With mask length "0" there are no identical bits. In this case, the entire IPv4 address is used to generate the delegated 6rd prefix.

The provider sets the mask length.

Example: The IPv4 address of the device is "192.168.1.99" (in hexadecimal: "c0a8:163"). In this case, the following are examples of possible combinations:

6rd domain	Mask length	6rd prefix
2001:db8::/32	0	2001:db8:c0a8:163::/64
2001:db8:2::/48	16	2001:db8:2:163::/64
2001:db8:2:3300::/56	24	2001:db8:2:3363::/64

SNMP ID:

2.70)

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > IPv4-Mask-Length

Possible values:

Max. 2 numbers in the range 0 – 32

Default:

0: The device uses the full IPv4 address.

DHCPv4 propagate

If you enable this function, the 6rd border relay distributes the prefix via DHCPv4 if the DHCPv4 client requests it.

SNMP ID:

2.70.1.2.6

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > DHCPv4-Propagate

Possible values:

Yes

No

Default:

No

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.



Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

SNMP ID:

2.70.1.2.7

Telnet path:**Setup > IPv6 > Tunnel > 6rd-Border-Relay > Firewall****Possible values:**

Yes

No

Default:

Yes

6rd

The table contains the settings for the 6rd tunnel.

SNMP ID:

2.70.1.3

Telnet path:**Setup > IPv6 > Tunnel > 6rd****Peer name**

Contains the name of the 6rd tunnel.

SNMP ID:

2.70.1.3.1

Telnet path:**Setup > IPv6 > Tunnel > 6rd > Peer-Name****Possible values:**

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.1.3.2

Telnet path:

Setup > IPv6 > Tunnel > 6rd > Rtg-Tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

Border relay address

Contains the IPv4 address of the 6rd border relay.

SNMP ID:

2.70.1.3.3

Telnet path:

Setup > IPv6 > Tunnel > 6rd4 > Border-Relay-Address

Possible values:

IPv4 address with max. 64 characters

Default:

Blank

IPv4 routing tag

Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4 anycast address
- 6in4 gateway address
- 6rd border relay address

SNMP ID:

2.70.1.3.4

Telnet path:

Setup > IPv6 > Tunnel > 6rd > IPv4-Rtg-tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

6rd prefix

Contains the prefix used by the provider for 6rd services, e.g. "2001:db8::/32".

 If the 6rd prefix is assigned through DHCPv4, you have to enter "::/32" here.

SNMP ID:

2.70.1.3.5

Telnet path:

Setup > IPv6 > Tunnel > 6rd > 6rd-Prefix

Possible values:

Max. 24 characters

Default:

Blank

IPv4 mask length

Defines the number of significant bits of IPv4 addresses that are identical within a 6rd domain. With mask length "0" there are no identical bits. In this case, the entire IPv4 address is used to generate the delegated 6rd prefix.

The provider sets the mask length.

Example: The IPv4 address of the device is "192.168.1.99" (in hexadecimal: "c0a8:163"). In this case, the following are examples of possible combinations:

6rd domain	Mask length	6rd prefix
2001:db8::/32	0	2001:db8:c0a8:163::/64
2001:db8:2::/48	16	2001:db8:2:163::/64
2001:db8:2:3300::/56	24	2001:db8:2:3363::/64

SNMP ID:

2.70.1.3.6

Telnet path:

Setup > IPv6 > Tunnel > 6rd > IPv4-Mask-Length

Possible values:

Max. 2 numbers in the range 0 – 32

Default:

0

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.

 Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

SNMP ID:

2.70.1.3.7

Telnet path:

Setup > IPv6 > Tunnel > 6rd4 > Firewall

Possible values:

Yes

No

Default:

Yes

6to4

The table contains the settings for the 6to4 tunnel.

 Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the selected relay can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

SNMP ID:

2.70.1.4

Telnet path:

Setup > IPv6 > Tunnel > 6to4

Peer name

Contains the name of the 6to4 tunnel.

SNMP ID:

2.70.1.4.1

Telnet path:

Setup > IPv6 > Tunnel > 6to4 > Peer-Name

Possible values:

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.1.4.2

Telnet path:

Setup > IPv6 > Tunnel > 6to4 > Rtg-Tag

Possible values:

Max. 5 characters in the range 0 – 65535

Default:

0

Gateway address

Contains the IPv4 address of the 6to4 relay or 6to4 gateway. Default value is the anycast address "192.88.99.1". In general, you can leave this address unchanged as it will always give you access to the closest 6to4 relay on the Internet.

 The 6to4 tunnel is only set up if the gateway can be reached by ping at this address.

SNMP ID:

2.70.1.4.3

Telnet path:

Setup > IPv6 > Tunnel > 6to4 > Gateway-Address

Possible values:

IPv4 address with max. 64 characters

Default:

192.88.99.1

IPv4 routing tag

Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4 anycast address
- 6in4 gateway address
- 6rd border relay address

SNMP ID:

2.70.1.4.4

Telnet path:

Setup > IPv6 > Tunnel > 6to4 > IPv4-Rtg-tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.

 Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

SNMP ID:

2.70.1.4.5

Telnet path:

Setup > IPv6 > Tunnel > 6to4 > Firewall

Possible values:

Yes

No

Default:

Yes

1.4.2 Router advertisement

These settings are used to manage the router advertisements, which are used to announce the device's availability as a router to the network.

SNMP ID:

2.70.2

Telnet path:

Setup > IPv6 > Router-Advertisement

Prefix options

The table contains the settings for IPv6 prefixes for each interface.

SNMP ID:

2.70.2.1

Telnet path:

Setup > IPv6 > Router-Advertisement > Prefix-Options

Interface name

Defines the name of the logical interface.

SNMP ID:

2.70.2.1.1

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

Prefix

Enter the prefix that is transmitted with the router advertisements, e. g. "2001:db8::/64".

The length of the prefix must always be exactly 64 bits ("/64"), or else the clients will not be able to generate their own addresses by adding their "interface identifier" (64 bits long).

 If you wish to automatically use the prefix issued by the provider, then configure "::/64" here and enter the name of the corresponding WAN interface in the field **PD-Source**.

SNMP ID:

2.70.2.1.2

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Prefix

Possible values:

Max. 43 characters

Default:

Blank

Subnet ID

Here you set the subnet ID that is to be combined with the prefix issued by the provider.

If the provider assigns the prefix "2001:db8:a::/48", for example, and you assign the subnet ID "0001" (or "1" for short), then the router advertisement on this interface is given the prefix "2001:db8:a:0001::/64".

The maximum subnet length with a 48-bit long, delegated prefix is 16 bits (65,536 subnets of "0000" to "FFFF"). With a delegated prefix of "/56", the maximum subnet length is 8 bits (256 subnets of "00" to "FF").



In general, the subnet ID "0" is used when the WAN IPv6 address is compiled automatically. For this reason you should start with "1" when assigning subnet IDs for LANs.

SNMP ID:

2.70.2.1.3

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Subnet-ID

Possible values:

Max. 19 characters

Default:

1

Adv.-OnLink

Indicates whether the prefix is "on link".

SNMP ID:

2.70.2.1.3

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Adv.-OnLink

Possible values:

Yes

No

Default:

Yes

Adv.-Autonomous

Indicates whether a host can use the prefix for a "Stateless Address Autoconfiguration". If this is the case, it can directly establish a connection to the Internet.

SNMP ID:

2.70.2.1.5

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Adv.-Autonomous

Possible values:

Yes

No

Default:

Yes

PD source

Use the name of the interface that receives a prefix issued by the provider. This prefix is combined with the string entered in the field **Prefix** to form a subnet that announces router advertisements (DHCPv6 prefix delegation).

SNMP ID:

2.70.2.1.6

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > PD-Source

Possible values:

Max. 16 characters

Default:

Blank

Advertise preferred lifetime

Defines the time in milliseconds for which an IPv6 address is to be "Preferred". The client also uses this lifetime for its generated IPv6 address. If the lifetime of the prefix has expired, the client no longer uses the corresponding IPv6 address. If the "preferred lifetime" of an address expires, it will be marked as "deprecated". This address is then used only by already active connections until those connections end. Expired addresses are no longer available for new connections.

SNMP ID:

2.70.2.1.7

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Adv.-Pref.-Lifetime

Possible values:

Max. 10 numbers in the range 0 – 2147483647

Default:

604800

Adv.-Valid-Lifetime

Defines the time in seconds, after which the validity of an IPv6 address expires. Expired addresses are no longer available for new connections.

SNMP ID:

2.70.2.1.8

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Adv.-Valid-Lifetime

Possible values:

Max. 10 numbers in the range 0 – 2147483647

Default:

2592000

Interface options

The table contains the settings for the IPv6 interfaces.

SNMP ID:

2.70.2.2

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options

Interface name

Defines the name of the logical interface to be used for sending router advertisements.

SNMP ID:

2.70.2.2.1

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

Send adverts

Enables the periodic transmission of router advertisements and the response to router solicitations.

SNMP ID:

2.70.2.2.2

Telnet path:

Setup > IPv6 > Router-Advertisement > Interface-Options > Send-Adverts

Possible values:

Yes

No

Default:

Yes

Min. RTR interval

Defines in seconds the minimum time allowed between the transmission of consecutive unsolicited multicast router advertisements. **Min-RTR-Interval** and **Max-RTR-Interval** form a time space within which the device sends a router advertisement at random.

SNMP ID:

2.70.2.2.3

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Min-RTR-Interval

Possible values:

Min. 3 seconds

Max. $0.75 * \text{Max-RTR-Interval}$

Max. 10 numbers

Default:

$0.33 * \text{Max-RTR-Interval}$ (if **Max-RTR-Interval** \geq 9 seconds)

Max-RTR-Interval (if **Max-RTR-Interval** $<$ 9 seconds)

Max. RTR interval

Defines in seconds the maximum time allowed between the transmission of consecutive unsolicited multicast router advertisements. **Min-RTR-Interval** and **Max-RTR-Interval** form a time space within which the device sends a router advertisement at random.

SNMP ID:

2.70.2.2.4

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Max-RTR-Interval

Possible values:

Min. 4 seconds

Max. 1800 seconds

Max. 10 numbers

Default:

600 seconds

Managed flag

Sets the "Managed address configuration" flag in the router advertisement.

Setting this flag causes the clients to configure all addresses via "Stateful Autoconfiguration" (DHCPv6). In this case the clients also automatically retrieve other information, such as DNS server addresses.

SNMP ID:

2.70.2.2.5

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Managed-Flag

Possible values:

Yes

No

Default:

No

Other config flag

Sets the "Other configuration" flag in the router advertisement.

If this flag is set, the device instructs the clients to retrieve additional information (but not the addresses for the client) such as DNS server addresses via DHCPv6.

SNMP ID:

2.70.2.2.6

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Other-Config-Flag****Possible values:**

Yes

No

Default:

Yes

Link MTU

Here you set the valid MTU for the corresponding link.

SNMP ID:

2.70.2.2.7

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Link-MTU****Possible values:**

Max. 5 numbers in the range 0 – 99999

Default:

1500

Reachable time

Specifies the time in seconds for which the router is considered to be reachable.

The default value of "0" means that the router advertisements have no specifications for reachable time.

SNMP ID:

2.70.2.2.8

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Reachable-Time****Possible values:**

Max. 10 numbers in the range 0 – 2147483647

Default:

0

Hop limit

Defines the maximum number of routers to be used to forward a data packet. One router corresponds to one "hop".

SNMP ID:

2.70.2.2.10

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Hop-Limit**

Possible values:

Max. 5 numbers in the range 0 – 255

Default:

0: No hop limit defined

Default lifetime

Specifies the time in seconds for which the router is considered to be reachable in the network.

 If this value is set to **0**, the operating system will not use this router as the default router.

SNMP ID:

2.70.2.2.11

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Def.-Lifetime

Possible values:

Max. 10 numbers in the range 0 – 2147483647

Default:

1800

Default router mode

Defines how the device advertises itself as the default gateway or router.

The settings have the following functions:

- **Auto:** As long as a WAN connection exists, the router sends a positive router lifetime in the router advertisement messages. The result is that a client uses this router as the default gateway. If there is no WAN connection, the router sets the router lifetime to "0". A client then stops using this router as the default gateway.
- **Always:** The router lifetime is always positive—i. e. greater than "0"—irrespective of the WAN connection status.
- **Never:** The router lifetime is always "0".

SNMP ID:

2.70.2.2.12

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Default-Router-Mode

Possible values:

Auto
Always
Never

Default:

Auto

Router preference

Defines the preference of this router. Clients enter this preference into their local routing tables.

SNMP ID:

2.70.2.2.13

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Router-Preference

Possible values:

Low

Medium

High

Default:

Medium

Route options

The table contains the settings for the route options.

SNMP ID:

2.70.2.3

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options

Interface name

Defines the name of the interface that this route option applies to.

SNMP ID:

2.70.2.3.1

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

Prefix

Set the prefix for this route. This should not exceed 64 bits in length if it is to be used for auto-configuration.

SNMP ID:

2.70.2.3.2

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options > Prefix

Possible values:

IPv6 prefix with max. 43 characters, e.g. 2001:db8::/64

Default:

Blank

Route lifetime

Set how long in seconds the route should remain valid.

SNMP ID:

2.70.2.3.3

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options > Route-Lifetime

Possible values:

Max. 5 numbers in the range 0 – 65335

Default:

0: No route lifetime specified

Route preference

This parameter specifies the priority of an advertised route. A router receiving a router advertisement with two routes of different preference will choose the route with the higher priority.

SNMP ID:

2.70.2.3.4

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options > Route-Preference

Possible values:

Low

Medium

High

Default:

Medium

RDNSS options

This table contains the settings of RDNSS extension (recursive DNS server).

 This function is not currently supported by Windows. Propagation of a DNS server, where required, is performed via DHCPv6.

SNMP ID:

2.70.2.4

Telnet path:

Setup > IPv6 > Router-Advertisements > RDNSS-Options

Interface name

Defines the name of the logical interface to be used for announcing the IPv6 DNS server in router advertisements.

SNMP ID:

2.70.2.4.1

Telnet path:

Setup > IPv6 > Router-Advertisements > RDNSS-Options > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

IPv6 DNS server

Contains the IPv6 address of the DNS server (RDNSS) to be announced in router advertisements.

SNMP ID:

2.70.2.4.2

Telnet path:**Setup > IPv6 > Router-Advertisements > RDNSS-Options > IPv6-DNS-Server****Possible values:**

Max. 39 characters

Default:

Blank

Lifetime

Defines the time in seconds for which a client may use this DNS server for name resolution.

SNMP ID:

2.70.2.4.3

Telnet path:**Setup > IPv6 > Router-Advertisements > RDNSS-Options > Lifetime****Possible values:**

- Max. 5 numbers in the range 0 – 65535
- 0: Discontinuation

Default:

900

1.4.3 DHCPv6

This menu contains the DHCPv6 settings.



In the LCOS Public Beta 1 version, the "link-local IPv6 address" of the device is automatically advertised as the DNS server and cannot be changed.

SNMP ID:

2.70.3

Telnet path:**Setup > IPv6 > DHCPv6****Server**

This menu contains the DHCP server settings for IPv6.

SNMP ID:

2.70.3.1

Telnet path:

Setup > IPv6 > DHCPv6 > Server

Address pools

If distribution of the DHCPv6 server is to be stateful, this table defines an address pool.

SNMP ID:

2.70.3.1.2

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Address-Pool

Address pool name

Specify the name of the address pool here.

SNMP ID:

2.70.3.1.2.1

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Address-Pools > Address-Pool-Name

Possible values:

Maximum 31 characters

Default:

Blank

Start address pool

Here you specify the first address in the pool, e. g. "2001:db8::1"

SNMP ID:

2.70.3.1.2.2

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Address-Pools > Start-Address-Pool

Possible values:

Maximum 39 characters

Default:

Blank

End address pool

Here you specify the last address in the pool, e. g. "2001:db8::9"

SNMP ID:

2.70.3.1.2.3

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Address-Pools > End-Address-Pool

Possible values:

Maximum 39 characters

Default:

Blank

Preferred lifetime

Here you specify the time in seconds that the client should treat this address as "preferred". After this time elapses, a client classifies this address as "deprecated".

SNMP ID:

2.70.3.1.2.5

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Address-Pools > Pref.-Lifetime****Possible values:**

Maximum 10 characters.

Default:

3600

Valid lifetime

Here you specify the time in seconds that the client should treat this address as "valid".

SNMP ID:

2.70.3.1.2.6

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Address-Pools > Valid-Lifetime****Possible values:**

Maximum 10 characters.

Default:

86400

PD pools

In this table, you specify the prefixes that the DHCPv6 server delegates to other routers.

SNMP ID:

2.70.3.1.3

Telnet path:**Setup > IPv6 > DHCPv6 > Server > PD-Pools****PD pool name**

Specify the name of the PD pool here.

SNMP ID:

2.70.3.1.3.1

Telnet path:**Setup > IPv6 > DHCPv6 > Server > PD-Pools > PD-Pool-Name****Possible values:**

Maximum 31 characters

Default:

Blank

Start PD pool

Here you specify the first prefix for delegation in the PD pool, e. g. "2001:db8:1100::"

SNMP ID:

2.70.3.1.3.2

Telnet path:

Setup > IPv6 > DHCPv6 > Server > PD-Pools > Start-PD-Pool

Possible values:

Maximum 39 characters

Default:

Blank

End PD pool

Here you specify the last prefix for delegation in the PD pool, e. g. "2001:db8:FF00::"

SNMP ID:

2.70.3.1.3.3

Telnet path:

Setup > IPv6 > DHCPv6 > Server > PD-Pools > End-PD-Pool

Possible values:

Maximum 39 characters

Default:

Blank

Prefix length

Here you set the length of the prefixes in the PD pool, e. g. "56" or "60"

SNMP ID:

2.70.3.1.3.4

Telnet path:

Setup > IPv6 > DHCPv6 > Server > PD-Pools > Prefix-Length

Possible values:

Maximum 3 characters.

Default:

56

Pref.-Lifetime

Define the time in seconds, in which the client should use the prefix as "preferred". After this time the client will handle this prefix as "deprecated".

SNMP ID:

2.70.3.1.3.5

Telnet path:**Setup > IPv6 > DHCPv6 > Server > PD-Pools > Pref.-Lifetime****Possible values:**

maximum 10 characters

Default:

3600

Valid-Lifetime

Define the time in seconds, in which the client should use the prefix as "valid".

SNMP ID:

2.70.3.1.3.6

Telnet path:**Setup > IPv6 > DHCPv6 > Server > PD-Pools > Valid-Lifetime****Possible values:**

maximum 10 characters

Default:

86400

Interface-List

In this table you can configure the basic settings of the DHCPv6-Servers and define, to which interfaces the settings should apply.

SNMP ID:

2.70.3.1.4

Pfad Telnet:**Setup > IPv6 > DHCPv6 > Server > Interface-List****Interface-Name-or-Relay**

Name of the Interfaces, on which the DHCPv6-Server is working, e. g. "INTRANET"

SNMP-ID:

2.70.3.1.4.1

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Interface-List > Interface-Name****Possible values:**

Selection of the LAN interfaces configured in the device, maximum 39 characters

Default:

empty

Operating

Activates or deactivates the DHCPv6 server.

SNMP ID:

2.70.3.1.4.2

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List > Operating

Possible values:

No

Yes

Default:

Yes

Primary DNS

IPv6 address of the primary DNS server.

SNMP ID:

2.70.3.1.4.3

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List > Primary-DNS

Possible values:

IPv6 address with max. 39 characters

Default:

::

Secondary DNS

IPv6 address of the secondary DNS server.

SNMP ID:

2.70.3.1.4.4

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List > Secondary-DNS

Possible values:

IPv6 address with max. 39 characters

Default:

Blank

Address pool name

Here you specify the address pool that the devices uses for this interface.



If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the table **Setup > IPv6 > DHCPv6 > Server > Address-Pools**.

SNMP ID:

2.70.3.1.4.5

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List > Address-Pool-Name

Possible values:

Maximum 31 characters

Default:

Blank

PD pool name

Determine the prefix-delegation pool that the devices is to use for this interface.

 If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table **Setup > IPv6 > DHCPv6 > Server > PD-Pools**.

SNMP ID:

2.70.3.1.4.6

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Interface-Liste > PD-Pool-Name****Possible values:**

Maximum 31 characters

Default:

Blank

Rapid commit

With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.

 The client must explicitly include the rapid commit option in its solicit message.

SNMP ID:

2.70.3.1.4.7

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Interface-Liste > Rapid-Commit****Possible values:**

No

Yes

Default:

No

Preference

Where multiple DHCPv6 servers are operated on the network, the preference parameter gives you the control over which server the clients will use. The primary server requires a higher preference value than the backup server.

SNMP ID:

2.70.3.1.4.8

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Interface-Liste > Preference****Possible values:**

0 to 255

Default:

0

Client

This menu contains the DHCP client settings for IPv6.

SNMP ID:

2.70.3.2

Telnet path:

Setup > IPv6 > DHCPv6 > Client

Interface list

This table determines the behavior of the DHCPv6 client.

 Normally client behavior is controlled by the auto-configuration.

SNMP ID:

2.70.3.2.1

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List

Interface name

Specify the name of the interface that the DHCPv6 client operates on. These may be LAN interfaces or WAN interfaces (remote stations), such as "INTRANET" or "INTERNET".

SNMP ID:

2.70.3.2.1.1

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List > Interface-Name

Possible values:

Selection from the list of LAN interfaces defined in the device; max. 16 characters

Default:

Blank

Operating

Here you specify if and how the device enables the client. Possible values are:

- **Autoconf:** The device waits for router advertisements, and then starts the DHCPv6 client. This option is the default setting.
- **Yes:** The device starts the DHCPv6 client as soon as the interface is active, without waiting for router advertisements.
- **No:** The DHCPv6 client is disabled on this interface. Even if the device receives router advertisements, it will not start the client.

SNMP ID:

2.70.3.2.1.2

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List > Operating

Possible values:

Autoconf

No

Yes

Default:

Autoconf

Request DNS

Here you specify whether the client should query the DHCPv6 server for DNS servers.

 You must enable this option in order for the device to obtain information about a DNS server.

SNMP ID:

2.70.3.2.1.3

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List > Request-DNS

Possible values:

No

Yes

Default:

Yes

Request address

Here you specify whether the client should query the DHCPv6 server for an IPv6 address.

 Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i. e. not distributed by 'SLAAC'.

SNMP ID:

2.70.3.2.1.4

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List > Request-Address

Possible values:

No

Yes

Default:

Yes

Request PD

Here you specify whether the client should request the DHCPv6 server for an IPv6 prefix. Activating this option is only necessary if the device itself functions as a router and redistributes these prefixes. This option is enabled by default on WAN interfaces in order for the DHCPv6 client to request a prefix from the provider for use in its local network. This option is disabled by default on LAN interfaces because devices in a local network are more likely to function as clients rather than as routers.

SNMP ID:

2.70.3.2.1.5

Telnet path:**Setup > IPv6 > DHCPv6 > Client > Interface-List > Request-PD****Possible values:**

No

Yes

Default:

No

Rapid commit

When rapid commit is activated, the client attempts to obtain an IPv6 address from the DHCPv6 server with just two messages. If the DHCPv6 server is configured correspondingly, it immediately responds to this solicit message with a reply message.

SNMP ID:

2.70.3.2.1.6

Telnet path:**Setup > IPv6 > DHCPv6 > Client > Interface-List > Rapid-Commit****Possible values:**

No

Yes

Default:

Yes

User class identifier

This assigns the device a unique user class ID.

SNMP ID:

2.70.3.2.2

Telnet path:**Setup > IPv6 > DHCPv6 > Client > User-Class-Identifier****Possible values:**

Maximum 253 characters

Default:

Blank

Vendor class identifier

This assigns the device a unique vendor class ID.

SNMP ID:

2.70.3.2.3

Telnet path:**Setup > IPv6 > DHCPv6 > Client > Vendor-Class-Identifier****Possible values:**

Maximum 253 characters

Default:

Device name according to the manufacturer

Relay agent

This menu contains the DHCP relay agent settings for IPv6.

SNMP ID:

2.70.3.3

Telnet path:

Setup > IPv6 > DHCPv6 > Relay-Agent

Interface list

This table determines the behavior of the DHCPv6 relay agent.

SNMP ID:

2.70.3.3.1

Telnet path:

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

Interface name

Define the name of the interface on which the relay agent receives requests from DHCPv6 clients, e. g. "INTRANET".

SNMP ID:

2.70.3.3.1.1

Telnet path:

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

Possible values:

Selection from the list of LAN interfaces defined in the device; max. 16 characters

Default:

Blank

Relay agent operating

With this option you define if and how the device enables the relay agent.

SNMP ID:

2.70.3.3.1.2

Telnet path:

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

Possible values:

Yes: Relay agent is enabled. This option is the default setting.

No: Relay agent is not enabled.

Default:

Yes

Interface address

Specify the relay agent's own IPv6 address at the interface that is configured under Interface Name. This IPv6 address is used as a sender address in DHCP messages that are forwarded. This sender address enables DHCPv6 clients to uniquely identify a relay agent. An explicit specification of the interface address is necessary because an IPv6 host can have multiple IPv6 addresses for each interface.

SNMP ID:

2.70.3.3.1.3

Telnet path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List > Interface-Address****Possible values:**

Maximum 39 characters

Default:

Blank

Destination address

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

SNMP ID:

2.70.3.3.1.4

Telnet path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List > Dest-Address****Possible values:**

Maximum 39 characters

Default:

ff02::1:2

Destination interface

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

SNMP ID:

2.70.3.3.1.5

Telnet path:**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List > Dest-Interface****Possible values:**

Maximum 39 characters

Default:

Blank

1.4.4 Network

Here you can adjust further IPv6 network settings for each logical interface supported by your device.

SNMP ID:

2.70.4

Telnet path:

Setup > IPv6 > Network

Addresses

This table is used to manage the IPv6 addresses.

SNMP ID:

2.70.4.1

Telnet path:

Setup > IPv6 > Network > Addresses

Interface name

Give a name to the interface that you want to assign the IPv6 network.

SNMP ID:

2.70.4.1.1

Telnet path:

Setup > IPv6 > Network > Addresses > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

IPv6 address prefix length

Specify an IPv6 address including the prefix length for this interface.



The default prefix length is 64 bits ("/64"). If possible do not use IPv6 addresses with longer prefixes, as many IPv6 mechanisms in the device are designed for a maximum length of 64 bits.

A possible address is, for example, "2001:db8::1/64". An interface can have multiple IPv6 addresses:

- A "global unicast address", e. g. "2001:db8::1/64",
- A "unique local address", e. g. "fd00::1/64".

"Link local addresses" are fixed and not configurable.

SNMP ID:

2.70.4.1.2

Telnet path:

Setup > IPv6 > Network > Addresses > IPv6-Address-Prefixlength

Possible values:

Max. 43 characters

Default:

Blank

Address type

Determine the type of IPv6 address.

Using the address type **EUI-64** causes IPv6 addresses to be 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".

SNMP ID:

2.70.4.1.3

Telnet path:

Setup > IPv6 > Network > Addresses > Address-Type

Possible values:

Unicast

Anycast

EUI-64

Default:

Unicast

Name

Enter a descriptive name for this combination of IPv6 address and prefix.

 Entering a name is optional.

SNMP ID:

2.70.4.1.4

Telnet path:

Setup > IPv6 > Network > Addresses > Name

Possible values:

Max. 16 characters

Default:

Blank

Comment

Enter a descriptive comment for this entry.

 Entering a comment is optional.

SNMP ID:

2.70.4.1.5

Telnet path:**Setup > IPv6 > Network > Addresses > Comment****Possible values:**

Max. 64 characters

Default:

Blank

Parameter

This table is used to manage the IPv6 parameters.

SNMP ID:

2.70.4.2

Telnet path:**Setup > IPv6 > Network > Parameter****Interface name**

Give a name to the interface for which the IPv6 parameters are to be configured.

SNMP ID:

2.70.4.2.1

Telnet path:**Setup > IPv6 > Network > Parameter > Interface-Name****Possible values:**

Max. 16 characters

Default:

Blank

IPv6 gateway

Specify the IPv6 gateway to be used by this interface.



This parameter overrides gateway information that the device may receive via router advertisements, for example.

SNMP ID:

2.70.4.2.2

Telnet path:**Setup > IPv6 > Network > Parameter > IPv6-Gateway****Possible values:**

- Global unicast address, e.g. 2001:db8::1
- Link-local address to which you add to the corresponding interface (%<INTERFACE>), e.g. fe80::1%INTERNET

Default:

::

Primary DNS

Specify the primary IPv6 DNS server to be used by this interface.

SNMP ID:

2.70.4.2.3

Telnet path:

Setup > IPv6 > Network > Parameter > Primary-DNS

Possible values:

IPv6 address with max. 39 characters

Default:

::

Secondary DNS

Specify the secondary IPv6 DNS server to be used by this interface.

SNMP ID:

2.70.4.2.4

Telnet path:

Setup > IPv6 > Network > Parameter > Secondary-DNS

Possible values:

IPv6 address with max. 39 characters

Default:

::

1.4.5 Firewall

This menu contains the settings for the firewall.

SNMP ID:

2.70.5

Telnet path:

Setup > IPv6 > Firewall

Operating

Enables or disables the firewall.

 This item enables the firewall globally. The firewall is only active if you enable it here. If you disable the firewall here and at the same time enable it for individual interfaces, it remains disabled for all interfaces.

SNMP ID:

2.70.5.1

Telnet path:

Setup > IPv6 > Firewall > Operating

Possible values:

Yes

No

Default:

Yes

1.4.6 LAN interfaces

This table contains the settings for the LAN interfaces.

SNMP ID:

2.70.6

Telnet path:

Setup > IPv6 > LAN-Interfaces

Interface name

Enter a name for the logical IPv6 interface that is defined by the physical interface (interface assignment) and the VLAN ID.

SNMP ID:

2.70.6.1

Telnet path:

Setup > IPv6 > LAN-Interfaces > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

Interface ID

Select the physical interface to be combined with the VLAN ID to form the logical IPv6 interface.

SNMP ID:

2.70.6.2

Telnet path:

Setup > IPv6 > LAN-Interfaces > Interface-ID

Possible values:

All physically available interfaces on the device

Default:

LAN-1

VLAN ID

Select the VLAN ID to be combined with the physical interface to form the logical IPv6 interface.



If you enter an invalid VLAN ID here, no communication will take place.

SNMP ID:

2.70.6.3

Telnet path:

Setup > IPv6 > LAN-Interfaces > VLAN-ID

Possible values:

0 to 4096

Max. 4 numbers

Default:

0

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.6.4

Telnet path:

Setup > IPv6 > LAN-Interfaces > Rtg-Tag

Possible values:

Max. 5 characters in the range 0 – 65535

Default:

0

Autoconf

Enable or disable "stateless address autoconfiguration" for this interface.

 If the device sends router advertisements from this interface, it does not generate any IPv6 addresses even with auto-configuration enabled.

SNMP ID:

2.70.6.5

Telnet path:

Setup > IPv6 > LAN-Interfaces > Autoconf

Possible values:

Yes

No

Default:

Yes

Accept RA

Enables or disables the processing of received router advertisement messages.

 With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

SNMP ID:

2.70.6.6

Telnet path:**Setup > IPv6 > LAN-Interfaces > Accept-RA****Possible values:**

Yes

No

Default:

Yes

Interface status

Enables or disables this interface.

SNMP ID:

2.70.6.7

Telnet path:**Setup > IPv6 > LAN-Interfaces > Interface-Status****Possible values:**

Up

Down

Default:

Up

Forwarding

Enables or disables the forwarding of data packets to other interfaces.



With forwarding disabled, no router advertisements are transmitted from this interface.

SNMP ID:

270.6.8

Telnet path:**Setup > IPv6 > LAN-Interfaces > Forwarding****Possible values:**

Yes

No

Default:

Yes

MTU

Specify the applicable MTU for this interface.

SNMP ID:

2.70.6.9

Telnet path:

Setup > IPv6 > LAN-Interfaces > MTU

Possible values:

Max. 4 numbers in the range 0 – 9999

Default:

1500

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.

 If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

SNMP ID:

2.70.6.10

Telnet path:

Setup > IPv6 > LAN-Interfaces > Firewall

Possible values:

Yes

No

Default:

No

Comment

Enter a descriptive comment for this entry.

 Entering a comment is optional.

SNMP ID:

2.70.6.11

Telnet path:

Setup > IPv6 > LAN-Interfaces > Comment

Possible values:

Max. 64 characters

Default:

Blank

1.4.7 WAN interfaces

This table contains the settings for the LAN interfaces.

SNMP ID:

2.70.7

Telnet path:

Setup > IPv6 > WAN-Interfaces

Interface name

Specify the name of the WAN remote peer here. Use the name as specified at the remote site.

SNMP ID:

2.70.7.1

Telnet path:

Setup > IPv6 > WAN-Interfaces > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.7.2

Telnet path:

Setup > IPv6 > WAN-Interfaces > Rtg-Tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

Autoconf

Enable or disable "stateless address autoconfiguration" for this interface.



If the device sends router advertisements from this interface, it does not generate any addresses even with auto-configuration enabled.

SNMP ID:

2.70.7.3

Telnet path:

Setup > IPv6 > WAN-Interfaces > Autoconf

Possible values:

Yes

No

Default:

Yes

Accept RA

Enables or disables the processing of received router advertisement messages.

 With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

SNMP ID:

2.70.6.6

Telnet path:

Setup > IPv6 > WAN-Interfaces > Accept-RA

Possible values:

Yes

No

Default:

Yes

Interface status

Enables or disables this interface.

SNMP ID:

2.70.7.5

Telnet path:

Setup > IPv6 > WAN-Interfaces > Interface-Status

Possible values:

Up

Down

Default:

Up

Forwarding

Enables or disables the forwarding of data packets to other interfaces.

SNMP ID:

2.70.7.6

Telnet path:

Setup > IPv6 > WAN-Interfaces > Forwarding

Possible values:

Yes

No

Default:

Yes

Firewall

Enables the firewall for this interface.

 If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

SNMP ID:

2.70.7.7

Telnet path:

Setup > IPv6 > WAN-Interfaces > Firewall

Possible values:

Yes

No

Default:

Yes

Comment

Enter a descriptive comment for this entry.

 Entering a comment is optional.

SNMP ID:

2.70.7.8

Telnet path:

Setup > IPv6 > WAN-Interfaces > Comment

Possible values:

Max. 64 characters

Default:

Blank

DaD attempts

Before the device can use an IPv6 address on an interface, it uses 'Duplicate Address Detection (DAD)' to check to see whether the IPv6 address already exists on the local network. In this way the device avoids address conflicts on the network.

This option specifies the number of times that the device attempts to find duplicate IPv6 addresses on the network.

Telnet path:

Setup > IPv6 > WAN-Interfaces > DaD-Attempts

Possible values:

Max. 1 number

Default:

1

1.4.8 Operating

Switches the IPv6 stack on or off, globally. With the IPv6 stack deactivated, the device does not perform any IPv6-related functions.

SNMP ID:

2.70.10

Telnet path:

Setup > IPv6 > Operating

Possible values:

Yes

No

Default:

No

1.4.9 Forwarding

If forwarding is turned off, the device transmits no data packets between IPv6 interfaces.



Forwarding is essential if you wish to operate the device as a router.

SNMP ID:

2.70.11

Telnet path:

Setup > IPv6 > Forwarding

Possible values:

Yes

No

Default:

Yes

1.4.10 Router

These settings are used to manage the router alignments.

SNMP-ID:

2.70.12

Telnet path:

Setup > IPv6 > Router

Routing table

The table contains the entries to be used for routing packets with IPv6 addresses.

SNMP ID:

2.70.12.1

Telnet path:

Setup > IPv6 > Router > Routing-Table

Prefix

This prefix denotes the network range from which the current remote site, e.g. 2001:db8::/32, is to receive data

SNMP ID:

2.70.12.1.1

Telnet path:

Setup > IPv6 > Router > Routing-Table > Prefix

Possible values:

Max. 43 characters

Default:

Blank

Routing tag

Specify the routing tag for this route. This route is active only for packets with the same tag. The data packets receive the routing tag either from the firewall or depending on the LAN or WAN interface used.



Routing tags are only necessary if used in combination with routing tags as set by firewall rules or as set at an interface.

SNMP ID:

2.70.12.1.2

Telnet path:

Setup > IPv6 > Router > Routing-Table > Routing-Tag

Possible values:

Max. 5 characters

Default:

Blank

Peer or IPv6

This is where you specify the remote site for this route. Enter one of the following options:

- An interface name
- An IPv6 address (e.g. 2001:db8::1)
- An interface supplemented with a link-local address (e.g. fe80::1%INTERNET)



The device stores the remote sites for IPv6 routing as (*WAN interfaces*).

SNMP ID:

2.70.12.1.3

Telnet path:

Setup > IPv6 > Router > Routing-Table > Peer-or-IPv6

Possible values:

Max. 56 characters

Default:

Blank

Comment

Enter a descriptive comment for this entry.



Entering a comment is optional.

SNMP ID:

2.70.12.1.4

Telnet path:**Setup > IPv6 > Router > Routing-Table > Comment****Possible values:**

Max. 64 characters

Default:

Blank

Destination cache timeout

The 'destination cache timeout' specifies how long the device remembers the path to a destination address when no packets are sent to it.

This value also influences the length of time the device takes to change the settings of the firewall: It accepts state changes after at least half of the 'destination cache timeout' time, on average after one quarter of the timeout. Thus with the default setting of 30 seconds, changes to the firewall come into effect on average after 7.5 seconds, but no later than after 15 seconds.

SNMP ID:

2.70.12.2

Telnet path:**Setup > IPv6 > Router > Dest.-Cache-Timeout****Possible values:**

Max. 3 characters

Default:

30 seconds

1.5 Tutorials

1.5.1 Setting up IPv6 Internet access

You can set up access to an IPv6 network if

- You have an IPv6-capable device,
- You use a tunneling technology and
- Your provider supports a native IPv6 network or you have access to a so-called tunnel broker who can mediate your IPv6 packets.

IPv6 access using the Setup Wizard in LANconfig

The Setup Wizard assists you with the configuration of IPv6 access with your equipment.

The Wizard presents following options:

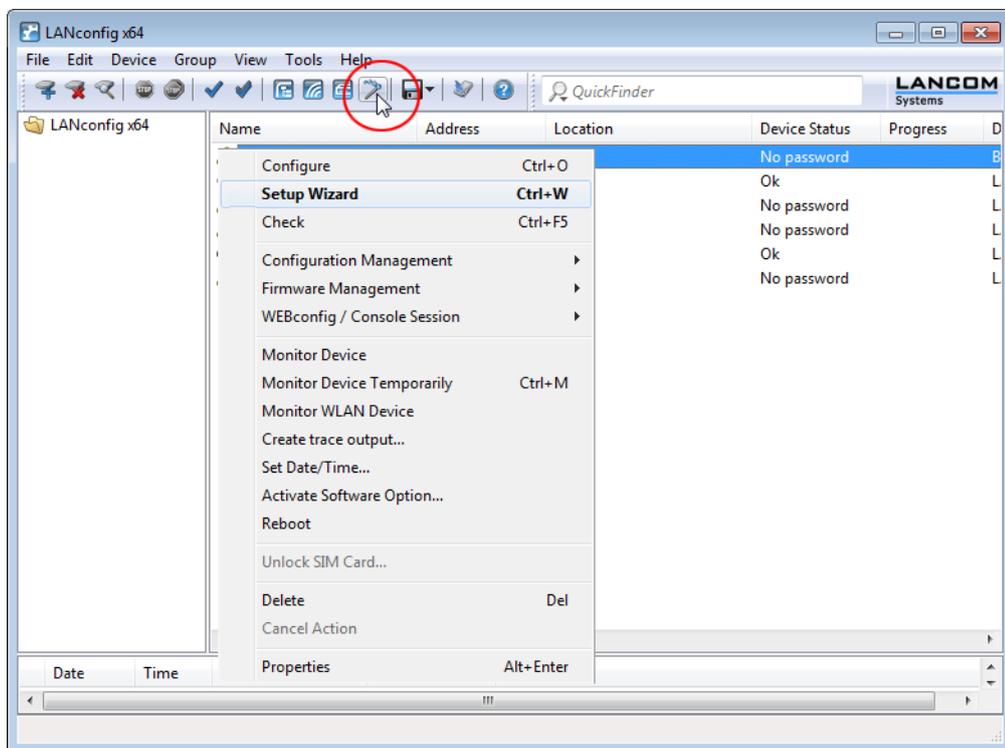
- *Set up IPv6 access for a new, unconfigured device.*
- *Set up IPv6 access in addition to a functioning IPv4 access for an existing device.*

Setup Wizard – setting up IPv6 in a new device

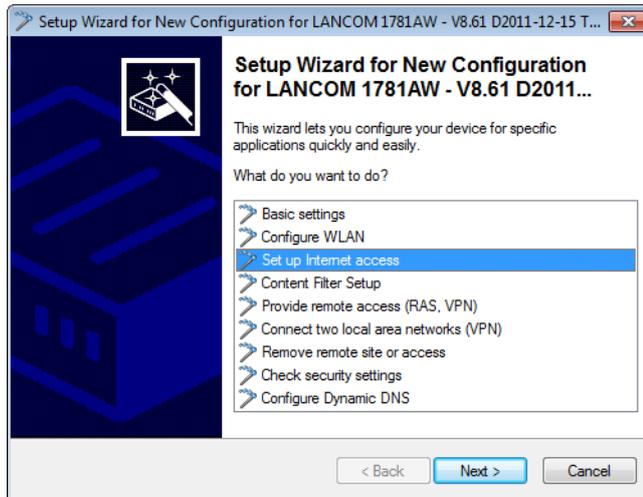
If you have connected up a new device but not have yet configured it, you have the option of using a Setup Wizard to set up IPv4 and IPv6 connections.

To save your entries and proceed to the next screen, click **Next**.

1. Then start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar



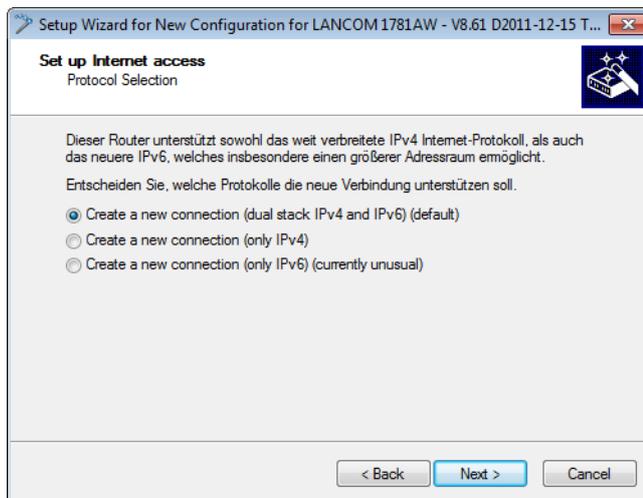
2. In the Setup Wizard, select the option **Set up Internet access**.



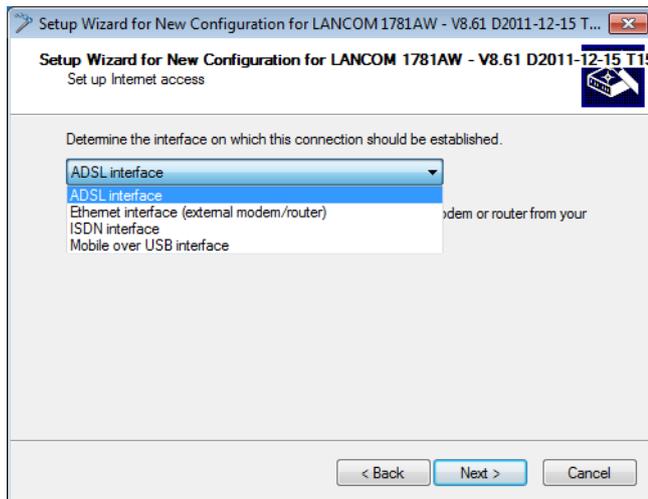
3. You can choose from the following options:

- Set up a dual-stack connection. This is IPv4-and IPv6-capable and currently the recommended option for a new device.
- Set up an IPv4-only connection.
- Set up an IPv6-only connection.

In the following we take you through the setup of a dual-stack connection. Activate the appropriate selection.



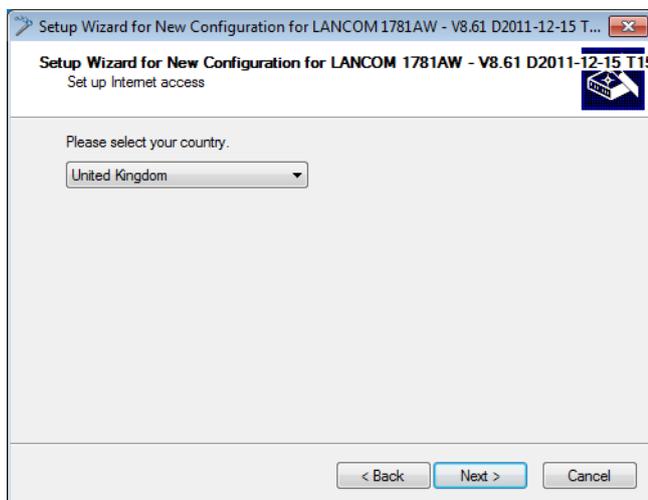
4. Set the interface to be used for the connection.



You can select from the following entries:

- ADSL interface
- Ethernet interface (external modem/router)
- ISDN interface
- Mobile over USB interface

5. Select your country from the list.

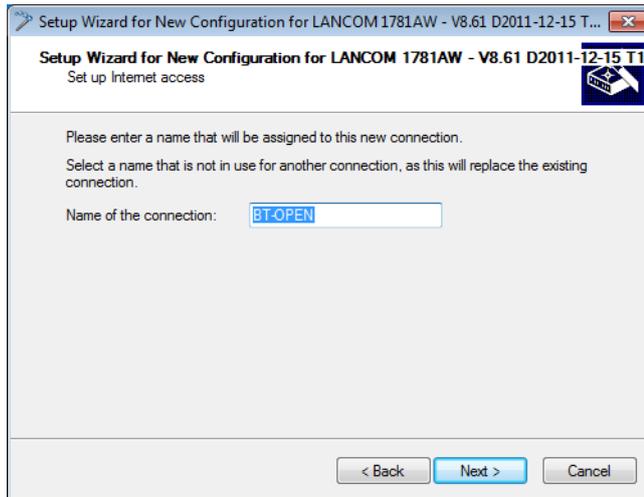


6. Select your Internet provider.

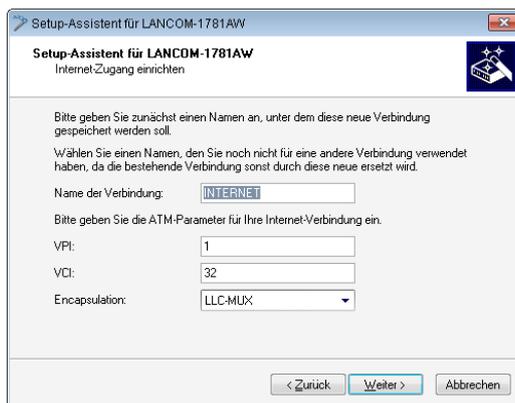
You can select from the following entries:

- A selection of the major Internet providers
- Alternative Internet providers over T-DSL
- Internet access via PPP over ATM (PPPoA)
- Internet access via PPP over Ethernet (PPPoE, PPPoEoA)
- Internet access via plain IP (IPoA)
- Internet access over Plain Ethernet (IPoE, IPoEoA)

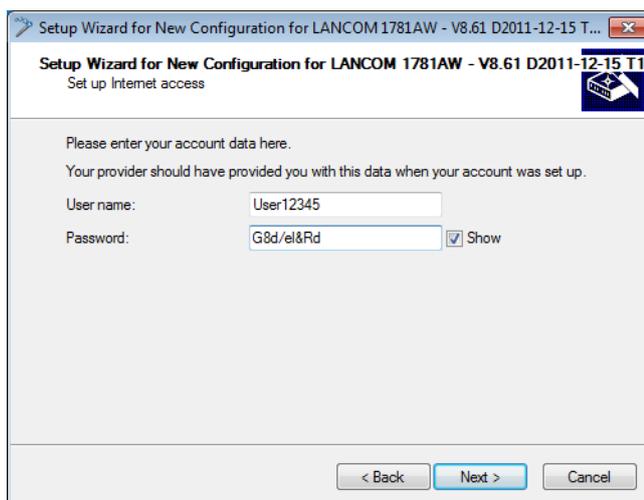
7. Enter a name for this connection.



If you access the Internet with an alternative connection, e. g. over a PPPoE connection, you should additionally enter the appropriate ATM parameters.

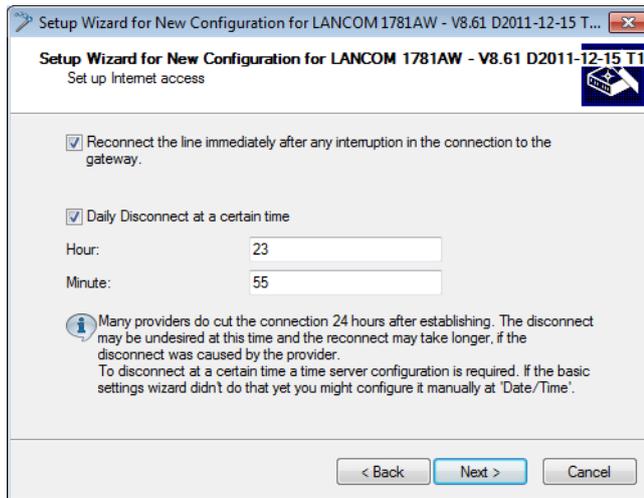


8. Enter the login details given to you by your provider for setting up your Internet access.

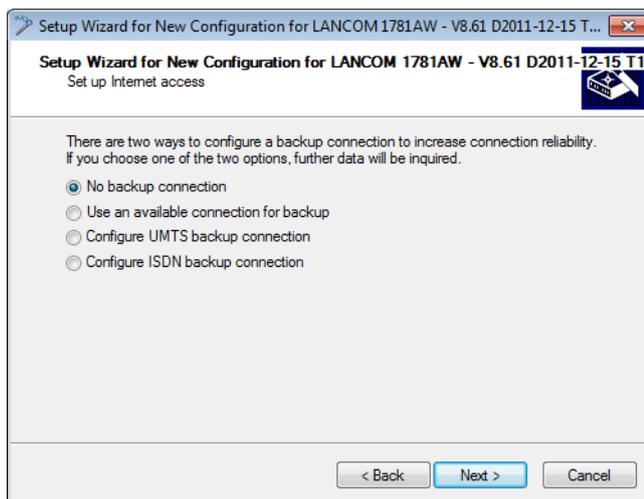


! Depending on the provider, the type and number of fields may vary.

9. Specify how you want the device to behave in case of disconnection. You can also specify if and when the device is to carry out a forced re-connection.



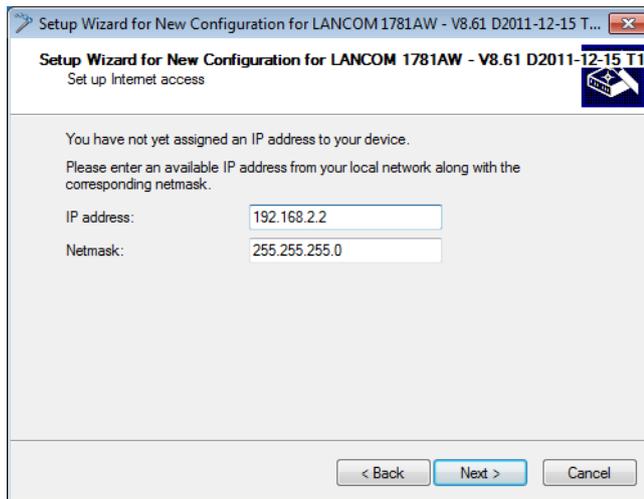
10. Define the type of backup connection to be used in case of connection failure.



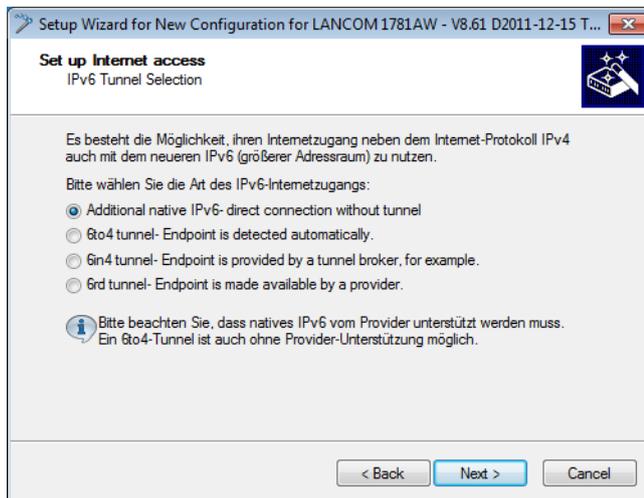
You can select from the following options:

- No backup connection: Skips the configuration of a backup.
- Use the connection already configured in case of backup: In the following dialog, select an already configured connection from a list.
- Setup a backup connection over UMTS: In the next dialog, set up a new UMTS connection. You will need the access data for your UMTS provider.
- Setup a backup connection over ISDN: In the next dialog, set up a new ISDN connection. You will need the access data for your ISDN provider.

11. If your device does not yet have an IP address, enter a new IP address and corresponding netmask.



12. Select the type of IPv6 Internet access.

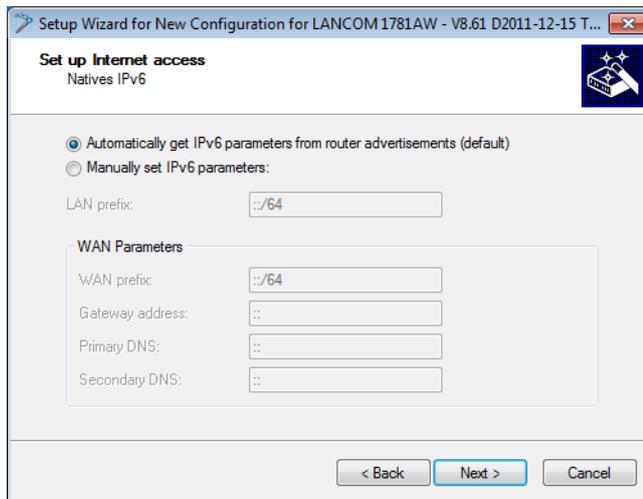


You can select from the following options:

- **Additional native IPv6:** Configure a direct connection without a tunnel.
- **6to4 tunnel:** Start the wizard to configure a 6to4 tunnel.
- **6in4 tunnel:** Use the input mask to set the parameters for the 6in4 tunnel.
- **6rd tunnel:** Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

13. Accept the default setting of **Automatically take IPv6 parameters from router advertisements.**



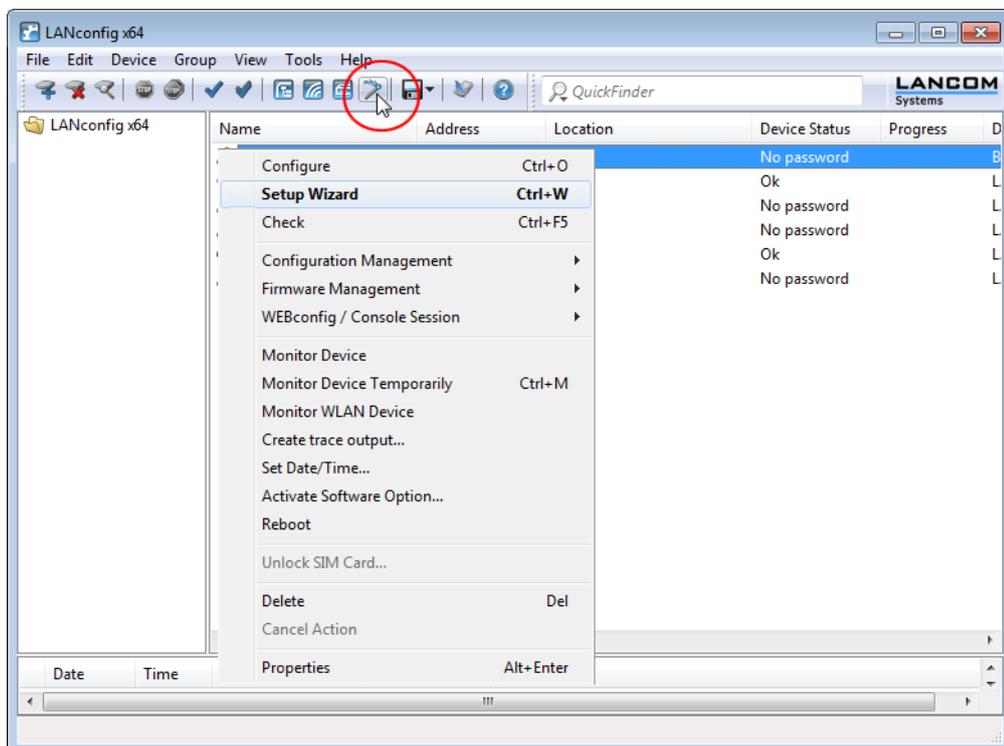
14. You have completed the setup of the native IPv6 Internet access. Click on **Finish** when you are done and the wizard will save your entries to the device.

Setup Wizard – Setting up IPv6 on an existing device

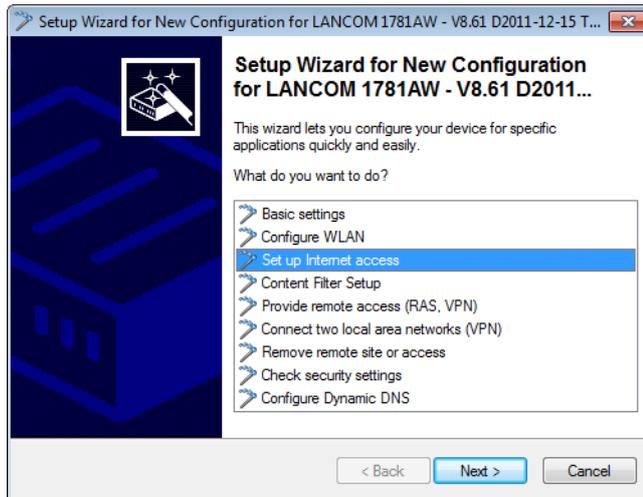
If you have a device configured for IPv4 and you wish to set up an additional IPv6 connection, you have the option of setting up the IPv6 connections with the Setup Wizard.

To save your entries and proceed to the next screen, click **Next**.

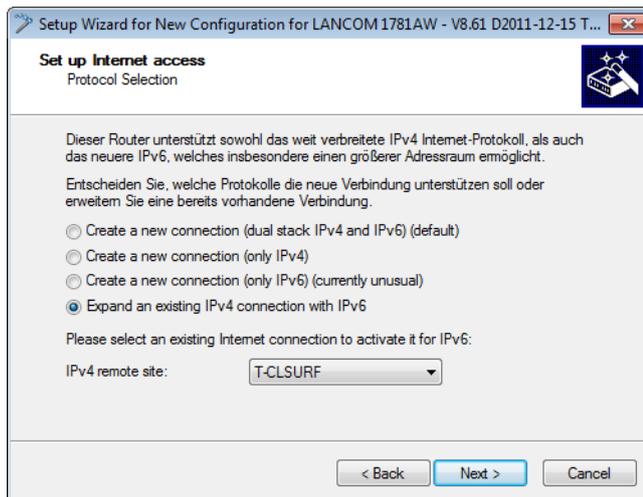
1. Then start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar



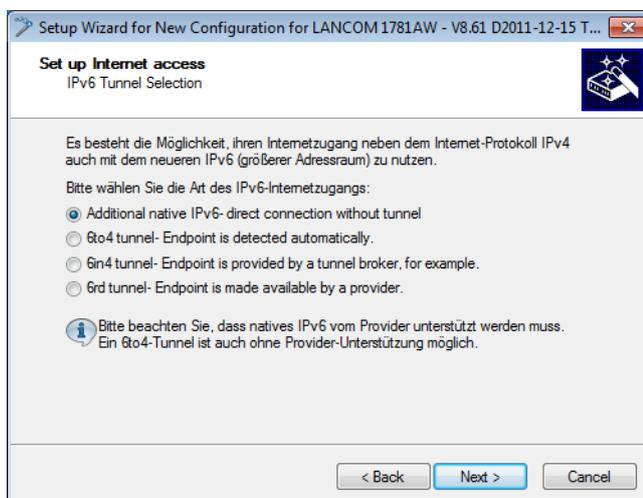
- In the Setup Wizard, select the option **Set up Internet access**. To continue, click on **Next**.



- Because your device is already IPv4-capable, the Setup Wizard gives you the opportunity to extend your existing settings with IPv6. Select this option and click on **Next**.



- Select the type of IPv6 Internet access.

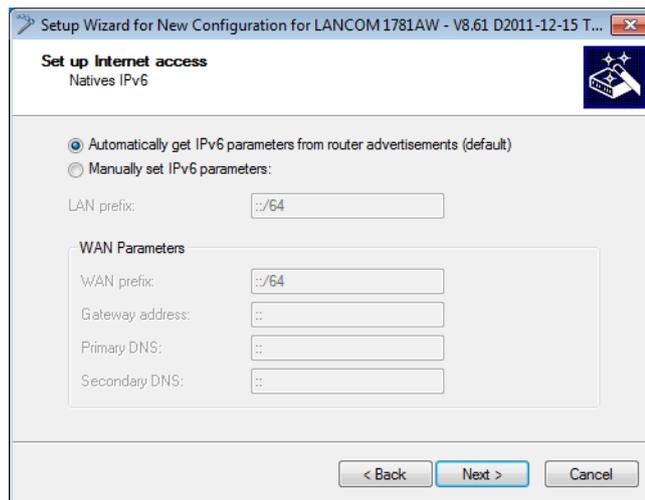


You can select from the following options:

- **Additional native IPv6:** Configure a direct connection without a tunnel.
- **6to4 tunnel:** Start the wizard to configure a 6to4 tunnel.
- **6in4 tunnel:** Use the input mask to set the parameters for the 6in4 tunnel.
- **6rd tunnel:** Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

5. Accept the default setting of **Automatically take IPv6 parameters from router advertisements**.



6. You have completed the setup of the native IPv6 Internet access. Click on **Finish** when you are done and the wizard will save your entries to the device.

1.5.2 Setting up a 6to4 tunnel

The use of a 6to4 tunnel is feasible when

- Your device is IPv6 capable and you want to access IPv6 services,
- Your provider does not support a native IPv6 network and
- You do not have access to a so-called tunnel broker who can mediate your IPv6 packets.

When using a 6to4 tunnel, the lack of support of IPv6 by the provider means the device does not receive an IPv6 address or an IPv6 prefix.

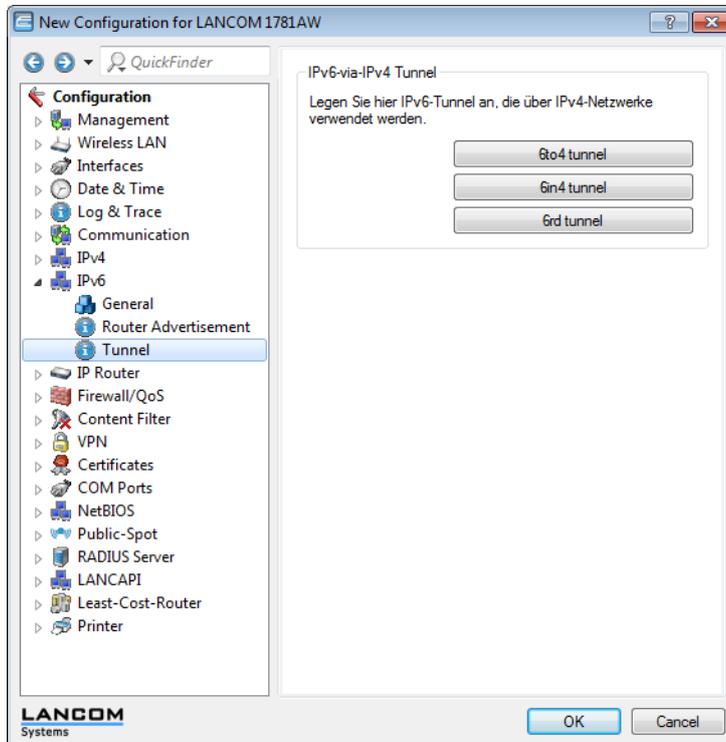
The device calculates its own unique prefix from "2002::/16" and the hexadecimal representation of its own public IPv4 address from the provider. This application only works if the device has a public IPv4 address. The device does not receive a public IPv4 address but an IPv4 address from a private address range only, for example when it accesses the Internet via UMTS and the provider supplies an IP address from its private address range, or if the device does not access the Internet directly, but is "behind" another router.

 Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the relay used can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

Working with LANconfig

To set up a 6to4 tunnel with LANconfig, proceed as follows:

1. LANconfig can be started from the Windows Start bar: Click on **Start > Programs > LANCOM > LANconfig**. LANconfig now automatically searches the local network for devices.
2. Select the device on which you want to set up a 6to4 tunnel. Select it with a left-click and start the configuration from the menu bar with **Device > Configure**.
3. Navigate to **IPv6 > Tunnel** and click on **6to4 tunnel**.



4. Click on **Add** to create a new 6to4 tunnel.

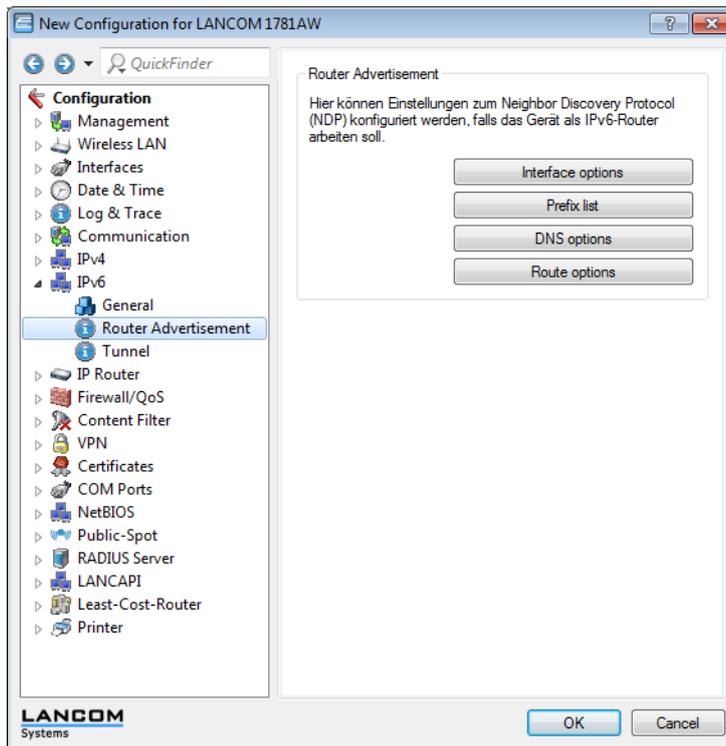


5. Set the name of the 6to4 tunnel.
6. Set the **Interface tag** to a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

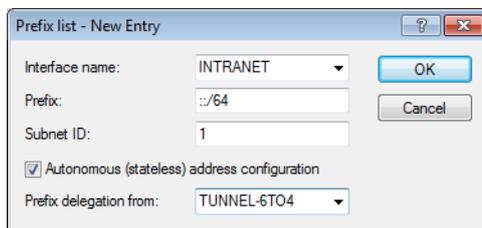
ⓘ Not yet functioning in LCOS 8.61 Public Beta 2.

7. The **Gateway address** is set by default to the anycast address "192.88.99.1". This address can only be changed with WEBconfig or Telnet.
8. Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The **IPv4 routing tag** specifies which tagged IPv4 route is to be used for the data packets to reach their destination address.
9. The default value is this tunnel's firewall.
If you disable the global firewall, you should also disable the firewall for the tunnel.
10. Accept your entries with **OK**.

11. Change to the directory **IPv6 > Router advertisements**.



12. Open the **Prefix list** and click on **Add**.



13. Enter a name for the interface that is used by the 6to4 tunnel, e. g. "INTRANET".

14. Set the value for the **Prefix** to "::/64" in order to accept the prefix issued by the provider automatically and in its entirety.

15. Accept the default value of "1" for the **Subnet ID**.

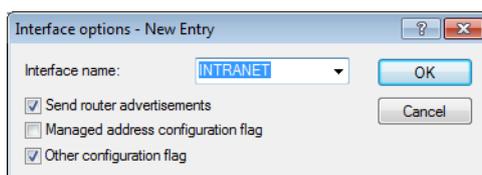
16. Accept the activated option **Stateless address configuration**.

17. In the field **Prefix delegation from**, enter the name of the tunnel that you have defined earlier, e.g. in the example above "TUNNEL-6TO4".

18. Accept your entries with **OK**.

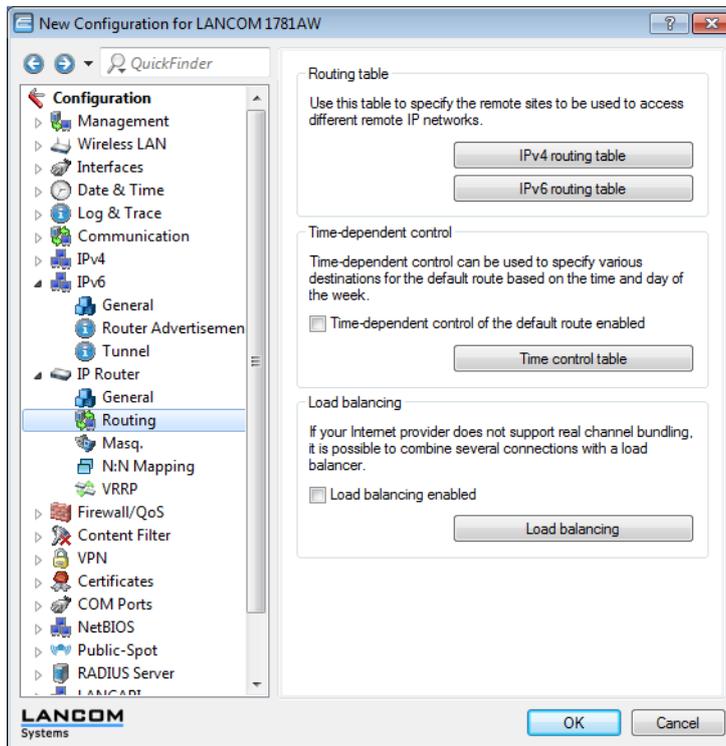
19. In the directory **IPv6 > Router advertisements**, open the **Interface options**, select the entry INTRANET and click on **Edit**.

20. Select the checkbox for **Send router advertisements**.

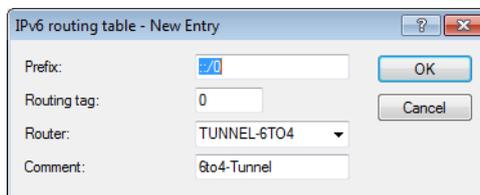


21. Accept all other default values without change.

22. Save your entries with **OK**.
23. Change to the directory **IP router > Routing**.



24. Open the **IPv6 routing table** and click on **Add**.

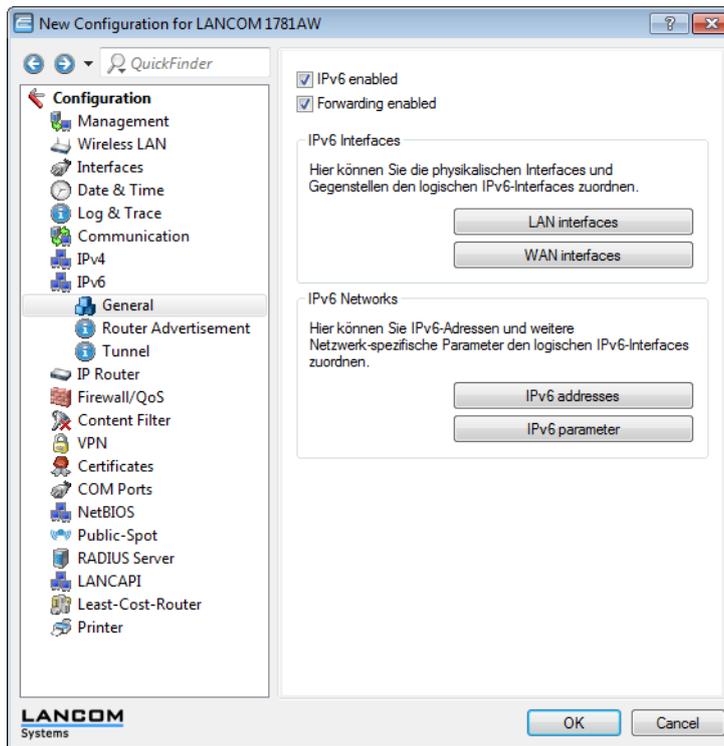


25. Set the **Prefix** to the value "::/0".
26. In the field **Routing tag** accept the default value "0".

⚠ Not yet functioning in LCOS 8.61 Public Beta 2.

27. In the field **Router**, select from the list the name of the tunnel that you defined earlier, e.g. in the example above "TUNNEL-6TO4".
28. Enter a descriptive **Comment** for this entry.
29. Save your entries with **OK**.

30. Change to the directory **IPv6 > General** and enable the IPv6 stack.



Working with WEBconfig

To set up a 6to4 tunnel with WEBconfig, proceed as follows:

1. Type into your browser's address bar the address of the device to be set up with a 6to4 tunnel.
2. Change to the directory **LCOS Menu Tree > Setup > IPv6 > Tunnel > 6to4** and click on **Add**.

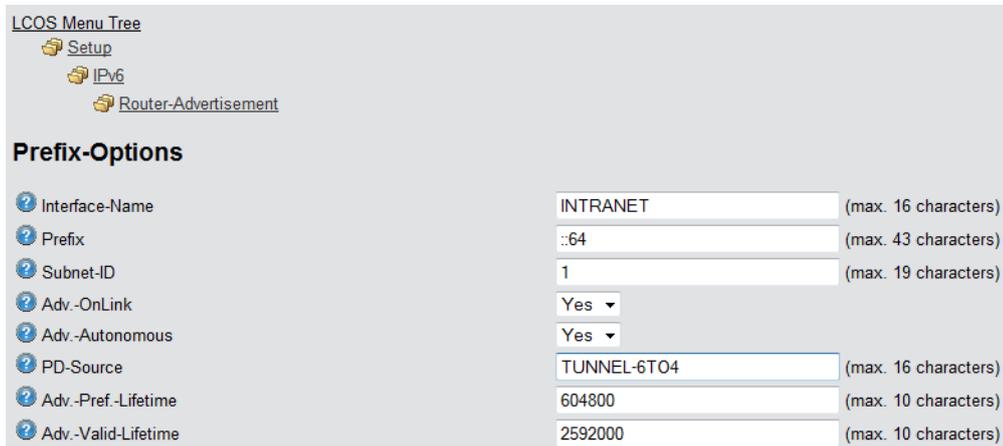
3. Enter a name for the remote peer, e. g. "TUNNEL-6TO4".
4. Leave the **Routing tag** unchanged as the default value "0".

⚠ Not yet functioning in LCOS 8.61 Public Beta 2.

5. As the **Gateway address** you can accept the default value "192.88.99.1". This is the default anycast address for 6to4 relays that your device connects to.

This address is the reason why 6to4 tunnels are unstable and insecure. There is no assurance that a 6to4 relay will be available, and publicly available 6to4 relays may not be trustworthy. There is no guarantee that the relay does not record your traffic.

6. In the field **IPv4-Rtg-tag** accept the default value "0"
7. Enable the **firewall** for this tunnel.
If you disable the global firewall, you should also disable the firewall for the tunnel.
8. Save your entries with **Send**.
9. Change to the directory **LCOS Menu Tree > Setup > IPv6 > Router-Advertisement**, open the **Prefix options** table and click on **Add**.



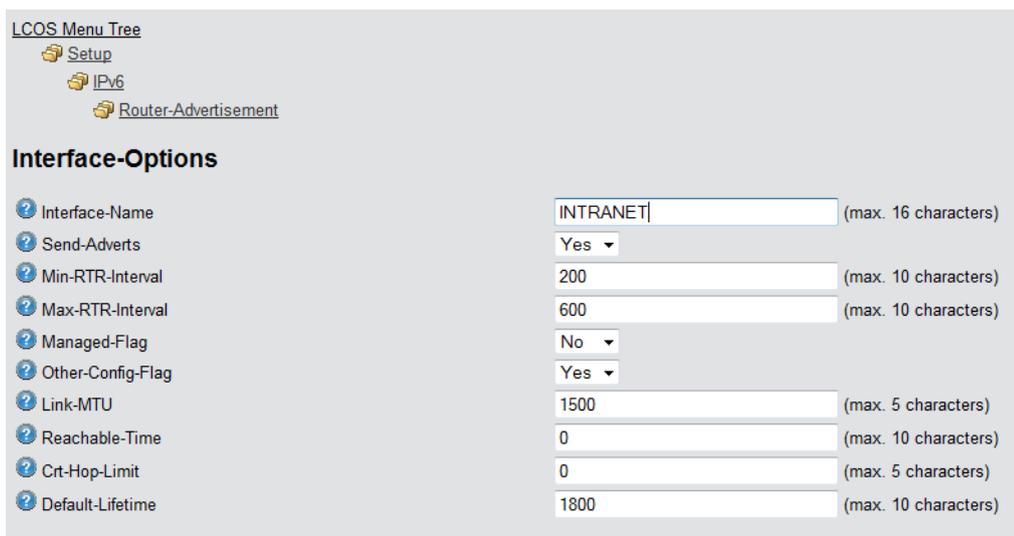
LCOS Menu Tree

- Setup
- IPv6
- Router-Advertisement

Prefix-Options

Interface-Name	<input type="text" value="INTRANET"/>	(max. 16 characters)
Prefix	<input type="text" value=":::64"/>	(max. 43 characters)
Subnet-ID	<input type="text" value="1"/>	(max. 19 characters)
Adv.-OnLink	Yes	
Adv.-Autonomous	Yes	
PD-Source	<input type="text" value="TUNNEL-6TO4"/>	(max. 16 characters)
Adv.-Pref.-Lifetime	<input type="text" value="604800"/>	(max. 10 characters)
Adv.-Valid-Lifetime	<input type="text" value="2592000"/>	(max. 10 characters)

10. Enter a name for the interface that uses the 6to4 tunnel, e. g. "INTRANET".
11. Set the value for the **Prefix** to ">:::64" in order to accept the prefix issued by the provider automatically and in its entirety.
12. Accept the default value of "1" for the **Subnet ID**.
13. Set **PD source** to the name of the remote peer that you previously defined in the example above, e.g. "TUNNEL-6TO4".
14. Save your entries with **Send**.
15. Change to the directory **LCOS Menu Tree > Setup > IPv6 > Router-Advertisement**, open the **Interface options** table and click on **Add**.



LCOS Menu Tree

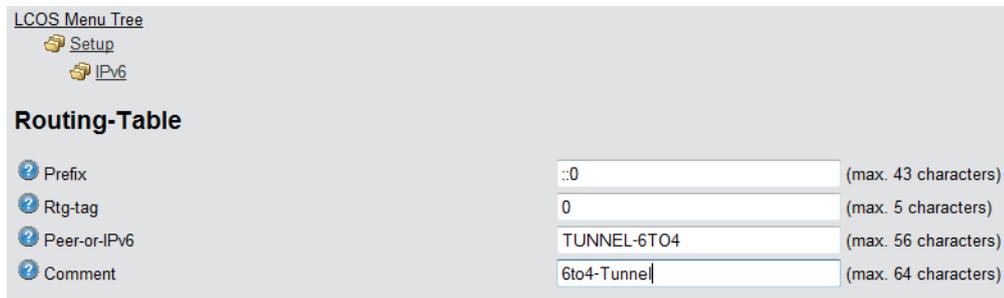
- Setup
- IPv6
- Router-Advertisement

Interface-Options

Interface-Name	<input type="text" value="INTRANET"/>	(max. 16 characters)
Send-Adverts	Yes	
Min-RTR-Interval	<input type="text" value="200"/>	(max. 10 characters)
Max-RTR-Interval	<input type="text" value="600"/>	(max. 10 characters)
Managed-Flag	No	
Other-Config-Flag	Yes	
Link-MTU	<input type="text" value="1500"/>	(max. 5 characters)
Reachable-Time	<input type="text" value="0"/>	(max. 10 characters)
Crt-Hop-Limit	<input type="text" value="0"/>	(max. 5 characters)
Default-Lifetime	<input type="text" value="1800"/>	(max. 10 characters)

16. Accept all other default values without change.
17. Save your entries with **Send**.

18. Change to the directory **LCOS Menu Tree > Setup > IPv6**, open the **Routing table** and click on **Add**.



19. Set the **Prefix** to the value "::/0".

20. In the field **Rtg-tag** accept the default value "0".

ⓘ Not yet functioning in LCOS 8.61 Public Beta 2.

21. In the field **Peer or IPv6**, enter the name of the interface that will use the 6to4 tunnel, e.g. "TUNNEL-6TO4" in the example above.

22. Enter a descriptive **Comment** for this entry.

23. Save your entries with **Send**.

24. Enable the IPv6 stack under **LCOS Menu Tree > Setup > IPv6** by setting the option **Operating** to "yes" and save with **Send**.

