HIRSCHMANN

User Manual

Dual-Band Industrial Access Point / Access Client / Access Bridge
BAT54-Rail

BAT54-Rail
Release 10/06

Technical Support
HAC-Support@hirschmann.de

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in Germany (1006)

Hirschmann Automation and Control GmbH
Stuttgarter Straße 45-51
72654 Neckartenzlingen
Tel. +49 1805 141538

-04-1006

Preface

The Hirschmann BAT54-Rail offers professional access point technology at a maximum of WLAN performance. With two integrated 108 Mbps WLAN modules according to IEEE 802.11a/h or IEEE 802.11b/g the Hirschmann Router work in the 2,4 and/or 5 GHz frequency range simultaneously. The device can be used e.g. for setting up infrastucture networks or for linking two networks in WLAN bridge mode.

The Hirschmann BAT54-Rail is equipped with a robust metal housing for mounting in switch cabinets and is supplied via 24 V voltage. It is hence well suited for application in industrial environments.

Security settings

For a carefree use of your device, we recommend to carry out all security settings (e.g. Firewall, encryption, access protection, charge lock), which are not already activated at the time of purchase of your device. The LANconfig wizard 'Check Security Settings' will support you accomplishing this.

We ask you additionally to inform you about technical developments and actual hints to your product on our Web page www.hirschmann-ac.com, and to download new software versions if necessary.

User manual and reference manual

The documentation of your device consists of three parts: the installation guide, the user manual and the reference manual.

You are now reading the user manual. It contains all information you need to start your device. It also contains the most important technical specification for the device.

The reference manual can be found on the CD as an Acrobat (PDF) document. It is designed as a supplement to the user manual and goes into detail on topics that apply to a variety of devices. These include for example:

- Systems design of the LCOS operating system
- Configuration
- Management
- Diagnosis
- Security
- Routing and WAN functions
- Firewall

- Quality of Service (QoS)
- Virtual Local Networks (VLAN)
- Wireless Networks (WLAN)
- Backup Solutions
- LANCAPI
- Further server services (DHCP, DNS, charge management)

This documentation was compiled …

...by several members of our staff from a variety of departments in order to ensure you the best possible support when using your Hirschmann product.

In case you encounter any errors, or just want to issue critics or enhancements, please do not hesitate to send an email directly to: HAC-support@hirschmann.de

ℹ Our online services (www.hirschmann-ac.com) are available to you around the clock should you have any queries regarding the topics discussed in this manual or require any further support. In addition support from Hirschmann is also available to you. Telephone numbers and contact information for Hirschmann support can be found on a separate insert, or at the Hirschmann website.

Notes symbols	
⚡	Very important instructions. If not followed, damage may result.
!	Important instruction that should be followed.
ℹ	Additional instructions which can be helpful, but are not required.

Contents

1 Introduction

1.1 What is a Wireless LAN?

The following sections describe the functionality of wireless networks in general. The functions supported by your device are listed in the table 'What can your Hirschmann Router do?'. Detailed information on Wireless LANs can be found in the LCOS reference manual.

A Wireless LAN connects single terminals (e.g. PCs or notebooks) to a local network (also LAN – **L**ocal **A**rea **N**etwork). In contrast to a conventional LAN, communication takes place via radio links rather than via network cables. This is the reason why a Wireless LAN is also called a **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

All functions of a cable-bound network are also available in a Wireless LAN: access to files, servers, printers etc. is as possible as the connection of individual stations to an internal mail system or to the Internet access.

The advantages of Wireless LANs are obvious: notebooks and PCs can be set up just where they are needed. Due to Wireless LANs, problems with missing connections or structural alterations belong to the past.

Apart from that, wireless LANs can also be used for connections over longer distances. Expensive leased lines and the associated construction measures can be spared.

1.1.1 Which hardware to use?

Each station of the Wireless LAN needs access to the Wireless LAN in the form of a wireless interface. Devices which have no built-in wireless interface can be upgraded with a supplement card or an adapter.

1.1.2 Operation modes of Wireless LANs and base stations

Wireless LAN technology and base stations in Wireless LANs are used in the following operation modes:

- Simple direct connections between terminals without base station (ad-hoc mode)
- Larger Wireless LANs, connection to LANs with one or more base stations (infrastructure network)
- Setting-up of an Internet access

- Connecting two LANs via a direct radio link (point-to-point mode)
- Connecting of devices with Ethernet interface via base stations (client mode)
- Extending an existing Ethernet network with WLAN (bridge mode)
- Relay function for connecting networks via multiple access points.

1.2 What can your Hirschmann Router do?

The following table shows the properties and functions of your device.

Applications
WLAN via point-to-point and relais mode (2 WLAN modules)
Industrial operation in compact housing for cabinet or rail mounting with 24 V supply (extended temperature range)
Internet access
IP router with Stateful Inspection Firewall
DHCP and DNS server (for LAN and WAN)
WLAN
Wireless transmission by IEEE 802.11g and IEEE 802.11b
Wireless transmission by IEEE 802.11a and IEEE 802.11h
Point-to-point mode (six P2P paths can be defined per WLAN interface)
Relay function to link two P2P connections
Turbo Mode: Double the bandwidth at 2.4 GHz and 5 GHz.
Super AG incl. hardware compression and bursting
Multi SSID
Roaming function
802.11i / WPA with hardware AES encryption
WEP encryption (up to 128 Bit key length, WEP152)
IEEE 802.1x/EAP
MAC address filter (ACL)
Individual passphrases per MAC address (LEPS)
Closed network function
Access to RADIUS server
VLAN
Traffic lock function
LAN connection

Fast Ethernet LAN port (10/100Base-TX)
DHCP and DNS server
WAN connection
Connection for DSL or cable modem
Internet-Zugang (IP-Router)
Stateful Inspection Firewall
Firewall filters (IP addresses, ports)
IP-Masquerading (NAT, PAT)
Quality of Service (QoS)
Power supply
Power-over-Ethernet (PoE) IEEE 802.3af
12 V via seperate power adapter (DC)
24 V (DC) via industrial interface
Redundant power supply via PoE, 12 V or 24 V
Configuration and firmware
Configuration with LANconfig or with web browser, additionally terminal mode for Telnet or other terminal programs, SNMP interface and TFTP server function., SSH connection.
Setup wizards
FirmSafe with firmware versions for absolutely secure software upgrades
Optional software extensions
LANCOM Public Spot Option
Housing
Industrial housing for cabinet or rail mounting

2 Installation

This chapter will assist you to quickly install hardware and software. First, check the package contents and system requirements. The device can be installed and configured quickly and easily if all prerequisites are fulfilled.

2.1 Package contents

Please check the package contents for completeness before starting the installation. In addition to the base station itself, the package should contain the following accessories:

2 dualband antennas with screw connection
2 RP-SMA terminators to avoid interspersions on un-used anntanna connections
4-pin 24 V plug for custom assembly
Connector cable for serial configuration interface
Wall and rail mounting accessories
PoE ethernet cable
Hirschmann CD
Printed documentation

If anything is missing, please contact your retailer or the address stated on the delivery slip of the unit.

2.2 System preconditions

Computers that connect to a Hirschmann Router must meet the following minimum requirements:

- Operating system that supports TCP/IP, e.g. Windows XP, Windows Millennium Edition (Me), Windows 2000, Windows 98, Windows 95, Windows NT, Linux, BSD Unix, Apple Mac OS, OS/2.
- WLAN adapter or access to the LAN (if the access point is connected to the LAN).

The LANtools also require a Windows operating system. A web browser is required for access to WEBconfig.

EN

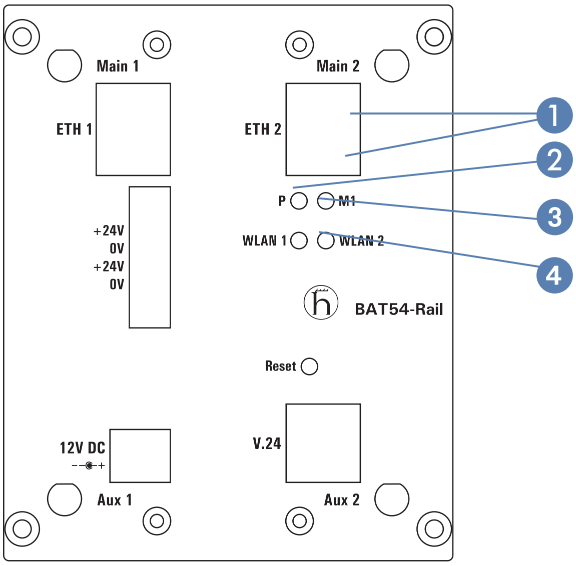
2.3 Status displays, interfaces and hardware installation

Meanings of the LEDs

In the following sections we will use different terms to describe the behaviour of the LEDs:

- **Blinking** means, that the LED is switched on or off at regular intervals in the respective indicated colour.
- **Flashing** means, that the LED lights up very briefly in the respective colour and stay then clearly longer (approximately 10x longer) switched off.
- **Inverse flashing** means the opposite. The LED lights permanently in the respective colour and is only briefly interrupted.
- **Flickering** means, that the LED is switched on and off in irregular intervals.

LEDs of Hirschmann BAT54-Rail



1 ETH 1 and ETH 2

Status of the four LAN ports in the integrated switch:

off		No network device connected
green	constantly on	Connection to network device operational, no data traffic
yellow	flickering	Data traffic

② Power

This LED indicates that the device is operational. After the device has been switched on, it will flash green for the duration of the self-test.

green	constantly on	Device ready for use
red/ green	blinking slow	Device insecure: configuration password not assigned
red	blinking	Time or connect-charge reached
red	blinking (fast)	hardware error

The power LED flashes red when a charge limit is reached ('Flashing Power LED but no connection?' → page 14).

③ M 1

Provides information via the relay contact M1. The relay contact can assume the following conditions:

off		No action
green	constantly on	An action from the action table has been executed successfully, the maker M1 has closed.
red	constantly on	An action from the action table could not be executed successfully, the maker M1 has **not** closed.

Future versions of LCOS are planned to work with relay contacts.

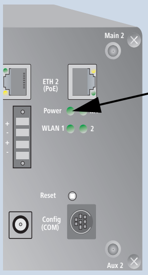
④ WLAN 1
WLAN 2

Gives information about the wireless LAN access and the data traffic of the internal WLAN modules:

off		No wireless networks configured, no beacons beeing broadcasted.
green		At least one wireless network ist configured. The WLAN module is active and broadcasting beacons.
green	invers flashing	Activity in wireless LAN (blinking frequency indicates the number of registered stations)
green	blinking	DFS or other scanning sequence.
green	flickering	TX data traffic
red	flickering	Errot in WLAN (TX error, z.B. sending error because of bad connection quality)
red	blinking	Hardware error in WLAN modulel

Flashing Power LED but no connection?

There's no need to worry if the Power LED blinks red and you can no longer connect to the WAN. This simply indicates that a preset time or connect-charge limit has been reached. There are three methods available for unlocking:



Signal for reached time or connect-charge limit

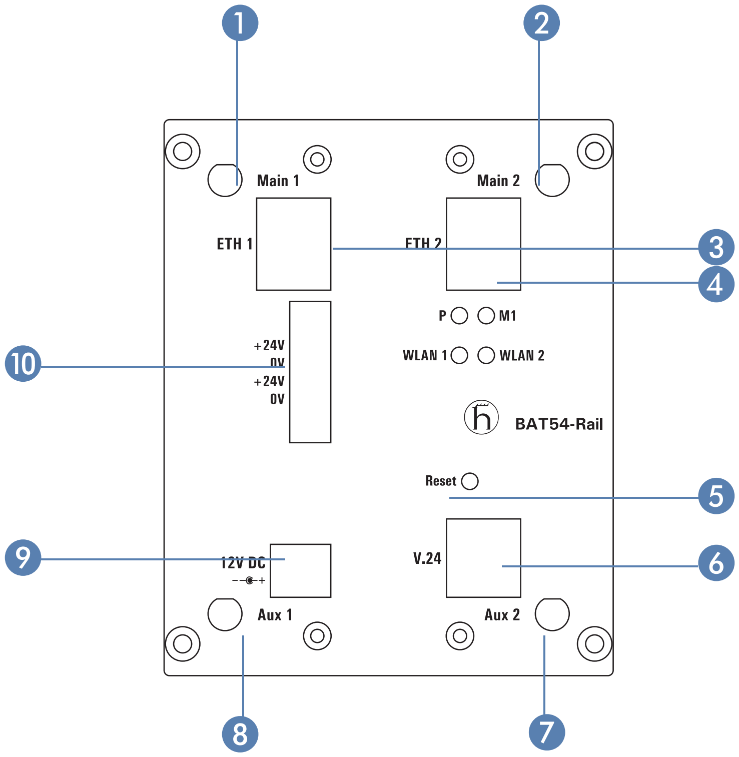
- Reset connect charge protection.
- Increase the limit that has been reached.
- Completely deactivate the lock that has been triggered (set limit to '0').

If a time or connect charge limit has been reached, you will be notified in LANmonitor. To reset the connect charge protection, select **Reset Charge and Time Limits** in the context menu (right mouse click). You can configure the connect charge settings in LANconfig under **Management / Costs** (you will only be able to access this configuration if 'Complete configuration display' is selected under **View / Options...**).

You will find the connect charge protection reset in WEBconfig and all parameters under **Expert Configuration / Setup / Charges-module**.

Interfaces of Hirschmann BAT54-Rail

The interfaces of the Hirschmann BAT54-Rail are located on the front panel.



1 Main connector for first WLAN module.

2 Main connector for second WLAN module.

3 First 10/100Base-Tx for connection to the LAN. Both 10 Mbit or 100 Mbit connections are supported. The available transfer rate is detected automatically (autosensing). The LAN connection features an automatic MDI/MDIX detector enabling the use of cross-over cables.

The LAN connector on the Hirschmann Router access point supports the Power over Ethernet standard (PoE). Further information about the operations with PoE can be found in the information box 'Power over Ethernet—elegant power supply over LAN cabling'.

By activated DSLoL option, the LAN connector can also be used for connecting the access point to a broadband modem.

4 Second ethernet connector.

5 Reset button (see "Reset button functions")

6 Serial configuration port

7 Aux connector for second WLAN modul.

⑧ Aux connector for first WLAN modul.

⑨ Connection for the safety extra-low voltage (SELV/PELV) power adapter

⑩ Connection for 24 V DC safety extra-low voltage (SELV/PELV) via 4-pin plug (Phoenix Contact, Combicon RM 3,81mm). Two 24 V voltage sources can be connected to the redundant power supply.

ⓘ The 24 V input in particular has been optimized for industrial settings. Variation of the input voltage between 20 V to 28 V can be tolerated.

Reset switch of Hirschmann BAT54-Rail

The reset switch has two different functions depending on the length of time that it is pressed:

- □ **Restarting the device** (soft reset) – push the button for less than five seconds. The device will restart.
- □ **Resetting the configuration** (hard reset) – push the button for more than five seconds. All the device's LEDs will light up green and stay on. As soon as the reset switch is released, the device will restart with factory default settings.

! This hard reset causes the device to start with the default factory settings; all previous settings are lost!

ⓘ Note that resetting the device leads to a loss on the WLAN encryption settings within the device and that the default WEP key is active again ('Standard WEP encryption' → page 45).

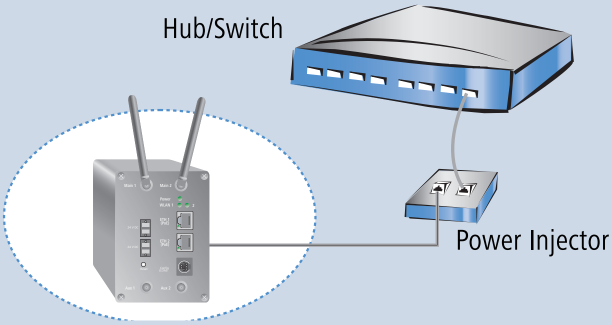
Power-over-Ethernet – elegant power supply through the LAN wiring

Hirschmann access points are prepared for the PoE power supply (Power-over-Ethernet), corresponding to the 802.3af standard. PoE-enabled network devices can be comfortably supplied with power feeding through the LAN wiring. A separate external power supply for each base station is unnecessary, which reduces the the installation complexity considerably.

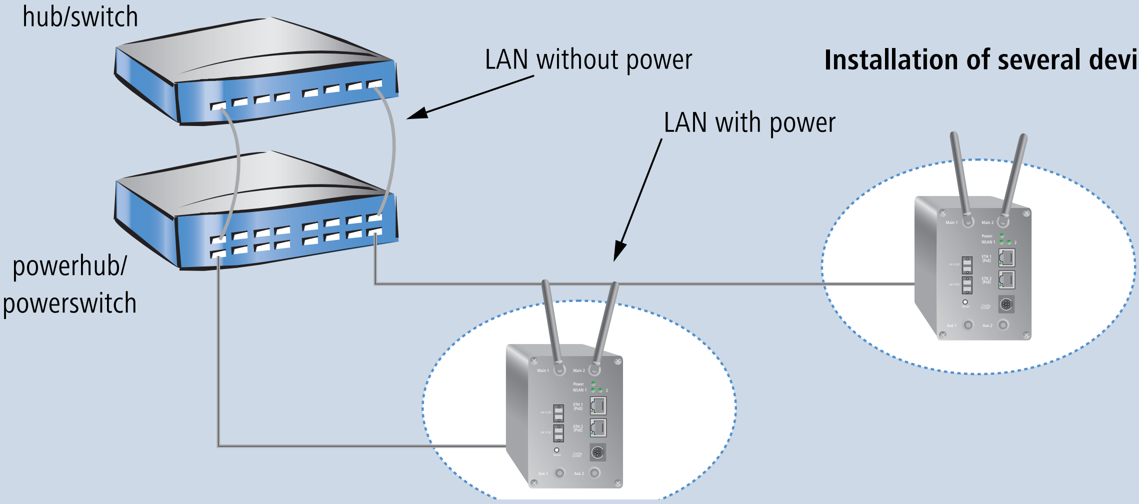
The power feeding into the LAN happens at a central position, either via a PoE power injector, or via a so-called powerhub/powerswitch. For the LAN wiring is to note that all 8 wires must be available by the cabling. PoE feeds the power over those four wires, which are normally not used for data transfer.

The PoE supply works only in such network segments, in which exclusively PoE-capable devices are operating. The protection of network devices without PoE support is guaranteed by an intelligent mechanism, that tests the network segment for devices without PoE support before starting the PoE power feeding. The power is only switched onto the segment, if no devices without PoE support were detected.

Installation of single devices



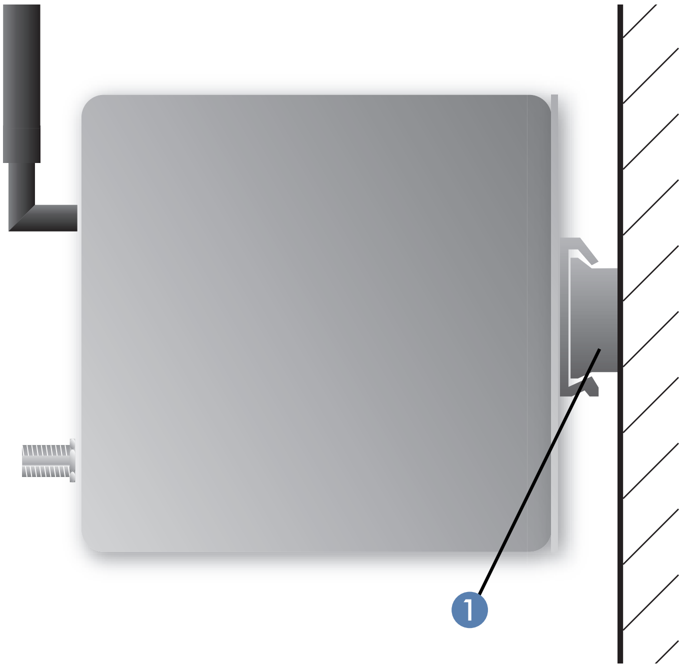
Installation of several devices



In a PoE installation use exclusively devices which corre spond to the 802.3af standard! For damages caused by inadmissible devices no warranty may be claimed.

Top hat rail mounting

① Mount your Hirschmann BAT54-Rail in in the required position on the top hat rail ❶.



Wall mounting

① Place the supplied top hat rail using the screws in the required position on the wall.

② Mount your Hirschmann BAT54-Rail on the top hat rail as described above.

Connecting

Installation of the access point devices involves the following steps:

① **Antennas** —screw the two supplied diversity antennas onto the front side of the device:

- □ Use the individual main connectors to build up sepetae Wireless networks (e.g. for point-to-point applications).
- □ Apply the main and the aux connector of a single WLAN module to use the diversity function. The diversity function increases the quality of the connection by transmitting and receiving via the antenna that provides the best contact to the client.

Unused connectors should be fitted with the terminators as supplied. This prevents stray signals from one WLAN module from interfering with the other WLAN module.

If the device is operated inside a switching cabinet, please take the attenuation caused by the cabinet itself into consideration when selecting the antenna to be used. For applications of this type, we recommend the use of an external antenna. For further information on external antennas and their mountings, please refer to ’’ → page 51.

② **LAN** – You can first connect the access point to your LAN. For that purpose, plug the included network cable (green plugs) into the LAN connector of the device ❸ or ❹ and the other end into a free network connecting socket of your local network (resp. into a free socket of a hub/ switch). Alternatively, you can connect also a single PC.

The LAN connector identifies automatically the transfer rate (10/100 Mbp) of the connected network device (autosensing).

For information about the installation of PoE see the info box ’Power-over-Ethernet – elegant power supply through the LAN wiring’ → page 17.

③ **DSLoL** – If you want to use your access point in DSLoL mode, you can either connect the device directly to the DSL modem (exclusive mode) or to a hub resp. switch of the cable-bound LAN (automatic mode).

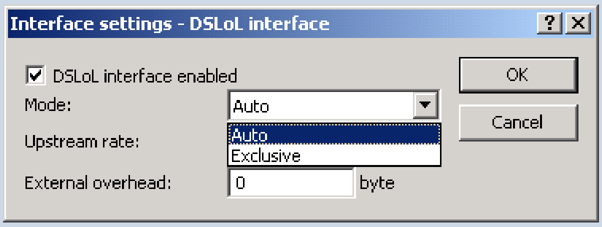
- □ For the exclusive mode insert the included network cable (green plugs) into the LAN connector of the device ❸ or ❹ and the other end into the corresponding interface of the DSL modem.
- □ For the automatic mode for simultaneous operating with LAN and DSLoL insert the included network cable (green plugs) into the LAN connector of the device ❸ or ❹ and the other end into a free network connecting socket of your local network (resp. into a free socket of a hub/switch).

④ Connect up the power supply – There are three options for supplying power to the Hirschmann BAT54-Rail:

- □ Use a safety extra-low voltage (SELV/PELV) power supply unit to provide the device with power via connector ❾.

LAN interface: exclusive or in parallel for DSLoL

There are two principle DSLoL operation modes available. Either use the exclusive mode when connecting your Hirschmann Router directly to a DSL modem, or use the automatic mode when connecting the Hirschmann Router to a hub or switch of a cable-bound LAN, and connect this hub/switch again to the DSL modem. If the Hirschmann Router is broadcasted as gateway via DHCP, computers in LAN and WLAN can use the internet connection **simultaneously** via one physical interface. Set the desired mode in LANconfig in the Interface settings of the DSLoL interface.


Interface settings - DSLoL interface

☑ DSLoL interface enabled

Mode: Auto

Upstream rate:

External overhead: 0 byte

DSLoL supports all PPPoE-based Internet access lines, as well as those that are supplied with a access router with multiple fixed IP addresses (such as many SDSL business lines).

The use of the wrong power supply unit can be of danger to the device or persons.

□ For power supplied via the Ethernet cable (PoE), use the device's LAN connectors 3 or 4. Information about the installation of PoE can be found in the information box 'Power-over-Ethernet – elegant power supply through the LAN wiring' → page 17

The PoE supply for the Hirschmann BAT54-Rail is equipped for redundancy, i.e. both LAN interfaces can be supplied by separate PoE Injectors.

□ Provide power to the device via one of the 24 V plug connectors 10. Use the supplied 24 V plug (wiring described in the Appendix) or another suitable 24 V plug (Phoenix Contact, Combicon RM 3.81mm).

The 24 V supply for the Hirschmann BAT54-Rail is equipped for redundancy, i.e. both 24 V connectors can be supplied by separate power supplies.

Multiple power sources can be connected in any combination, which ensures that the power supply is redundant and fail safe. The device itself selects the power source to be used.

If a power outage causes a switch between power sources, the device reboots so that the power feed is reactivated, if appropriate.

⑤ **Operational?** – After a short device self-test the Power LED will be permanently lit green resp. will blink alternately red and green as long as no configuration password has been given.

2.4 Software installation

This section covers the installation of the included system software LANtools for Windows.

You may skip this section if you use your Hirschmann Router exclusively with computers running operating systems other than Windows.

2.4.1 Which software should you install?

- **LANconfig** is the configuration program for all Hirschmann routers and Hirschmann Router base stations. WEBconfig can be used alternatively or in addition via a web browser.
- **LANmonitor** lets you monitor on a Windows PC all Hirschmann routers and Hirschmann Router base stations
- **Hirschmann Online Documentation:** Copy the documentation files on your PC.

3 Basic configuration

The basic configuration can be performed on a step-by-step basis using a convenient setup wizard to guide you through the setup process and prompt you for the required information.

First, this chapter will tell you which information is required for the basic configuration. Use this section to assemble the information you will need before you launch the wizard.

Next, enter the data in the setup wizard. Launching the wizard and the process itself are described step by step — with separate sections for LANconfig and WEBconfig. Thanks to the information that you have collected in advance, the basic configuration is quick and effortless.

At the end of this chapter we will show you the settings that are needed for the LAN's workstations to ensure trouble-free access to the router.

3.1 Which information is necessary?

The basic configuration wizard will take care of the basic TCP/IP configuration of the router and protect the device with a configuration password. The following descriptions of the information required by the wizard are grouped in these configuration sections:

- TCP/IP settings
- protection of the configuration
- information related to the Wireless LAN
- information on DSL connection
- configuring connect charge protection
- security settings

3.1.1 TCP/IP settings

The TCP/IP configuration can be realized in two ways: either as a fully automatic configuration or manually. No user input is required for the fully automatic TCP/IP configuration. All parameters are set automatically by the setup wizard. During manual TCP/IP configuration, the wizard will prompt you for the usual TCP/IP parameters: IP address, netmask etc. (more on these topics later).

Fully automatic TCP/IP configuration is only possible in certain network environments. The setup wizard therefore analyses the connected LAN to determine whether it supports fully automatic configuration.

New LAN—fully automatic configuration possible

If all connected network devices are still unconfigured, the setup wizard will suggest fully automatic TCP/IP configuration. This may be the case in the following situations:

- a single PC is connected to the router
- setup of a new network

Fully automatic TCP/IP configuration will not be available when integrating the Hirschmann Router in an existing TCP/IP LAN. In this case, continue with the section ’Information required for manual TCP/IP configuration’.

The result of the fully automatic TCP/IP configuration: the router will be assigned the IP address '172.23.56.1' (netmask '255.255.255.0'). In addition, the integrated DHCP server will be enabled so that the Hirschmann Router can automatically assign IP addresses to the devices in the LAN.

Configure manually nevertheless?

The fully automatic TCP/IP configuration is optional. You may also select manual configuration instead. Make your selection after the following considerations:

- Choose automatic configuration if you are **not** familiar with networks and IP addresses.
- Select manual TCP/IP configuration if you are familiar with networks and IP addresses, and one of the following conditions is applicable:
  - □ You have not yet used IP addresses in your network but would like to do so now. You would like to specify the IP address for your router, selecting it from the address range reserved for private use, e.g. '10.0.0.1' with the netmask '255.255.255.0'. At the same time you will set the address range that the DHCP server uses for the other devices in the network (provided that the DHCP server is switched on).
  - □ You have previously used IP addresses for the computers in your LAN.

Information required for manual TCP/IP configuration

During manual TCP/IP configuration, the setup wizard will prompt you for the following information:

- **IP address and netmask for the Hirschmann Router**
  Assign a free IP address from the address range of your LAN to the Hirschmann Router and specify the netmask.
- **Enable DHCP server?**
  Disable the DHCP server function in the Hirschmann Router if you would like to have a different DHCP server assign the IP addresses in your LAN.

3.1.2 Configuration protection

The password for configuration access to the Hirschmann Router protects the configuration against unauthorized access. The configuration of the router contains a considerable amount of sensitive information such as your Internet access information. We therefore strongly recommend protecting it with a password.

> ⓘ Multiple administrators can be set up in the configuration of the Hirschmann, each with differing access rights. For a Hirschmann, up to 16 different administrators can be set up. Further information can be found in the section 'Managing rights for different administrators' in the LCOS reference manual.

3.1.3 Settings for the Wireless LAN

The network name (SSID)

The basic configuration wizard asks for the network name of the base station (often designated as SSID – **S**ervice **S**et **Id**entifier). The network name will be registered in the base stations of the Wireless LAN. You can choose any name. Several base stations with the same network name form a common Wireless LAN.

> ⓘ As of LCOS version 4.0, WEP128 encryption is activated for every unconfigured device as standard. Further information can be found in the LCOS reference manual under "Standard WEP encryption".

Open or closed Wireless LAN?

Mobile radio stations dial-in the wanted Wireless LAN by declaration of the network name. The specification of the network name is facilitated by two technologies:

- Mobile radio stations can search for Wireless LANs in the environs („scan“) and offer for selection the found Wireless LANs in a list.

- By using the network name 'ANY', the mobile radio station will enrol in the next available Wireless LAN.

The Wireless LAN can be „closed“ to prevent this procedure. In this case, no enrolment with the network name 'ANY' will be accepted.

For standard, Hirschmann base stations are responsive under the network name 'Hirschmann'. The wireless basic configuration of a base station takes therefore place via this network name. If another network name is set during the basic configuration, also the Wireless LAN access of the configuring mobile base station must be changed to this new network name after closing the basic configuration.

Selection of a radio channel

The base station operates in a certain radio channel. The radio channel will be selected from a list of up to 11 channels in the 2,4 GHz frequency range or up to 19 channels in the 5 GHz frequency range. (in various countries some radio channels are restricted, see appendix).

The used channel and frequency range define the operating of the common radio standard, in doing so the 5 GHz frequency range correspond to the IEEE 802.11a/h standard and the 2,4 GHz frequency range to the IEEE 802.11g and IEEE 802.11b standard.

If no further base stations operate in reach of the base station, any radio channel can be adjusted. Otherwise, the channels in the 2,4 GHz band must be chosen in the way that they preferably do not overlap one another or have a distance as great as possible respectively. The automatic setting is normally enough in the 5 GHz band, in which the Hirschmann Router base station itself adjust the best channel via TPC and DSF.

3.1.4 Settings for the DSL connection

For the WAN connection it may be necessary to enter the transfer protocol being used. The wizard will e.g. automatically enter the correct settings for major DSL providers. You only need to enter the protocol used by your access provider if the wizard does not list your provider.

3.1.5 Connect charge protection

Connect charge protection blocks DSL connections that go beyond a previously set limit, thus protecting you from unexpectedly high connection charges.

If you run the Hirschmann Router via DSL access with a flat-rate tariff, you can set the maximum connecting-time in minutes.

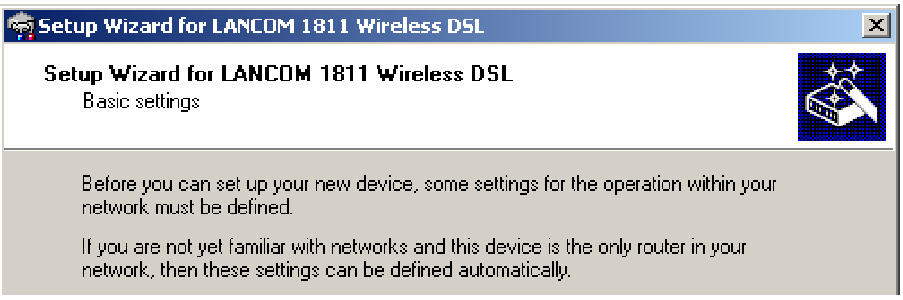
Any budget can be deactivated by entering the value '0.'

In basic settings the charge protection is defined to maximum 600 minutes within seven days. Adapt this setting to your personal needs or deactivate the charge protection if you have arranged a flatrate with your provider.

3.2 Instructions for LANconfig

① Start up LANconfig by clicking **Start** ▶ **Programme** ▶ **Hirschmann** ▶ **LANconfig**

LANconfig automatically detects the new Hirschmann Router in the TCP/IP network. Then the setup wizard starts that will help you make the basic settings of the device or will even do all the work for you (provided a suitable network environment exists).



Setup Wizard for LANCOM 1811 Wireless DSL
Basic settings

Before you can set up your new device, some settings for the operation within your network must be defined.

If you are not yet familiar with networks and this device is the only router in your network, then these settings can be defined automatically.

If you cannot access an unconfigured Hirschmann Router, the problem may be due to the netmask of the LAN: with less than 254 possible hosts (netmask > '255.255.255.0'), please ensure that the IP address 'x.x.x.254' is located in your own subnet.

If you have chosen automatic TCP/IP configuration, please continue with Step ④.

② If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the Hirschmann Router. Confirm your choice with **Next**.

③ Specify whether or not the router should act as a DHCP server. Make your selection and confirm with **Next**.

④ In the following window, specify the password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

In addition, you may specify whether the device may only be configured from the local network or whether remote configuration via the WAN (i.e. a remote network) is also permissible.

ⓘ Please note that enabling this will also permit remote configuration via the Internet. You should always make sure that the configuration access is protected with a password.

⑤ Enter the wireless parameters. Select a network name (SSID) and a radio channel. Turn on if necessary the function for ’closed network’. Confirm your choice with **Next**.

⑥ In the next window, select your DSL provider from the list that is displayed. If you select 'My provider is not listed here,' you must enter the transfer protocol used by your DSL provider manually. Confirm your choice with **Next**.

⑦ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Next**.

⑧ Complete the configuration with **Finish**.

ⓘ Section 'TCP(IP settings to workstation PCs' will describe the settings required for the individual workstations in the LAN.

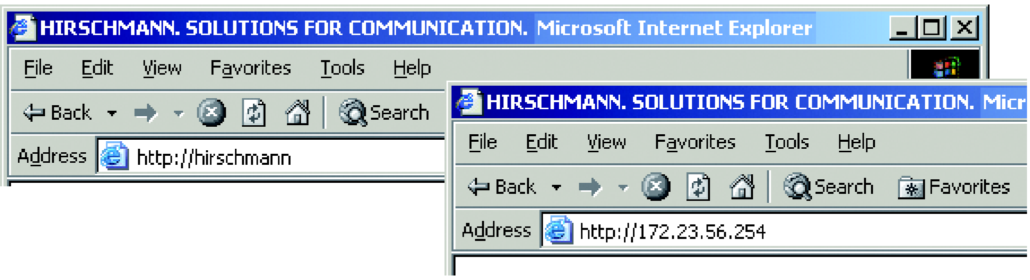
3.3 Instructions for WEBconfig

To configure the router with WEBconfig you must know how to address it in the LAN. The reaction of the devices, as well as their accessibility for configuration via web browser is dependent on whether a DHCP server and a DNS server are already active in the LAN, and whether these two server processes exchange the assignment of IP addresses to symbolic names within the LAN between each other.

After powered on, unconfigured Hirschmann devices check first, whether a DHCP server is already active in the LAN. Dependent on the situation, the device is able to switch on its own DHCP server or, alternatively, to activate its DHCP client mode. In this second operating mode, the device itself can obtain an IP address from a DHCP server already existing in the LAN.

Network without DHCP server

In a network without DHCP server, unconfigured Hirschmann devices activate their own DHCP server service after starting, and assign appropriate IP addresses and gateway information to the other workstations within the LAN, provided that the workstations are set to obtain their IP address automatically (auto-DHCP). In this constellation, the device can be accessed with any web browser from each PC with activated auto-DHCP function through the name **Hirschmann** or by its IP address **172.23.56.254**.


HIRSCHMANN. SOLUTIONS FOR COMMUNICATION. Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search
HIRSCHMANN. SOLUTIONS FOR COMMUNICATION. Micr
File Edit View Favorites Tools Help
Back Search Favorites

Address http://hirschmann

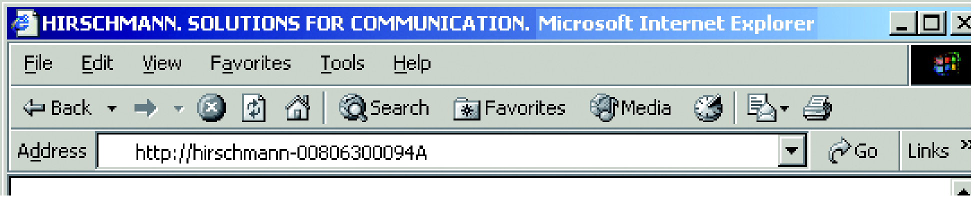
Address http://172.23.56.254

If the configuration PC does not obtain its IP address from the Hirschmann DHCP server, figure out the current IP address of this PC (with **Start** ▶ **Execute** ▶ **cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start** ▶ **Execute** ▶ **cmd** and the command **winipcfg** at the prompt under Windows Me and Windows 9x, or with the command **ifconfig** on the console under Linux). In this case, the Hirschmann is reachable under the IP address **x.x.x.254** (“x” stands for the first three blocks in the IP address of the configuration PC).

Network with DHCP server

If a DHCP server is active in the LAN to assign IP addresses, an unconfigured Hirschmann device will turn off its own DHCP server. It will change into DHCP client mode and will obtain an IP address from the DHCP server of the LAN. This IP address is not known at first. The accessibility of the device depends on the name resolution:

- If there is a DNS server for name resolution in the LAN, which interchanges the assignment of IP addresses to names with the DHCP server, then the device can be accessed by the name “Hirschmann <MAC address>” (e.g. “Hirschmann-008063xxxxxx”).


HIRSCHMANN. SOLUTIONS FOR COMMUNICATION. Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go
Links

Address http://hirschmann-00806300094A

ⓘ The MAC address can be found on a label at the bottom of the device.

- If there is no DNS server in the LAN, or it is not linked to the DHCP server, then the device can not be reached by the name. The following options remain in this case:
  - □ Figure out the DHCP-assigned IP address of the Hirschmann by suitable tools and contact the device directly with this IP address.
  - □ Use LANconfig.
  - □ Connect a PC with a terminal program via the serial configuration interface to the device.

Starting the wizards in WEBconfig

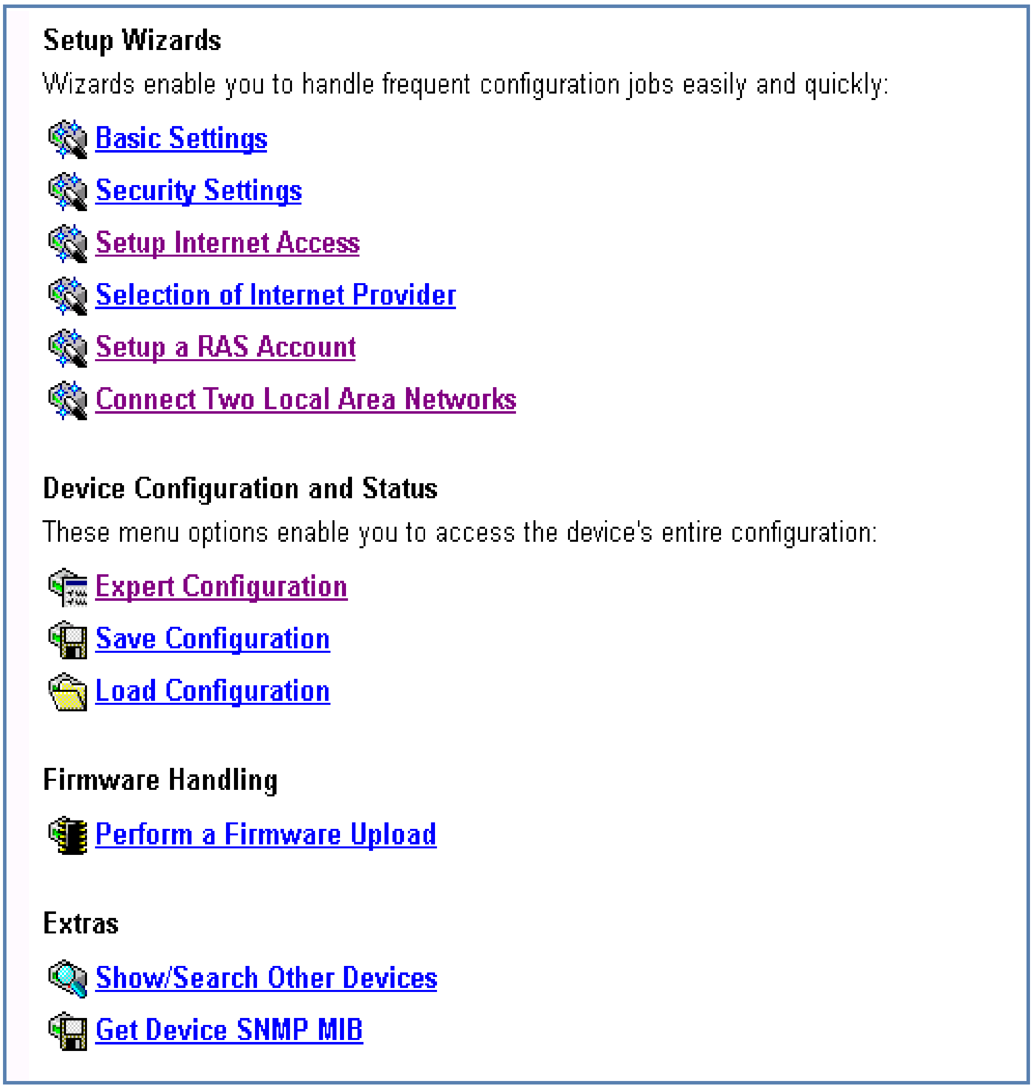
① Start your web browser (e.g. Internet Explorer, Netscape Navigator, Opera) and call the Hirschmann Router there:

```
http://<IP address of the Hirschmann device>
```

(or with a name as discribed above)

ⓘ If you cannot access an unconfigured Hirschmann Router, the problem may be due to the netmask of the LAN: with less than 254 possible hosts (netmask > '255.255.255.0'), please ensure that the IP address 'x.x.x.254' is located in your own subnet.

The WEBconfig main menu will be displayed:



Setup Wizards

Wizards enable you to handle frequent configuration jobs easily and quickly:

- Basic Settings
- Security Settings
- Setup Internet Access
- Selection of Internet Provider
- Setup a RAS Account
- Connect Two Local Area Networks

Device Configuration and Status

These menu options enable you to access the device's entire configuration:

- Expert Configuration
- Save Configuration
- Load Configuration

Firmware Handling

- Perform a Firmware Upload

Extras

- Show/Search Other Devices
- Get Device SNMP MIB

The setup wizards are tailored precisely to the functionality of the specific Hirschmann Router. As a result, your device may offer different wizards than those shown here.

If you have chosen automatic TCP/IP configuration, please continue with Step ③.

② If you would like to configure the TCP/IP settings manually, assign an available address from a suitable address range to the Hirschmann Router. Also set whether or not it is to operate as a DHCP server. Confirm your entry with **Apply**.

③ Enter the wireless parameters. Select a network name (SSID) and a radio channel. Turn on if necessary the function for ’closed network’. Confirm your choice with **Next**.

④ In the following 'Security settings' window, specify a password for configuration access. Note that the password is case-sensitive and ensure that it is sufficiently long (at least 6 characters).

You may specify whether the device may only be configured from the local network or whether remote configuration via the WAN (i.e. a remote network) is also permissible.

Please note that enabling this will also permit remote configuration via the Internet. You should always make sure that the configuration access is suitably protected, e.g. with a password.

⑤ In the next window, select your DSL provider from the list that is displayed. Confirm your choice with **Apply**.

If you select 'My provider is not listed here,' you must enter the transfer protocol used by your DSL provider manually in the next window. Confirm your choice with **Apply**.

⑥ Connect charge protection can limit the cost of DSL connections to a predetermined amount if desired. Confirm your choice with **Apply**.

⑦ The basic setup wizard reports that all the necessary information has been provided. You can end the wizard with **Go on**.

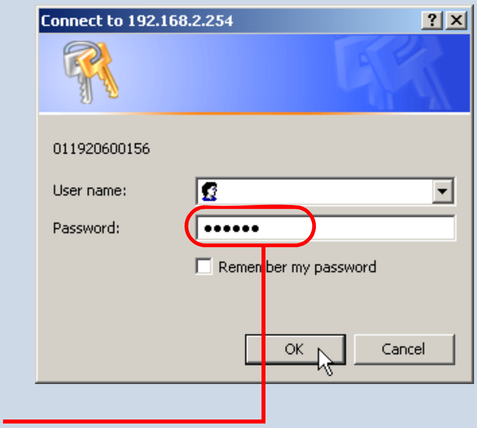
3.4 TCP/IP settings to workstation PCs

The correct addressing of all devices within a LAN is extremely important for TCP/IP networks. In addition, all computers must know the IP addresses of two central points in the LAN:

Entering the password in the web browser

When you are prompted for a user name and password by your web browser when accessing the device in the future, enter your personal values to the corresponding fields. Please note that the password is case-sensitive.

If you are using the common configuration account, enter the corresponding password only. Leave the user name field blank.


Connect to 192.168.2.254

011920600156

User name:

Password: ••••••

□ Remember my password

Entering the configuration password

- Default gateway – receives all packets that are not addressed to computers within the local network.
- DNS server – translates network names or names of computers to actual IP addresses.

The Hirschmann Router can perform the functions of both a default gateway and a DNS server. In addition, as a DHCP server it can also automatically assign valid IP addresses to all of the computers in the LAN.

The correct TCP/IP configuration of the PCs in the LAN depends on the method used to assign IP addresses within the LAN:

- **IP address assignment via the Hirschmann Router (default)**

  In this operating mode the Hirschmann Router not only assigns IP addresses to the PCs in the LAN, it also uses DHCP to specify its own IP address as that of the default gateway and DNS server. The PCs must therefore be configured so that they automatically obtain their own IP address and the IP addresses of the standard gateway and DNS server (via DHCP).

- **IP address assignment via a separate DHCP server**

  The workstation PCs must be configured so that they automatically obtain their own IP address and the IP addresses of the standard gateway and DNS server (via DHCP). The IP address of the Hirschmann Router must be stored on the DHCP server so that the DHCP server transmits it to the PCs in the LAN as the standard gateway. In addition, the DHCP server should also specify the Hirschmann Router as a DNS server.

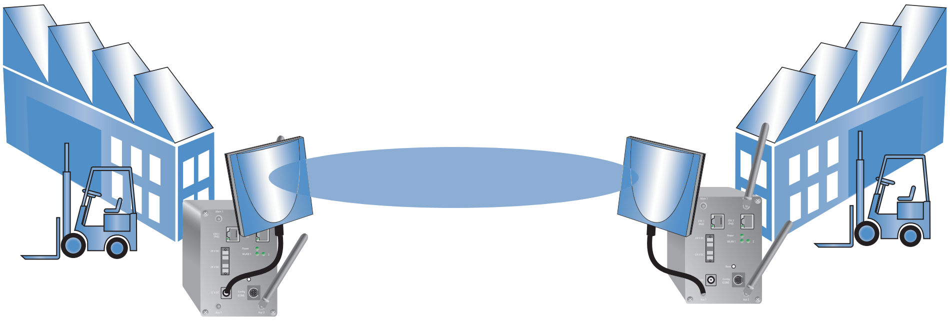
- **Manual IP address assignment**

  If the IP addresses in the network are assigned static ally, then for each PC the IP address of the Hirschmann Router must be set in the TCP/IP configuration as the standard gateway and as a DNS server.

For further information and help on the TCP/IP settings of your Hirschmann Router, please see the reference manual. For more information on the network configuration of the workstation computers, please refer to the documentation of your operating system.

4 Point-to-point connections

Hirschmann Wireless access points serve not only as central stations within a wireless network, they can also operate in point-to-point mode to bridge longer distances. For example, they can provide a secure connection between two networks that are several kilometers apart—without direct cabling or expensive leased lines.

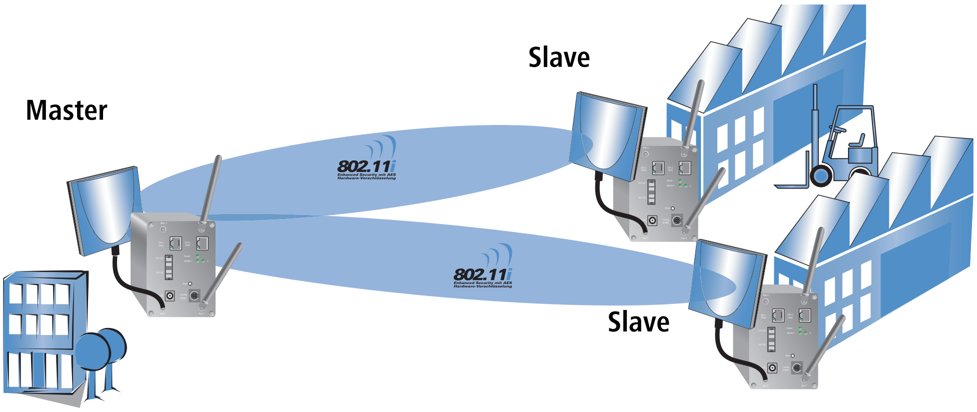


The behavior of an access point when exchanging data with other access points is defined in the "Point-to-point operation mode".

- **Off:** The access point only communicates with mobile clients
- **On:** The access point can communicate with other access points and with mobile clients
- **Exclusive:** The access point only communicates with other base stations

In the 5 -GHz band, the automatic search for vacant WLAN channels can lead to several simultaneous test transmissions from multiple access points, with the result that they do not find each other. This stalemate situation can be avoided with the appropriate "Channel selection scheme":

- **Master:** This access point takes over the leadership when selecting a free WLAN channel.
- **Slave:** All other access points will search for a channel until they have found a transmitting Master.

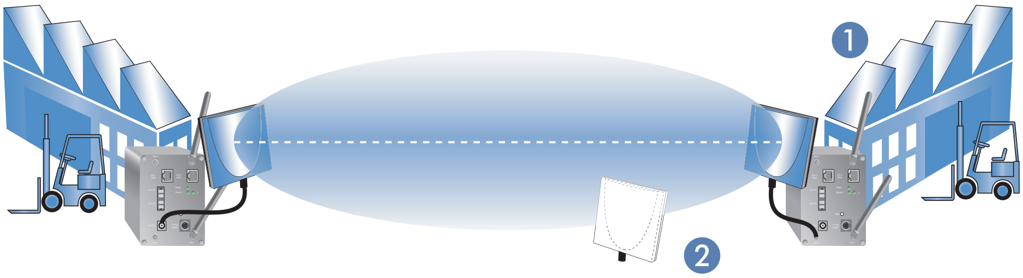


Thus it is recommended for the 5 GHz band that one central access point should be configured as 'Master' and all other point-to-point partners should be configured as 'Slave'. In the 2.4 GHz band, too, this setting simplifies the establishment of point-to-point connections if the automatic channel search is activated.

ⓘ It is imperative that the channel selection scheme is configured correctly if the point-to-point connections are to be encrypted with 802.11i/WPA.

4.1 Antenna alignment for P2P operations

The precise alignment of the antennas is of considerable importance in establishing a P2P path. The more central the receiving antenna is located in the "ideal line" of the transmitting antenna, the better is the actual performance and the effective bandwidth ❶. If the receiving antenna is outside of this ideal area, however, significant losses in performance will be the result ❷.



ⓘ Further information about the geometrical alignment of wireless paths and the alignment of antennas with the help of Hirschmann software can be found in the LCOS reference manual.

4.2 Configuration

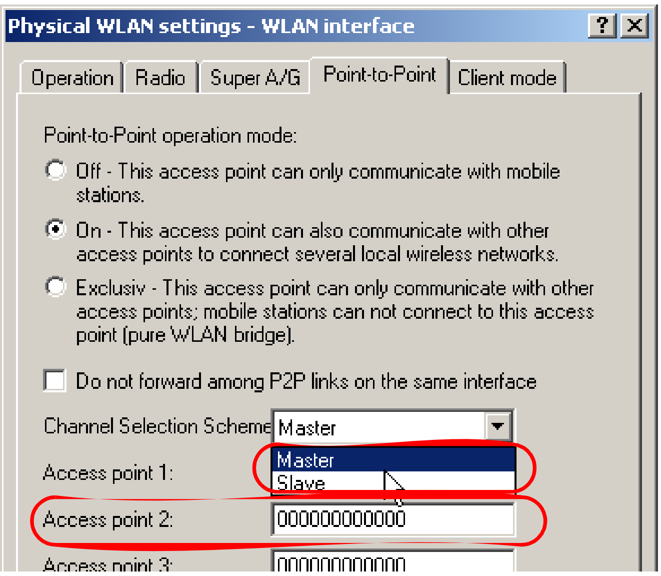
In the configuration of point-to-point connections, entries have to be made for the point-to-point operation mode, the channel selection scheme and the MAC addresses of the remote sites.

Configuration with LANconfig

For configuration with LANconfig you will find the settings for P2P connections under the configuration area 'Interfaces' on the 'Wireless LAN' tab.

① Click on the button **Physical WLAN settings** to open the corresponding WLAN interface and select the tab for 'Point-to-Point'.

② Activate the suitable point-to-point operation mode here and set the channel selection scheme to either 'Master' or 'Slave'. Enter the appropriate MAC address for the WLAN card at the remote station (maximum 6).



Physical WLAN settings - WLAN interface

Point-to-Point operation mode:

○ Off - This access point can only communicate with mobile stations.

● On - This access point can also communicate with other access points to connect several local wireless networks.

○ Exclusiv - This access point can only communicate with other access points; mobile stations can not connect to this access point (pure WLAN bridge).

□ Do not forward among P2P links on the same interface

Channel Selection Scheme: Master

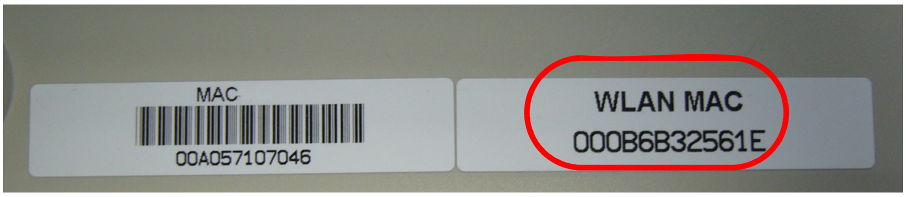
Access point 1:

Access point 2: 000000000000

Access point 3: 000000000000

Please observe that only the MAC addresses of the WLAN cards at the other end of the connections are to be entered here! Not the access point's own MAC address, and not the MAC addresses from any other interfaces that may be present in the access points.

You will find the WLAN MAC address on a sticker below the corresponding antenna connector. Only use the string that is marked as the "WLAN MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.



Alternatively you will find the MAC addresses for the WLAN cards in the devices under WEBconfig, Telnet or a terminal program under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Status ▶ WLAN-statistics ▶ Interface-statistics
Terminal/Telnet	`Status/WLAN-statistics/Interface-statistics`

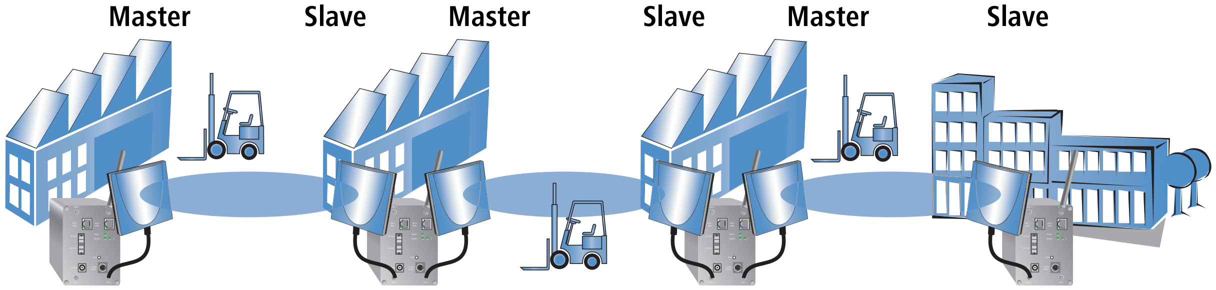
Configuration with WEBconfig or Telnet

Under WEBconfig or Telnet you can set the settings for the point-to-point connections under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces▶ Interpoint-Settings
Terminal/Telnet	`cd /Setup/Interfaces/WLAN-Interfaces/Interpoint-Settings`

4.3 Access points in relay mode

Access points equipped with two wireless modules can be used to establish wireless bridges across multiple stations. Each wireless module is configured as a 'Master' and then 'Slave' in turn.



The use of relay stations each equipped with two WLAN modules simultaneously solves the problem of the "hidden station", by which the MAC addresses of the WLAN clients are not transferred over multiple stations.

4.4 Security for point-to-point connections

IEEE 802.11i can be used to attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the LANCOM Enhance Passphrase Security (LEPS).

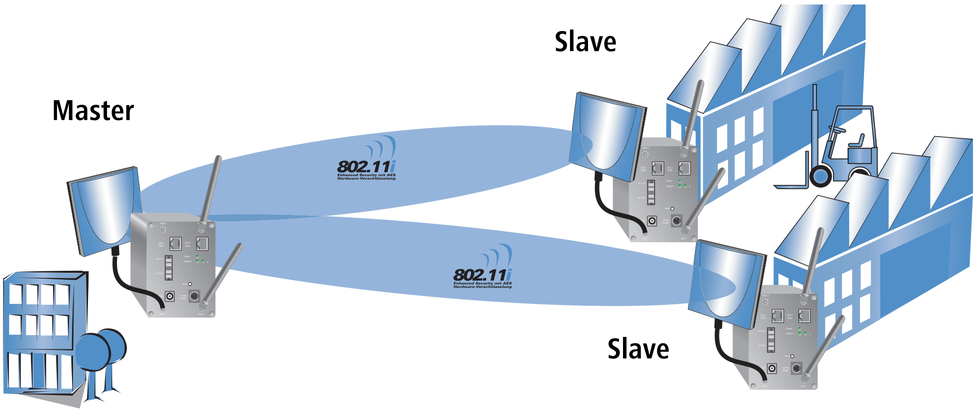
4.4.1 Encryption with 802.11i/WPA

To activate the 802.11i encryption for a correctly configured P2P connection, adjust the settings for the first logical WLAN network in the appropriate WLAN interface (i.e. WLAN-1 if you are using the first WLAN card for the P2P connection, WLAN-2 if you are using the second card, e.g. as with an access point with two WLAN modules).

- Activate the 802.11i encryption.
- Select the method '802.11i (WPA)-PSK'.
- Enter the passphrase to be used.

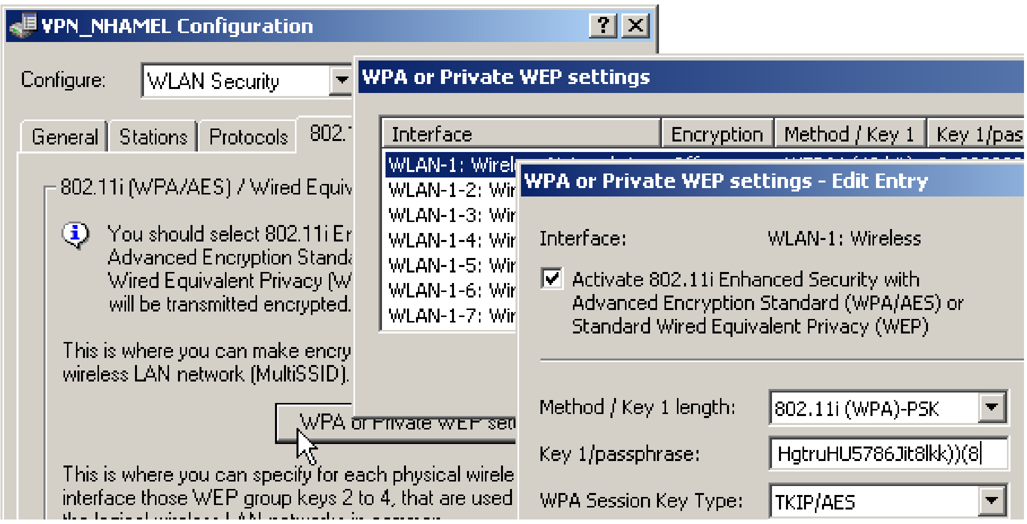
The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the access point transfers this information to register with the remote site.



Configuration with LANconfig

For configuration with LANconfig you will find the encryption settings under the configuration area 'WLAN Security' on the '802.11i/WEP' tab.



Configure: WLAN Security

802.11i (WPA/AES) / Wired Equiv

You should select 802.11i Er
Advanced Encryption Stand
Wired Equivalent Privacy (W
will be transmitted encrypted.

This is where you can make encry
wireless LAN network (MultiSSID).

This is where you can specify for each physical wirele
interface those WEP group keys 2 to 4, that are used

Interface: WLAN-1: Wireless

☑ Activate 802.11i Enhanced Security with Advanced Encryption Standard (WPA/AES) or Standard Wired Equivalent Privacy (WEP)

Method / Key 1 length: 802.11i (WPA)-PSK

Key 1/passphrase: HgtruHU5786Jit8lkk))(8

WPA Session Key Type: TKIP/AES

Configuration with WEBconfig or Telnet

The encryption settings for the individual logical WLAN networks can be found under WEBconfig or Telnet under the following paths:

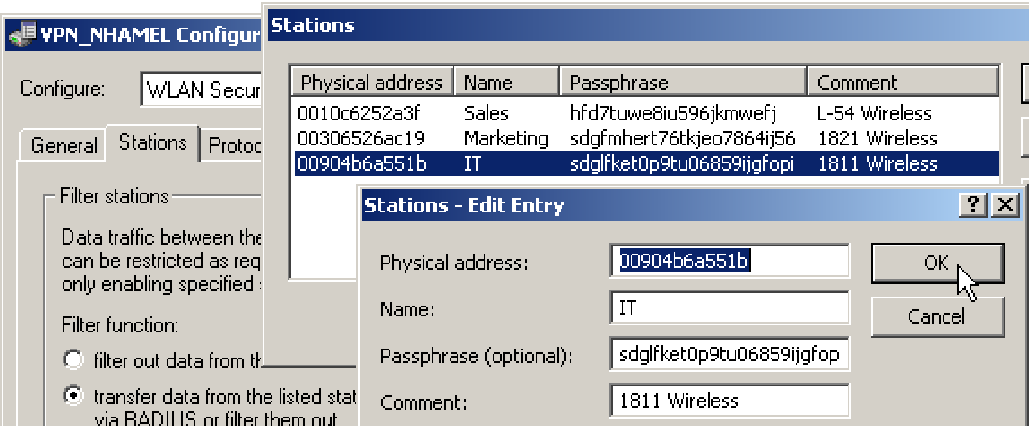
Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ Interfaces ▶ WLAN-Interfaces ▶ Encryption-Settings
Terminal/Telnet	`/Setup/Interfaces/WLAN-Interfaces/Encryption-Settings`

4.4.2 LEPS for P2P connections

A further gain in security can be attained by additionally using LANCOM Enhanced Passphrase Security (LEPS) which involves the matching of MAC address and passphrase.

LEPS can be used to secure single point-to-point (P2P) connections with an individual passphrase. Even if an access point in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS remain secure, particularly when the ACL is stored on a RADIUS server.

When using LANconfig for the configuration, you enter the passphrases of the stations approved for the WLAN in the configuration area 'WLAN Security' on the 'Stations' tab under the button **Stations**.



Filter stations

Data traffic between the can be restricted as req only enabling specified

Filter function:

○ filter out data from th

● transfer data from the listed stat via RADIUS or filter them out

Physical address	Name	Passphrase	Comment
0010c6252a3f	Sales	hfd7tuwe8iu596jkmwefj	L-54 Wireless
00306526ac19	Marketing	sdgfmhert76tkjeo7864ij56	1821 Wireless
00904b6a551b	IT	sdglfket0p9tu06859ijgfopi	1811 Wireless

Physical address: 00904b6a551b

Name: IT

Passphrase (optional): sdglfket0p9tu06859ijgfop

Comment: 1811 Wireless

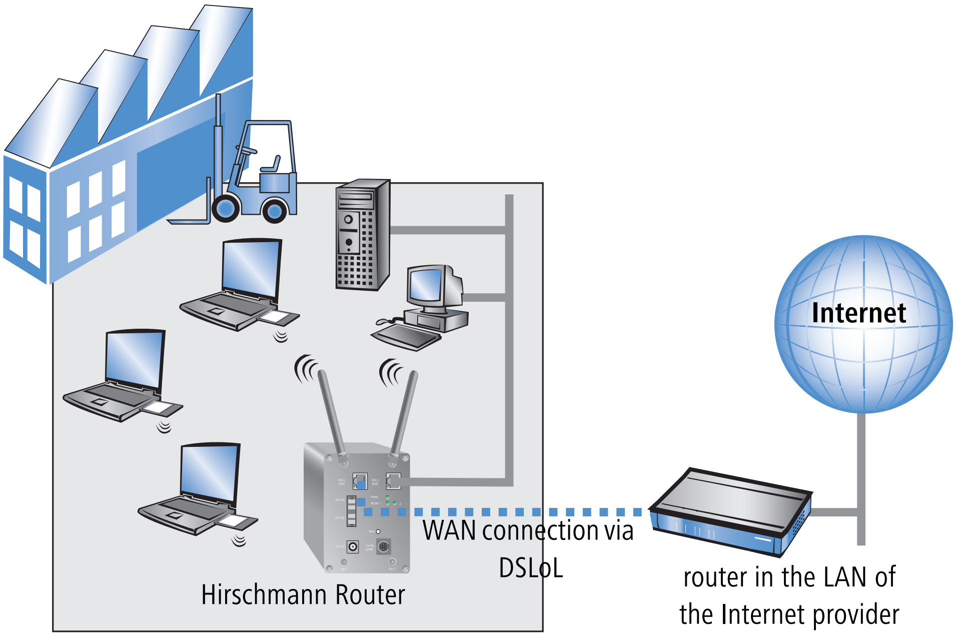
Configuration with WEBconfig or Telnet

The access list for the matching of MAC addresses to the passphrases (LEPS) can be found under WEBconfig or Telnet under the following paths:

Configuration tool	Menu/Table
WEBconfig	Expert configuration ▶ Setup ▶ WLAN-module ▶ Access-list
Terminal/Telnet	`Setup/WLAN-module/Access-list`

5 Setting up Internet access

All computers in the LAN can take advantage of the central Internet access of the Hirschmann Router.



Does the setup wizard know your Internet provider?

A convenient wizard is available to help you set up Internet access. The wizard knows the access information of major Internet providers and will offer you a list of providers to choose from. If you find your Internet service provider on this list, you normally will not have to enter any further transfer parameters to configure your Internet access. Only the authentication data that are supplied by your provider are required.

Additional information for unknown Internet providers

If the setup wizard does not know your Internet provider, it will prompt you for all of the required information step by step. Your provider will supply this information.

- **Verbindung zu einem DSL-Modem**
  - □ Protocol: PPPoE
- **Verbindung zu einem Access-Router mit festen IP-Adressen**
  - □ Protocol: Plain Ethernet

Additional connection options

You may also enable or disable further options in the wizard, depending on whether or not they are supported by your Internet provider:

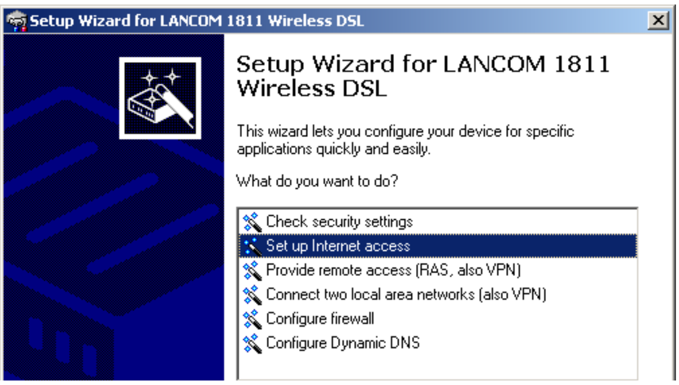
- Time-based billing or flat rate – select the accounting model used by your Internet provider.
  - □ When using time-based billing, you can set the Hirschmann Router to automatically close existing connections if no data has been transferred within a specified time (the so-called idle time).

    In addition, you can activate a line monitor that identifies inactive remote stations faster and therefore can close the connection before the idle time has elapsed.
  - □ Active line monitoring can also be used with flat rate billing to continuously check the function of the remote station.

    You also have the option of keeping flat rate connections alive if required. Dropped connections are then automatically re-established.

5.1 Instructions for LANconfig

① Highlight the Hirschmann Router in the selection window. From the menu bar, select **Tools** ▶ **Setup Wizard**.



Setup Wizard for LANCOM 1811 Wireless DSL

Setup Wizard for LANCOM 1811 Wireless DSL

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Check security settings
- Set up Internet access
- Provide remote access (RAS, also VPN)
- Connect two local area networks (also VPN)
- Configure firewall
- Configure Dynamic DNS

② From the menu, select the **Setup Internet access** wizard and click **Next**.

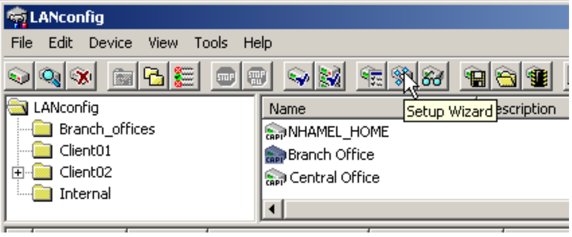
③ In the following window select your country and your Internet provider if possible, and enter your access information.

④ Depending on their availability, the wizard will display additional options for your Internet connection.

⑤ The wizard will inform you as soon as the entered information is complete. Complete the configuration with **Finish**.

LANconfig:
Quick access to the setup wizards

Under LANconfig, the fastest way to launch the setup wizards is via the button on the toolbar.



5.2 Instructions for WEBconfig

① In the main menu, select **Setup Internet access**.

② In the following window select your country and your Internet provider if possible, and enter your access information.

③ Depending on their availability, the wizard will display additional options for your Internet connection.

④ The wizard will inform you as soon as the entered information is complete. Complete the configuration with **Apply**.

6 Security settings

Your Hirschmann Router base station has numerous security functions. You find in this chapter all information needed for an optimal protection of the base station.

6.1 Security for the Wireless LAN

Reflecting on Wireless LANs often entails substantial doubts concerning security. Many people suppose that abuse of data transmitted via radio links is relatively simple.

Wireless LAN devices by Hirschmann permit the employment of modern security technologies:

- Closed network
- Access Control (via MAC-addresses)
- LANCOM Enhanced Passphrase Security
- Encryption of data transfer (802.11i/WPA or WEP)
- 802.1x / EAP
- optional IPSec over WLAN (VPN), in combination with external VPN gateway

6.1.1 Closed network

Each Wireless LAN according to IEEE 802.11 has its own network name (SSID). This network name serves as identification and enables administration of Wireless LANs.

A Wireless LAN can be established in such a way that any user gets access to this network. Such networks are called open networks. Any user can access an open network also without knowledge of the WLAN network name reserved specifically for this network. Only requirement is the input of the network name 'ANY'.

In a closed network the access via 'ANY' is not possible. User have to specify the correct network name. Unknown networks stay hidden to them.

6.1.2 Access control via MAC address

Each network device has an special identification number. This identification number is the so-called MAC address (**M**edia **A**ccess **C**ontrol), which is worldwide unique per device.

The MAC address is programmed into the hardware and cannot be changed. Wireless LAN devices by Hirschmann have got a MAC address label on the casing.

The access to an infrastructure network can be restricted to known MAC addresses for certain Wireless LAN devices solely. To do so, Access Control lists are available within the Hirschmann base stations, in which the granted MAC addresses can be deposited.

This method of access control is not available for ad-hoc networks.

6.1.3 LANCOM Enhanced Passphrase Security

With LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) LANCOM Systems has developed an efficient method which uses the simple configuration of IEEE 802.11i with passphrase and yet which avoids the potential error sources of passphrase sharing. LEPS uses an additional column in the ACL to assign an individual passphrase consisting of any 4 to 64 ASCII characters to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is only possible with the right combination of passphrase and MAC address.

LEPS can be used locally in the device and can also be centrally managed with the help of a RADIUS server, and it works with all WLAN client adapters currently available on the market without modification. Full compatibility to third-party products is assured as LEPS only involves configuration in the access point.

An additional security aspect: LEPS can also be used to secure single point-to-point connections (P2P) with an individual passphrase. Even if an access point in a P2P installation is stolen and the passphrase and MAC address become known, all other WLAN connections secured by LEPS remain protected, particularly when the ACL is stored on a RADIUS server.

Guest access with LEPS: LEPS can also be set up to allow access to guests. To this end, all users of the internal WLAN network are given individual passphrases. Guests can make use of their own dedicated SSID and a global passphrase. To avoid abuse, this global passphrase can be changed on a regular basis—every few days, for example.

6.1.4 Encryption of the data transfer

A special role comes up to the encryption of data transfer for Wireless LANs. For IEEE 802.11 radio transfer the supplementing encryption standards are

802.11i/WPA and WEP. The function of the encryption is to ensure the security level of cable-bound LANs also in Wireless LANs.

- Use encryption on the data transferred in the WLAN. Activate the strongest possible encryption available to you ((802.11i with AES, WPA or WEP) and enter the appropriate keys or passphrases into the access point and the WLAN clients.
- Regularly change the WEP keys in your access points. The passphrases for 802.11i or WPA do not have to be changed regularly as new keys are generated for each connection anyway. This is not the only reason that the encryption with 802.11i/AES or WPA/TKIP is so much more secure than the now aged WEP method.
- If the data is of a high security nature, you can further improve the encryption by additionally authenticating the client with the 802.1x method or activate an additional encryption of the WLAN connection as used for VPN tunnels ('IPSec over WLAN'). In special cases, a combination of these two mechanisms is possible.

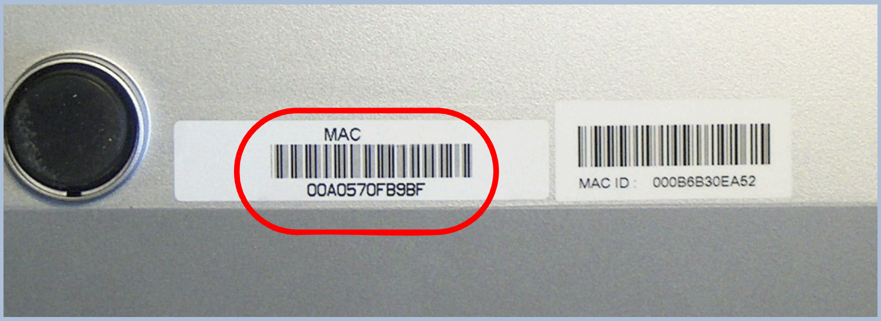
ⓘ Further details to WLAN security and the used encoding methods can be found in the LCOS reference manual.

! Please take note of the information in the box “Standard WEP encryption“.

Standard WEP encryption

As of LCOS version 4.0, WEP128 encryption is activated for every unconfigured device as standard.

The key consists of the first letter "L" followed by the LAN MAC address of the access point in ASCII characters. The LAN MAC addresses of the Hirschmann devices always begin with the character string "00A057". You will find the LAN MAC address on a sticker on the base of the device. **Only** use the number labeled as "MAC address" that starts with "00A057". The other numbers that may be found are **not** the LAN MAC address!



A device with the LAN MAC address "00A0570FB9BF" thus has a standard WEP key of "L00A0570FB9BF". This key is entered into the 'Private WEP settings' of the device for each logical WLAN network as 'Key 1'.

To use a WLAN adapter to establish a connection to a new Hirschmann access point, the WEP128 encryption must be activated for the WLAN adapter and the standard 13-character WEP key entered.

After registering for the first time, change the WEP password to ensure that you have a secure connection.

Note that a reset also causes the WLAN key settings to be lost from the device and the standard WEP key comes into effect again. WLAN access can only work after a reset if the standard WEP key is programmed into the WLAN adapter as well.

6.1.5 802.1x / EAP

The international industry standard IEEE 802.1x and the **E**xtensible **A**uthentication **P**rotocol (EAP) enables the realization of reliable and secure access controls for base stations. The access data is centrally administered on a RADIUS server then, and can be retrieved by the base station if required.

Moreover, this technology makes enables a secured dispatch and a regular automatic change of WEP keys. In this way IEEE 802.1x improves the protection efforts of WEP.

In Windows XP the IEEE-802.1x technology is already integrated by default. For other operating systems 802.1x client software is available.

6.2 Tips for handling keys

The security of encryption procedures can be substantially increased the by paying attention to some important rules for handling keys.

- **Keep keys as secret as possible.**
  Never note a key. Popular, but completely unsuitable are for example: notebooks, wallets and text files in PCs. Do not share a key unnecessarily.
- **Select a random key.**
  Use randomized keys of character and number sequences. Keys from the general linguistic usage are insecure.
- **Change a key immediately in case of suspicion.**
  It is time to change the key of the Wireless LAN if an employee with access to a key leaves your company. The key should also be renewed in case of smallest suspicion of a leak.
- **LEPS prevents the global spread of passphrases.**
  Activate LEPS to enable the use of individual passphrases.

6.3 The security settings wizard

Access to the configuration of a device permits not only to read out critical information (e.g. WEP key, Internet password). Rather, also the entire settings of the security functions (e.g. firewall) can be altered then. So an unauthorized configuration access endangers not only a single device, but the entire network.

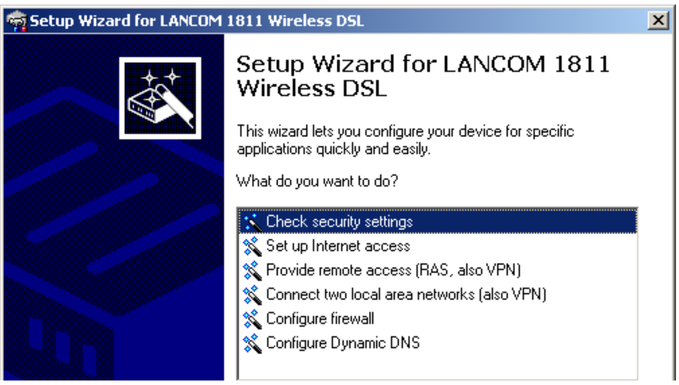
Your Hirschmann Router has a password protection for the configuration access. This protection is already activated during the basic configuration by entering a password.

The device locks access to its configuration for a specified period of time after a certain number of failed log-in attempts. Both the number of failed attempts and the duration of the lock can be set as needed. By default, access is locked for a period of five minutes after the fifth failed log-in attempt.

Besides these general settings you can also check the security settings of the wireless network with the security wizard as far as your device has a WLAN interface.

6.3.1 Wizard for LANconfig

① Mark your Hirschmann Router in the selection window. Select from the command bar **Extras** ▶ **Setup Wizard**.



Setup Wizard for LANCOM 1811 Wireless DSL

Setup Wizard for LANCOM 1811 Wireless DSL

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Check security settings
- Set up Internet access
- Provide remote access (RAS, also VPN)
- Connect two local area networks (also VPN)
- Configure firewall
- Configure Dynamic DNS

② Select in the selection menu the setup wizard **Control Security Settings** and confirm your choice with **Next**.

③ Enter your password in the following windows and select the allowed protocols for the configuration access from local and remote networks.

④ In a next step parameters of the configuration lock like number of failed log-in attempts and the duration of the lock can be adjusted.

⑤ Now you can set the security settings for the WLAN. These include the name of the wireless network, the closed network function and the WEP encryption. You can type in the parameters for both wireless networks separately on devices with the option of a second WLAN interface.

⑥ Now you specify filter lists for stations (ACL) accessing the WLAN and protocols. Thereby, you restrict data exchange between the wireless network and the local network.

⑦ Now activate Stateful Inspection, ping-blocking and Stealth mode in the the firewall configuration.

⑧ The wizard will inform you when entries are complete. Complete the configuration with **Finish**.

6.3.2 Wizard for WEBconfig

Under WEBconfig you have the possibility to run the wizard **Security settings** to control and change the settings. The following values are handled:

- password for the device
- allowed protocols for the configuration access of local and remote networks
- parameters of configuration lock (number of failed log-in attempts and duration of the lock)
- security parameters as WLAN name, closed network function, WEP key, ACL list and protocol filters

6.4 The firewall wizard

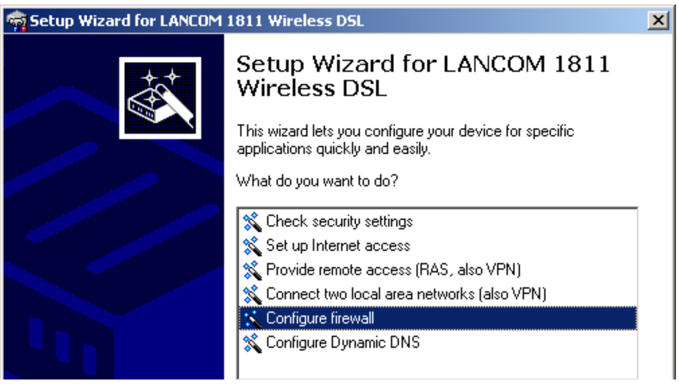
The Hirschmann Router incorporates an effective protection of your WLAN when accessing the Internet by its Stateful Inspection firewall and its firewall filters. Basic idea of the Stateful Inspection firewall is that only self-initiated data transfer is considered allowable. All unasked accesses, which were not initiated from the local network, are inadmissible.

The firewall wizard assists you to create new firewall rules quickly and comfortably.

Please find further information about the firewall of your Hirschmann Router and about its configuration in the reference manual.

6.4.1 Wizard for LANconfig

① Mark your Hirschmann Router in the selection window. Select from the command bar **Extras** ▶ **Setup Wizard**.



Setup Wizard for LANCOM 1811 Wireless DSL

Setup Wizard for LANCOM 1811 Wireless DSL

This wizard lets you configure your device for specific applications quickly and easily.

What do you want to do?

- Check security settings
- Set up Internet access
- Provide remote access (RAS, also VPN)
- Connect two local area networks (also VPN)
- Configure firewall
- Configure Dynamic DNS

② Select in the selection menu the setup wizard **Configuring Firewall** and confirm your choice with **Next**.

③ In the following windows, select the services/protocols the rule should be related to. Then you define the source and destination stations for this rule and what actions will be executed when the rule will apply to a data packet.

④ You finally give a name to the new rule, activate it and define, whether further rules should be observed when the rule will apply to a data packet.

⑤ The wizard will inform you as soon as the entries are complete. Complete the configuration with **Finish**.

6.4.2 Configuration under WEBconfig

Under WEBconfig it is possible to check and modify all parameters related to the protection of the Internet access under **Configuration ▶ Firewall / QoS ▶ Rules ▶ Rule Table.**

7 Options and accessories

Your Hirschmann Router base station has numerous extensibilities and the possibility to use a broad choice of Hirschmann accessories. You find in this chapter information about the available accessories and how to use them with your base station.

- The range of the base station can be increased by optional antennas of the Hirschmann Wireless Router series and can be adapted to special conditions of environs.
- With the LANCOM Public Spot Option option it is possible to extend the Hirschmann Router for additional billing and accounting functions in order to upgrade it to a Wireless Public Spot.

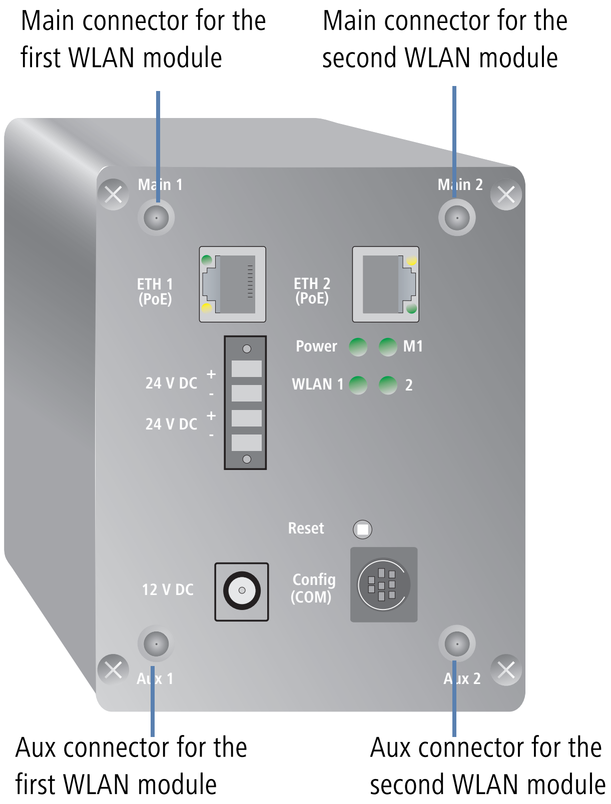
7.1 Optional Hirschmann Wireless Router antennas

To increase the range of the Hirschmann Router base station or to adapt the base station to special conditions of environs, you can connect Hirschmann Wireless Router antennas at the base station. An overview of suitable antennas can be found on the Hirschmann web site under
www.hirschmann-ac.com.

For help with calculating the correct antenna setup for external antennas or for antennas of other vendors, please refer to
www.hirschmann-ac.com

When installing external antennas, ensure that you observe the statutory limitations of the country in which the WLAN device is being operated.

To install the optional external antenna, switch the Hirschmann Wireless Router off by deactivating its power supply (via 12 V power-supply unit, 24 V interface or PoE). Then carefully unscrew the existing antenna and the terminators, if applicable. Connect the external antenna to the appropriate 'Antenna Main' connector.

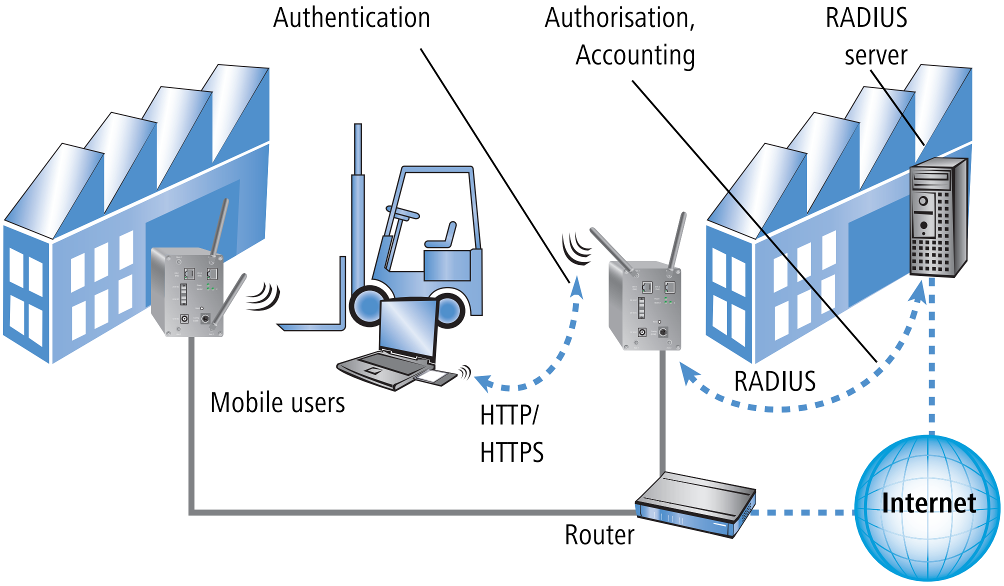

Main connector for the first WLAN module
Main connector for the second WLAN module
Main 1
Main 2
ETH 1 (PoE)
ETH 2 (PoE)
Power
M1
WLAN 1
2
24 V DC
24 V DC
Reset
12 V DC
Config (COM)
Aux 1
Aux 2
Aux connector for the first WLAN module
Aux connector for the second WLAN module

Relay operation requires the connection of external antennas to the first and to the second WLAN modules.

7.2 LANCOM Public Spot Option

Wireless public spots are publicly accessible points, at which users with their own mobile computers can dial wirelessly into a network, usually into the Internet.

The LANCOM Public Spot Option is ideal for use to authenticate staff who need access to a certain machine or network, for example. Access rights are controlled by a central server (e.g. in the Production department). Staff members then have to register anew each time the wish to use a certain IP address range.



With the LANCOM Public Spot Option you extend a base station additionally with these functions and upgrade it to a Wireless Public Spot.

8 Troubleshooting

In this chapter, you will find suggestions and assistance for a few common difficulties.

8.1 No DSL connection is established

After start-up the router automatically attempts to connect to the DSL provider. During this process, the LAN-link LED will blink green. If successful, the LED will switch over to steady green. If, however, the connection can't be established, the LAN-link LED will light up red. The reason for this is usually one of the following:

Problems with the cabling?

Only the cable provided with your device should be used to connect to DSL. This cable must be connected to the Ethernet port of your broadband access device. The LAN link LED must light green indicating the physical connection.

Has the correct transfer protocol been selected?

The transfer protocol is set along with the basic settings. The basic setup wizard will enter the correct settings for numerous DSL providers automatically. Only if your DSL provider is not listed, you will have to enter manually the protocol being used. In any case, the protocol that your DSL provider supplies you with should definitely work.

You can monitor and correct the protocol settings under:

Configuration tool	Run command
LANconfig	Management ▶ Interfaces ▶ Interface settings ▶ WAN Interface
WEBconfig	Expert Configuration ▶ Setup ▶ Interfaces ▶ WAN Interface

8.2 DSL data transfer is slow

The data transfer rate of an broadband (Internet) DSL connection is dependent upon numerous factors, most of which are outside of one's own sphere of influence. Important factors aside from the bandwidth of one's own Internet connection are the Internet connection and current load of the desired target. Numerous other factors involving the Internet itself can also influence the transfer rate.

Increasing the TCP/IP window size under Windows

If the actual transfer rate of a DSL connection is significantly below the fastest rate listed by the provider, there are only a few possible causes (apart from the above-mentioned external factors) which may involve one's own equipment.

One common problem occurs when large amounts of data are sent and received simultaneously with a Windows PC using an asynchronous connection. This can cause a severe decrease in download speed. The cause of this problem is what is known as the TCP/IP receive window size of the Windows operating system that is set to a value too small for asynchronous connections.

Instructions on how to increase the Windows size can be found in the Knowledge Base of the support section of the Hirschmann web site (www.hirschmann-ac.de).

8.3

8.4 Unwanted connections under Windows XP

Windows XP computers attempt to compare their clocks with a timeserver on the Internet at start-up. This is why when a Windows XP in the WLAN is started, a connection to the Internet is established by the Hirschmann.

To resolve this issue, you can turn off the automatic time synchronization on the Windows XP computers under **Right mouse click on the time of day** ▶ **Properties** ▶ **Internet time**.

9 Appendix

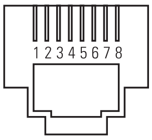
9.1 Performance data and specifications

		Hirschmann BAT54-Rail
Frequency band		Two WLAN modules with 2400 - 2483,5 MHz (ISM) or 5150 - 5750 MHz each
Connections	LAN	10/100Base-TX, Autosensing, Auto Node-Hub
	WAN	Utilisation of LAN connection for simultaneous DSL-over-LAN (DSLoL).
	WLAN1	2x reverse SMA connectors with antenna diversity
	WLAN2	2x reverse SMA connectors with antenna diversity
Power supply		■ 12V DC over external power adapter ■ 2x Power-over-Ethernet as per IEEE 802.3af ■ 2x 24 V DC with 4-pin plug (Phoenix Contact, Combicon RM 3,81mm)
Antennas		Two dualband dipole antennas supplied. Please respect the restrictions given in your country when setting up an antenna system. For information about calculating the correct antenna setup, please refer to www.hirschmann-ac.com.
Housing		ca. 8 x 12 x 13 cm (W x H x D), robust metal housing, IP40, ready for wall and top hat rail mounting.
Approvals		CE compliant according to ETSI EN 300 328, EN 301893, EN 301 893, EN 55022, EN 301 489-17, EN 61000-6-2, EN 60950
Regulations		see data sheet at www.hirschmann-ac.com
Environment/Temperature		Temperature range –20 °C to +50 °C at 95 % max. humidity (non condensing)
Support		Via hotline and Internet

9.2 Contact assignment

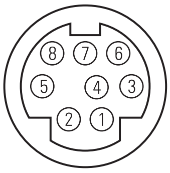
9.2.1 Ethernet interface 10/100Base-TX, DSL interface

8-pin RJ45 socket, corresponding to ISO 8877, EN 60603-7

Connector	Pin	IAE
	1	T+
	2	T-
	3	R+
	4	PoE/G
	5	PoE/G
	6	R-
	7	PoE/- 48 V
	8	PoE/- 48 V

9.2.2 Configuration interface (Outband)

8-pin mini-DIN socket

Connector	Pin	IAE
	1	CTS
	2	RTS
	3	RxD
	4	RI
	5	TxD
	6	DSR
	7	DCD
	8	DTR
	U	GND

9.3 Declaration of conformity

Hirschmann herewith declares that the devices of the type described in this documentation are in agreement with the basic requirements and other relevant regulations of the 1995/5/EC directive.

The CE declarations of conformity for your device are available for download on the Hirschmann web site (www.hirschmann-ac.de).

Index

FAQ

Answers to frequently asked questions can be found at the Hirschmann Website:

www.hirschmann.com

Under Products/Support inside Automation and Control GmbH is located on the pages Products the area FAQ.

For detailed information on all services offered by the Hirschmann Competence Center, please visit the Web site http://www.hicomcenter.com/.

HIRSCHMANN