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.

© 2017 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

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.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
## Contents

**Safety instructions**  
**About this manual**  

### 1 Introduction  
1. Device Roles  
   1.1 Access Point  
   1.2 WLAN Bridge (point-to-point)  
   1.3 WLAN Bridge Relay  
   1.4 WLAN Distribution Point - (Point-to-Multipoint)  
   1.5 WLAN Client  
   1.6 WLAN Roaming Clients  

1.2 Components of the WLAN system  
   1.2.1 Access Points  
   1.2.2 Power supply to the Access Points  
   1.2.3 External antennas  
   1.2.4 Lightning and surge protection equipment  

1.3 Selecting the frequency band  
   1.3.1 2.4 or 5 GHz band  
   1.3.2 Special regulations for the 5 GHz band  

### 2 Setting up P2P connections  
2.1 The Antenna Calculator  
   2.1.1 Data throughput: Nominal vs. Actual  

2.2 Geometric dimensioning of P2P links  

2.3 Antenna alignment  

2.4 Measuring wireless bridges  

### 3 Lightning and surge protection  
3.1 Formation of lightning discharges  

3.2 External lightning protection  

3.3 Internal lightning protection  
   3.3.1 Selecting the lightning and surge protective components  
   3.3.2 External lightning protection  
   3.3.3 Internal lightning protection
3.3.4 Surge-protection adapter LAN 48
3.3.5 Example applications 49

4  Installation  53

4.1 Mounting Notes 54

4.2 Mounting the Access Points 56
  4.2.1 Selecting the location for mounting 56
  4.2.2 Installing the device onto or on a flat surface 57
  4.2.3 Installing the device on a pole 58

4.3 Mounting antennas 59
  4.3.1 Selecting the location for mounting 59
  4.3.2 Flat surface mounting 60
  4.3.3 Pole mounting 61

4.4 Mounting the lightning rods 62
  4.4.1 Dimensioning of the lightning rod 62
  4.4.2 Distance to the components at risk 63
  4.4.3 Lightning charge conduction (grounding) 65

A  Appendix  67

A.1 Antenna characteristics 68

A.2 Troubleshooting 69

B  Further support  71
Safety instructions

Notes on safety
This manual contains instructions to be observed for ensuring your personal safety and for preventing damage. The warnings appear next to a warning triangle with a different heading depending on the degree of danger posed:

Danger!
Means that death, serious physical injury or significant damage to property will occur if the corresponding safety measures are not carried out.

Warning!
Means that death, serious physical injury or significant damage to property could occur if the corresponding safety measures are not carried out.

Caution!
Means that minor physical injury or damage to property can occur if the required safety measures are not carried out.

Note: Contains important information on the product, on how to manage the product, or on the respective section of the documentation to which your special attention is being drawn.
About this manual

The advantages of wireless LANs are obvious – they offer flexibility, mobility and convenience at a lower cost than cabled networks. WLANs can be quickly installed without any changes to the building’s construction, and they offer new applications not available with cabled LANs. Access Points in combination with suitable antennas are ideal for setting up wireless LANs, either indoors or outdoors.

This document applies for all BAT Access Points in combination with appropriate antennas and it provides general information on the outdoor operation of wireless LAN systems. Information on the installation and basic configuration of the various Access Points and antennas is available from the corresponding installation manual.

**Note:** Protecting the components employed from the consequences of lightning strikes and other electrostatic influences is one of the most important aspects to be considered when designing and installing wireless LAN systems for outdoor use. Please refer to the appropriate notes (see on page 39 “Lightning and surge protection”) as otherwise Hirschmann cannot provide any guarantee for damage to the components.

**Note:** Safety notices concerning the mounting and installation of wireless LAN system components are to be found at relevant locations in the following chapters.
1 Introduction

This chapter presents the basic roles for wireless local area network (LAN) outdoor systems. It also lists the type of components required to set up a wireless LAN system outdoors.
1.1 Device Roles

Wireless local area networks (WLANs) can either extend or replace a traditional cable-based network. In some cases, a wireless LAN provides new application design possibilities, providing streamlined work flows and cost savings.

You can use the Access Point in many different roles, depending upon the specific features and the requirements of your network design. These roles include:

- **Access Point:**
  The Access Point provides client devices with a means of wireless entry to a cable-based local area network.

- **WLAN Bridge:**
  Two Access Points provide a wireless point-to-point communication link between two cable-based LANs.

- **WLAN Bridge Relay:**
  One or more dual radio Access Points serve as message relay stations providing a communications link between two cable-based LANs.

- **WLAN Distribution Point:**
  A single master Access Point connects multiple slave access points to a central LAN in a point-to-multipoint design.

- **WLAN Client:**
  A Access Point is designed or configured to serve as an Ethernet adapter and provide a wireless communication link to a WLAN access point.

- **WLAN Roaming Client:**
  WLAN clients wirelessly connect one or more mobile units as they move between multiple WLAN access points, providing continuous, dynamic communications.

Each of these roles is briefly described below. The following chapter describes how to configure a Access Point to perform each of these roles.
1.1.1 Access Point

The Access Point can act as a central access point, connected to multiple wireless clients. In this role, the Access Point provides client access to one or more wireless local area networks and regulates:

- each client’s rights to access the radio cell
- communications between clients
- access to networks linked to other networks

In larger scale WLAN scenarios (e.g. in companies with facilities extending between several buildings or floors) multiple access points can provide WLAN clients with access to a common, shared network. The clients can roam between the different access points, if necessary. Such a design is commonly referred to as campus coverage because this solution has been adopted by a large number of colleges and universities to provide students and staff with network access.

![Figure 1: A single access point connected to wireless clients](image_url)
1.1.2 WLAN Bridge (point-to-point)

Outdoor WLAN systems are especially useful for providing a point-to-point link between two Access Points. This design makes it possible, for example, to easily integrate a distant production building into the company network using two Access Points.

![Figure 2: A wireless link between two access points](image)

You can also use a point-to-point connection to span difficult terrain (such as mountainous areas or water) to provide network access in areas where cabling would be too expensive. With a direct line of sight between the two Access Points and a sufficient fresnel zone, you can bridge distances of several kilometers by this type of wireless link.

![Figure 3: Point-to-point connection with a direct line of sight](image)
1.1.3 WLAN Bridge Relay

Sometimes the required distance between two Access Points may exceed the maximum radio range of a wireless link. Also, physical obstacles may exist that prevent an uninterrupted line-of-sight connection between two Access Points.

In these cases, you can connect the two end points by stringing together multiple Access Points, where each intermediate Access Point is equipped with two radios. Because the intermediate Access Points often operate solely as relay stations, this design is referred to as Relay mode.

![WLAN bridge in relay mode](image)

BAT Access Points can run several P2P links simultaneously on each wireless module, in addition to supporting WLAN clients. However, for performance reasons we recommended the use of BAT Access Points with 2 wireless modules for the relay stations. If you use directional antennas, the relay station needs to be equipped with 2 radios.
1.1.4 WLAN Distribution Point - (Point-to-Multipoint)

A special type of wireless link is the connection of several distributed Access Points to a central point—the point-to-multipoint (P2MP) WLAN or Wireless Distribution System (WDS). With this mode of operation you can establish connections for several buildings on a company’s premises with the central administrative building, for example. The central Access Point or wireless router is configured as ‘master’ and the remote stations as ‘slaves’.

![Diagram of Point-to-Multipoint wireless LAN]

*Figure 5: Point-to-multipoint wireless LAN*
1.1.5 WLAN Client

A WLAN client can be either:
- equipped with an Ethernet interface (for example, a PC or printer), or
- an Access Point that is configured to serve as a conventional wireless LAN adapter, and avoids to use its full capability as an Access Point. You can purchase special BAT access points that can operate exclusively as a WLAN client.

Figure 6: BAT Access Point operating as WLAN client
1: Authentication, Authorization and Accounting server
2: WLAN device in AP mode
3: WLAN device in client mode
4: WLAN device in client mode
1.1.6 WLAN Roaming Clients

Using BAT Access Points, you can develop WLAN systems in industrial environments for the transmission of data to and from mobile objects. In the following logistics example, fork-lift trucks remain continuously connected to the company network via the WLAN. When combined with mobile barcode scanners, this system permits the real-time monitoring of the flow of inventory within a warehouse. Data obtained in this system pass through to an enterprise resource planning (ERP) system, which continuously provides up-to-the-minute information on current inventories.

Figure 7: A WLAN client roaming between access points
1.2 Components of the WLAN system

An outdoor WLAN system consists of the following components:

1.2.1 Access Points

Hirschmann supplies Access Points for various applications. You can use Access Points to establish WLAN networks Service Set Identifiers (SSIDs) or wireless links Point to Point (P2P). Some models also provide router functionality, including a WAN interface. The following characteristics are important when considering the use of WiFi devices:

- Environmental conditions: Some Access Points are suitable for operation in an office environment (IP20); some are suitable for rugged conditions such as those found in logistics warehouses (IP40); some are for water resistance in extreme weather conditions (IP67); and some models are designed for operation in hazardous environments (ATEX).

- Standards supported: Depending on model type, the Access Points support one of the following standards: IEEE 802.11a (5 GHz band), IEEE 802.11b or IEEE 802.11g (2.4 GHz band), IEEE 802.11n (2.4 and 5 GHz bands) or IEEE 802.11ac (2.4 and 5 GHz bands). The 5 GHz band is highly suitable for directional radio links due to the higher performance.

- Number of WiFi modules: For operating directional radio links over distances that exceed the range of a single P2P connection, such as when operating a relay, you can use devices fitted with two radios.

Note: Please refer to the appendix in this manual for more information on the frequency bands and their permitted use in different countries.
1.2.2 Power supply to the Access Points

Refer to the Installation Guide for further information. This document is available for download as a PDF file on the Hirschmann product pages (www.hirschmann.com).

1.2.3 External antennas

Refer to the Antenna Guide for further information. This document is available for download as a PDF file on the Hirschmann product pages (www.hirschmann.com).

1.2.4 Lightning and surge protection equipment

Besides the central components (access point, antenna and power supply), the most important accessories in an outdoor wireless LAN system are those for lightning and power surge protection. Lightning and other electrostatic occurrences can impinge on the wireless LAN system and cause harm to people, machines and equipment. Hirschmann provides accessories (BAT-ANT-Protector m-f, BAT-LAN-Protector IP68) to be used as part of an installation of a lightning protection system for your outdoor installation. These accessories by themselves are part of a lightning protection solution. It is your responsibility to take appropriate measures to mitigate the effects of lightning strikes. Make sure the equipment is installed in accordance with local, regional and national regulations for codes and standards (such as VDE 0182 and IEC 62305) and according to best practices for your application and environment.
**DANGER**

**LIGHTNING STRIKE AND VOLTAGE SURGES**

Protect devices or antennas installed outdoors using lightning arrester devices, such as lightning rods.

Install over voltage protector devices on every cable.

**Failure to follow these instructions will result in death, serious injury, or equipment damage.**
1.3 Selecting the frequency band

1.3.1 2.4 or 5 GHz band

One of the first steps in the planning of a WLAN system is to determine which frequency band to use. The following aspects are helpful for making this decision:

- **Advantages of the 2.4 GHz band**
  - Simple technical implementation with no need for functions such as Transmission Power Control (TPC) or Dynamic Frequency Selection (DFS).
  - Widespread WLAN client base.
  - Better transmission through obstacles (e.g. walls)

- **Disadvantages of the 2.4 GHz band**
  - Frequency band is also used by Bluetooth, microwave ovens, etc., and is thus prone to interference.
  - There are three separate channels, meaning that three networks can be operated in parallel without interference.

- **Advantages of the 5 GHz band**
  - The frequency band is sparsely used, so that interference from other applications is uncommon.
  - Depending on local regulations, there may be between 13 and 21 non-overlapping channels. This makes it possible to operate channel bundling or multiple overlapping radio cells.
  - High ranges due to power levels of up to 1000 mW.
### 1.3 Selecting the frequency band

**Note:** You can use up to 4000 mW Equivalent Isotropic Radiated Power (EIRP) for applications in Broadband Fixed Wireless Access (BFWA) on. See “Broadband Fixed Wireless Access (BFWA)” on page 23..

#### Disadvantages of the 5 GHz band

- Regulations in Europe require techniques such as DFS for channel selection and TPC for power control.
- Small WLAN client base.

**Note:** WLAN systems based on the 2.4 GHz band suit well to applications where WLAN clients need short-range connection to Access Point (e.g. access points). The advantages of the 5 GHz band lie mainly with point-to-point systems, in which two Access Points can connect by a wireless link (WLAN bridge) over longer distances.

### 1.3.2 Special regulations for the 5 GHz band

With the 802.11h enhancement of September 2003, the private use of the 5 GHz band became possible outside closed spaces. To help protect military applications in the 5 GHz band, the European Telecommunications Standards Institute (ETSI) prescribed DFS and TPC procedures. However, when using DFS and TPC with a maximum of 1000 mW, or 4000 mW for commercial network operators in compliance with Broadband Fixed Wireless Access (BFWA) regulations, much higher transmission power can be generated than allowed by previous standards.
Dynamic Frequency Selection

Observe certain requirements for the outdoor operation of 5 GHz WLANs in order to utilize the maximum permitted performance of 1 or 4 watts. It is vital to avoid interference with radar systems that are active in this spectrum (e.g. meteorological, military). For this reason the European Telecommunications Standards Institute (ETSI) regulates WLAN devices operating at 5 GHz to employ the Dynamic Frequency Selection (DFS) mechanism.

With DFS, radar and WLAN systems can co-exist without interfering with one another and capacity utilization is spread evenly across available frequencies. When starting a WLAN wireless cell, the access point checks all channels for the presence of radar systems. The check uses an inactive period of one minute, during which the wireless cell is not available. During this interval, the access point generates a list of radar-free channels which is valid for 24 hours. The Access Point selects a channel for operation from this list. During operation, the device checks the current channel continuously for radar activity.

If a radar system subsequently starts operation, the device releases the channel immediately. In this case, the access point selects the next available channel, informs the participants in the wireless cell of the impending change, and switches to that channel.

Note: The currently selected channel can be used for any length of time, unless radar signals are detected, or the radio cell is restarted (e.g. due to device reconfiguration, firmware upload or reboot).

Note: If the system is able to respond to a channel switch instantaneously, the device repeats the check within 24 hours, following a one-minute period of inactivity. The parameter "DFS Rescan Hours" (available in the HiLCOS menu tree under "Setup/Interfaces/WLAN/Radio settings") allows a time to be set for conducting the channel check (assuming that the time is available, for example via Network Time Protocol (NTP).

DFS is stipulated for the frequency ranges 5250 – 5350 MHz, 5470 – 5725 MHz and 5775 – 5875 (BFWA). It is optional for the frequency range 5150 – 5250 MHz.
1.3 Selecting the frequency band

- **Transmission Power Control**
  Automatic adjustment of the transmission power reduces radio interference.
  Without DFS and TPC, you use a maximum of 200 mW EIRP. When operating DFS and TPC, you have permission to use a maximum of 200 mW (5150 to 5350 MHz) and 1000 mW EIRP (5470 to 5725 MHz) as transmitting power (as compared to 100 mW for 802.11b/g, 2.4 GHz, where DFS and TPC are unnecessary). The higher maximum transmission power compensates for the higher attenuation of 5 GHz radio waves in air and also allows for significantly longer ranges than in the 2.4 GHz range.

- **Broadband Fixed Wireless Access (BFWA)**
  In July 2007, Germany’s Federal Network Agency released additional frequencies for broadband fixed wireless bridges in the 5 GHz band. These additional frequencies, located in the range between 5755 MHz - 5875 MHz, are also referred to as BFWA. You can use the additional frequencies for long-distance point-to-point (P2P) or point-to-multipoint (P2M) links to help provide high-speed Internet access to other users from a central node. You can use this method to help provide rural areas with high-speed Internet access.
  Exclusively commercial providers may use the operation of BFWA. There are no charges for using these frequencies, but providers need to register at the Federal Network Agency. This band covers 120 MHz and offers 6 channels with a bandwidth of 20 MHz each. Maximum transmission power is 36 dBm or 4000 mW. Operating BFWA links require TPC and DFS.

- **Available channels in the 5 GHz band**
  In the available frequency range of 5.13 to 5.875 GHz, you can use the following channels in Europe, divided into frequency ranges to which different conditions of use apply:
  - 5150 – 5350 MHz (channels 36, 40, 44 and 48)
  - 5250 – 5350 MHz (channels 52, 56, 60 and 64)
1.3 Selecting the frequency band

- 5755 – 5875 MHz
  - Channels 151, 155, 159, 163, 167: For commercial use in Germany and only in combination with DFS (BFWA).
  - Channels 149, 153, 157, 161, 165: For FCC use in the USA, without DFS.

**Note:** Channels 120, 124 and 128 were available in the past but are now blocked.

The following table shows which channels you can use in the different regions:

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency</th>
<th>ETSI (EU)</th>
<th>FCC (US)</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>5180 MHz</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>40</td>
<td>5200 MHz</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>44</td>
<td>5220 MHz</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>48</td>
<td>5240 MHz</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>52</td>
<td>5260 MHz</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>56</td>
<td>5280 MHz</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>60</td>
<td>5300 MHz</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>64</td>
<td>5320 MHz</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>100</td>
<td>5500 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>104</td>
<td>5520 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>108</td>
<td>5540 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>112</td>
<td>5560 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>116</td>
<td>5580 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>132</td>
<td>5660 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>136</td>
<td>5680 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>140</td>
<td>5700 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>147</td>
<td>5735 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>149</td>
<td>5745 MHz</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>151</td>
<td>5755 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>153</td>
<td>5765 MHz</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>155</td>
<td>5775 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>157</td>
<td>5785 MHz</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>159</td>
<td>5795 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>161</td>
<td>5805 MHz</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>163</td>
<td>5815 MHz</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>165</td>
<td>5825 MHz</td>
<td>no</td>
<td>yes</td>
</tr>
</tbody>
</table>
1.3 Selecting the frequency band

The use of the methods described in ETSI 301 893 for reducing mutual interference in the 5 GHz band (TPC and DFS) is stipulated for some fields of application. The following table provides information about the permitted use and corresponding transmission powers within the European Union (EU):

<table>
<thead>
<tr>
<th>Frequency bands (GHz)</th>
<th>Transmission power (mW/dBm)</th>
<th>Use</th>
<th>DFS</th>
<th>TPC</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.15-5.25</td>
<td>200/23</td>
<td>Indoor</td>
<td>not stipulated</td>
<td>not stipulated</td>
</tr>
<tr>
<td>5.25-5.35</td>
<td>200/23</td>
<td>Indoor</td>
<td>stipulated</td>
<td>stipulated</td>
</tr>
<tr>
<td>5.470-5.725</td>
<td>1000/30</td>
<td>Indoor/Outdoor</td>
<td>stipulated</td>
<td>stipulated</td>
</tr>
<tr>
<td>5.755-5.875</td>
<td>4000/36</td>
<td>Outdoor (BFWA)</td>
<td>stipulated</td>
<td>stipulated</td>
</tr>
</tbody>
</table>

Note: Other regulations may apply for use in other countries. Please refer to the current wireless network regulations for the country in which you wish to operate a WLAN device, and set the country of operation in the WLAN settings.

The USA and Asia use frequency bands and maximum signal strengths that are different than the European standard.

In the USA, you can use three subbands, each 100 MHz wide, for wireless networks in the 5 GHz band. These are the "lower band" ranges from 5150 – 5250 MHz; the "middle band" ranges from 5250-5350 MHz and the "upper band" ranges from 5725 – 5825 MHz. In the lower band, you have permission to use a maximum average EIRP of 50 mW; in the middle band this is 250 mW; and 1 W in the upper band.

In Japan, limited use of the 5 GHz band is possible. You may use the lower band of 5150 – 5250 MHz for private use exclusively.
2 Setting up P2P connections

This chapter introduces the basic principles involved in designing point-to-point links, and provides tips on aligning the antennas.

Note: Refer to the appendix for information on the frequency ranges used. For instructions on configuration of the Access Point, refer to the HiLCOS Configuration Guide.

BAT Access Points can serve as central stations in a wireless network, and also can operate in point-to-point mode to bridge longer distances. For example, they can help provide a reliable connection between two networks that are several kilometers apart — without direct cabling or expensive leased land lines.

Figure 8: Point-to-point (WLAN bridge) connection

When you use Access Points and appropriately polarized antennas in accordance with IEEE 802.11n, you may establish two wireless links (spatial streams) simultaneously between the end points of a point-to-point connection. This allows you to achieve higher data throughput, or to cover greater distances, than when using other standards.
Setting up P2P connections

Figure 9: Usage of two spatial streams
2.1 The Antenna Calculator

You can use the Antenna Calculator to calculate the output power of the access points, as well as the achievable distances and data rates. You can download the program from our Web site at www.hirschmann.com. After selecting your components (access points, antennas, lightning protection and cable) the calculator works out the data rates, ranges, and antenna gain settings that you need to enter into the access point’s configuration.

2.1.1 Data throughput: Nominal vs. Actual

One calls the throughput for WLANs the 'nominal data rate'. This is the result of the signal quality and the WLAN standard you use and its method of modulation. Security methods and collision avoidance result in more overhead than in cabled networks. The actual data rate comes up to 50% of the nominal data rate. 802.11g/a WLANs with a nominal data rate of 54 Mbps achieves a maximum net data rate of 24 Mbps. WLANS using the current 802.11n standard with 300 Mbps nominal data rate achieve a maximum net value of approximately 130 Mbps. Depending on the existing signal quality, WLAN systems may reduce their throughput performance step by step in order to counteract impairments in radio signals. When there is radio interference, packet retransmissions are necessary, leading to a reduction in net throughput. You need to consider time delays over distances of several kilometers, which require greater tolerances when they access the radio medium.

In the 5 GHz band it is helpfull for you to configure one central access point as "master" and the other point-to-point partners as "slaves". Even in the 2.4 GHz band with automatic channel selection this setting helps to establish point-to-point connections.
2.2 Geometric dimensioning of P2P links

Answer the following basic questions when you design wireless links:

- Which antennas are suitable for the desired application? You can find answers to these questions with the help of the BAT Antenna Calculator (see on page 29 “The Antenna Calculator”).
- How do you align the antennas to enable reliable connections?
- What performance characteristics do the antennas need to provide sufficient data throughput within the legal regulations?

**Positioning the antennas**

Antennas broadcast their signals within an angle that depends on the model in question. The spherical expansion of the signal waves produces amplification or interference of the effective power output at certain distances along the connection between the transmitter and receiver. The areas where the waves amplify or cancel themselves out are known as Fresnel zones.
Ensure that Fresnel zone 1 is free from obstruction so that an acceptable level of output from the transmitting antenna reaches the receiving antenna. Any obstructing element protruding into this zone will significantly impair the effective signal power. The object screens off a portion of the Fresnel zone and the resulting reflections also lead to a significant reduction in signal reception.

You can calculate the radius \( R [m] \) of Fresnel zone 1 by using the following formula, assuming that you know the signal wavelength \( \lambda [m] \) and the distance between transmitter and receiver \( d [m] \):

\[
R = 0.5 \times \sqrt{\lambda \times d}
\]

The wavelength in the 2.4 GHz band is approximately 0.125 m (0.41 ft), and in the 5 GHz band approximately 0.05 m (0.16 ft).

Example: With a separating distance of 8 km (5 miles) between the two antennas, the radius of Fresnel zone 1 in the 2.4 GHz band is 15.8 m (51.8 ft), and in the 5 GHz band is 10 m (32.8 ft).

So that the Fresnel zone 1 remains unobstructed, it is necessary that the height of the antennas is bigger than the highest obstruction within this radius. You can calculate the full height of the antenna mast \( M \) as depicted below:
Figure 11: Mast height calculation
- 1 Fresnel zone
- 2 Radius R
- 3 Security: 1m
- 4 Obstruction height H
- 5 Earth curvature E

\[ M = R + 1m + H + E \] (earth's curvature)

You can calculate the allowance for the earth's curvature (E) at a distance (d) with the following formula for the metric length system:
\[ E[m] = d[km]^2 \times 0.0147 \] – e.g., at a distance of 8 km this is approximately 1 m.

For the anglo-american length system the formula is:
\[ E[ft] = d[miles]^2 \times 0.1234 \] – e.g., at a distance of 5 miles this is approximately 3.1 ft.

Example:
With a distance of 8 km (5 miles) between the antennas, the result in the 2.4 GHz band is a mast height above the level of the highest obstruction of approximately 17.8 m (58.4 ft), and in the 5 GHz band 12 m (39.4 ft).

**Note:** You can compute the necessary mast heights with the BAT Antenna Calculator.
### Antenna power

Ensure that the power of the antennas is high enough to allow acceptable data transfer rates. In addition, the antenna power needs to comply with the country-specific legal regulations regarding maximum transmission power.

The calculation of effective power considers everything from the radio module in the transmitting access point to the radio module in the receiving access point. In between there are attenuating elements such as the cable, plug connections and the air transmitting the signals, as well as amplifying elements such as the external antennas.

![Diagram](image)

**Figure 12: Elements influencing power**

1. Output power of the radio module
2. Loss through cable, plugs and lightning protection
3. Amplification with antenna gain
4. Free-space loss
5. Input signal at the radio module
2.3 Antenna alignment

The precise alignment of the antennas is important in establishing P2P connections. The more central you locate the receiving antenna in the "ideal line" of the transmitting antenna, the better the actual performance and effective bandwidth. As shown in the following illustration, if the receiving antenna is outside of this ideal area (1) significant losses in performance (2) will be the result.

![Figure 13: Antenna alignment](image)

**Note:** You can find further information on the geometrical design of wireless paths and the alignment of antennas in the LANconfig in the BAT User Installation Guide.

You can display the current signal quality over a P2P connection device's LEDs, or in the LANmonitor, to help find the optimal alignment for the antennas. You can activate the display of signal quality on the LEDs for the WLAN interface (LANconfig: WLAN > General > Physical WLAN settings > Operation). The faster the LED blinks, the better the connection (a blinking frequency of 1 Hz represents a signal quality of 10 dB, double this frequency indicates that the signal strength is twice as high).
Figure 14: Link LED function in physical WLAN settings in LANconfig

In LANmonitor, you can open the connection quality display by using the context menu. Right-clicking with the mouse on 'Point-to-point' activates the option 'Adjusting Point-to-Point WLAN Antennas...
Setting up P2P connections

2.3 Antenna alignment

Figure 15: Adjusting Point-to-Point WLAN antennas in LANConfig

Note: The 'Point-to-Point' entry is visible in the LANmonitor if the monitored device has at least one base station defined as a remote site for a P2P connection (LANconfig: WLAN > General > Physical WLAN settings > Point-to-Point).

In the dialog for setting up point-to-point connections, LANmonitor prompts for the information necessary to establish the P2P connection:

- Is the P2P connection configured at both ends with MAC address or station name of the remote base station?
- Is the point-to-point mode of operation activated?
- Which access point do you want to monitor? Select any of the base stations defined as P2P remote sites in the device.
- Are both antennas approximately aligned? Ensure that the basic P2P connection work before you can perform fine-tuning with the aid of LANmonitor.

Once signal monitoring has commenced, the P2P dialog displays the absolute values for the current signal strength and the maximum value since starting the measurement. LANmonitor displays the development of the signal strength over time and the maximum value, as shown below:
2.3 Antenna alignment

Initially adjust one of the two antennas until a maximum value is achieved. Then secure this first antenna and adjust the second antenna to attain the optimal signal quality.

*Figure 16: Diagram displaying the development of signal strength*
2.4 Measuring wireless bridges

After planning and installation, you can analyze the wireless bridge with a benchmark program (e.g. iPerf) to determine the actual data throughput.
3 Lightning and surge protection

When you mount devices and / or antennas outdoors, there is a risk of them being struck by lightning. Additionally, voltage surges may get into the interior of the building. It is your responsibility to take appropriate measures to mitigate the effects of lightning strikes. Make sure to install the equipment in accordance with local, regional and national regulations for codes and standards (such as VDE 0182 and IEC 62305) and according to best practices for your application and environment.

⚠️ DANGER

LIGHTNING STRIKE AND VOLTAGE SURGES

Protect devices or antennas installed outdoors using lightning arrester devices, such as lightning rods.

Install over voltage protector devices on every cable.

Failure to follow these instructions will result in death, serious injury, or equipment damage.
3.1 Formation of lightning discharges

Lightning flashes are electromagnetic discharges that are caused by differences in electric potential. Water particles are charged through friction when there is weather movement in the atmosphere. The predominantly positively charged particles rise upwards while the negatively charged particles tend to remain at the lower levels. This uneven distribution of electrical charge can cause discharges within the clouds that can be observed as cloud-to-cloud lightning.

![Formation of lightning discharges](image)

Figure 17: Formation of lightning discharges
1 Leader lightning
2 Conductive discharge
3 Lightning discharge

As the earth is predominantly positively charged, a difference between the potential of the cloud and the earth arises. As soon as this potential difference is large enough, leader lightning descends earthwards.
Direct lightning strike
The most frequent type of lightning is cloud-earth lightning. A so-called lightning leader develops from a negatively charged center of a thundercloud. This leader descends, and when it is between 10 m and several 100 m from the earth the electrical field strength increases so strongly in exposed places – for example at the roof of a house or top of a tree or even the tip of an antenna – that similar and opposite discharges to the lightening leader develop there, the so-called conductive discharges. One of possibly many conductive discharges meets the lightning leader and "earths" it. This determines the point where lightning strikes. If an antenna is struck by lightning, the instant increase in voltage is conducted via the coaxial cable to any connected devices, i.e. the Access Point in a wireless LAN system, and this generally results in their destruction. Additionally, any ungrounded components of a wireless LAN system may be subject to sparks or arcing to any earthed metal parts in the vicinity.

Partial discharges
Even if a conductive discharge originates in an antenna it does not necessarily mean that lightning will strike the antenna. In order to feed the conductive discharge in the antenna, a momentary electrical impulse flows through the antenna system – this is called a partial discharge. A partial discharge is therefore a conductive discharge without leading to a direct lightning strike. These partial discharges can also result in damage to connected electronic equipment such as Access Points unless you take protective measures.

DANGER
INVISIBLE ELECTRICAL DISCHARGES
Even when there are no visible phenomena such as thunderstorms or a direct lightning strike, invisible electrical discharges from the atmosphere can still occur that can destroy or damage sensitive wireless LAN modules or other electronic devices.

Failure to follow these instructions will result in death, serious injury, or equipment damage.
Risks to antennas
Antennas for wireless LAN systems are at particular risk from lightning strike as they tend to be mounted in exposed positions and they are designed to be very good electrical conductors. The more pointed, needle-shaped and exposed antennas are, the greater the danger posed by a conductive discharge that could result in a direct lightning strike or partial discharge.

Note: Please note that the explanations of lightning protection in this documentation only refer to protection for wireless LAN systems. Ensure to plan and install the protection of the buildings themselves and other equipment and associated networks (LANs) separately, if necessary.
3.2 External lightning protection

External lightning protection includes all measures for you to prevent a direct lightning strike in the equipment to be protected. This includes, for example, arrester equipment such as lightning rods etc. which intentionally offer an exposed point for electrical discharges. Any lightning striking this equipment is channeled by a conductor along the shortest path to the grounding system. Intentionally "catching" the lightning with the arresting equipment creates a spatial shield where direct lightning strike is impossible. The actual design and construction of the external lightning protection depends on the prevailing structural circumstances.

Figure 18: External lightning protection
1 Spatial shield
2 Protective angle = 45°
3 Safety clearance >100 cm
4 Lightning rod
5 Conductor
6 Grounding
7 Antenna
3.3 Internal lightning protection

Internal lightning protection refers to measures which counteract the effects of lightning strikes and surges that may arise despite the external lightning protection. The following events can cause these disturbances:

- A lightning strike some distance away, which subsequently diffuses through the power network.
- Discharges in the atmosphere that are not accompanied by visible lightning.

There are two ways in which these surges can get into a building and then spread: Via the connection to the public power supply or via cable entry points, for example antennas fixed to the outside of the building.

The following is a description of how to protect the system from the perspective of antennas. Only a specialist electrician is authorized to plan and implement the protection for equipment connected to the power supply from surges emanating from the public power supply.

Figure 19: BAT-ANT-Protector m-f between the access point and the antenna
The central component for internal lightning protection is the BAT-ANT-Protector m-f. The employment of the BAT-ANT-Protector m-f is essential under all circumstances—despite outer lightning-protection measures, partial discharges can still give rise to surges that can damage sensitive WLAN modules.

Make sure that the specialist electrician always mounts The BAT-ANT-Protector m-f between the Access Point and the antenna, preferably as near as possible to the Access Point. It should be positioned behind the endangered portion of the antenna cable in a location where it can be grounded. If the Access Point is installed outside, the electrician connects its grounding and that of the BAT-ANT-Protector m-f with the antenna's conductor, for example via the clamps on the antenna's mounting.

In addition to this, the specialist electrician can use an LAN surge adapter to reduce possible surges in the Ethernet or PoE cable.

*Figure 20: Surge protection for outdoor installations*
3.3.1 Selecting the lightning and surge protective components

Classification of surge protective devices
So-called surge protective devices (SPDs) are used to protect electrical and electronic devices in buildings. These are divided into various categories depending on the purpose of their application:

- **Buildings**: The biggest danger from the effects of lightning strikes lies in the transmission of lightning current over the cables leading from exposed objects such as antennas directly into the building. Additionally to the lightning current, surges can occur. Make sure that the specialist electricians fit so-called lightning arresters (type 1) to the relevant cables directly where they enter the building, and further surge protection adapters (e.g. BAT-ANT-Protector m-f).

- **Power supply**: Surges can also find their way into the building via the power supply and thereby endanger electronic equipment. Surge arresters (type 2) can protect against such surges. They work by reducing the voltage peaks to a sufficiently low level. These type 2 adapters are fitted for example in the electrical cabinet.

- **Devices**: The final link in the surge protective chain is the protection of the devices themselves. Make sure that the specialists use type 3 surge protective devices for this, for example in the form of power socket adapters. This type of SPD works by lowering any surges that may occur to a level that is not dangerous for highly sensitive equipment.

The assessment of risk and the resulting design of a suitable lightning protection system is always dependent on local conditions (for example the frequency with which lightning strikes are to be expected) and ideally needs to be carried out by trained experts.

**Note**: Please make sure that in addition to implementing lightning protection for wireless LAN systems, specialist electricians plan and install protection for the building itself and for other equipment separately.

The following considerations are intended to assist with planning the components to use:
3.3.2 External lightning protection

- **Lightning rod**
  - When? Required if the antenna or any other element of the wireless LAN system is mounted in an exposed position.
  - Where? At least 50 cm safety clearance to the antenna or other conductive element of the wireless LAN system, and preferably more than 100 cm.
  - Conductor? Grounding via potential equalization line (PEL, 16 mm² Cu) is always required.

- **Antenna potential equalization**
  - Separate conductor: Via separate potential equalization line (PEL, 16 mm² Cu) if there is no lightning rod present (antenna installed in a protected position).
  - Separate conductor: Via separate potential equalization cable (16 mm² Cu) if the safety clearance between the the lightning and the antenna is more than 100 cm.
  - Via lightning rod conductor: Grounding via the existing potential equalization cable of the lightning rod when the safety clearance between lightning rod and antenna or other conductive element of the wireless LAN system is more than 50 cm but less than 100 cm.

**Note:** If the safety clearance is less than 100 cm, make sure that the specialists connect the grounding of the lightning rod with the grounding of the antenna.
3.3.3 Internal lightning protection

- **Surge-protection adapter BAT-ANT-Protector m-f**
  - When? Always required. Also protects against partial discharges that can damage sensitive wireless LAN modules when there is no direct lightning strike.
  - Where? Position as near as possible to antenna connector on the Access Point.
  - Conductor? Potential equalization via the building's grounding system using a PE line (protective earth – 1.5 mm² Cu).

  **Note:** Hirschmann will exclusively fulfill its warranty obligations when you operate WLAN devices in combination with a BAT-ANT-Protector m-f surge protection adapter. This lightning protection is explicitly designed for the WLAN modules in BAT devices. Hirschmann fulfills no warranty obligations if you use different surge-protection adapters.

3.3.4 Surge-protection adapter LAN

- When? Depends on the individual risk and protection requirements of the devices and cabling in the LAN, e.g. the outdoor equipment with integrated antennas.
- Where? As near as possible to the Access Point’s ETH connector.
- Conductor? Potential equalization via the building’s grounding system using a PE line (protective earth – 1.5 mm² Cu).
3.3.5 Example applications

Depending on where the Access Point, antennas and lightning rods are positioned there are numerous combinations of lightning and surge protective equipment. The following illustrations show some sample scenarios that are frequently found in practice. With this knowledge you will be able to put together the components required for other constellations.

- **Scenario 1:**
  Antenna in a protected place.

*Figure 21: Antenna in a protected place*

1. Surge protection adapter
2. Antenna in a protected place
3. Potential-equalization line (PEL), 16 mm² Cu
The basic situation shows an application where the antenna is mounted in a protected place – there is therefore no danger of a direct lightning strike.

- It is sufficient for lightning protection to have an adequately dimensioned potential equalization line for the antenna.
- Make sure to protect The Access Point with a BAT-ANT-Protector m-f for internal protection in any case.

**Scenario 2:**
Antenna in an exposed place, safety clearance to arresting device observed.

*Figure 22: Antenna in an exposed place*

1 Surge protection adapter
2 Antenna in an exposed place
3 Safety clearance >100 cm
4 Potential-equalization line (PEL), 16 mm² Cu
In this example the specialist electrician mounted the antenna in such a way that a direct lightning strike is possible. As a protective measure the specialist installed a lightning rod with a sufficiently large safety clearance of more than 100 cm.

- As external lightning protection both the antenna and the lightning rod are separately grounded with their own potential equalization lines.
- There are no other aspects to be considered for internal lightning protection.

**Scenario 3:**
Instead of installing the access point inside the building, the specialist did it outdoors, for example directly next to the antenna, in order to reduce the length of cable between the antenna and the access point.

*Figure 23: Access Point installed outdoors*
1. LAN Surge protection adapter
2. Surge protection adapter
3. Safety clearance >100 cm
4. Potential-equalization line (PEL), 16 mm² Cu
In this case, the specialist installs the BAT-ANT-Protector m-f surge-protection adapter directly between Access Point and antenna and grounds it for example via the antenna's potential equalization line. If you operate any outdoor access point with the supplied rod antenna instead of with an external antenna, you cannot employ the lightning protection adapter BAT-ANT-Protector m-f due to the connector shape. In this case it is imperative for you to employ a lightning rod!

- If the specialist installs the Access Point outside, the specialist connects its grounding and that of the BAT-ANT-Protector m-f with the antenna's conductor, for example via the clamps on the antenna's mounting.

- The specialist can fix the BAT-ANT-Protector m-f directly to the antenna socket with the aid of a short adapter (gender changer), depending on the model of the Access Point.
4 Installation
4.1 Mounting Notes

Note: Do not mount Access Points or antennas in weather conditions when lightning may be expected. Similarly, refrain from connecting or disconnecting cables during weather of this type. The components of a wireless LAN can be subject to variations in electrical charge even in normal weather conditions. Please perform all work with the utmost care.

Note: Access Points, antennas and mounting equipment such as masts intended for outdoor operation must be grounded. Exclusively work with Access Points and antennas if you are certain of proper ground. Please seek advice from a qualified electrician to clarify this issue.

Assign the installation and mounting of Access Points and antennas only to experienced IT personnel or trained electricians. Observe the following notices to avoid accidents:

☐ Carry out work of this type with a minimum of two people. This ensures that help can be quicker to hand if an accident occurs despite all safety precautions.

☐ Only use ladders with the appropriate insulation.

☐ Only work in dry weather without wind. If necessary, use a safety harness.

☐ Wear suitable working clothing, such as close-fitting clothing and safety shoes with non-slip soles.

☐ If you should drop components of the antenna or mountings, let them fall without attempting to catch them. Falling antennas, masts or cables may come into contact with live contacts and cause electric shock.

☐ The mounting location should be easily accessible in the interests of future maintenance work or for checking cable connections.

☐ Before commencing with mounting, ensure that you have all the necessary tools and accessory parts. Similarly, ensure that any openings required for the entry of the coaxial or Ethernet cable into the building are already available.
**Note:** In the interests of your own safety, only experienced specialists are allowed to install antennas, masts and the grounding system. Make sure that the specialists are familiar with local conditions and any legal regulations which apply. Furthermore, observe the notices in section “Lightning and surge protection” on page 39 and ensure that the grounding system meets requirements.
4.2 Mounting the Access Points

The method for mounting the Access Points depends on the model's design. This section presents the various mounting types, illustrated by examples. Please refer to the documentation for the relevant Access Points for more specific instructions.

Note: Exclusively a lightning rod with a safety clearance of more than 100 cm protects Access Points installed outside from direct lightning strikes. Make sure that the electrician grounds the Access Points installed outside with an adequately dimensioned potential equalization line (PEL) with a cross-section of at least 16 mm² CU. For the protection of sensitive wireless LAN modules, use an surge-protection device.

4.2.1 Selecting the location for mounting

A suitable location for mounting Access Points should meet the following conditions:

► Avoid covering up of the Access Points and antennas, in order to avoid interference or overheating during transmission and reception.
► Choose a location that is as close as possible to the necessary connections, such as Ethernet cabinets or power sockets.
► Position the Access Points as close as possible to the antennas. The length of the coaxial cable between Access Point and antenna has a considerable influence on the attenuation in the WLAN system as a whole, thus influencing such factors as the available range and data rates.
► Observing maximum separation distances is also important for Access Points and PoE injectors. For example, some Access Points have an increased power requirement that can exclusively be supplied over a specific length of Ethernet cable. You can find detailed advice in the documentation for the ConneXium WiFi Devices or the PoE Injector.
For components which are mounted outdoors, select a location as close as possible to the point where the coaxial or Ethernet cables enter the building. Excessive stretches of outdoor cabling are exposed to increased atmospheric effects.

Avoid locations that are very dusty.

In outdoor areas, avoid locations that are close to exposed metallic conductors, such as gutters, pipes, etc.

### 4.2.2 Installing the device onto or on a flat surface

You have the option of attaching the device with suitable hardware to a vertical flat surface.

- The diameter of the mounting hardware is maximum 0.20 in (5 mm).
- The head diameter is maximum 0.47 in (12 mm).
- The diameter of a flat washer used is maximum 0.48 in (12 mm).

Proceed as follows:
- Prepare the assembly at the installation site.
- Install the device with suitable fastening components.
- Seal all unused connections and ports with protection screws.
4.2.3 Installing the device on a pole

You have the option of installing the device on a pole, pipe, strut, or on a similarly stable construction using a pole mounting set. The pole mounting set you obtain as an accessory.

- The clamping diameter of the mast clamp is maximum 2.56 in (65 mm).
- Tightening straps, available from a specialist dealer, enable you to clamp a larger mast diameter.
  - maximum width of the tightening strap: 0.63 in (16 mm)
  - maximum thickness of the tightening strap: 0.05 in (1.3 mm)
4.3 Mounting antennas

The method for mounting the antenna depends on the model's design. This section presents the various mounting types, and is illustrated with examples. Refer to the documentation of the relevant antenna for more specific instructions.

Note: Make sure that an electrician fixes a lightning rod to antennas mounted outside in an exposed location where direct lightning strikes can occur. Ensure that the specialist installs the lightning rod at a distance of at least 100 cm. Make sure that the specialist electrician grounds antennas mounted with an adequately dimensioned potential equalization line (PEL) with a cross-section of at least 16 mm² Cu. For the protection of sensitive wireless LAN modules, use a surge-protection device.

4.3.1Selecting the location for mounting

Before mounting any antennas, a suitable location for mounting antennas should meet the following conditions:

➤ Mount the antennas in a place offering a good line of sight for transmitting data to mobile WLAN clients or remote P2P stations.

➤ Mount antennas as close as possible to the Access Point. The length of the coaxial cable between Access Point and antenna has a considerable influence on the attenuation in the WLAN system as a whole, thus impacting the available range and possible data rates.

➤ Locations where you mount components outdoors have to be as close as possible to the point where the coaxial or Ethernet cables enter the building. Excessive stretches of outdoor cabling are exposed to increased atmospheric effects.

➤ In outdoor areas, avoid locations that are close to exposed metallic conductors, such as gutters, pipes, etc.
4.3.2 Flat surface mounting

Permanent mounting can take place directly on a flat surface or with the adjustable swivel fixture.

Figure 24: Flat surface mounting
4.3.3 Pole mounting

Alternatively mount the antenna directly on a pole or similar structure, giving the antenna a high degree of exposure.

Figure 25: Pole mounting
4.4 Mounting the lightning rods

Lightning rods create a spatial shield that is designed to protect the components in a wireless LAN such as antennas or Access Points from a direct lightning strike. You should consider the following aspects when choosing where to mount them:

- Dimensioning of the lightning rod
- Vertical and horizontal distance from the components at risk
- Lightning rod grounding

**Note:** Only trained electricians are allowed to perform the dimensioning, installation and grounding of the lightning rods.

4.4.1 Dimensioning of the lightning rod

The task of the lightning rod is to be able to conduct the complete charge of a lightning strike. For this reason it is important for you to select rods made from highly conductive metals, for example copper alloys or steel. It is important for you to select rods with a cross-section that allows the conduction of the lightning charge without damaging the rod. In general, you need rods with a diameter of between 10 and 16 mm.
4.4.2 Distance to the components at risk

The specialist electrician uses the height and the safety clearance of the lightning rod to the equipment to be protected (e.g. antenna) to dimension the lightning rods for a sufficiently large spatial shield.
4.4 Mounting the lightning rods

Figure 26: External lightning protection
1 Spatial shield
2 Protective angle = 45°
3 Safety clearance >100 cm
4 Lightning rod
5 Conductor
6 Grounding
7 Antenna

- Distance of the lightning rods from the antenna: Positioning the lightning rod a sufficient distance away from the antenna prevents the conducted lightning charge from flashing over to the antenna or other conductive components. The specialist electrician can exactly calculate this distance on the basis of several factors. However, in practice a safety clearance of more than 100 cm is generally sufficient.

- Lightning rod height: Make sure that the lightning rod is high enough so that the equipment that is to be protected, such as antennas, is within the spatial shield. Besides the exact rolling sphere method used to determine the areas at risk there is the simpler protective angle method which the specialist electrician can use to approximate the spatial shield formed by
4.4 Mounting the lightning rods

a lightning rod. This method assumes an area of 45° under the lightning rod to be safe from direct lightning strikes.

**Note:** The distance between lightning rod and antenna has a direct influence on the grounding required by the components. Please observe the advice about grounding the lightning rods and grounding the antennas and Access Points.

### 4.4.3 Lightning charge conduction (grounding)

Make sure that the specialist electrician always grounds the lightning rods with a separate, adequately dimensioned potential equalization line (PEL) with a cross-section of at least 16 mm² Cu. Make sure to establish the connection to the grounding system using the shortest path.

**Note:** If the lightning rod and antenna are mounted together on the same mast and the distance to the antenna is more than 100 cm, make sure to adequately insulate the lightning rod from the mast since in this case the lightning rod and the antenna require separate grounding.
Appendix

A Appendix
A.1 Antenna characteristics

Refer to the Antenna Guide for further information. This document is available for download as a PDF file on the Hirschmann product pages (www.hirschmann.com).
A.2 Troubleshooting

If your outdoor WLAN bridge produces throughput rates that are significantly lower than expected, consider the following possibilities:

- **Antenna polarization**
  Some antennas for WLAN transmission rely on certain directions of polarization of the electromagnetic waves. For point-to-point links, align the direction of polarization of the antennas at each end of the connection precisely in the same direction. If the directions of polarization are opposite, the data throughput can be reduced. For this reason check the correct alignment—both in direction and polarity—to provide optimal data throughput when installing outdoor WLAN systems.

- **Weathering**
  When mounted correctly, the Access Points and antennas of outdoor WLAN systems are protected from the effects of rainfall, humidity and other environmental influences. If the seals on the housing or cable connections are mounted deficiently, or if they become damaged, water or water vapor may enter the device, with adverse effects for the electronic components. If you experience sudden variations in data throughput over the WLAN bridge, check the cabling and seals for damage.

- **Free line of sight and Fresnel zones**
  Maximum performance requires a line of sight on one hand and a minimum separation between the line of sight and the ground or other obstructions on the other hand. Use the BAT Antenna Calculator tool that you can download from our Web site at [www.hirschmann.com](http://www.hirschmann.com) to calculate the necessary mast heights for obstruction-free Fresnel zones.
- **Antenna cable**
  To improve performance, use a short length of antenna cable with a low attenuation value.

- **DFS channel selection**
  Check if the Access Point detects vacant channels (see the HiLCOS menu tree under Status/WLAN/Channel scan results).

- **40 MHz mode**
  To improve performance of 802.11n access points, provide a neighboring channel for channel bundling. The HiLCOS menu tree informs you whether an "extension channel" is available under "Status/WLAN/Radios."

- **Distance settings**
  For longer-range wireless links to function properly, specify the range between the two antennas (rounded up to the nearest kilometer). This allows you to adjust the system's internal timing values accordingly.

- **General diagnosis**
  You can inspect packet transmission statistics under Status/WLAN/Packets and status/WLAN/Errors. High values may indicate an environment with strong interference. Check the following values for an indication of the signal/noise ratio and for detecting rogue WiFi Devices: Status/WLAN/Channel scan results, Status/WLAN/WLAN parameters and Status/WLAN/Competing networks. If error rates are 100%, the most probable cause is a value for distance that is too low.
B Further support

Technical questions
For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You find the addresses of our partners on the Internet at http://www.hirschmann.com.

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at https://hirschmann-support.belden.eu.com.

This site also includes a free of charge knowledge base and a software download section.

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  You find the training courses on technology and products currently available at http://www.hicomcenter.com.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:
http://www.hicomcenter.com