



Manual
artem Wx000



Copyright © 2005 Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nuremberg, Germany

No part of this documentation may be reprinted without the prior written permission of Artem GmbH.

<http://www.funkwerk-ec.com>

.....
Windows, Windows NT and Windows 2000 are registered trademarks of Microsoft Corporation.

Other company, trademark, or product names not explicitly mentioned here are trademarks or registered trademarks of their respective owners and are protected.

.....
Imprint

This documentation was compiled and translated by ExperTeach GmbH.

Status: 14. Oktober 2005

Table of Contents

Preface	III
Knowledge Prerequisites	V
Manual Conventions	V
Important Text Passages	VI
artem Service	VI
The ComPoint Product Package	VII
Hardware Description and Commissioning	1-1
ComPoint	1-1
The Power Supply	1-3
The Wall Mounting	1-4
Commissioning	1-4
After Successful Commissioning	1-8
The Basic Configuration	1-10
Booting the ComPoint Manager	1-10
Selecting the Frequency in the 2.4 GHz Band	1-15
Configuring the Ethernet	1-16
Security Measures for your Wireless LAN	1-17
Resetting the Password	1-20
The artem ComPoint Manager	2-1
The User Interface of the ComPoint Manager	2-2
The Functions of the ComPoint Manager	2-4
The ComPoint Enterprise User Interface	3-1
The User Interface via Telnet	3-1
The Browser-Based User Interface	3-5
The User Interface via SSH	3-9
The User Interface via Secure Web	3-9
ComPoint AccessPoint	4-1
The Status Menu	4-2
The Config Menu	4-20
The Control Menu	4-72
The Refresh Command	4-93
The Help Command	4-93

The Exit Command	4-93
ComPoint Bridge Port	5-1
Using the ComPoint Bridge	5-1
Preconditions for Use of Links with ComPoint Bridges	5-5
Configuring the ComPoint Bridge	5-8
Double Bridge	5-33
VLAN Configuration	6-1
Setting up a VLAN	6-2
Adding a Port to a VLAN	6-2
Viewing the VLAN Configuration	6-4
Defining Rules for Receiving Frames on Individual Ports	6-4
Viewing the Receive Rules	6-6
The LED States	A-1
Assignment of LEDs to Ports	A-1
LED States when Booting	A-5
LED States in Wireless Operation	A-6
Technical Data and Specifications	B-1
Frequencies and Channels	B-1
Specifications	B-2
Declaration of Conformity (Page 1)	B-4
Declaration of Conformity (Page 2)	B-5
Glossary	C-1
Index	D-1

Preface

With the products of the ComPoint family, Funkwerk Enterprise Communications offers a complete range of infrastructure solutions to enable wireless communications between a variety of mobile devices as well as entire networks. Utilizing the latest wireless LAN technology, the ComPoint platform has been specifically designed to match the performance requirements of the most demanding professional applications.

Whether deployed as an extension of the existing wired infrastructure or to form an independent wireless network, ComPoint meets the ever-increasing communication needs of your corporate workforce.

Introduction

Flexibility and mobility have become crucial factors in today's business environment, stipulating the need to provide highly efficient and ubiquitous access to data. A wireless infrastructure, as provided by Funkwerk Enterprise Communications with the artem ComPoint product family, serves to offer new opportunities to the most diverse target groups.

New Flexibility

Your decision to build a wireless infrastructure with the artem ComPoint will result in many benefits beyond the mere use of a wireless network. Now, you are much more flexible. Within the wireless infrastructure provided by Funkwerk Enterprise Communications, end devices are able to access the network at any given site, the network can grow with the demands made and according to the requirements of the users, and even bridging to other networks is possible. Without complicated installation and the hassle of wiring. At any location you choose. Right where and when you need it.

New Mobility

Modern work processes and new forms of collaboration rely more and more on the mobility and self-sufficiency of the workforce, but also on instant and ubiquitous access to critical data. Wireless communication with your artem ComPoint offers you the option in demand:

When speaking with your colleague, in the meeting, in the warehouse, on the production site, in the seminar room, in the hotel room, at the airport, on your garden bench, in your living room. —Congratulations, the future of efficient workflows has just begun for you!



Objectives

Simply send your data along the most efficient route—directly over the air. The artem ComPoint product family of Funkwerk Enterprise Communications provides the ideal set of options for all of your demands. The modular concept and versatility of the ComPoint family offer you the freedom and investment protection you'd expect from a cutting-edge wireless infrastructure solution.

Whether you plan to implement a large-scale wireless network spanning multiple sites, enhance the operational efficiency of your small- or medium-sized office with wireless connectivity, or wirelessly network your home:

With the ComPoint family, Funkwerk Enterprise Communications offers solutions appropriate for each and every wireless user.

Knowledge Prerequisites

It is assumed that the reader possesses or is in the process of acquiring the following knowledge:

- Basic knowledge of the setup of networks,
- Knowledge of the basic networking terms and concepts, such as server, client, and IP address,
- Basic understanding of Microsoft Windows operating systems.

Manual Conventions

This manual uses the following text styles for the purpose of guiding through the instructions:

- References to other manuals, chapters, or sections are represented in [blue](#) (on the online help screen and in the PDF version of the manual) and are underlined.

Example:

See [Manual Conventions](#).

- Menus, folders, functions, hardware labels, switch settings, systems messages, etc. are represented in *italics*.

Example:

Push the switch to the *off* position.

- Menus, functions, and subfunctions are separated from each other by the “>” character.

Example:
Select *File* > *Open...*

- Keys you need to press simultaneously are indicated by a “+” character preceding the second key.

Example:
Press Alt+A.

Important Text Passages

Important text passages are marked with symbols in the margin, which have the following meanings:



Caution:

Contains information which has to be observed in order to avoid damaging the hardware or software.



Note:

Contains important general or additional information on a specific topic.



Prerequisite:

Advises you of any prerequisites which have to be fulfilled to perform the subsequent steps.

artem Service

Do you have any questions on our products or do you require specific information on artem ComPoint?

You can contact us, as follows:

- Internet: <http://www.funkwerk-ec.com>
- E-mail (hotline): hotline@funkwerk-ec.com

The ComPoint Product Package

The following components should be contained in your ComPoint product package.

- ComPoint
- Power supply (12 V/220 V)
- Wall mounting for assembling the ComPoint on the wall
- Self-adhesive feet, for use of ComPoint as desktop device
- 2 external, screw-on standard antennas
- Quick start flyer
- Installation CD-ROM
- Flyer with information for the user and declaration of conformity



Note:

If your ComPoint product package does not meet your demands, please contact our artem Service (see Section [artem Service](#)).

You can find a description of the standard components of the ComPoint product package in Chapter [Hardware Description and Commissioning](#).

Hardware Description and Commissioning

This section contains photographs and figures of the individual components of the ComPoint product package, as well as further information on the parts in question.

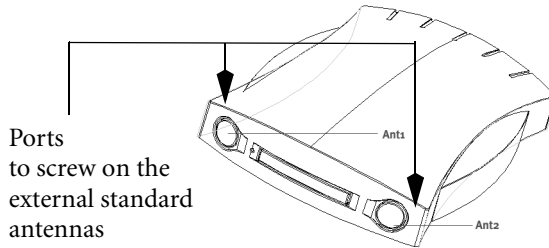
ComPoint

ComPoint can be equipped with various antenna systems. Optionally, external standard antennas, which are screwed on, can be used. ComPoint can either be employed as a desktop device or be mounted on the wall with the help of the wall mounting contained in the product package.



Front View of the ComPoint

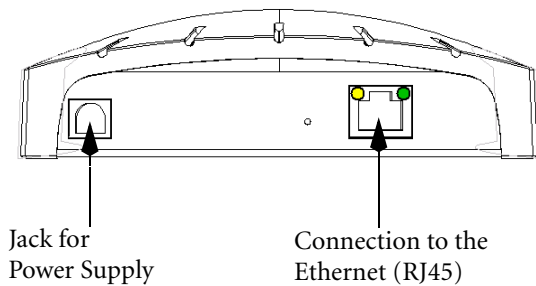
The front side of the ComPoint accommodates the two ports to screw on the external standard antennas.



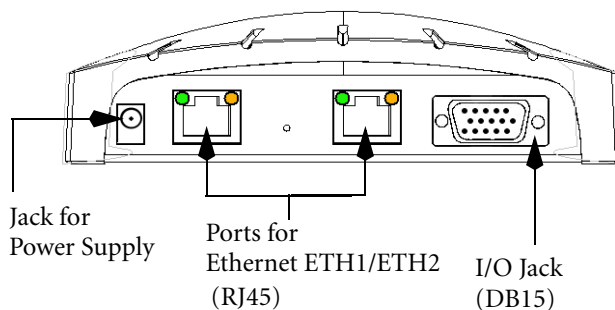
Rear View of the ComPoint

The rear side of the ComPoint accommodates the jack for the power supply and an RJ45 jack for the Ethernet connection.

Compoint (until 2003/01/31)



Compoint II (from 2003/02/01)

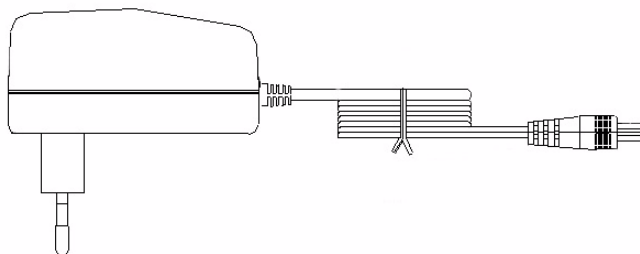


Note:

Please use exclusively ETH 1 or ETH2 for the connection of the ComPoint.

The Power Supply

The power supply is shipped as plug-in power supply.





Note:

If you require foreign adapters or power supplies, please contact our artem Service (see Section [artem Service](#)).

The ComPoint product package contains a power supply with the following specifications:

- Input voltage: 90 V - 264 V
- Input frequency: 47 Hz - 63 Hz
- Output voltage: 12 V DC
- Output current: maximally 1 A

The Wall Mounting

The wall mounting delivered with the package serves to mount the ComPoint on the wall. The required screws and dowels are contained in the product package.

Commissioning

The following section describes how to commission the ComPoint. This procedure is performed in several steps:

1. Screwing on the external standard antenna(s) (optionally).
2. Gluing on the feet if you wish to use the ComPoint as desk-top device, respectively assembly on the wall.
3. Connection to the power supply.
4. Connect the ComPoint to the Ethernet. Select either port ETH1 or ETH2. The second port serves to cascade several devices.

Screwing on the External Standard Antennas

If you wish to use external standard antennas to set up a radio link via the ComPoint, these have to be screwed in at the corresponding ports at the front.

1. Screw in the external standard antenna, respectively both external standard antennas at the corresponding ports. Please adjust the antenna to the desired position before tightening the screw nut. Once you have tightened the screw nut, the radiator can no longer be rotated.
2. If two antennas are connected to the ComPoint in order to use Antenna Diversity, these must be installed so that they keep a minimum distance of 6 cm. The optimum distance is 12 cm. In strongly reflecting environments, it is advisable to adjust the standard antennas in an angle of 90°. In order to do this, adjust the antennas in V form.

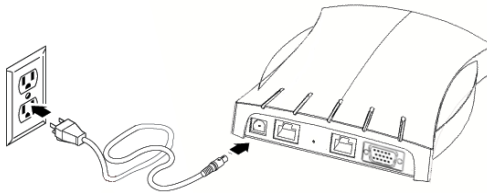
The ComPoint as Desktop Device

1. To use the ComPoint as desktop device, attach the four self-adhesive feet at the lower side of the ComPoint.

Mounting the ComPoint on the Wall

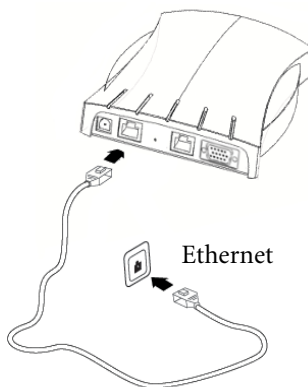
To mount the ComPoint on the wall, use the supplied wall mounting. The required screws and dowels are contained in the product package.

Connection to the Power Supply



1. Take the power supply unit and insert the corresponding plug into the respective jack of the ComPoint.
2. Subsequently, insert the power supply into the mains socket (110 - 240 V).
3. The status LEDs indicate whether the ComPoint is properly connected to the power supply.

Connection to the Ethernet



1. Take one end of an RJ45 patch cable and insert it into the ETH1 or the ETH2 jack of the ComPoint. Please only use an Ethernet port for the connection or configuration of the device.



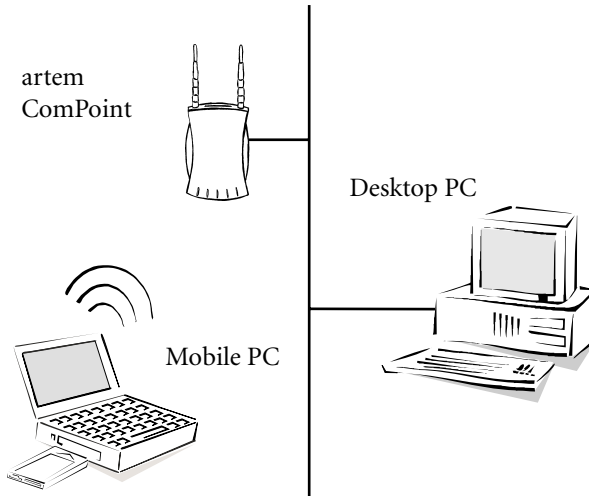
Note:

The standard patch cable (RJ45-RJ45) is designed symmetrically. It is therefore not possible to confuse the cable ends.

2. Insert the other end into a free Ethernet port.

After Successful Commissioning

After connecting the ComPoint to the power supply and setting up a connection to your Ethernet, the ComPoint is ready for use if the following prerequisites are fulfilled:



Prerequisite:

If you are using a PC with an artem radio client, e.g. a laptop with an artem ComCard, you can immediately access your Ethernet via the ComPoint, since the communications parameters match in this configuration.

You may also use any other standard-compatible radio card. In this case, the radio card ought to be in the state of the first commissioning, i.e. it should not be preconfigured.



Note:

To adapt the radio client to already existing configurations of wireless networks, specific settings of the communications parameters are required.



Prerequisite:

To make the required settings, you have to assign an IP address to the ComPoint via the artem ComPoint Manager (see Section [The Basic Configuration](#) on page [Page 1–10](#)). Afterwards, you can start the configuration via a terminal program (e.g. Telnet) or a browser.

The Basic Configuration

This chapter describes which steps have to be performed in order to assign an IP address to your ComPoint via the artem ComPoint Manager.

To configure an IP address for your ComPoint, carry out the following steps:



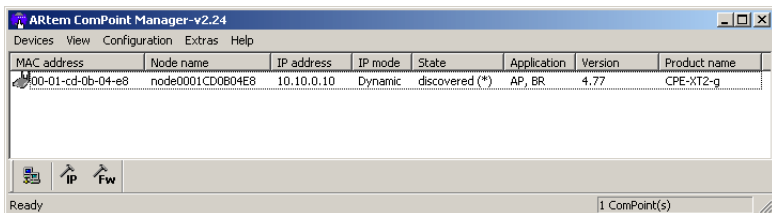
Prerequisite:

The PC which you use to configure the IP address for your ComPoint has to be connected to the same network as the ComPoint to be configured.

Booting the ComPoint Manager

1. Insert the supplied CD into the drive of the corresponding computer.
2. Carry out the instructions of the CD wizard and install the ComPoint Manager.
3. Start the Artem ComPoint Manager from the *Start > Programs > artem > ComPoint Manager menu*.

The following dialog box is displayed:

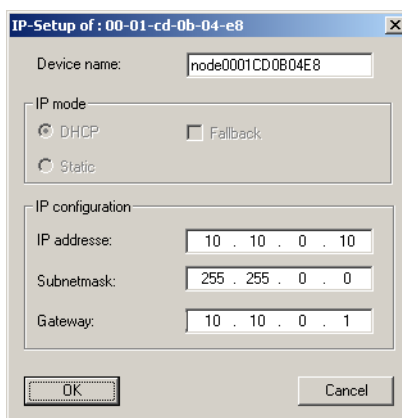


The artem ComPoint Manager identifies the ComPoints installed in your network.

Performing the Basic Configuration

1. Double-click the MAC address of the device to be configured in the list. If you do not know the MAC address of the device: there is a label attached to each device which contains the most important specifications, among them the MAC address.

The following dialog box is displayed:



2. Enter the network parameters (*Device name*, *IP address*, *Subnetmask*, and *Gateway*) and confirm them with *OK*.



Note:

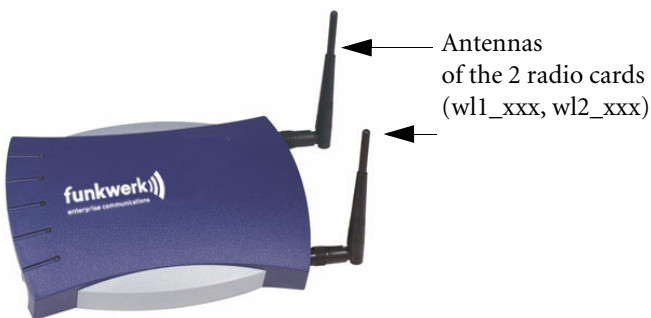
The parameter *Device name* may consist of 32 characters, as a maximum.

When entering the parameter *Device name*, only the letters from “a” to “z”, “A” to “Z”, the digits “0” to “9”, the hyphen “-”, and the dot “.” must be used to avoid errors caused if other systems interpret the parameter *Device name*. The first character has to be a letter, the last character must not be a dot “.” or a hyphen “-”. A single character is not permitted as a name.

Your ComPoint can now be reached with its IP address over the Ethernet via a web browser and/or via Telnet and can be configured.

Conventions for Interface Names

This chapter illustrates the conventions for the ComPoint interface names.



The following table shows the connections between the LEDs and the radio cards of the ComPoint.

Symbol	Function	Slot Number of the Radio Card	Position of Radio Card	Designation in the User Interface
- 1 - ((p))	Radio activity	1	(see figure above)	wl1_XXX
	[S] Radio status			
- 2 - ((p))	Radio activity	2	(see figure above)	wl2_XXX
	[S] Radio status			
	Ethernet activity	-	-	eth1/eth2



Note:

Please observe that in the case of older ComPoint casings, the labels of the ports are reversed.



Note:

With ComPoints which are only equipped with the one card, the card is designated *wl1_xxx* on the interface.

Name Conventions for the Wireless Ports

The names of the wireless ports on the user interface of the ComPoint consist of the following elements:

1. *wl*, *wl* stands for *wireless*
2. Number of the physical port (1 or 2)
3. *_ap*, *ap* stands for AccessPoint port type
4. *_br*, *br* stands for bridge port type

For example:

- *wl2_ap*

In the following descriptions, the designation <Wireless Port> will be used.

Name Conventions for the Ethernet Port

The name of the Ethernet port on the user interface of the ComPoint consists of the following elements:

1. *eth*, *eth* stands for *Ethernet*

The name of the Ethernet port is:

- *eth1* (100 Mbps)

In the following descriptions, the designation <Ethernet port> will be used.

Name Conventions for the Interfaces

The names of the interfaces on the user interface of the ComPoint consist of the following elements:

1. `le`
for the *Ethernet interface type*
2. Number of the interface
(e.g. `le0` or `le1`)

Selecting the Frequency in the 2.4 GHz Band

Although wireless networks can be logically separated by setting the *network name*, they can still physically interfere with each other if they are operated on the same radio channel or on channels which are close together.

Consequently, if you operate two or more wireless networks within short distance, it is advisable to assign different channels to the networks. Since a network also allocates a part of its adjacent channels, these channels should be at least 4 channels apart from each other.

To select the channel frequency, proceed as follows:

1. In order to set up a Telnet connection, boot the ComPoint Manager and select Configuration > Telnet.
2. When the password prompt appears, log in as an administrator by entering the password “admin”. This password has been preset for the admin user level as a factory default.
3. Select *Config* > *Ports* > <*Wireless Port*> > *RF settings*, select the entry *Channel*, and confirm by pressing “Enter” or the right arrow key.
4. On the right side of the table, a list of channels or frequency options will be displayed.

5. The factory default setting for all ports is “Auto_DFS”, i.e. automatic channel selection. You can also select channels manually. If you wish to do this, make sure that the clients in question do support the channels selected by you.



Note:

The number of the available channels is not identical for all device generations. You should, therefore, also refer to the current data sheet for your ComPoint. As a rule, however, channels 1 to 11 are available.

In the case of devices where the factory default setting is not “Auto_DFS”, the preset parameter for port w11 is channel 1 with 2412 MHz, i.e. 2.412 GHz. The preset value for port w12 is channel 11 with 2,462 MHz.

6. Select the desired frequency by using the arrow keys and confirm by pressing *Enter*.

Configuring the Ethernet

With the basic configuration of the ComPoint Manager, you have already configured the IP address, the subnet mask, and the gateway for the ComPoint.

You will find further parameters for configuring the Ethernet port under *Config > Ports > <Ethernet Port>* (e.g. *eth1*).

These parameters are:

- Interface
- Auto neg mode
- Actual value

You will find the description of the individual parameters in [Section Config > Ports > Port <Ethernet Port>, Page 4–24](#).

Security Measures for your Wireless LAN

In order to prevent unauthorized access to your wireless LAN, you ought to take the following measures:

Changing the Passwords for the User Levels

In order to prevent unauthorized access, you should immediately change the passwords of the three user levels *admin*, *user*, and *view*. In [Section Initiating the Telnet Connection and Login, Page 3–1](#), you will find a detailed description of the user-specific rights for each user level.

The following provides a brief introduction on how to determine the passwords of the user levels. If required, you can find more detailed information in [Section Control > Security, Page 4–73](#).

1. In order to set up a Telnet connection, boot the ComPoint Manager and select *Configuration > Telnet*.
2. When the password prompt appears, log on as an administrator by entering the password *admin*. This password has been preset for the *admin* user level as a factory default.
3. On the Telnet interface, select *Control > Security > User control > Edit*.
4. In the list of available user levels on the right side of the table, select the user level for which you want to change the password (*view*, *user*, or *admin*) and confirm by pressing *Enter*.
5. Enter the admin password into the prompt once more and press *Enter*.
6. Now you have to enter the desired new password twice and confirm by pressing *Enter*.
7. The new password will become valid upon the next log-on attempt.



Note:

In case you forget the admin password, you can reset it to the factory default yourself. Proceed as described in Section [Resetting the Password](#).

Setting the Network Name

In contrast to LANs configured via Ethernet, a wireless LAN does not provide cabling to permit a permanent connection between server and clients. This is why malfunctions or access violations can occur in directly adjacent wireless networks.

In order to prevent this, there is a parameter comparable to a domain name in each wireless network which clearly identifies the network. Only clients whose network configuration matches that of the ComPoint can communicate in this WLAN.

The corresponding parameter of the ComPoint is the *Network name*. In the network environment, it is sometimes also called SSID.

In order to set the *network name* on your ComPoint, proceed as follows:

1. Set up a Telnet connection (as described above) and log on as an administrator.
2. Select *Config > Ports > <Wireless Port> (e.g. wl1_ap) > Service sets > <Wireless Port SSID> (e.g. wl1_ap01)*, select the entry *Network name*, and confirm with *Enter* or the right arrow key.
3. Enter the desired network name (*Network name*) into the prompt and press *Enter*.
4. Deactivate *Bcast SSID* under *Config > Ports > <Wireless port> > Service sets > <Wireless port SSID>*. Thus, you prevent the ComPoint from sending the SSID and making it available to hackers.

Merely clients for which this network name (*Network name*) has been set will now be able to access this WLAN.

Defining a Security Level

To prevent the data transmitted via radio technology from being eavesdropped easily, you should provide for an appropriate security level by means of encryption. There are three security levels, namely WEP, WPA2 PSK, and WPA2 Enterprise. WPA2 Enterprise offers the highest security level. This option is rather suited for enterprises, since it requires a central authentication server. Private users should use the WEP encryption method or rather WPA-PSK, which provides a higher degree of security.

1. Set up a Telnet connection (as described above) and log on as an administrator.
2. Select *Config > Ports > <Wireless port> (e.g. wl1_ap) > Service sets > <Wireless port SSID> (e.g. wl1_ap01) > Security > Privacy*
3. Select the desired security level and press *Enter*.
4. According to the security level selected, enter further security parameters.
5. To activate the required security level, select *Config > Ports > <Wireless port> > Service sets > <Wireless port SSID> > Security > State*. Subsequently, select *enable*.

Now, only clients will be able to communicate with the ComPoint for which the same security level and the required security settings have been selected.

You can find further information on security settings in [Section *Config > Ports > <Wireless Port> > Service Sets > <Wireless Port SSID> > Security, Page 4–35*](#).

Creating a Security Access Control List

By creating an access control list, you can control which clients are allowed to access your wireless LAN via the ComPoint. In the access control list, specify the MAC addresses of the clients which are allowed to access to your wireless LAN. Access will be denied to all other clients.

To create an access control list, proceed as follows:

1. Set up a Telnet connection (as described above) and log on as an administrator.
2. Select *Control > Security > Authenticate > ACL local > Add*.
3. Specify the MAC addresses of the clients which are allowed to access your wireless LAN.

For more details on the access control list, refer to [Section Control > Security > Authenticate, Page 4–76](#).

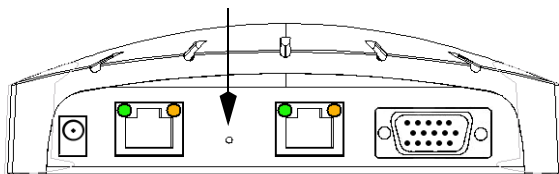
Resetting the Password

If you have forgotten your password, you do not have to return the device to the manufacturer. Please consult our support. The support staff will perform the further steps together with you. For this purpose, keep the serial number and the MAC address of your device at hand.

To obtain this information, you have to stop the ComPoint in the monitor status. Proceed as follows:

At the rear of the ComPoint, there is a little hole. The monitor button is accommodated behind this hole.

Monitor button



1. Keep the monitor button pressed for approximately 4 seconds with the help of a small object, e.g. a paper clip, while booting the device.



The monitor button must be pressed before connecting the ComPoint to the mains supply.

2. The monitor status will then be displayed via a special LED status.

Our Support will inform you of further steps to be taken.

The artem ComPoint Manager

This chapter describes additional configuration options for the artem ComPoint Manager, which go beyond the basic configuration.

The basic configuration comprises the following settings:

- Entering the *name*
- Entering the *IP address*
- Entering the *netmask*
- Entering the *standard gateway*

Further configurations which can be performed via the artem ComPoint Manager are:

- Setting up a *Telnet connection* (not with CPI, CPW, CPB)
- Setting up a *web connection*
- *Firmware upgrading*
- *Restart* (restarting the device)
- Resetting the device to the *factory default settings*
- Saving/loading/resetting the configuration
- Password change
- Calling up the software version
- Calling up hardware information



Prerequisite:

The PC which you use to configure your device must be installed in the same network as the device to be configured.



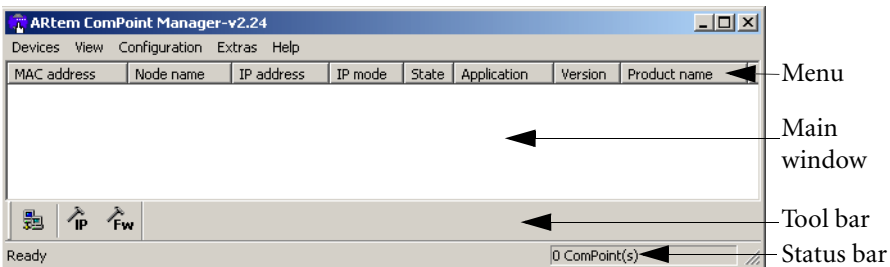
Working with the ComPoint Manager

- The computer has to be provided with a working and sensibly configured TCP/IP stack.
- If the router does not forward multicasts, the search function is limited to the subnetwork of the PC on which the ComPoint Manager is installed.

- The device can only be configured via a password. For security reasons, it is recommended to change the preset password as soon as possible.
- If your computer accommodates various network interfaces, you can configure a special multicast interface in the artem ComPoint Manager with which you can search for the devices (see [How to Define a Multicast Interface](#) on [Page 2–19](#)).

The User Interface of the ComPoint Manager

The user interface of the ComPoint Manager consists of four components which will be explained in the following:



The Main Window

The main window is designed like a table and is divided into the columns *MAC address*, *Node name*, *IP address*, *IP mode*, and *State*. According to the configuration, it also contains the columns *Application*, *Version*, and *Product name*.

After booting the ComPoint Manager, it immediately searches the network for devices. As soon as the ComPoint Manager has found devices, the columns are filled with data referring to the corresponding devices.

If the main window remains empty, the ComPoint Manager has not found any devices.

The Menu

The menu is located at the upper margin of the ComPoint Manager and contains the menu items *Devices*, *View*, *Configuration*, *Extras*, and *Help* with up to 9 items each. The numerous functions which can be activated via this menu will be discussed in detail later on in this chapter.

The Tool Bar

The tool bar is located directly below the main window and provides fast access to *Discovery*, *IP-Setup*, and *Load firmware*, the three main functions of the ComPoint Manager. These three functions, which can also be selected via the menu, will be illustrated in detail in the following.

1. Select *View > Tool Bar* to show or hide the tool bar.

The Status Bar

The status bar at the lower margin of the window displays the current status of the ComPoint Manager, as well as a short description of the menu item above which the mouse pointer is currently located. Moreover, the number of the discovered devices and the progress of the search process are displayed here.

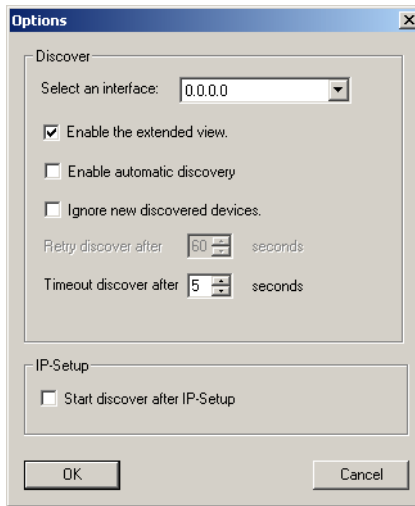
If the ComPoint Manager searches for devices, the *Cancel* button is displayed in the status bar. If you click on this button, the search is canceled.

1. Select *View > Status Bar* to show or hide the status bar.

The Functions of the ComPoint Manager

Searching for Available Devices

You can configure search options via the *Extras > Options dialog box*.

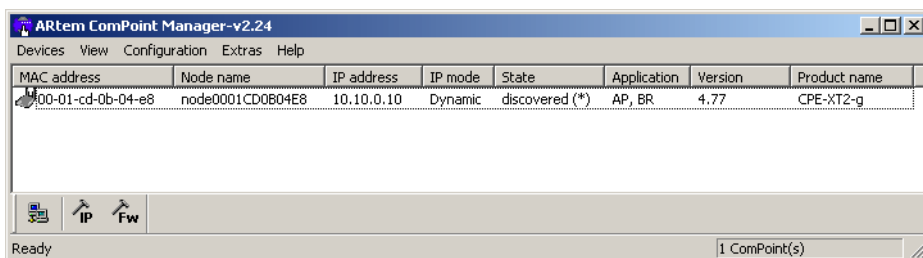


- If you check the *Enable extended view* option, the main window is extended by the *Application*, *Product name*, and *Version* columns.
- If you want to repeat the discovery process automatically, check the *Enable automatic discovery* option. Under *Retry discover after*, you can select values from 10 to 60 seconds. After the expiration of this time interval, the ComPoint Manager will automatically restart the discovery process.
- If you want the ComPoint Manager only to update the parameters for the devices already found during the search, select the *Ignore new discovered devices* option. In this case, the ComPoint Manager will not search for new devices. This option is helpful if a very large number of devices is operated in the network.
- You can abort the discovery process after a defined time interval. In small networks with only a few devices, for instance, you can reduce this time span to 3 seconds. The maximum value is 10 seconds.

After making all settings, click *OK* to take over these settings.

The *Discovery* function can be activated both via *Devices > Discovery* or directly via the *Discovery* button in the tool bar.

The ComPoint Manager will then automatically identify the devices which have been installed in the network and display them in the main window together with the corresponding parameters (*MAC address, Node name, IP address, IP mode, State*). According to the setting of the options, the working mode (*Application*), the firmware version (*Version*), and the *Product name* will also be displayed.



- **IP mode**

- static: The IP address of the device was assigned statically. DHCP has been deactivated on the device.
- DHCP: The IP address of the device was assigned by a DHCP server. DHCP has been activated on the device.
- Fallback: DHCP has been activated on the device, but the device has not been assigned any IP address. The address which is automatically set by the device in the case of a fallback corresponds to the IP address which was statically assigned. If the IP address set in the delivery state is displayed here (0.0.0.0), you have to assign the IP address manually under *Configuration > IP-Setup*.



Note:

If an IP address is assigned manually via the ComPoint Manager and/or the web/Telnet interface, DHCP is automatically deactivated. This means that the IP address of the device will no longer be assigned via the DHCP server as soon as the device has been rebooted.

- **State**

In the *State* column, the following entries can be made:

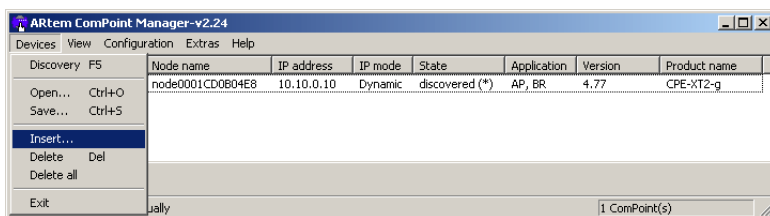
- discovered: discovered by the ComPoint Manager
- not found: device was not found during the new search.

The subsequent brackets may contain the following additional specifications:

- (MAC): Means that a device was found via the artem discovery protocol, but cannot be reached via IP. This will happen, for instance, if the device still uses the default setting 0.0.0.0 or an invalid IP configuration.
 - (IP): Means that the device cannot be reached via the artem discovery protocol, but can be addressed via IP. This usually happens if the IP configuration of the device does not correspond to the current subnetwork, e.g. because a device has been entered manually.
 - (*): Means that the device was found via the artem discovery protocol and can be reached via IP.
 - [Time] (only if not found): Specifies the period of time passed since the last successful search process. This time specification is only updated if a search process is carried out either manually or automatically, according to the individual settings.
- **Application**
The *Application* column indicates in which mode the device is working.
 - AP: access point
 - BR: bridge (will only be displayed for ComPoint Enterprise)
 - AC: access client
 - SC: serial client

Editing Entries Manually

The *Devices* menu items provides functions for manual editing of the devices.

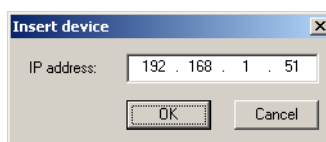


How to Add a Device Manually

You can add devices manually if you cannot find them via the discovery function of the ComPoint Manager. This may be the case if a router is operated between the device and the PC on which the ComPoint Manager has been installed and if this router does not forward the group address of the artem discovery protocol (239.239.239.239).

1. Select *Devices > Insert*.

A dialog box is opened in which you can enter the IP address of the new device.



2. Confirm the entry by clicking the *OK* button.

The manually added device will now be added to the list displayed in the main window. In the *State* column, the *discovered (IP)* entry is displayed.

How to Delete Device Entries

1. Select the MAC address of the entry to be deleted. If you push the “*Shift*” button, you can select several devices simultaneously using the arrow keys.

2. Select *Devices > Delete*. Alternatively, you can also press the “Del” button on your keyboard.

How to Delete All Device Entries

Select *Devices > Delete all*, to delete all entries simultaneously from the list in the main window.



Note:

If you have deleted all devices, the *Ignore new discovered devices* option (available under *Extras > Options*) will be deactivated for a defined time interval.

Saving Information on Devices and Loading It

You can save information on devices in the form of a text file (.txt) or of a csv file (.csv). You can also open these files in the ComPoint Manager later on and import them. This is helpful, for instance, if you wish to add devices manually which will probably not be found via the artem discovery protocol after restarting the ComPoint Manager.

The MAC address, the IP address, the host name, the network mask, and the default gateway are saved.

Proceed as follows to save information on the devices.

1. Select the device for which you wish to save information.
2. Select *Devices > Save*.
3. Specify a directory and a file name.

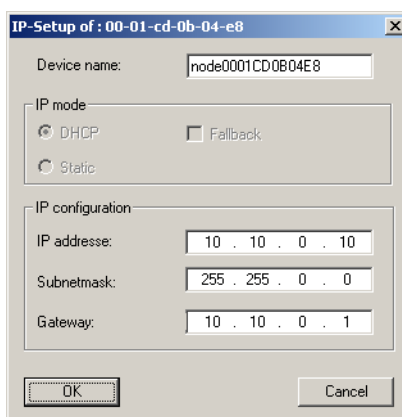
If you wish to import the data into the ComPoint Manager later on, select *Devices > Open*.

Configuring Devices

Basic Configuration

1. Double-click the MAC address of the device to be configured in the list. If you do not know the MAC address of the device: there is a label attached to each device which contains the most important specifications, among them the MAC address.

The following dialog box is displayed:



The image shows a dialog box titled "IP-Setup of : 00-01-cd-0b-04-e8". It contains the following fields and options:

- Device name: node0001CD0B04E8
- IP mode: DHCP, Fallback, Static
- IP configuration:
 - IP address: 10 . 10 . 0 . 10
 - Subnetmask: 255 . 255 . 0 . 0
 - Gateway: 10 . 10 . 0 . 1
- Buttons: OK, Cancel

2. Enter the network parameters (*Device name*, *IP address*, *Subnetmask*, and *Gateway*) and confirm them with *OK*.



Note:

The parameter *Device name* may consist of 32 characters, as a maximum.

When entering the parameter *Device name*, only the letters from “a” to “z”, “A” to “Z”, the digits “0” to “9”, the hyphen “-”, and the dot “.” must be used to avoid errors caused if other systems interpret the parameter *Device name*. The first character has to be a letter, the last character must not be a dot “.” or a hyphen “-”. A single character is not permitted as a name.

Your ComPoint can now be reached with its IP address over the Ethernet via a web browser and/or via Telnet and can be configured.

How to Save and Load a Configuration

The ComPoint Manager, Version 2.08 and higher, offers you the option to save the configuration of the device and (re)load it, if required. Please observe that this function can be guaranteed to run without faults only for Firmware Version 3.10 and higher.

To save a configuration, select the device for which you want to save the configuration. Subsequently, select *Configuration > Configuration save*.

To load a configuration, select the device for which you want to load the new configuration. Subsequently, select *Configuration > Configuration load*.



Note:

Passwords and IP settings which you have already assigned will not be saved or loaded in this process.

How to Reset a Configuration

1. Select the device for which you want to reset the configuration.
2. Subsequently, select *Configuration > Configuration reset*.
3. Confirm the following query with *OK*.

The configuration of the device is reset and the device is restarted.



Note:

If you reset the configuration, the IP settings and the passwords will be maintained. If you wish to delete the IP settings and the passwords as well, you have to reset the device to the factory default settings. Refer to [Section Resetting the Device to the Factory Defaults, Page 2–20](#).



Note:

If you reset the configuration, DHCP will be activated on the device. If you have assigned a static IP address to the device and if you wish to continue using this address after resetting the configuration, you have to deactivate DHCP via the web or Telnet interface under *Configuration > Interface*.

Administrating the Password

Function of the Password

The password is required to use the following functions of the ComPoint Manager:

- Load firmware
- Restart
- Factory default
- IP-Setup
- Configuration load
- Password change
- Configuration reset

How to Enter the Password

To enter the password, proceed as follows:

1. Select the device in the list and select *Extras > Password*.

The following dialog box is opened.



2. Enter the password for the device.

The factory-set password on the administrator user level is *admin*.

If you check the *Assign password to all ComPoints* option, the password will also be used for all other devices displayed in the main window. For new devices which are added you have to re-enter the password.

If you exit the ComPoint Manager, you have to re-enter the password after restarting the ComPoint Manager.

You can delete the password in the user interface of the device under *Configuration > Administration*. Moreover, you can change the password in the ComPoint Manager under *Configuration > Password change*.

Password Change



Note:

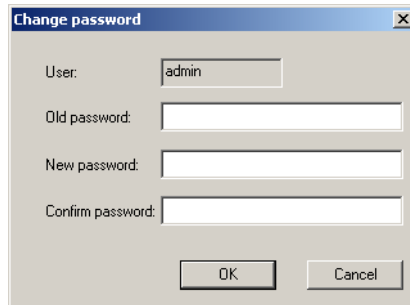
The default password of the device is “admin”. You should change it immediately after commissioning the device to protect it from unauthorized access. Moreover, you should change the password in regular intervals.

If the device has to be repaired by Artem, you should reset the password to the factory default parameter “admin”.

To change the password of your device, proceed as follows:

1. Select the device in the list and select the *Configuration > Password change* menu.

The following dialog box is opened:

A screenshot of a 'Change password' dialog box. The dialog has a title bar with the text 'Change password' and a close button (X). Inside the dialog, there are four input fields: 'User:' with the text 'admin' entered, 'Old password:', 'New password:', and 'Confirm password:'. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

2. Enter the old password for the device.
3. Enter the new password and confirm it under *Confirm password*.
4. Click the OK button.

You have changed the password for the device.

How to Set up a Web Connection

1. In the main window, select the device which you want to access via the web (browser-based interface) and select *Configuration > Web*. Alternatively, you can select the *Web* function with the right mouse button.
2. A browser window is opened.
Your web browser opens a dialog box in which you can enter the password.
3. Enter the password of the device under *Password* and click the *Login* button. The factory-set password is "admin".

You can delete the password in the user interface of the device under *Configuration > Administration* and change it in the ComPoint Manager under *Configuration > Password change*.

How to Upgrade the Firmware

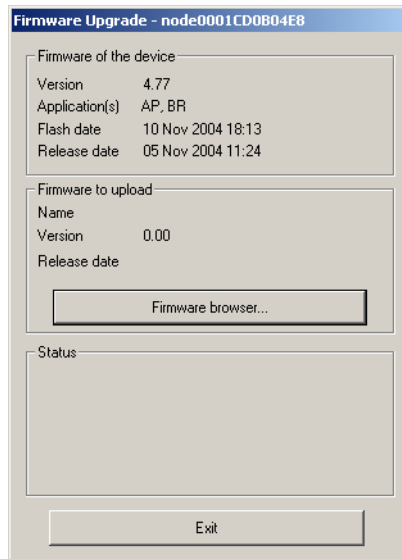


Caution!

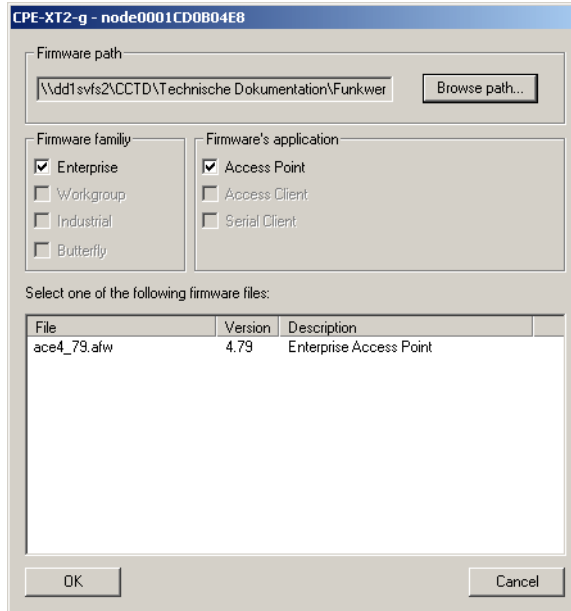
During the firmware upgrade, you must neither turn off the device nor interrupt the data connection. Otherwise, the software installed in the device will be damaged. You will then have to return the device to the vendor.

1. Before upgrading, make sure that the new firmware version (files ending with *.afw) is available on your hard disk or on another data carrier.
2. Under *Extras > Password*, enter the password of the administrator user level if this has not been done yet. Otherwise, an update will not be possible.
3. In the main window of the ComPoint Manager, select the device which you want to upgrade and select *Configuration > Firmware upload...* Alternatively, you can use the firmware upgrade option *Fw* in the toolbar.

4. In the new dialog box, click the *Firmware browser...* button.



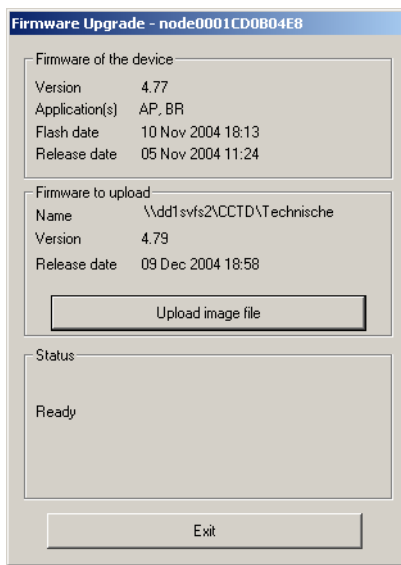
The following dialog box is opened:



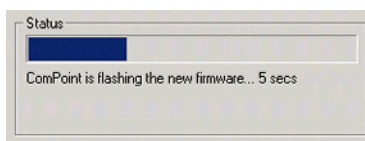
The ComPoint Manager makes the settings under *Firmware family* and *Firmware's application* automatically, based on the settings of the device.

5. Click *Browse path...* and select the folder which contains the firmware.
6. Select the file which contains the new firmware. In our example, this is the file *ace4_70.afw*.
7. Click the *OK* button.

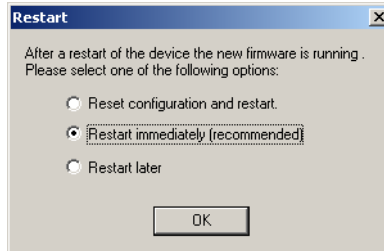
The path for the firmware in the control box under *Firmware path* is automatically updated, and the ComPoint Manager checks whether an upgrade is possible and makes sense.



8. Start the firmware upgrade by clicking the *Upload image file* button. Under *Status*, a progress bar and the current process are displayed.



9. As soon as the firmware upgrade has been finished successfully, the following dialog box appears:



You can choose between a simple restart of the device, a restart with a simultaneous reset of the configuration to the factory defaults, or a restart at a later point of time.



Note:

The ComPoint Manager has already selected the option you require. If the *Restart immediately (recommended)* option is activated, you can also check the *Reset configuration and restart.* option to reset the device to the factory default settings.



Caution!

If the ComPoint Manager suggests the *Reset configuration and restart.* option, you must never select the *Restart immediately (recommended)* option.

10. To restart the device, confirm by clicking *Yes*.



Note:

The restart of the device is not displayed on your computer screen. With the help of the LEDs of your device, however, you can check the radio activity, the radio status, and the Ethernet activity.

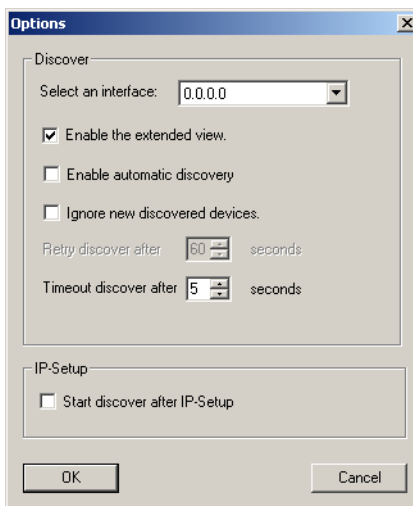
11. Finally, check the operability of the device, for instance by searching for devices installed in the network via the ComPoint Manager.

How to Define a Multicast Interface

If the PC on which the ComPoint Manager is installed is provided with various network interfaces, you can use this function to determine via which interface devices are searched.

1. To select a multicast interface manually, go to *Extras > Options*.

The following dialog box is displayed:



2. Select the IP address of the NIC of your PC which you want to use as a multicast interface and confirm by clicking *OK*.

If the multicast interface 0.0.0.0 is defined, the search is performed via all network interfaces of the PC.

Resetting the Device to the Factory Defaults



Note:

The complete configuration of the device is reset to the factory defaults, including the password and the IP settings.

1. To cancel configurations made and to reset the device to the factory defaults, select *Configuration > Factory default*.

The device will be automatically restarted.



Note:

If you do not want to reset the password and the IP settings, select the *Configuration > Configuration reset* option.

Restart the Device

1. Select *Configuration > Restart* to restart the device.

How to Exit the ComPoint Manager

1. Select *Devices > Exit* to exit the ComPoint Manager.

The ComPoint Enterprise User Interface

The User Interface via Telnet

This section describes the setup of the Telnet user interface.

Initiating the Telnet Connection and Login

1. In the artem ComPoint Manager, initiate your Telnet connection via *Configuration > Telnet*.

The initial screen of the terminal opens in a new window. You are requested to enter a password to log on to one of the user levels.

```

                                     Welcome to artem WLAN products!

                                     Funkwerk Enterprise Communications GmbH, Neu-Ulm, Germany
                                     http://www.funkwerk-ec.com

                                     artem W2000 V5.0

Node Name:  node0001CD0B4F66                UpTime :  2:39:14

password:
```

There are three different user levels: *Admin*, *user*, and *view*.

The *admin* user level allows unlimited access to all ComPoint functions.

The factory default for the password of this user level is *admin*.

If you log on as a *user*, the access to specific system-relevant configuration options will be denied. In particular, the *user* user level does not allow you to make any settings leading to the termination of the network connection between ComPoint and clients.

The factory default for the password of this user level is *user*.

The *view* user level does not allow you to configure the ComPoint in any way. You can merely view some status screens.

The factory default for the password of this user level is *view*.

2. Enter the password for the desired user level and confirm with *Enter*. Now you have access to the main menu.



Note:

For safety reasons, it is recommended to change the preset passwords as soon as possible. You can learn how to change the passwords in [Section Control > Security > User control > Edit](#), [Page 4–74](#).

Setup of the Telnet User Interface





Title section	artem WLAN products by Funkwerk-EC)))																					
Path	artem W2000 V5.0 Main node0001CD0B4F66																					
Menu and command section	<table border="1"> <thead> <tr> <th>Menu</th> <th>Main</th> <th>Submenu</th> </tr> </thead> <tbody> <tr> <td>1 - Status [->]</td> <td></td> <td>Summary</td> </tr> <tr> <td>2 - Config [->]</td> <td></td> <td>Ports [->]</td> </tr> <tr> <td>3 - Control [->]</td> <td></td> <td>ARP cache [1]</td> </tr> <tr> <td>4 - Refresh [5]</td> <td></td> <td>Buffer util. [18%]</td> </tr> <tr> <td>5 - Help</td> <td></td> <td></td> </tr> <tr> <td>6 - Exit</td> <td></td> <td></td> </tr> </tbody> </table>	Menu	Main	Submenu	1 - Status [->]		Summary	2 - Config [->]		Ports [->]	3 - Control [->]		ARP cache [1]	4 - Refresh [5]		Buffer util. [18%]	5 - Help			6 - Exit		
Menu	Main	Submenu																				
1 - Status [->]		Summary																				
2 - Config [->]		Ports [->]																				
3 - Control [->]		ARP cache [1]																				
4 - Refresh [5]		Buffer util. [18%]																				
5 - Help																						
6 - Exit																						
Status section	Show status.																					
Input section	User is authorized at 'admin' level. Enter a number or name. 0:23:53 [admin] >																					

The user interface is divided into five main sections:

- **Title section**
Contains general information, for instance, the ComPoint version used (in the example: *V4.81*) and the name of the ComPoint to be configured (in the example: *node0001CD0B4F66*).
- **Path**
The path (e.g. *Main*) indicates your current position on the user interface.
- **Menu and command section**
Displays the individual menus and commands in the form of a table. The left-hand column of the table indicates the menu you are currently in. The currently selected menu item is highlighted. In our example, *Status* has been selected. The right-hand side of the table displays the submenu of the currently selected menu item, if available. This means that the *Status* menu item has a submenu with the following options:
Summary, *Ports*, *ARP cache*, and *Buffer util.*

Menu items (e.g. *Config*) or commands (e.g. *Exit*) are represented by a number, a name, and, if applicable, by a value stated in square brackets. If an arrow is displayed next to the name of a menu item instead of a value, this means that a sub-menu exists.

As Telnet does not support the use of the mouse, you have to use the arrow keys of your keyboard to navigate the individual menus.

Key	Meaning
 	Move upwards or downwards in the menu item list or command list.
	Move to the submenu of the selected menu item.
	Return to the previous menu.

You can also directly call a menu item or command by entering its number or name. You will find a detailed list of all keyboard commands under the *Help* command.

- Status section
Shows information on the menu item or command you have selected at present, as well as the status of currently performed actions.
- Input section (prompt)
Displays the currently available keyboard commands as well as the active user level. Here, you will also find the prompt where you can enter the keyboard commands.

The Browser-Based User Interface

This section describes the structure of the browser-based user interface and explains how to start it. The browser-based interface is dependent on the browser used (Internet Explorer, Netscape, Opera, etc.), not on the operating system. In the below example, the Internet Explorer was used for the purpose of configuration.

Starting the Browser-Based User Interface

You have 2 options to start the web interface:

- Starting directly via the browser
- Starting via the *Configuration* menu in the ComPoint Manager

Option 1—Starting via the Browser

1. Start the browser which you normally use, e.g. Microsoft Internet Explorer.
2. Enter the following into the address line:
http://<IP address of the ComPoint>
e.g.: http://192.168.1.5

Option 2—Starting via the ComPoint Manager

1. In the main window of the ComPoint Manager select the ComPoint which you want to access via the Web (browser-based interface) and select the *Configuration > Advanced > Web* menu or use the right mouse button and select the *Web* menu in the pop-up list.

The browser-based user interface of the ComPoint will now be displayed.



2. Enter your password into the *Password* input field.

This is factory-set for the admin user interface.

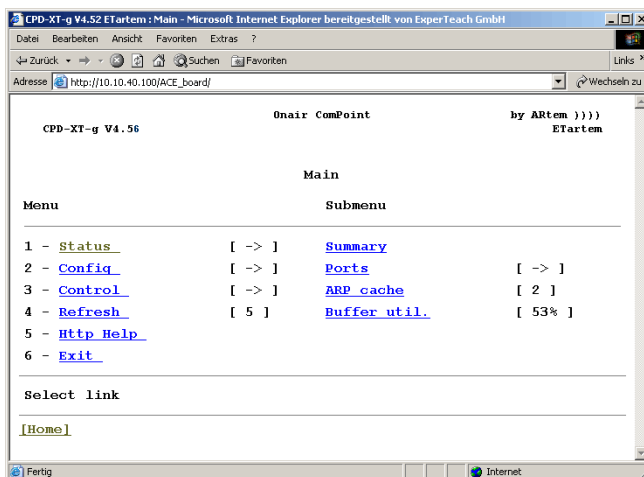
Password: admin

You can change the password on the ComPoint user interface under *Control > Security > User Info > Edit* (see [Section Changing the Passwords for the User Levels, Page 1–17](#)).

The Structure of the Browser-Based User Interface

The browser-based user interface is designed similarly to the Telnet user interface.

Section [Section Setup of the Telnet User Interface, Page 3–3](#) provides further information on this subject.

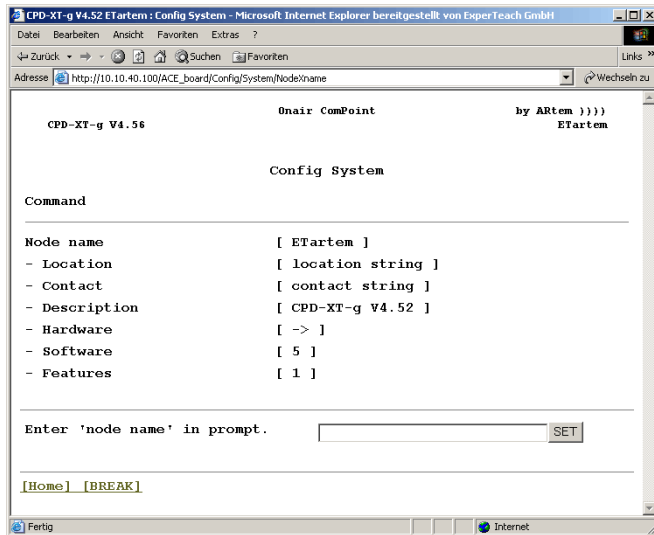


Navigating the Browser-Based User Interface

You can navigate the browser-based user interface like an Internet page.

By clicking links, you will reach the next level.

If you have to enter values, an input window will be displayed in which you can enter the values.



Menus and Parameters of the Browser-Based User Interface

You will find the illustrations and descriptions of all menus and commands as well as the corresponding parameters in Chapter [ComPoint AccessPoint](#), starting with [Section The Status Menu, Page 4-2](#).

The User Interface via SSH

If you are working with an SSH client, you can use SSH (Secure Shell) instead of Telnet and, thus, perform the configuration in the secure mode. The setup of the user interface corresponds to the setup of the Telnet user interface, as described on [Page 3-1](#) ff.

The User Interface via Secure Web

Secure Web also permits the setup of a secure configuration. In this case, you can configure the device via HTTPS. The setup of the user interface corresponds to the setup of the browser-based user interface, as described on [Page 3-5](#) ff.



ComPoint AccessPoint

This chapter describes the different functions of the ComPoint in the operating mode as access point. These functions include, for example:

- Displaying various ComPoint status values,
- Configuration of system, interface, and filter settings,
- Access rights control.



Prerequisite:

The PC which you use to configure your ComPoint has to be connected to the same network as the ComPoint to be configured.






Note:

All settings made via the ComPoint Manager can be made via routers, as well.



Note:

The artem ComPoints are operated with different technologies. Depending on which technology is used, the configuration interface varies at some points. The differences are indicated by means of the following symbols:

Symbol	Meaning
	Menu item or option only applies to devices operated according to IEEE 802.11a.
	Menu item or option only applies to devices exclusively operated according to IEEE 802.11b.
	Menu item or option only applies to devices operated according to IEEE 802.11g.

The Status Menu

The information on the ComPoint summarized in the *Status* menu can only be displayed but not configured by the user. The values displayed as statistical values can be reset to ZERO by the authorized user logged in on the ADMIN user level.

This does not apply to information given in the summary view.

```
artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

                                Main
Menu                             Submenu
-----|-----
1 - Status [ -> ]                Summary
2 - Config [ -> ]                Ports [ -> ]
3 - Control [ -> ]                ARP cache [ 2 ]
4 - Refresh [ 5 ]                Buffer util. [ 43% ]
5 - Help
6 - Exit

                                Show status.

User is authorized at 'admin' level.
Enter a number or name.
5:31:19 [admin] >
```


Status > Summary

1. Select *Status > Summary* to get an overview of all important network parameters.

```

                                artem WLAN products                by Funkwerk-EC ))))
artem W2000 V5.0                                node0001CD0B4F66

                                Status

-----

Primary If  IP config      DHCP      SNMP Filter      Uptime
-----
IP address  010.010.000.009  in use    off  Prot: macFlt    2:27:47
Subnet mask 255.255.000.000                Mflt: forward
Gateway     010.010.000.001                Sessions
                                           1

Port        MAC address      Speed      Mode Link      Info
-----
eth1        00:01:CD:0B:4F:66 10          HD   +
eth2        00:01:CD:0B:4F:67 100         HD
wl1_ap01    00:01:36:0B:6C:9C --@06-2437* AP   -          ARtem      0 Cl.
wl2_br1     00:01:36:0B:6C:A0 --@11-2462* BR   - S --- N --- dBm S/N -- dB

Enter [SPACE]refresh, [q]quit:

```

The following table gives an explanation of the terms and parameters used on the screen.

Parameter	Meaning
Primary If	Displays the IP address, the subnet mask, and the gateway of the ComPoint.

Parameter	Meaning
DHCP	<p>States whether the IP address was requested from a DHCP server, or whether a preconfigured IP address is used.</p> <ul style="list-style-type: none"> • <i>disabled</i>—DHCP is deactivated. A preconfigured IP address is used. • <i>in use</i>—DHCP is activated. An IP address was assigned by the DHCP server. • <i>failure</i>—DHCP is activated. No IP address was assigned by the DHCP server. <p>You can make your DHCP settings under Config > Interfaces > DHCP.</p>
SNMP	<p>Shows whether SNMP is active (<i>on</i>) or inactive (<i>off</i>). See Section Control > SNMP, Page 4–83.</p>
Filter	<p>Displays the filter settings (see Config > Filtering, Page 4–47).</p>
Uptime	<p>Displays the period of time since the last restart.</p>
Sessions	<p>Number of active user connections.</p>
Port	<p>Displays all active ports.</p>
MAC address	<p>Displays the MAC addresses of the individual ports.</p>
Speed	<p>Displays the preset speed of the individual ports in Mbps. In the case of wireless ports, the MAXIMUM technology-dependent frequency is displayed. The display is set up as follows: ss@cc-ffff; ss=max. speed, cc=channel number, ffff=frequency in MHz.</p> <p>You can set the transmission speed under Config > Ports > <Wireless Port>.</p>

Parameter	Meaning
Mode	<p>Displays the transmission mode for the Ethernet port and the wireless port.</p> <p>The following modes are possible for the individual ports:</p> <p>Ethernet port</p> <ul style="list-style-type: none"> • <i>FD</i> stands for full duplex mode. • <i>HD</i> stands for half duplex mode. <p>Wireless port</p> <ul style="list-style-type: none"> • <i>AP</i> stands for AccessPoint mode. • <i>BR</i> stands for bridge mode. • <i>DBR</i> stands for double bridge mode. <p>You can set the transmission mode under Config > Ports > <Wireless Port>.</p>
Link	<p>Specifies whether a connection is currently active at the corresponding port.</p> <ul style="list-style-type: none"> • +: connection is active • -: connection is inactive • no symbol: The Ethernet port is disconnected.
Info	<p>Provides general information on the status of the ComPoint, such as:</p> <ul style="list-style-type: none"> • Swung dash (~): Bcst SSID is enabled. For safety reasons, we recommend to disable Bcst SSID. • S: Reception strength of the signal at the wireless port in dBm • N: Reception strength of the noise at the wireless port in dBm • S/N: Signal-to-noise ration in dB. Indicator of the transmission quality. • Cl.: Number of wireless clients currently connected to the ComPoint.

Status > Ports

The *Ports* menu item leads you to the status screen and to further data on the ComPoint ports.



Note:

It depends on the hardware configuration of the ComPoint which ports are displayed here.

Status > Ports > <Ethernet Port>

This menu item displays the MAC address, the maximum transmission speed, and the status screen with the most important parameters of an Ethernet port (e.g. eth1).

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Status Ports eth1

Command
-----|-----
1 - MAC           [ 00:01:CD:0B:4F:66 ] |
2 - Max speed     [ 100 ]                |
3 - Port stat     [          ]           |

                                Show traffic statistics of this port.

Enter a number or name, "=" main menu, [ESC] previous menu.
6:08:44 [admin] >
  
```

The following table provides a detailed explanation of the commands.

Command	Meaning
MAC	Here, the MAC address of the Ethernet port is displayed. It cannot be changed on any user level, however.
Max speed	The number in brackets shows the maximum transmission speed of the Ethernet port in Mbps. This entry cannot be changed.
Port Stat	Under <i>Port Stat</i> , you can view statistics of the frames received, sent, and filtered at the Ethernet port.

Port stat

Via *Status > Ports > <Ethernet Port> > Port Stat*, you can go to the following screen:

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Status Ports eth1

Parameters                        Value
-----
Received frames since last reset  50793
Transmitted frames since last reset  1076
Filtered frames since last reset    22072
MULTICAST received frames since last reset  0
MULTICAST transmitted frames since last reset  206
MULTICAST filtered frames since last reset    0
Filtered frames (on all ports) since last reset  22072

Enter [SPACE]refresh, [r]reset, [q]quit:

```

The following table gives an explanation of the terms and parameters used on the screen.

Parameter	Meaning
Received frames since last reset	Number of received frames since the last reset.
Transmitted frames since last reset	Number of sent frames since the last reset.
Filtered frames since last reset	Number of filtered frames since the last reset.
MULTICAST received frames since last reset	Number of received multicast frames since the last reset.
MULTICAST transmitted frames since last reset	Number of transmitted multicast frames since the last reset.
MULTICAST filtered frames since last reset	Number of filtered multicast frames since the last reset.
Filtered frames (on all ports) since last reset	Number of filtered frames of all ports since the last reset.

Status > Ports > <Wireless Port>

This menu item indicates the key parameters of a wireless port (e.g. wl1_ap).

```

artem W2000 V5.0                                artem WLAN products                                by Funkwerk-EC ))))
                                                node0001CD0B4F66

                Status Ports wl1_ap01

Command
-----|-----
1 - MAC           [ 00:01:36:0B:6C:9C ] |
2 - Max speed     [ 54 ]                 |
3 - Network name [ ARtem ]              |
4 - Card type     [ -> ]                 |
5 - Card firmware[ 2.12.11. ]           |
6 - Port stat     [ ]                     |
7 - Wireless stat [ ]                     |
8 - Node table    [ ]                     |

                Show traffic statistics of this port.

Enter a number or name, "=" main menu, [ESC] previous menu.
6:26:54 [admin] >

```

The table below provides a detailed description of the parameters.

Command	Meaning
MAC	MAC address of the wireless port. Cannot be changed on any user level.
Max speed	Displays the maximum technology-dependent speed of the wireless port in Mbps. This entry cannot be changed. For devices of the new generation in accordance with IEEE 802.11g/a, entry 54 will be listed.

Command	Meaning
Network name	Network name (SSID) of the WLAN network of your ComPoint. Must be entered manually at all stations which are to be granted access to the WLAN network of your ComPoint.
Card type	Type of the radio card installed in the ComPoint.
Card firmware	Firmware version of the radio card installed in the ComPoint. On all user levels, this entry can be viewed only.
Port stat	Under <i>Port stat</i> , you can view statistics of the frames received, sent, and filtered at the wireless port. See Section Port stat, Page 4–11 .
Wireless stat	Provides detailed information on sent and filtered frames. See Section Wireless stat, Page 4–13 .
Node table	List of clients associated with this port, see Section Node table, Page 4–16

Port stat

Via *Status > Ports > <Wireless Port> > Port Stat*, you can obtain an overview of the transmitted data packets:

```

artem W2000 V5.0          artem WLAN products          by Funkwerk-EC ))))
                        node0001CD0B4F66

Parameters                Status Ports wll_ap01          Value
-----
Received frames since last reset          1
Transmitted frames since last reset       0
Filtered frames since last reset          0
MULTICAST received frames since last reset 0
MULTICAST transmitted frames since last reset 0
MULTICAST filtered frames since last reset  0
Filtered frames (on all ports) since last reset 22678

Enter [SPACE]refresh, [r]reset, [q]quit:

```

The following table gives an explanation of the terms and parameters used on the screen.

Parameter	Meaning
Received frames since last reset	Number of received frames since the last reset.
Transmitted frames since last reset	Number of sent frames since the last reset.
Filtered frames since last reset	Number of filtered frames since the last reset.
MULTICAST received frames since last reset	Number of received multicast frames since the last reset.

Parameter	Meaning
MULTICAST transmitted frames since last reset	Number of transmitted multicast frames since the last reset.
MULTICAST filtered frames since last reset	Number of filtered multicast frames since the last reset.
Filtered frames (on all ports) since last reset	Number of filtered frames on all ports since the last reset.

Wireless stat

Via *Status > Ports > <Wireless Port> > Wireless stat*, you can obtain a detailed overview of the type of data packets transmitted.

```

artem W2000 V5.0          artem WLAN products          by Funkwerk-EC )))
                           node0001CD0B4F66

Name                      Status Ports w11_ap01          Value
-----
Number of unicast MSDUs transmitted successfully          0
Number of multicast MSDUs transmitted successfully        0
Number of transmitted MPDUs                               897
Number of unicast MSDUs received successfully             0
Number of multicast MSDUs received successfully           0
Number of unicast MPDUs received successfully             320
Number of received frames (without any filter)            2098
Number of MSDUs dropped before transmission               0
Number of MSDUs successfully sent after one retry         3
Number of MSDUs successfully sent after more retries      0
Number of MSDUs that could not be transmitted            0
Number of frame transmissions without ACK received        307
Number of duplicate received MSDUs                       0
Number of CTS frames received in response to an RTS      0
Number of received MPDU without decryption key            0

Enter [SPACE]refresh, [q]quit, [+]next, [-]previous, [ESC] break.:

```

Parameter	Meaning
Number of unicast MSDUs transmitted successfully	Number of MSDUs transmitted successfully to unicast addresses since the last reset. An acknowledgement has been received for each of these packets.
Number of multicast MSDUs transmitted successfully	Number of MSDUs transmitted successfully to multicast addresses (including the broadcast MAC address).

Parameter	Meaning
Number of transmitted MPDUs	Total of packets (data and management) transmitted successfully. Refers to unicast and multicast packets transmitted and acknowledged, as well as to broadcast packets transmitted.
Number of unicast MSDUs received successfully	Number of MSDUs transmitted with a unicast address and received successfully.
Number of multicast MSDUs received successfully	Number of MSDUs transmitted with a multicast address and received successfully.
Number of unicast MPDUs received successfully	Number of MPDUs transmitted with a unicast address and received successfully.
Number of received frames without any filter	Number of frames received unfiltered.
Number of MSDUs dropped before transmission	Number of MSDUs lost before transmission.
Number of MSDUs successfully sent after one retry	Number of MSDUs transmitted successfully after one retry.
Number of MSDUs successfully sent after more retries	Number of MSDUs transmitted successfully after several retries.
Number of MSDUs that could not be transmitted	Number of MSDUs which could not be transmitted.
Number of frame transmissions without ACK received	Number of transmitted frames for which no acknowledgement frame was received.
Number of duplicate received MSDUs	Number of duplicate MSDUs received.

Parameter	Meaning
Number of CTS frames received in response to an RTS	Number of CTS (Clear to Send) frames received in response to an RTS (Request to Send).
Number of received MPDUs without decryption key	Number of received MPDUs for which there was no decryption key available.

Press + to view the next page of the overview:

```

artem W2000 V5.0          artem WLAN products          by Funkwerk-EC )))
                           node0001CD0B4F66

Name                      Status Ports wll_ap01          Value
-----
Number of received MPDU that couldn't be decrypted          0
Number of RTS frames with no CTS received                   0
Number of aborted frames                                    32
Number of PHY aborted frames                                817
Number of unsuccessfully received frames                     230
Number of MPDUs which could not be transmitted              308
Number of rejected unencrypted MPDUs                        0
Number of dropped received unicast and multicast MSDUs      0
Number of partially or erroneously received MSDUs           0
Number of MPDUs received without required encryption        0
MPDUs received without appropriate privacy configuration      0

Enter [SPACE]refresh, [q]quit, [+]next, [-]previous, [ESC] break.:

```

Parameter	Meaning
Number of received MPDUs that could not be decrypted	Number of received MPDUs that could not be decrypted. The reason for this might be that no appropriate key was entered.
Number of RTS frames with no CTS received	Number of RTS frames for which no CTS was received.

Parameter	Meaning
Number of aborted frames	Number of received frames which were aborted, e.g. due to inadmissible lengths or unsupported data rate.
Number of PHY aborted frames	Number of frames already aborted by the receiver.
Number of unsuccessfully received frames	Number of frames received incompletely or with errors.
Number of MPDUs which could not be transmitted	Number of MPDUs which could not be transmitted.
Number of rejected unencrypted MPDUs	With activated encryption: number of unencrypted frames which were dropped.
Number of dropped received unicast and multicast MSDUs	Number of unicast and multicast MSDUs which were received and rejected. These may be frames received from unknown clients logged on to other access points.
Number of partially or erroneously received MSDUs	Number of MSDUs received incompletely or with errors.
Number of MPDUs received without required encryption	With activated encryption: number of MPDUs received without encryption.
MPDUs received without appropriate privacy configuration	Number of received MPDUs without appropriate encryption settings, e.g. which arrive with encryption although encryption is disabled.

Node table

Via *Status > Ports > <Wireless Port> > Node table*, you can go to the following screen:

```

artem W2000 V5.0          artem WLAN products          by Funkwerk-EC )))
                          Status Ports w11_ap01          node0001CD0B4F66

Name      MAC_address      IP_address  Assoc_time  Type      Rate
-----
802.11    00:60:1D:22:96:64    192.168.001.001  00:27:10    Client    11
802.11    00:60:1D:1C:A9:EB    192.168.001.006  00:47:20    Client    5

Enter [SPACE]refresh, [q]quit:

```

The node table displays all clients currently accessing the ComPoint via radio link. The following table gives an explanation of the terms and parameters used on the screen.

Parameter	Meaning
Name	Indicates the name of the associated client.
MAC_address	Indicates the MAC address of the associated client.
IP_address	Indicates the IP address of the client.
Assoc_time	Indicates (in hours, minutes, and seconds) how long the client has been logged on.
Type	Specifies the log-on mode at the ComPoint. (Example: Client, Spectralink)
Rate	Shows the current transmission rate to this client in Mbps. The following transmission rates are possible: IEEE 802.11b: 11, 5.5, 2, and 1 Mbit; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit When using the 5 GHz frequency band, the display of 11, 5.5, 2, and 1 Mbit with IEEE 802.11b is deactivated.

Status > ARP cache

The digit in square brackets next to *ARP cache* indicates the number of entries in the ARP table.

1. Select *Status > ARP cache* to view the ARP table of the ComPoint.

All IP stations (such as routers and PCs), which have been in direct contact with this ComPoint (via Telnet, http, or ping) within the last 20 minutes, are listed in this table. If an IP station has been inactive for 20 minutes, the corresponding entry will be deleted.

The counter for the 20 minutes is reset every time a packet is sent or received.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

IP address          MAC address          Status          Type
-----
010.010.000.001    00:01:30:0B:53:00    dynamic
010.010.000.020    00:B0:D0:B8:2F:B8    dynamic

Enter [SPACE]refresh, [q]quit:

```

Parameter	Meaning
IP address / MAC address	IP address and MAC address of the client

Parameter	Meaning
Type	Indicates whether the entry in question is a <i>static</i> or <i>dynamic</i> entry.

Status > Buffer util.

The value indicated here can be viewed at all user levels, but it cannot be changed.

It is a relative value referring to the utilization of the buffer pool. Normally, the values will be between 30% and 50%.

The Config Menu

In the *Config* menu, you can configure a variety of ComPoint parameters, depending on the user level on which you are logged on.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Main
                                Submenu
-----|-----
1 - Status      [ -> ]          System      [ -> ]
2 - Config     [ -> ]          Ports       [ -> ]
3 - Control     [ -> ]          Interfaces  [ -> ]
4 - Refresh     [ 5 ]          Filtering   [ -> ]
5 - Help       [ -> ]          IP routes  [ -> ]
6 - Exit       [ -> ]          BLD        [ -> ]
                                VLAN          [ -> ]

                                Configuration menu.

Enter a number or name.
7:45:32 [admin] >

```

Config > System

Config > System > Node name

Under *Config > System > Node name*, you can view the name of the ComPoint if you are logged on on the *user* or *view* user level. If you are logged on on the *admin* user level, you are, in addition, allowed to modify it. However, this can be performed much more conveniently by means of the ComPoint Manager. Refer to Chapter [The artem ComPoint Manager](#) on [Page 2-1 ff.](#)

Config > System > Location

Under *Config > System > Location*, you can specify the location of the ComPoint. Example: “Second floor”

Config > System > Contact

Under *Config > System > Contact*, you can specify a contact person, e.g. an administrator, for the maintenance of the device. Moreover, you can specify how this contact person can be reached.

Config > System > Description

Under *Config > System > Description*, you can find the device description and the specification of the firmware version.

Config > System > Hardware

Under *Config > System > Hardware*, you can view the version number of the ComPoint circuit board, as well as the serial number of the ComPoint circuit board. Moreover, you can view the hardware equipment, depending on the hardware version, under *Capabilities* (e. g. *Option Connector*, *Ethernet 1 and 2*, *Memory Expansion*, *PCMCIA A and B* as well as *MiniPCI A, B and C*).

Under *Options*, you can check whether *PoE* (Power over Ethernet) is supported. You can use this technology to perform the power supply for network-capable devices via the 8-lead Ethernet cable. Furthermore, the MAC addresses of the two Ethernet ports of the ComPoint are specified.

Config > System > Software

Under *Status > Software*, you will find a table providing information on the software available in the FLASH memory of the ComPoint.

artem W2000 V5.0		artem WLAN products		by Funkwerk-EC)))) node0001CD0B4F66	
Name	Version	Config System Flash Date		Release Date	
-----	-----	-----	-----	-----	-----
Bootloader	7.03	Feb 10	14:35:47 2005	Nov 12	16:06:58 2004
VPD	3.08	Feb 10	14:35:39 2005	Feb 10	14:35:39 2005
Monitor	1.90	Feb 10	14:35:50 2005	Nov 12	16:12:15 2004
CM	5.01	{none}		Feb 9	08:23:30 2005
Firmware	5.01	Feb 10	14:35:55 2005	Feb 9	08:23:30 2005

Enter [SPACE] refresh, [q] quit:

The *Name* column indicates the individual firmware components, the version numbers of which you can find in the *Version* column to the right.

The date and time given in the *Flash Date* column indicate when the last upgrade of the corresponding software was carried out. The *Release Date* column indicates the release date of the version used.

Some entries do not indicate the FLASH date *{none}*, as they are generated by another firmware component. The release date of this generated software always corresponds to the release date of the generator software.

Config > System > Features

Under *Config > System > Features*, you can view the additional modes of the device. These are:

- Bridge
- Double Bridge
- Enterprise

You can find more detailed information on the double bridge in Section [Double Bridge](#).



Note:

This option is only available with ComPoint II and higher. Version I of the ComPoint merely indicates the current mode of the device (e.g. access point, bridge).

Config > System > Reg. Domain

Under *Config > System > Reg. Domain*, you can select the country you live in. This ensures that the stipulations of the corresponding regulatory authorities are observed when operating the device.

Config > System > Usage area

Under *Config > System > Usage area* you can select whether the device is to be operated only in indoor environments (*indoor*), only in outdoor environments (*outdoor*), or both in indoor and outdoor environments (*anywhere*). According to the admission regulations of the country selected, one or several options (*indoor*, *outdoor*, *anywhere*) are offered.

Config > Ports

In the *Config > Port* menu, you can configure the individual active ports.

Config > Ports > Port <Ethernet Port>

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Ports eth1
                                Parameters
-----|-----
1 - Interface [ le0 ]           | interface name
2 - Auto neg mode[ enabled ]   |
3 - Actual value [ 10BaseT_HD ] |

                                Interface assignment for this port.

Enter a number or name, "=" main menu, [ESC] previous menu.
8:01:38 [admin] >

```

The following table provides an explanation of the terms and options used in the menu.

Option	Meaning
Interface	Interface name of the port
Auto neg mode	Using this function, you can <i>enable</i> and <i>disable</i> the auto negotiation mode. If the auto-negotiation mode is enabled, the ComPoint automatically identifies the transmission rate and the duplex mode of the remote side. As a default, this mode is activated. If you wish to adjust the transmission rate and the duplex mode of the port manually, set the auto neg mode to <i>disable</i> .
Actual value	Current transmission rate and duplex mode of the port. You can only change the indicated value if you have disabled the auto-negotiation mode.

Config > Ports > <Wireless Port>

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Ports wll_ap
                                Parameters
-----|-----
1 - Interface    [ le0 ]           | interface name
2 - OperatingMode[ AP ]           |
3 - RF settings [ -> ]           |
4 - Extended     [ -> ]           |
5 - Service sets [ -> ]           |

                                Interface assignment for this port.




Enter a number or name, "=" main menu, [ESC] previous menu.
8:12:53 [admin] >

```

The table below explains the options used in the menu.

Option	Meaning
Interface	Interface name of the port
OperatingMode	On the <i>admin</i> user level, this menu item allows you to select the desired <i>OperatingMode</i> (access point or bridge) of the port from a list or enter it manually into the prompt. On the <i>user</i> and <i>view</i> user levels, the <i>OperatingMode</i> cannot be changed.

Option	Meaning
RF settings	<p>Menu for the configuration of both channels and the transmission rate. Changes which you make here will be activated on all <i>Service Sets</i> of the wireless module. See Section Config > Ports > <Wireless Port> > Service Sets, Page 4–32.</p> <ul style="list-style-type: none"> • Channel As <i>admin</i> or as <i>user</i>, you can set the radio channel frequency here. If you select <i>Auto_DFS</i>, the access point will automatically check the frequency band after starting and select one of the channels with the lowest load. Manual channel selection is regulated by means of the corresponding country settings. In Germany, channel selection is only admitted for the 2.4 GHz frequency band. On the 5 GHz frequency band, only <i>Auto_DFS</i> can be selected. • Sel. Channel If you select <i>Auto_DFS</i>, the radio channel currently selected will be displayed. • Radio band Here, you can change the frequency band. You can select the frequencies 2.4 GHz (Mode 802.11b and Mode 802.11g) and 5 GHz (Mode 802.11a). According to the country-specific admission regulations, the radio module will scan the frequency band after changing the band and search for a free channel if the channel setting <i>Auto_DFS</i> has been selected. On the 5 GHz frequency band, this will take exactly 60 seconds. • Speed mode Serves to configure automatic speed adaptation or a fixed value for the transmission speed. Selectable values: <ul style="list-style-type: none"> • Auto_fallback (automatic adaptation) • According to IEEE 802.11b/g, selectable values are: 1_MbpsFixed, 2_MbpsFixed, 5.5_MbpsFixed, 11_MbpsFixed. • According to IEEE 802.11a/g, additionally selectable values are: 54_MBitFixed, 48_MBitFixed, 36_MBitFixed, 24_MBitFixed, 18_MBitFixed, 12_MBitFixed, 9_MBitFixed, 6_MBitFixed.

Option	Meaning
  	<ul style="list-style-type: none"> • Mcast rate Allows you to set the transmission rate for multicast frames. This item is displayed on all user levels, depending on the configuration. It can, however, only be changed on the <i>user</i> and <i>admin</i> level. • Tx power Allows you to set the maximum value for the radiated antenna power. The actually radiated antenna power may be lower than the maximum value set, depending on the data rate transmitted. The maximum value for the available <i>Tx power</i> (transmit power) depends on the regulations of the country in question. • Ant. Diversity Antenna diversity. Specifies how many and which antennas were used for transmitting and receiving. <ul style="list-style-type: none"> • none: Merely the main antenna transmits and receives signals. • receive: Two antennas receive signals, the better signal will be evaluated.
Extended	This menu contains extended settings. For more details, refer to Section Config > Ports > <Wireless Port> > Extended, Page 4–28.
Service sets	This menu enables you to configure service sets (virtual access points) for this access point and to make numerous security settings. For more details, refer to Section Config > Ports > <Wireless Port> > Service Sets, Page 4–32.

Config > Ports > <Wireless Port> > Extended

This menu contains extended settings.

```


artem W2000 V5.0          artem WLAN products          by Funkwerk-EC )))
                        node0001CD0B4F66




      Config Ports w11_ap Extended
      Command          Parameters
-----|-----
1 - RTS threshold [ always_off ]          threshold
2 - DTIM period [ 2 ]
3 - Mode 802.11g [ mixed ]
4 - Nitro mode [ enabled ]
5 - Nitro xm [ -> ]
6 - PHY settings [ -> ]


Set threshold in bytes for RTS/CTS. If set to 'always on'
RTS/CTS mechanism is always used. If set to 'always off'
it's never used. Any other value in the range [1..2346] may
be entered directly.



Enter a number or name, "=" main menu, [ESC] previous menu.
5:25:46 [admin] >
  
```

The following table provides an explanation of the terms and options used in the menu.

Option	Meaning
MW robustness 	Provides transmission security in environments with strong interferences through microwave ovens. Frames are fragmented in order to decrease the probability of interferences. This setting will be distributed to all associated clients if Medium distr. is enabled. The prerequisite is that the clients support this function.
RTS threshold	Here, you can enter the threshold in bytes (1..2346), from which on the RTS/CTS mechanism is to be applied. This makes sense if several clients which are not able receive each other are operated at one access point. This mechanism can be enabled or disabled any time.

Option	Meaning
DTIM period	<p>This value specifies the interval for the Delivery Traffic Indication Message (DTIM). The DTIM field is a countdown field which informs the clients via the window on the next broadcast or multicast transmission. If the clients are operated in the power-saving mode, they will wake up in time and will receive the data. The default value is 1. The value can be configured from 1 to 65535.</p>
AP distance 	<p>This function modifies the roaming behavior of the clients. The smaller the setting of the wireless cell, the sooner will the clients roam to the next ComPoint. The prerequisite is that you have selected <i>Medium distr. enabled</i> and that the clients support this function.</p>
Load balanc. 	<p>Activate <i>Load balancing</i> if the clients are supposed to select their ComPoints dynamically depending on the load distribution. In this case, ComPoint transmits the corresponding information in the probe response and beacon frames.</p>
Mode 802.11g 	<p>Here, you can make settings regarding the technology ComPoint is supposed to use.</p> <ul style="list-style-type: none"> • 802.11b_only: ComPoint exclusively operates according to 802.11b and forces all clients to adapt themselves. • mixed: ComPoint adapts itself to the technology applied by the clients. • shortrange_mixed: ComPoint adapts itself to the technology applied by the clients. All clients must support the data rates 5.5 and 11 Mbps (basic rates). • longrange_mixed: ComPoint adapts itself to the technology applied by the clients. Only the data rates 1 and 2 Mbps (basic rates) must be supported by all clients. • 802.11g_only: ComPoint exclusively operates according to 802.11g. 802.11b clients do not have access.

Option	Meaning
Nitro mode 	<p>By activating this function, you can achieve higher transmission speeds for 802.11g via frame bursting. Several packets are transmitted in sequence without waiting periods. Particularly effective in 11b/g mixed operation.</p>
Nitro xm	<p>Here, you can find extended Nitro XM functions for this port.</p> <ul style="list-style-type: none"> • Frame compr Activate Nitro XM (R) <i>Frame Compression</i> to increase the transmission rate. The default setting for this functions is “disabled”. • Frame concat Activate Nitro XM (R) <i>Frame Concatenation</i> to increase the transmission rate. The default setting for this functions is “enabled”. • Piggyback ack Activate Nitro XM (R) <i>Piggyback Frame Acknowledgment</i> to increase the transmission rate. The default setting for this functions is “enabled”. • Direct link Activate Nitro XM (R) <i>Direct Link</i> to increase the transmission rate. The default setting for this functions is “enabled”.

Option	Meaning
PHY settings	<p>With this option, you can perform extended configurations for this port on the physical network layer.</p> <ul style="list-style-type: none"> • ACK window With this function, you can define an additional timeout for the acknowledgment of unicast frames. In the case of longer radio links (starting with approximately 900 m), a value of 10 ms per bridged kilometer has to entered. • ED threshold Here, you can set the energy detection threshold value for CCA (Clear Channel Assessment). • CW min Here, you can define the maximum size of the contention window. • CW max Here, you can define the minimum size of the contention window.
Medium distr. 	<p>Activate this function if the parameters defined above (MW robustness, RTS threshold, AP distance, load balanc.) are to be distributed to clients. If the clients support this function, their local settings will be overwritten by the ComPoint settings.</p>
Encapsulation 	<p>This function can only be accessed on the <i>admin</i> user level after corresponding configuration. This menu item has several submenus, which will be explained in detail under Config > Ports > <Wireless Port> > Extended > Encapsulation, Page 4–41.</p>

Config > Ports > <Wireless Port> > Service Sets

In this menu, you can configure the *Service Sets* for this access point. A *Service Set* is a virtual access point, where the clients can log on and with which they can exchange data. For each wireless module, you can configure up to 16 *Service Sets*.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66


Menu                               Config Ports w11_ap Service_sets
                                Submenu
-----|-----
1 - w11_ap01 [ -> ]              | Port state           [ disabled ]
2 - Add SSID                      | Network name         [ ARtem ]
                                | Repeating             [ enabled ]
                                | Bcst SSID            [ disabled ]
                                | Security              [ -> ]


Select the service set you want to configure.

Enter a number or name, "=" main menu, [ESC] previous menu.
3:57:31[admin]>

```

The following table provides an explanation of the terms and options used in the menu.

Command	Parameter
<Wireless port SSID>	<p>Select the wireless port service set (wl1_ap01, wl1_ap02 etc.), for which you want to make the below settings.</p> <ul style="list-style-type: none"> • Port state With this option, you can activate or deactivate the selected wireless port. • Network name Enter the network name (SSID) of the WLAN network of your ComPoint. This option is only displayed on the <i>admin</i> user level. You can assign an individual network name for each <i>service set</i>, independent from all other service sets. • Repeating Allows direct communication between wireless clients connected to the same ComPoint. If repeating is deactivated, the wireless clients logged on at this ComPoint will not be able to exchange data with each other. On the <i>admin</i> level, the <i>Repeating</i> option can be changed. On the <i>user</i> level, the settings will be displayed, whereas, on the <i>view</i> level, the option is not available. • Bcst SSID By deactivating this option, you can prevent the wireless clients which do not know the network name of the ComPoint from logging on to the WLAN network. This entry exists on the <i>Admin</i> level only. <p> Note: For each service set, you can configure individually whether or not it will be visible in the wireless network. If there is more than one active service set, no SSID will be propagated in the 802.11 beacons. Anonymous probe requests will continue to be answered.</p>

Command	Parameter
	<ul style="list-style-type: none"> • Security Allows you to configure the encryption of the wireless traffic. The parameters are only available on the <i>admin</i> level and this is where they can be configured exclusively. For more details, refer to Section Config > Ports > <Wireless Port> > Service Sets > <Wireless Port SSID> > Security, Page 4–35. <p>Note: For reasons of security, you should always select a security level immediately after commissioning the ComPoint.</p>
Add SSID	Adding SSIDs to this access point. This option will only be offered as long as the maximum number of <i>service sets</i> (16 per wireless module) has not been reached.
Remove SSID	Removing SSIDs from this access point. The last <i>service set</i> cannot be deleted. There must be at least one <i>service set</i> per wireless module.

Config > Ports > < Wireless Port > > Service Sets > <Wireless Port SSID> > Security

Allows you to configure the encryption of the wireless traffic. The parameters are only available on the *admin* level and this is where they can be configured exclusively.

```


artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

      Config Ports wll_ap Service_sets wll_ap01
      Menu                               Submenu
-----|-----
1 - Port state [ disabled ]             Privacy [ WPA2 PSK ]
2 - Network name [ ARtem ]              State [ disabled ]
3 - Repeating [ enabled ]                Mixed mode [ enabled ]
4 - Bcst SSID [ disabled ]              PassPhrase [ ***** ]
5 - Security [ -> ]                     Accounting [ disabled ]

      Configuration of Wireless security.

Enter a number or name, "=" main menu, [ESC] previous menu.
4:07:23[admin]>
  
```

The following table provides an explanation of the terms and options used in the menu.

Command	Parameter
Privacy 	Select a security level. Note: For reasons of security, you should always select a security level immediately after commissioning the ComPoint. <ul style="list-style-type: none"> • none: no encryption of the wireless traffic. • WEP: Wireless Equivalent Privacy • WPA2 Enterpr. (WiFi Protected Access): encryption and authentication method on a high security level. For the WPA method you require an authentication server. • WPA2 PSK (WPA2 Pre-Shared Key): You can assign an access password, the so-called passphrase, for ComPoint and for all clients. Further secure keys will be created automatically from the passphrase. For the WPA method you do not require an authentication server. For more detailed information on the various security levels, refer to Page 4–38 ff.
State	After entering the valid keys, you can use this option to activate the selected security level.
Mixed mode	If you wish to enable clients which do only support WPA encryption to log on to this AP, you have to activate this function. If you wish to enable only WPA2-capable clients to log on, you must deactivate this function.

Command	Parameter
Server config	<ul style="list-style-type: none"> • Edit server Allows you to modify the settings for the authentication servers. The following options are available: <ul style="list-style-type: none"> • Select server Selects the server to be edited from a list. • IP address IP address of the server. • Port number Number of the port where the communication with the server is to take place. The default value is 1812. • Shared secret Key with which the data packets transmitted between ComPoint and server are to be encrypted. Enter the same key as on the server. • Add server Creates a new server entry. <p>This submenu is only available if you have selected <i>WPA2 Enterprise</i> as encryption method.</p>
PassPhrase	<p>Enter a password with a length of 8 to 63 characters under <i>Passphrase</i>. For reasons of security, the <i>Passphrase</i> should be as long as possible and should be hard to guess. To make dictionary-supported attacks more difficult, you should mix lower-case and upper-case letters and use digits and special characters in the passphrase.</p> <p>This option is only available if you have selected <i>WPA2 PSK</i> as encryption method.</p>
Accounting	<p>With this function, you can activate the <i>Accounting</i> service according to RFC 2886 and, thus, permit the detailed accounting of the WALN service. The accounting information is sent to the server specified as accounting server. If you have activated the accounting service and if the accounting server cannot be accessed, all clients will be rejected.</p> <p>This option is only available if you have selected <i>WPA2 Enterprise</i> or <i>WPA2 PSK</i> as encryption method.</p>

Encryption according to WEP

1. Select the option *WEP* under *Config > Ports > <Wireless Port> Service sets > <Wireless Port SSID> > Security > Privacy* .

You will be led to the following screen:

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

      Config Ports w11_ap Service_sets w11_ap01 Security
      Command                                     Parameters
-----|-----
1 - Privacy [ WEP ]                               state
2 - State   [ disabled ]
3 - Key number [ 1 ]
4 - Key 1    [ * NOT SET * ]
5 - Key 2    [ * NOT SET * ]
6 - Key 3    [ * NOT SET * ]
7 - Key 4    [ * NOT SET * ]

      Selected method for wireless privacy (authentication and
      encryption).

Enter a number or name, "=" main menu, [ESC] previous menu.
8:21:27 [admin]>

```

2. For instance, enter a key of your choice for Key 1.

The ComPoint is able to decrypt a radio frame encrypted with a key it knows. It is important to use the key of the corresponding entry for the decryption.

If the client is encoded with key 3, this means that key 3 must have the same value on the ComPoint and on the client. Naturally, this applies to both directions.

The length of the key used determines the encryption strength.

If you enter 5 characters, a 40-bit key will be generated and 64-bit encryption will be performed (effective cryptographic key + 24-bit initialization vector).

If you enter 13 characters, a 104-bit key will be generated and 128-bit encryption will be performed. The keys can be entered using ASCII (a-z, A-Z,0-9) or the hexadecimal number system (0x, followed by the corresponding number of hexadecimal numbers).

Examples:

64-bit encryption

"ABCDE" (ASCII) = "0x4142434445" (hexadecimal)

128-bit encryption

"1234567890123" (ASCII) =

"0x31323334353637383930313233" (hexadecimal)

Set keys are represented by the * character.

3. Select the option *enable* for *State*.
4. Also enter the key on your client which is to be granted access to the wireless LAN.

The data transmitted between ComPoint and client will now be encrypted. You should regularly enter a new key via *clear_key*.

Encryption according to WPA2 Enterprise

WPA2 Enterprise is an encryption and authentication method on a high security level. For WPA2 Enterprise you require an authentication server. The server concerned usually is a radius server. After setting up your authentication server, you have to enter the IP address of the authentication server under *Config > Ports > <Wireless Port> > Service sets > Wireless Port SSID > Security > Server config > Edit server*.

Encryption according to WPA2-PSK

If your client supports this WPA method, you should activate it. It provides more security than WEP encryption.

1. Select the option *WPA2-PSK* under *Config > Ports > <Wireless Port> Service sets > <Wireless Port SSID> > Security > Privacy*.

You will be led to the following screen:

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

      Config Ports wll_ap Service_sets wll_ap01 Security
      Command                                     Parameters
-----|-----
1 - Privacy [ WPA2 PSK ] | state
2 - State   [ disabled ] |
3 - Mixed mode [ enabled ] |
4 - PassPhrase [ ***** ] |
5 - Accounting [ disabled ] |

      Selected method for wireless privacy (authentication and
      encryption) .

Enter a number or name, "=" main menu, [ESC] previous menu.
8:26:08 [admin] >
  
```

2. Enter a password with a length between 8 and 63 characters under *Passphrase*. For reasons of security, the *Passphrase* should be as long as possible and should be hard to guess. To make dictionary-supported attacks more difficult, you should mix lower-case and upper-case letters and use digits and special characters in the passphrase.
 3. Select the option *enable* for *State*.
 4. If you wish to enable only WPA2-capable clients to log on to this AP, you must deactivate the *Mixed mode*.
 5. If you wish to activate the accounting service, you must set *Accounting* to *Enabled*.
 6. Enter the same password on your client.
- Client and ComPoint will now generate a dynamic key.



Config > Ports > <Wireless Port> > Extended > Encapsulation

A wireless port can send LLC frames only. An LLC header has to be added to any other frame. The *Encapsulation* menu item allows the configuration of this procedure and specifies the way it is reversed upon receipt.



Note:

The *Encapsulation* function should only be used by experienced administrators.

In the *Encapsulation* menu, you can choose between the options *Mode* and *Customize*.

1. By selecting *Mode Default*, you can undo all settings made regarding the frame processing, and the initial values will be restored.

Under *Customized*, you can specify the way incoming and outgoing data packets are to be processed.

1. Select *Config > Ports > <Wireless Port> > Extended > Encapsulation > Customize > Transmit* to process outgoing packets, or *Config > Ports > <Wireless Port> > Extended > Encapsulation > Customize > Receive* to determine the configuration for incoming packets.



Config > Ports > <Wireless Port> > Extended > Encapsulation > Customize > Transmit

The table below explains the options used in the menu, as well as the resulting setting options.

Option	Meaning
Encapsulation	Use this option to specify the default <i>encapsulation</i> , i.e. set the basic default for the transmission of frames without <i>LLC header</i> . The standards <i>RFC_1042</i> and <i>IEEE_802.1H</i> are available. You can select them from the list or directly enter them into the prompt.
Exceptions	<p>Here, you can specify the protocols for which <i>default encapsulation</i> will not apply.</p> <p>Using the <i>Show</i> option, you can view all the protocols excluded so far. The value in square brackets indicates the number of excluded protocols.</p> <p>Select <i>Add</i> to add further protocols to the list of exceptions (max. 10). These can either be selected from the list or entered into the prompt.</p> <p>Accordingly, you can remove protocols from the exception list using the <i>Remove</i> menu item. The <i>default encapsulation</i> will then be applied again for these protocols.</p>



Config > Ports > <Wireless Port> > Extended > Encapsulation > Customize > Receive

Under this menu item, select the standard for which you want to define an action to be performed when receiving a data packet. By default, the specifications *RFC_1042* and *IEEE_802.1H* are available.

As the submenus of these two options are set up identically, they will both be explained in the following table.

Parameter	Meaning
Def. action	Here, you can define whether the <i>LLC header</i> of incoming data packets is to be removed by default. Select <i>remove</i> to have the header removed, or <i>unchanged</i> to leave the data packet unchanged.
Exceptions	<p>Here, you can specify the protocols for which the <i>default action</i> is not to be applied.</p> <p>Using the <i>Show</i> option, you can view all the protocols excluded so far. The value in square brackets indicates the number of excluded protocols.</p> <p>Select <i>Add</i> to add further protocols to the list of exceptions (max. 10). These can either be selected from the list or entered into the prompt.</p> <p>Accordingly, you can remove protocols from the exception list using the <i>Remove</i> menu item. The <i>default action</i> will then be applied again for these protocols.</p>

Config > Interfaces

Use the *Interfaces* option on the *admin* user level to configure the IP settings of the device.

For example, to modify the IP settings of the *le0* interface, select *Config > Interfaces > le0*.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Interfaces le0
                                Parameters
-----|-----
1 - IP address [ 010.010.000.009 ] | IP address
2 - Subnet mask [ 255.255.000.000 ] | Subnet mask
3 - Gateway    [ 010.010.000.001 ] | Gateway
4 - DHCP      [ -> ]                |

                                IP address of this interface.

Enter a number or name, "=" main menu, [ESC] previous menu.
8:30:13 [admin] >

```

Here, you can configure the IP address, netmask, and gateway.

On the *user* and *view* user level, this menu item is a static display only.

1. For example, in the *le0* menu, select *IP address* and enter the corresponding IP address into the prompt.
2. Enter the subnet mask. If you wish to maintain the original subnet mask, enter *no_change*.
3. Enter the gateway. If you wish to maintain the original gateway, enter *no_change*.



Note:

If you want to, you can also select and enter the subnet mask or gateway prior to the IP address. In this case, you will automatically be led to the corresponding input fields and be requested to enter further parameters. If these are to remain unchanged, you have to enter *no_change* for them

The options for the DHCP menu are explained in the following.

Config > Interfaces > DHCP

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

                                Config Interfaces le0 DHCP
                                Parameters
-----|-----
1 - Status      [ enabled ]          | operation
2 - Lease Status [ in use ]          |
3 - Lease IP    [ 010.010.000.009 ] |
4 - Client ID   [ default ]          |

                                Dynamically request, rebind, or release a lease resp. an IP
                                address from a DHCP server.

Enter a number or name, "=" main menu, [ESC] previous menu.
8:35:27 [admin] >

```

The table below explains the terms and parameters used in the menu and lists the available options of the individual menu items.

Option	Meaning
Status	<p>Via this option, you can activate DHCP (<i>enable</i>) or deactivate it (<i>disable</i>).</p> <p>If DHCP is enabled, a request will automatically be sent to the DHCP server when booting the ComPoint, and the ComPoint will be assigned a valid IP address (<i>Lease</i>).</p> <p>If DHCP is disabled, the ComPoint will be booted with the IP address defined in the ComPoint Manager.</p>
Lease Status	<p>Shows the status during the request for an IP address. This option is also available if DHCP has been deactivated.</p> <ul style="list-style-type: none"> • in use An IP address requested from a DHCP server is active. • failure Indicates that the assignment of an IP address was not successful. Available actions are in this case <i>release</i> and <i>rebind</i>. • none Is displayed if DHCP is set to <i>disabled</i>. <p>Possible actions</p> <ul style="list-style-type: none"> • request Here, you can request an IP address from a DHCP server if no address has been allocated yet. • release Releases the address. It may then be allocated again by the DHCP server. • rebind Corresponds to a <i>release</i> with a <i>request</i> following.
Lease IP	Here, the currently used IP address of the lease is displayed.
Client ID	<p>Serves to identify clients at the DHCP server unambiguously.</p> <p>By default, the MAC address of the Ethernet port will be used (<i>default</i>). However, you can also use this option to allocate a client ID (<i>client ID</i>).</p>

Config > Filtering

This menu enables you to configure the individual filters for an efficient data exchange.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Filtering
                                Parameters
-----|-----
1 - ARP process. [ off ]        | mode
2 - Protocol      [ -> ]
3 - MAC filter    [ -> ]

                                Turn special ARP processing ON or OFF.

Enter a number or name, "=" main menu, [ESC] previous menu.
8:39:00 [admin]>

```

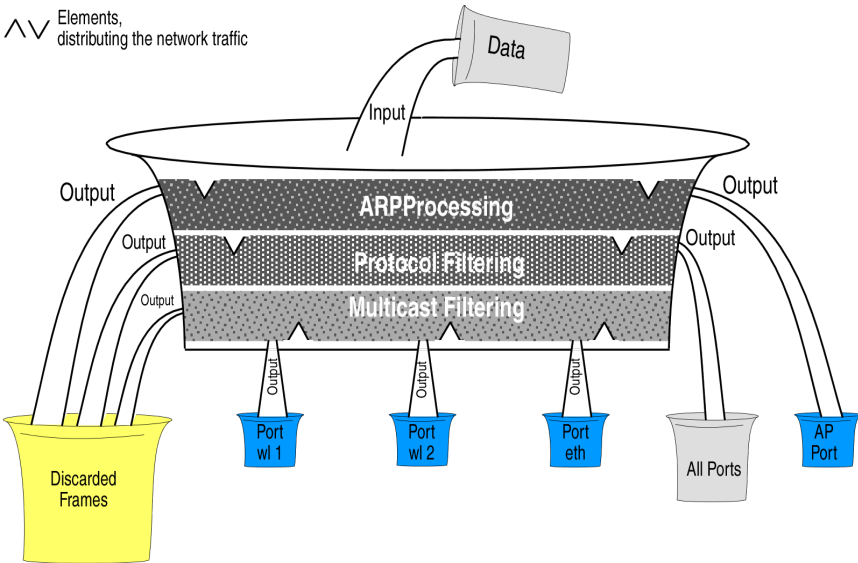


Note:

The *Filtering* function should only be used by experienced administrators.

As a rule, all packets used for direct communication with the ComPoint (e.g. Telnet session on the ComPoint) will not be filtered in any case.

How the Filtering Process Works

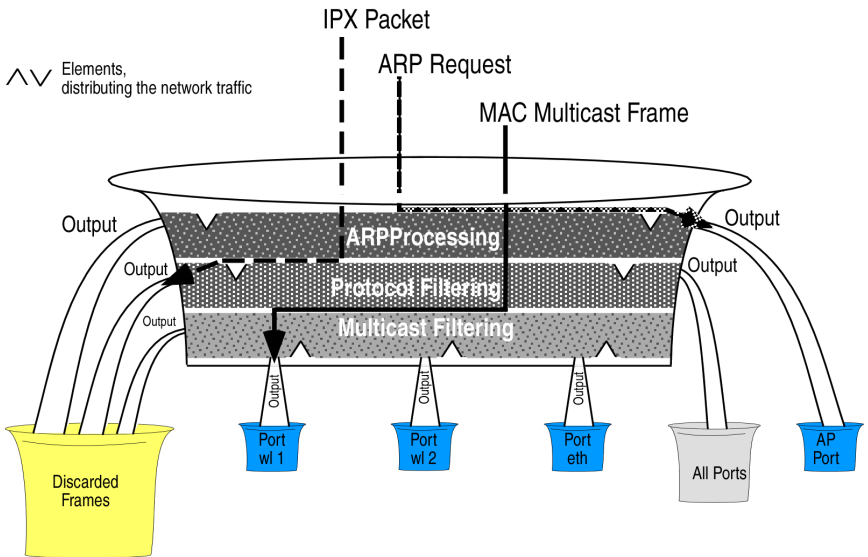


Example for the Filtering Process

- ARP process.: *on*
- Protocol: as a default *procMcastFlt*
- Protocol: IPX is to be discarded
- Multicast filter default rule:
 - Source=*any*;
 - Destination=*any Multicast*;
 - Destination Port=*wl1_br*

The incoming data traffic consists of:

1. IPX packet
2. ARP request to an associated client
3. Multicast frame



Config > Filtering > ARP process.

If the ARP process is activated (*on*), all ARP packets coming from or determined for associated clients will be forwarded to the corresponding ports without filtering.

In the process, ARP requests for associated clients are converted from MAC multicast to MAC unicast.

At the same time, ARP requests not determined for associated clients are filtered.

An entry is generated in the protocol list, displaying ARP (0x806) in the "procARP" state. This entry cannot be changed.

ARP processing is configured separately for each ComPoint and does only apply to AccessPoint ports.

Config > Filtering > Protocol

The *Protocol* menu allows you to define, change, and delete rules for the forwarding or filtering of protocols.

```

artem W2000 V5.0                                artem WLAN products                                by Funkwerk-EC )))
                                                node0001CD0B4F66

          Config Filtering Protocol
          Command                               Parameters
-----|-----
1 - Default mode [ MAC_filter ]                mode
2 - Show      [ 0 ]
3 - Add

          Processing rule for all those protocols, for which no
          specific actions are defined.

Enter a number or name, "=" main menu, [ESC] previous menu.
0:22:11 [admin] >

```


The table below explains the terms and parameters used in the menu and lists the available options of the individual menu items.

Option	Meaning
DefaultMode	<p>Displays the DefaultMode, which will be applied to all protocols not specified in the list.</p> <ul style="list-style-type: none"> • forward All packets of not listed protocols will be forwarded according to the normal AccessPoint function, without being processed by the multicast filters. • discard All packets of not listed protocols will be discarded. • MAC_filter All packets of not listed protocols will be forwarded to the multicast filters. The multicast filters decide to which port(s) the packets will be forwarded.
Show	<p>Displays the protocol list.</p> <ul style="list-style-type: none"> • Protocol The protocol name, the name of the protocol suite, or the protocol numbers in hexadecimal code will be displayed and can be selected via <i>Add</i> or entered. • Mode forward, fwrd some, discard, MAC-filter, procARP (special case, with ARP process. on)

Option	Meaning
Add	<p>Adds a protocol or a protocol suite to the list. For each added protocol, one action has to be chosen. The protocol list may contain a maximum of 32 entries.</p> <p>There are two ways to enter a protocol or suite:</p> <ul style="list-style-type: none"> • Select a protocol or suite from the predefined list. <p>Predefined protocols and protocol groups</p> <ul style="list-style-type: none"> 1 – AppleTalk (AppleTalk, ARP for AppleTalk) 2 – Vines (protocols by Banyan Vines) 3 – DEC (DEC – Digital Equipment Corporation protocols) 4 – IPX (IPX protocol) 5 – SNAServices (IBM SNA Services on Ethernet protocol) 6 – IP 7 – ARP 8 – RARP <p>or</p> <ul style="list-style-type: none"> • Enter the protocol number as hexadecimal code into the prompt (e.g. 0x800 for IP, 0x806 for ARP).
Remove	<p>Removes the selected protocol from the list. By selecting <i>all</i> from the list, you will remove all protocols from the list.</p> <p>There are two ways to specify the protocol to be removed:</p> <ul style="list-style-type: none"> • Select the protocol from the list. <p>or</p> <ul style="list-style-type: none"> • Enter the protocol number as hexadecimal code into the prompt (e.g. 0x800 for IP, 0x806 for ARP).

Config > Filtering > MAC filter

The *MAC filter* menu allows you to define, change, and delete rules for the forwarding or filtering of multicast frames on the *user* or *admin* user level.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Filtering MAC_filter

Command
-----|-----
1 - Rule table [ 1 ]
2 - Edit rule  [ -> ]
3 - Add rule

                                Show all rules relating to the current configuration.

Enter a number or name, "=" main menu, [ESC] previous menu.
0:30:47 [admin]>

```

The table below explains the terms and parameters used in the menu and lists the available options of the individual menu items.

Option	Meaning
Rule table	The number in brackets indicates the number of filter rules defined. Select <i>Rule table</i> in order to view an overview of all filter rules defined.
Edit rule	Edits a filter rule. For further information, refer to Section Config > Filtering > MAC filter > Edit rule, Page 4–54 .
Add rule	Allows you to create a new filter rule.

Config > Filtering > MAC filter > Edit rule

Only on the admin and user level. Here, you can edit and delete filter rules.

Option	Description
Rule number	Select the filter rule you wish to edit.
Rule status	<i>Enable</i> or <i>disable</i> the selected filter rule. The <i>conflict</i> status points out that the rules have to be checked in terms of their consistency. Rules with the <i>conflict</i> status cannot be activated.
Src MAC	Defines the source address of the multicast frames to be processed with this rule. <i>any</i> = any <i>local</i> = placeholder for the MAC address of the corresponding ComPoint (Config Interface)
Dst MAC	Defines the destination address for which the rule is to apply. <ul style="list-style-type: none"> • <i>broadcast</i>: Frames addressed to all nodes (FF:FF:FF:FF:FF:FF). • <i>IP multicast</i>: Frames addressed to any group of devices belonging to an IP multicast group. • <i>multicast</i>: Frames addressed to a group of devices on MAC basis (MAC address MSB = 1) • <i>any</i>: any frames In addition, you can enter any address as destination address into the prompt.

Option	Description
DST Ports	Use this menu to define for the selected rule to which ports the frames are to be forwarded. <ul style="list-style-type: none"> • Show Ports Displays a list of all ports to which the frames are forwarded according to the currently edited rule. • Add port Adds further ports which are to receive the forwarded frames. • Remove port Specific frames are removed from the list, i.e. excluded from the forwarding procedure.
Remove rule	Removes the selected filter rule.

Simple Example for Setting up Filter Rules

To ensure the functioning of your hotspot and to protect your hotspot users from unauthorized access, you must define a few filter rules. You can, thus, prevent the users within the hotspot from communicating with each other and from unintentionally making their resources (shared permissions for directories) available to other hotspot users.

Proceed as follows:

1. Under *Config > Filtering > Protocol*, define which protocols are permitted for transmission.

To grant your users access to the Internet, the protocols IP and ARP have to be transmitted.

2. Under *Add*, select the protocols *IP* or *ARP*.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Filtering Protocol
                                protocol
-----|-----
- Default mode [ MAC_filter ]   | AppleTalk
- Show          [ 0 ]           | Vines
- Add           [ ]             | DEC
                                | IPX
                                | SNAServices
                                | IP
                                | ARP
                                | RARP

                                Add a protocol or a suite to the list (or change its action)
                                and define a specific action for this protocol(s). Select
                                from list or enter the ISO protocol number at the prompt.

                                Select from list or enter 'protocol' in prompt. [ESC] break.
                                4:22:57[admin]>
  
```

3. Select the filter mode *MAC_filter* for the suite.

Finally, you just have to disable the forwarding of all other protocols:

4. To do so, set the *Default mode* to *discard*.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

                                Config Filtering Protocol
                                mode
-----|-----
- Default mode [ MAC_filter ] | forward
- Show          [ 0 ]          | discard
- Add           |              | MAC_filter

                                Processing rule for all those protocols, for which no
                                specific actions are defined.

Select from list or enter 'mode' in prompt. [ESC] break.
4:29:41[admin]>

```

With these settings, all protocols apart from IP and ARP, for which you have made special settings, will not be forwarded by the ComPoint; they will be discarded.



Note:

After having specified these rules, you will only be able to configure the ComPoint via the Ethernet interface (wired network).

Processing Order of the Rules

If more than one rule is allowed, the rules will be processed in a fixed order.

If the frame does not fulfill the conditions of the rules applied before, it will be compared to the conditions of the following rules. Frames which do not match with any of the rules added by the user or any allowed rule, will be processed via the default rule.

Source MAC	Destination MAC	Destination Port	Order of Processing
Specific	Specific	Specific	1
Specific	Specific	Any	2
Specific	Any	Specific	3
Specific	Any	Any	4
Any	Specific	Specific	5
Any	Specific	Any	6
Any	Any	Specific	7
Any	Any	Any	8

Example for Multicast Filtering

ComPoint with 2 wireless cards and 1 Ethernet port.

- *Rule table* command

Rule_number	Status	Source_MAC	Dest_MAC	Dest port
0	enabled	ANY	Multicast	eth1
1	enabled	ANY	broadcast	wl1_ap
2	disabled	00:01:02:03:04:05 00:02:01:03:04:05	any	wl1_ap, wl2_ap

Processing Order

1, 0. Rule number 2 is not activated at the moment.

Effect

1. All broadcasts are only forwarded to port wl1_ap, irrespective of where they come from.
2. All other multicast frames are forwarded to port eth1 only.

In this case, the wireless network at port wl2_ap (and at port eth1, but it is not so important there, as the speed is very high) is fully relieved of all broadcasts. The wireless client registered at port wl2_ap, however, is not available for ARP requests (and for data communication, either).

Config > IP routes

This menu allows you to configure the routing table on the *admin* user level.

Here, you can enter additional routes to networks accessible via other routers.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config IP_routes

Command
-----|-----
1 - Show      [ 5 ]
2 - Add
3 - Remove

Shows the routing table

Enter a number or name, "=" main menu, [ESC] previous menu.
0:43:28 [admin] >

```

The table below provides a detailed description of the commands.

Command	Description
Show	<p>Displays the routing table. Every entry consists of:</p> <ul style="list-style-type: none"> • Destination IP address of the destination network. • Gateway IP address of the router via which the data packets are routed into the destination network. • Mask Netmask of the destination network. • Flags Meaning of the entries: <ul style="list-style-type: none"> • <i>U</i>: Route can be used. • <i>G</i>: Destination is a gateway. • <i>H</i>: Host entry; if there is no H, the entry in question is a network entry. • <i>R</i>: Host or network cannot be accessed. • <i>D</i>: Generated dynamically • <i>m</i>: Modified dynamically • <i>C</i>: Direct route; if there is no C, the route concerned is an indirect route. • <i>X</i>: Name resolution via external daemon. • <i>L</i>: Generated via IPv4 ARP or IPv6 NDP • <i>S</i>: Added manually • if Indicates the ComPoint interface. • metric Indicates the number of routers between ones own network and the destination network.

Command	Description
Add	<p>Use this option to add routing entries to the routing table. For a routing entry, specify the following parameters:</p> <ul style="list-style-type: none">• Destination IP address of the destination network.• Gateway IP address of the router via which the data packets are routed into the destination network.• Mask Netmask of the destination network. The number of subnet bits is displayed. 32, for example, stands for 255.255.255.255.
Remove	<p>Use this option to remove routing entries from the routing table.</p> <p>The default route, the route to the local host, and the route to your own network cannot be deleted.</p>

Config > BLD

You can use this menu to activate broken link detection, to request its status, and to configure it.

This function serves to detect a broken cable link and to switch off the wireless port.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

                                Config BLD
                                Parameters
-----
1 - BLD status [ disabled ]      status
2 - Link status [ up ]
3 - IP address [ 000.000.000.000 ]
4 - Test interval [ 300 ]
5 - Timeout [ 1 ]
6 - Retries [ 5 ]
7 - Show ports [ none ]
8 - Add port

                                Status of the BLD configuration.

Enter a number or name, "=" main menu, [ESC] previous menu.
0:49:31 [admin]>

```

The table below provides a detailed description of the commands.

Command	Description
BLD status	Enables or disables broken link detection as a whole. <ul style="list-style-type: none"> enabled Enables BLD. disabled Disables BLD.
Link status	Indicates whether the device is connected to an IP-based network. <i>Up</i> indicates a verified connection.
IP address	Displays the IP address used by the BLD agent for verification.

Command	Description
Test interval	Indicates the time interval (in seconds) between individual verifications of the connection.
Timeout	Indicates the time (in seconds) after which a link will be rated as broken.
Retries	Number of retries in the case of a broken link.
Show ports	Displays an overview of the wireless ports disabled during the link breakdown.
Add port	Adds a wireless port to the list of ports disabled during the link breakdown.
Remove port	Removes a wireless port from the list of ports disabled during the link breakdown.

Config > VLAN

You can use this menu to make settings for VLANs (virtual LANs), request their statuses, and configure them. Basic settings for setting up a VLAN are explained in Chapter [VLAN Configuration](#) on [Page 6-1](#) ff.

```

artem W2000 V5.0          artem WLAN products          by Funkwerk-EC )))
                        node0001CD0B4F66

                                Config VLAN
                                Submenu
-----|-----
Menu                                     |
-----|-----
1 - Admin [ -> ]                         | Status [ disabled ]
2 - VLANs [ -> ]                         | Mgmt VID [ 1 ]
3 - PVID [ -> ]
4 - WL VLAN [ -> ]

Global VLAN administration of the device.

Enter a number or name, "=" main menu, [ESC] previous menu.
0:52:19 [admin] >

```

The table below provides a detailed description of the commands.

Option	Description
Admin	Administrates global VLAN settings.
VLANs	Use this menu to configure and maintain a VLAN.
PVID	Configuration of the port VIDs.
WL VLAN	Serves to activate or deactivate the wireless VLAN function and to view the WL VLAN cache.

Config > VLAN > Admin

Use this option to make the following general settings for a VLAN:

Command	Description
Status	Enables or disables the ComPoint for VLAN.
Mgmt VID	Enter the VLAN ID of the VLAN in which the ComPoint is to be operated.

Config > VLAN > VLANs

Here, you can view all VLANs configured so far and edit their settings.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config VLAN VLANs
                                Submenu
-----|-----
1 - Show          [ 1 ]          | Select VLAN          [ 1 ]
2 - Add          [ - ]          | Edit Port
3 - Edit         [ -> ]         | Del Port
4 - Remove

                                Configure the VLAN's port members, i.e. add or delete a port
                                of this VLAN and set the prot's egress rule .

Enter a number or name, "=" main menu, [ESC] previous menu.
0:56:11 [admin] >

```


The table below provides a detailed description of the options.

Option	Description
Show	<p>Shows all VLANs set up and their configuration properties.</p> <ul style="list-style-type: none"> • VID (VLAN Identifier): Character which identifies the VLAN. • Name: Name of the VLAN. • Port: Ports belonging to this VLAN. As a matter of fact, a port can belong to several VLANs. • Egress Rule: Specifies whether the frames transmitted by this port are transmitted in tagged or untagged form.
Add	<p>Here, you can set up a new VLAN. Specify a VLAN Identifier (VID) and a name.</p> <p>Under <i>Config > VLAN > Admin > Mgmt VID</i>, you can select which VLAN you want to use to configure your ComPoint.</p>

Option	Description
Edit	<p>Here, you can make the settings for a VLAN.</p> <ul style="list-style-type: none">• Select VLAN: Enter the VID of the VLAN which you wish to edit.• Add Port: Add a port to the VLAN and specify whether the frames transmitted by this port are to be transmitted in tagged form (i.e. including VLAN information) or in untagged form (i.e. without VLAN information).• Edit Port: Serves to edit the egress rule for a port at a later point of time.• Del Port: Deletes the egress rule for the selected port.
Remove	Removes a VLAN entry.

Config > VLAN > PVID

This menu allows you to determine and view rules for receiving frames on the ports of the VLAN.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

                                Config VLAN PVID
                                Submenu
-----|-----
1 - Show          [ 4 ]         | Select Port      [ eth1 ]
2 - Edit         [ -> ]         | PVID             [ 1 ]
                                | Drop Untagged   [ disabled ]
                                | Drop NonMemb.   [ enabled ]

                                Edit PVID configuration.

Enter a number or name, "=" main menu, [ESC] previous menu.
1:10:50 [admin] >

```

The table below provides a detailed description of the options.

Option	Description
Show	Indicates the current receipt rules for the ports. You can make your settings under <i>Edit</i> . You can find the meaning of the individual columns under <i>Edit</i> .

Option	Description
Edit	<p>Make your settings for the port rules.</p> <ul style="list-style-type: none"> • Select Port Select the port whose rules you wish to edit. • PVID Allows you to assign a PVID to the selected port. • Drop untagged frames If this option is <i>enabled</i>, untagged frames will be discarded. If this option is disabled, untagged frames will be tagged with the PVID. • Drop non Memb. If this option is enabled, all frames tagged with the ID of a VLAN of which the selected port is not a member will be dropped.

Config > VLAN > WL VLAN

This menu allows you to activate or deactivate the wireless VLAN function and to view the WL VLAN cache. To configure the WL VLAN function, you require the Security Manager 3.0. Local configuration is not possible.

```

artem W2000 V5.0                               artem WLAN products                               by Funkwerk-EC ))))
                                                node0001CD0B4F66

          Config VLAN WL_VLAN
          Submenu
-----
1 - w11 ap01 [ -> ] | WL VLAN [ disabled ]
2 - VLAN manager [ -> ] | Network name [ ARtem ]
3 - VLAN cache [ 0 ] | Leave VLAN

Wireless VLAN operating modes

Enter a number or name, "=" main menu, [ESC] previous menu.
1:42:27 [admin]>

```

The table below explains the options used in the menu:

Option	Meaning
<Wireless port SSID>	<p>Here, you can make the settings for the wireless port in question (wl1_ap01, wl1_ap02 etc.):</p> <ul style="list-style-type: none"> • WL VLAN <ul style="list-style-type: none"> • <i>enabled</i> Activates the WL VLAN function for this port. • <i>disabled</i> Deactivates the WL VLAN function for this port. • Network name Here, you can change the network name. • Leave WLAN With this function, you can remove the port from the VLAN.
VLAN manager	<ul style="list-style-type: none"> • IP address Here, you can define the IP address of the Security Manager. • Port number Here, you can define the port number of the Security Manager. • Comm. state Indicates the status of the communication with the Security Manager. • Sync period With this function you can change the interval for the synchronization with the Security Manager (specified in minutes).
VLAN cache	Displays the entries of the WL VLAN cache.

The Control Menu

Use the *Control* menu to modify the passwords of the user levels, to carry out a system restart, or to reset the parameters to the factory defaults.

Furthermore, you can find the Security and SNMP menus here and you can view the log files of the ComPoint.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Main
Menu                             Submenu
-----|-----
1 - Status                        [ -> ]
2 - Config                        [ -> ]
3 - Control                        [ -> ]
4 - Refresh                        [ 5 ]
5 - Help
6 - Exit

                                Security [ -> ]
                                SNMP    [ -> ]
                                SNTP    [ -> ]
                                Logging  [ -> ]
                                Admin cmds [ -> ]

Control menu.

Enter a number or name.
1:28:27 [admin] >

```

Control > Security

Use this menu to view the individual user levels, to change their passwords, and to edit the Access Control List (ACL).

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Control Security
                                Parameters
-----|-----
1 - WL admin [ allowed ]        | WL Config allowed
2 - User control [ -> ]         |
3 - UI control [ -> ]          |
4 - Authenticate [ -> ]        |

                                Block access to administration via wireless port. A MAC
                                filter rule is generated that effectively prohibits wireless
                                access to the Telnet and Web configuration.

Enter a number or name, "=" main menu, [ESC] previous menu.
1:32:44 [admin]>

```

Control > Security > WL Admin

For security reasons, activate the option *forbidden*. Consequently, no clients will be granted access to the configuration interface of the ComPoint via WLAN.

Control > Security > User control

Use this menu to view the individual user levels.

If you know the password for the *admin* user level, you may change the passwords for all user levels.

Control > Security > User control > Show

Displays the names of the individual user levels. These are *admin*, *user*, and *view*.

The passwords of the user levels are displayed in encrypted mode.

Control > Security > User control > Edit

This menu item allows you, as *admin* or as *user*, to change the passwords of the three user levels. This menu item is not available on the *view* level.



Prerequisite:

You have to know the password for the *admin* user level.

1. Select *Control > Security > User control > Edit*.
2. In the submenu on the right side of the table, select the user level (*view*, *user*, or *admin*) for which you want to change the password and confirm by pressing *Enter*.
3. Enter the admin password into the prompt and press *Enter*.
4. Now you have to enter the desired new password twice and confirm by pressing *Enter*.
5. From the next Telnet session onwards, you will be able to log on with the new password.



Note:

In case you forget the admin password, you can reset it yourself. Proceed as described in [Section Resetting the Password, Page 1–20](#).

Control > Security > UI control

With this menu item you can define from which user interfaces ComPoint Enterprise can be accessed.

Select the option you wish to activate or deactivate and change the status to *enabled* or *disabled*. As a rule, at least one interactive user interface must be activated (*Telnet*, *SSH*, *Web* or *Secure Web*).

- *Telnet*
Here, you can activate or deactivate the access via Telnet.

- *SSH*
This option permits the secure configuration via Secure Shell. If you are operating an SSH client, you can activate or deactivate the access via SSH here.
- *Web*
Here, you can activate or deactivate the access via Web.
- *Secure Web*
Here, you can activate or deactivate the access via Web. This option permits the secure configuration via HTTPS.
- *WPA Agent*
If you activate the *WPA Agent* option, you can monitor the exchange of wireless security information between the access point and the wireless client via an ARtem-proprietary analysis program (WPA Agent).

You can find more detailed information on the setup of the user interfaces via *Telnet*, *SSH*, *Web*, and *Secure Web* in Chapter [The ComPoint Enterprise User Interface, Page 3–1](#) ff.

Control > Security > Authenticate

This menu allows you to configure the local access control list and the access to an external access control server. Moreover, the settings for IEEE802.1x are made in this menu. By activating these functions, you can limit the access to your data network via the ComPoint. Only clients whose MAC addresses are specified in the local or remote access control list are permitted to access your LAN via the ComPoint. In addition, you can perform an authentication of the users via password and user name on an authentication server.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Control Security Authenticate
                                Submenu
-----
1 - w11_ap01 [ -> ]             AclLocal [ disabled ]
2 - ACL local [ -> ]           AclRemote [ disabled ]
3 - ACL remote [ -> ]
4 - EAP [ -> ]
5 - Auth. cache [ 0 ]

                                Wireless authentication operating modes

Enter a number or name, "=" main menu, [ESC] previous menu.
2:04:36 [admin] >

```



Note:

If you select *Acl local*, the list of MAC addresses is kept by the ComPoint. Consequently, you will have to keep a separate list in every ComPoint.

If you want to use *ACL remote*, you will have to purchase a Security Manager from artem. It will centrally administrate the list for all wireless cells and all wireless networks. You will find further information on this topic on our homepage under www.funkwerk-ec.com.de.

The table below provides a detailed description of the parameters.

Parameter	Meaning
<Wireless port SSID>	<p>Use this parameter to configure access control for the corresponding wireless port.</p> <ul style="list-style-type: none"> <li data-bbox="571 403 1050 496"> <p>• AcLocal Here, you can <i>enable</i> or <i>disable</i> a local access control list to be used.</p> <li data-bbox="571 512 1050 604"> <p>• AcRemote Here, you can <i>enable</i> or <i>disable</i> the authentication via the Security Manager.</p> <li data-bbox="571 620 1050 767"> <p>• IEEE802.1x Here, you can <i>enable</i> or <i>disable</i> the use of an external authentication server. This option is not available if you have selected <i>WPA-PSK</i> or <i>WPA2 Enterpr.</i> as encryption method.</p>

The priority of the three different options for access control corresponds to the sequence ACL local, ACL remote, IEEE802.1x. This means that the access control at the first position will be applied at first.

For example: all three access controls are enabled. A client will initially be compared to the entries in the local list. If it is found there, no request will be sent to the Security Manager. Instead, authentication according to IEEE will be performed.

The request to the Security Manager will only be carried out if the client is not found in the local list.

This means that only clients with a known MAC address and access permission will be authenticated according to IEEE802.1x.

Parameter	Meaning
ACL local	<p>Configuring a local access control list.</p> <ul style="list-style-type: none">• Show Displays the local access control list.• Add Adds a new entry to the access control list.<ul style="list-style-type: none">• client MAC addr Indicates the MAC address of the client to be added to the access control list.• port Select the wireless port of the ComPoint which the client is to access.<ul style="list-style-type: none">- <i>all ports</i>, access to all wireless ports of the ComPoint- <i><wireless port></i>, access to the corresponding wireless port in question.• Remove Removes an entry from the access control list.<ul style="list-style-type: none">• client MAC addr Indicates the MAC address of the client to be removed from the access control list.

Parameter	Meaning
ACL remote	<p data-bbox="367 292 1031 343">Serves to configure the communication settings with an external ACL server.</p> <ul data-bbox="367 363 1048 911" style="list-style-type: none"><li data-bbox="367 363 1048 422">• IP address Enter the IP address of the ACL server.<li data-bbox="367 443 1048 531">• Port number Enter the IP port via which the ACL server can be accessed. The default value is 1112.<li data-bbox="367 552 1048 667">• Comm. state Indicates the status of the connection to the ACL server.<ul data-bbox="404 616 820 667" style="list-style-type: none"><li data-bbox="404 616 820 639">• Disconnected—Connection is not active.<li data-bbox="404 644 754 667">• Connected—Connection is active.<li data-bbox="367 687 1048 802">• Def. access Indicates the access code used if the ACL server cannot be accessed.<ul data-bbox="404 751 673 802" style="list-style-type: none"><li data-bbox="404 751 654 775">• denied—Access denied.<li data-bbox="404 780 673 802">• granted—Access granted.<li data-bbox="367 823 1048 911">• Sync period Enter the time interval (in minutes) after which the ACL cache is to be updated. This interval is calculated separately for each client.

Parameter	Meaning
EAP	<p>Make your entries for authentication according to IEEE 802.1x.</p> <ul style="list-style-type: none"> • Prim. server Indicates the number of the primary authentication server. If several servers are entered, the primary server can be selected from a list. • Server config <ul style="list-style-type: none"> • Edit server Allows you to modify the settings for the authentication servers. The following options are available: <i>Select Server:</i> Selects the server to be edited from a list. <i>IP Address:</i> IP address of the server <i>Port number:</i> Number of the port where the communication with the server is to take place. The default value is 1812. <i>Shared secret:</i> Key with which the data packets transmitted between ComPoint and server are to be encrypted. Enter the same key as on the server. • Add server Creates a new server entry. • Comm. state Indicates the status of the connection to the server. <ul style="list-style-type: none"> • Disconnected—Connection is not active. • Connected—Connection is active.

Parameter	Meaning
EAP (Continued)	<ul style="list-style-type: none"> • Def. access Specifies the behavior of the ComPoint in case the primary server is not available. <ul style="list-style-type: none"> • denied—access denied. • granted—access granted. • Advanced Here, you can make further settings. <ul style="list-style-type: none"> • Max. reauth Maximum number of automatic reauthentication attempts. • EAPOL timeout Maximum waiting period of the access point port after a request has been sent to the client. • Serv. timeout Maximum waiting period of the access point port after a request has been sent to the authentication server. • Supp. timeout Timeout (in seconds) for requests sent to the access point by the client. • Max. requests Maximum number of user requests after which authentication will be aborted. • Quiet period Waiting period after an authentication abort.

Parameter	Meaning
EAP (Continued)	<ul style="list-style-type: none"> • Reauth. switch Serves to enable or disable automatic reauthentication of clients. <i>Enabled:</i> The user will be reauthenticated automatically after the specified time interval. <i>Disabled:</i> The user will not be reauthenticated. • Reauth period Interval after which a user will be reauthenticated automatically (in seconds). <p>If you have activated WPA, you can determine a key change by activating the reauthentication function. If you are working in the pure IEEE 802.1x mode (WPA deactivated), a complete reauthentication will be carried out.</p>
Auth. cache	<p>The number in square brackets indicates the current number of internal and external entries in the authentication list. This list contains entries by ACL and EAP.</p> <p>You can view this list by pressing <ENTER>. You will find information on the MAC address of the client, the port at which the client is registered, whether the access has been granted or denied (Error/InProgress/Granted/Denied), and the source of the authentication (ACL local, ACL remote, or EAP).</p> <p>In the case of ACL remote and EAP, the status of the request, as well as the time left until the next timeout will be displayed.</p>

Control > SNMP

Use this menu to configure the SNMP settings. ComPoint supports SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

and the Management Information Bases:

- MIBII
- IEEE 802.11 MIB

and the security model

- USM (User-Based Security Model),

as well as the access control model

- VACM (View-Based Access Control Model).

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Control SNMP
                                Parameters
-----|-----
1 - Status [ enabled ]         status
2 - Traps  [ -> ]
3 - Communities [ -> ]
4 - USM users [ -> ]

Current status of the SNMP agent.

Enter a number or name, "=" main menu, [ESC] previous menu.
1:17:40 [admin] >

```

The table below provides a detailed description of the commands.

Command	Description
Status	Activates or deactivates SNMP as a whole. <ul style="list-style-type: none"> • enabled Activates SNMP. • disabled Deactivates SNMP.
Traps	Configuration of the traps. <ul style="list-style-type: none"> • Version Enter the SNMP version which is to be used in the SNMP trap messages. • Dst address Enter the destination address for the SNMP trap messages. • Dst port Enter the destination port for the SNMP trap messages. • V3 user If you are using SNMPv3, enter the SNMPv3 user for the SNMP traps. • Community If you are using SNMPv1 or SNMPv2, enter the community user for the SNMP traps. • Agent address If you are using SNMPv1, enter the address of the agent for the SNMP traps. <p>According to the factory defaults, traps are deactivated, since the SNMP version, destination address, community, or the USM user have to specified if traps are used.</p>
Communities	Configuration of communities. For further information, refer to Section Control > SNMP > Communities, Page 4–85 .

Command	Description
USM users	Serves to configure USM users. For further information, refer to Section Control > SNMP > USM users, Page 4-86.

Control > SNMP > Communities

Serves to configure communities.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Control SNMP
                                Submenu
-----|-----
1 - Status      [ disabled ]      | Comm. table      [ 2 ]
2 - Traps       [ -> ]           | Edit             [ -> ]
3 - Communities [ -> ]           | Add
4 - USM users   [ -> ]           |

Community configuration.

Enter a number or name, "=" main menu, [ESC] previous menu.
7:55:16 [admin] >

```

Control > SNMP > Communities > Comm. table

Here, you can view all defined communities of the SNMP agent.

Control > SNMP > Communities > Edit

Serves to edit a community of the SNMP agent. The table below provides a detailed description of the commands.

Command	Description
Select	Select the numbers of the community you wish to edit.
Name	Enter the name of the community.

Command	Description
Host address	Enter the IP address of the host in question in the community. If you set the IP address to 0.0.0.0, the community will be valid for all sender addresses.
Subnet mask	Enter the address mask of the host in question in the community.
Access	Here, you can define the access rights for the community. Selectable values are <i>ro (read only)</i> and <i>rw (read write)</i> .
Remove	With this command, you can remove a community from the SNMP agent.

Control > SNMP > Communities > Add

Here, you can add a community to the SNMP agent.

Control > SNMP > USM users

SNMPv3 offers the option to control the user access rights via USM and VACM. In this context, it can precisely be defined which objects in the SNMP tree will be visible for individual users.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Control SNMP USM_users
                                Submenu

-----|-----
1 - USM table   [ 1 ]           | Select           [ 1 ]
2 - Edit       [ -> ]           | Status           [ enabled ]
3 - Add                                     | Name             [ admin ]
                                           | Security         [ -> ]
                                           | VACM views      [ -> ]
                                           | Access          [ rw ]
                                           | Remove

                                Edit an USM user of the SNMP agent.

Enter a number or name, "=" main menu, [ESC] previous menu.
1:09:50 [admin] >

```

Control > SNMP > USM users > USM table

Shows a list of all defined SNMPv3 USM users known to the SNMP agent.

Control > SNMP > USM users > Edit

Serves to edit the SNMP user.

Control > SNMP > USM users > Edit > Select

Select the number of the of the USM user you wish to edit.

Control > SNMP > USM users > Edit > Status

Serves to activate or deactivate USM users.

Control > SNMP > USM users > Edit > Name

Enter the name of the USM user.

Control > SNMP > USM users > Edit > Security

Serves to configure the USM user security.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Control SNMP USM_users Edit
                                Submenu
-----|-----
1 - Select      [ 1 ]           | Sec.level      [ authPriv ]
2 - Status      [ enabled ]    | Auth.proto     [ SHA1 ]
3 - Name        [ admin ]      | Auth.passwd    [ * admin * ]
4 - Security    [ -> ]         | Enc.proto      [ DES ]
5 - VACM views  [ -> ]         | Enc.passwd     [ * admin * ]
6 - Access      [ rw ]         |
7 - Remove      |

                                USM user security configuration.

Enter a number or name, "=" main menu, [ESC] previous menu.
0:39:19 [admin] >

```

The table below provides a detailed description of the commands.

Command	Description
Sec. level	Enter the security level which is to apply to the communication between user and SNMP agent. Selectable options are <i>NoAuthNoPriv</i> (neither authentication nor encryption), <i>authNoPriv</i> (authentication, but no encryption), and <i>authPriv</i> (both authentication and encryption).
Auth. proto	Select the authentication algorithm. Selectable options are <i>none</i> , <i>MD5</i> , and <i>SHA1</i> .
Auth. passwd	Enter the password for authentication. Subsequently, the authentication key will be generated.
Enc. proto	As encryption algorithm, select <i>DES</i> or select no encryption (<i>none</i>).
Enc. passwd	Enter the password for encryption. Subsequently, the encryption key will be generated.

Control > SNMP > USM users > Edit > VACM views

For each user, various VACM views can be configured.

```

                                     artem WLAN products           by Funkwerk-EC )))
artem W2000 V5.0                               node0001CD0B4F66

                                     Control SNMP USM_users Edit VACM_views
                                     Menu                               Submenu
-----|-----
1 - VACM table [ 1 ] | Select [ 1 ]
2 - Edit [ -> ] | OID [ 1 ]
3 - Add | Subtree [ included ]

Edit a VACM view of the SNMP agent.

Enter a number or name, "=" main menu, [ESC] previous menu.
0:56:54 [admin] >

```

The table below provides a detailed description of the commands.

Command	Description
VACM table	Displays an overview of the defined views.
Edit	<ul style="list-style-type: none"> • Select Select the number of the of the VACM view you wish to edit. • OID Enter the object identifier of the subtree which corresponds to the VACM view. • Subtree Specify whether this subtree is to be included in the corresponding VACM view (<i>included</i>) or not (<i>excluded</i>).
Add	With this option, you can add a VACM view to the SNMP agent.

Control > SNMP > USM users > Edit > Access

Here, you can define the access rights for the user. Selectable values are *ro* (*read only*) and *rw* (*read write*).

Control > SNMP > USM users > Edit > Remove

With this command, you can remove a user from the SNMP agent.

Control > SNMP > USM users > Add

Adds an USM user to the SNMP agent.

Control > SNTP

The menu serves to configure the time synchronization with an SNTP server.

The table below provides a detailed description of the commands.

Command	Description
SNTP Status	Activates or deactivates SNTP as a whole. <ul style="list-style-type: none"> • enabled Activates SNTP. • disabled Deactivates SNTP.
Current date	Displays the current date.
Current time	Displays the current time.
IP address	Enter the IP address of the SNTP server here.
Time zone	Specify how many minutes must be added to calculate GMT (Greenwich Mean Time) from the local time zone.
Poll interval	Enter the interval for polling the time at the SNTP server (in seconds).
Poll count	Specify for how many times the client is to repeat the polling request to the SNTP server, if required.
Poll timeout	Specification of the timeout between the polling attempts in minutes.

Control > Logging

Displays the stored system messages. The last 50 messages since the last system boot are stored.

The table below provides a detailed description of the options.

Option	Description
View logs	This option serves to view the systems messages.
Syslog	Activating or deactivating the syslog option. If you activate this option, the logs will be forwarded for central administration to the syslog daemon.
Priority	Select which priority level causes messages to be logged. The individual priority levels are: <i>LOG_EMERG</i> , <i>LOG_CRIT</i> , <i>LOG_ERR</i> , <i>LOG_WARNING</i> , <i>LOG_NOTICE</i> , and <i>LOG_INFO</i> (sorted according to decreasing priority).
IP address	IP address of the syslog daemon.
Port number	UDP port number of the syslog daemon.

Control > Admin cmds

The *Admin commands* menu item enables you to reboot the ComPoint, to reset the configuration, or to restore the factory defaults.

Control > Admin cmds > Restart

Select *Control > Admin cmds > Restart* to reboot the ComPoint.

Control > Admin cmds > Reset config

If you select the *Control > Admin Cmds > Reset config* option, the ComPoint will be rebooted. At the same time, the configuration will be reset to the factory defaults. This action can only be carried out at the *admin* user level.



Caution:

The passwords for the user levels and the IP configuration for the primary interface can be reset with the *Reset config* command.

Control > Admin cmds > Reset to FD

With the *Control > Admin Cmds > Reset to FD* command you can reset all settings to the factory defaults and reboot the ComPoint. This command can only be carried out on the *admin* user level.



Caution:

The passwords for the user levels and the IP configuration for the primary interface can be reset with the *Reset to FD* command.

The Refresh Command

Using the *Refresh* command, you can define the time interval after which a table screen (e.g. *Status > Summary*) will be updated. The preset value is five seconds.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

Command                          Main
-----                          -
1 - Status      [ -> ]           seconds
2 - Config      [ -> ]
3 - Control     [ -> ]
4 - Refresh     [ 5 ]
5 - Help
6 - Exit

Refresh intervall [sec].

Enter a number or name.
2:13:18 [admin]>

```

The Help Command

Use this command to launch the integrated help. The help can be called by pressing the <F1> key or the number <o>.

The Exit Command

Select the *Exit* command to terminate your Telnet connection.

ComPoint Bridge Port

With the bridge function, you can interconnect one ComPoint with another or several other ComPoints in the wireless mode.

Depending on the antennas used, this wireless connection can cover a distance amounting up to several kilometers.



Note:

Always use the original antennas and antenna cables supplied in order to avoid breaking governing law inadvertently. If you have special requirements, e.g. with regard to the cable length, please contact your vendor or Funkwerk Enterprise Communications GmbH.

Using the ComPoint Bridge

Chapter [ComPoint AccessPoint](#) of the manual on [Page 4–1](#) ff. describes the function, application, and configuration of the ComPoint as an access point.

Our ComPoint Bridges form a product family which by far exceeds this field of application. The ComPoint Bridges offer all the features described above, and many more.



Note:

Every wireless bridge port of a ComPoint can be run in the *Bridge* mode, as well as in the *Access Point* mode.

Bridges are generally used to connect different LAN segments on layer 2 of the OSI 7 layer model. The special feature of the ComPoint Bridges is that although the distances between these segments can amount up to several kilometers, no cable is required.

If you use a wireless port in the bridge mode, it can be used for a bridge link only. This means:

- The port does not have any network name.
- No wireless clients will be able to associate with (register at) this port.
- There is no node table for the port (as there are no clients).
- There is no Access Control List (ACL) for this port.

This port will only set up connections to the port of the partner bridge configured by you and will only accept connections from this port.

The ComPoint Bridges offer transmission rates far exceeding the capacities of ISDN BRI, ISDN PRI, and ADSL. The ComPoint High Speed Bridge even exceeds standard Ethernet (10BaseT, 10Base2, 10Base5).

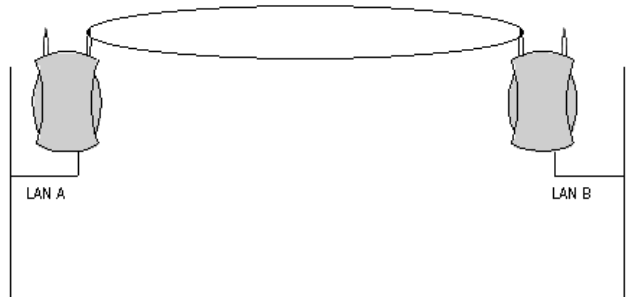


Caution:

Be sure not to plug two bridges connected by radio into the same LAN segment. This will inevitably cause a network overload, leading to a total breakdown of your network traffic.

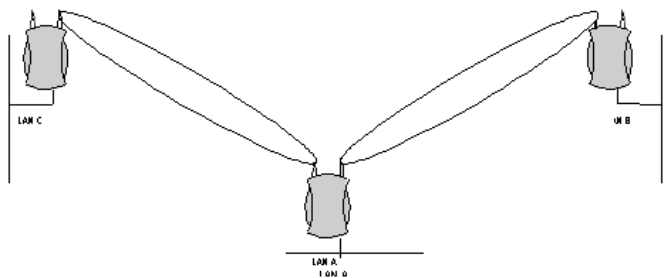
To give you an overview of the options offered by ComPoint Bridges, some possible network topologies will be described in the following.

1. Point-to-Point Topology



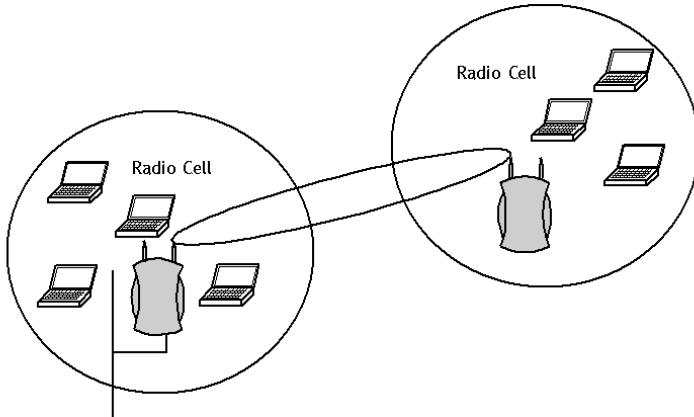
Interconnection of two LAN segments with 11/54 Mbps

2. Point-to-Multipoint Topology



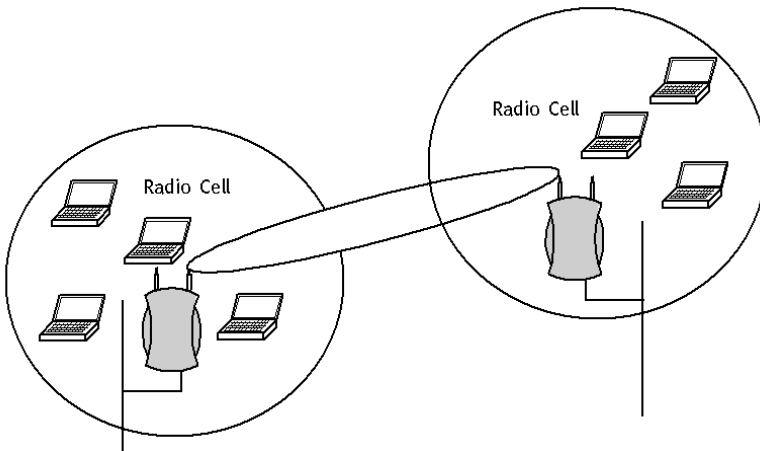
Interconnection of three LAN segments with 11/54 Mbps

3. Wireless Backbone



Access point with a wireless connection to the LAN, without losses in throughput

4. Wireless Bridge Connected to Wireless Clients



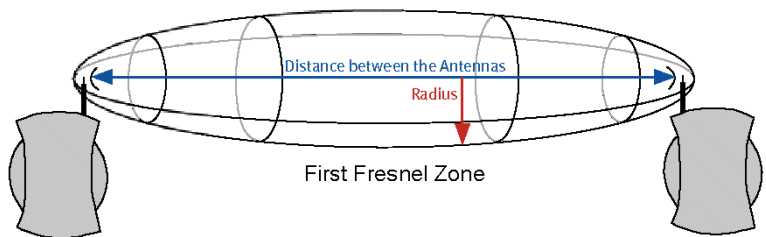
Interconnection of two wireless cells without LAN cable

Preconditions for Use of Links with ComPoint Bridges

To set up a wireless link with ComPoint Bridges, there has to be an unobstructed line of sight (LOS) between the antennas on both sides.

The term "line of sight" does not merely refer to a straight visual line of sight, but to a kind of tunnel, which must not be hampered by obstacles.

This "tunnel" is the so-called first Fresnel zone. The Fresnel zone has the form of an ellipsis rotating around a longitudinal axis. At least 60% of the first Fresnel zone have to be unhampered. The radius (or small semi-axis) depends on the frequency used and the distance between the antennas.



Example:

Radius of the first Fresnel zone as a function of the distance to the transmitting antenna, for an antenna spacing of 5 km at 2.45 GHz.

Distance to the Transmitting Antenna [km]	Radius of the First Fresnel Zone [m]	Radius at 60% First Fresnel Zone [m]
0.250	5.4	4.2
0.500	7.4	5.7
0.750	8.8	6.8
1.000	9.9	7.7
1.250	10.7	8.3
1.500	11.3	8.8
1.750	11.8	9.1
2.000	12.1	9.4
2.250	12.3	9.5
2.500	12.4	9.6
2.750	12.3	9.5
3.000	12.1	9.4
3.250	11.8	9.1
3.500	11.3	8.8
3.750	10.7	8.3
4.000	9.9	7.7
4.250	8.8	6.8
4.500	7.4	5.7
4.750	5.4	4.2

Example:

Radius of the Fresnel zone as a function of the distance to the transmitting antenna, for an antenna spacing of 700 m at 2.45 GHz.

Distance to the Transmitting Antenna [m]	Radius of the First Fresnel Zone [m]	Radius at 60% First Fresnel Zone [m]
100	1.6	1.25
200	2.1	1.6
300	2.3	1.75
400	2.3	1.75
500	2.1	1.6
600	1.6	1.25



Note:

When setting up a bridge link, please make sure that no obstacles (no trees, either) reach the Fresnel zone. If this is the case, the transmission rate will decline or the link may even break down.

In the case of short distances within buildings, the LOS must not necessarily be taken into account, as the radius of the Fresnel zone is very small there.

If these preconditions are observed, the link can be set up and maintained without any further restrictions. Weather conditions, in particular, do not influence ComPoint Bridge links at all.

Configuring the ComPoint Bridge

Every bridge port of a ComPoint can be operated as a bridge or as an Access Point (AP).

If a bridge port is run in AP mode, all parameters are identical to the parameters described in the first part of the manual.

This is why these parameters will not be discussed here once more.

In some menus, there are only small differences between bridge and access point. The options for the contents of many parameters, as well as their meanings, remain unchanged. In this chapter, only the differences and new parameters will be discussed.



Note:

Please refer to chapter [ComPoint AccessPoint](#) in this manual. Many general parameters are explained there.



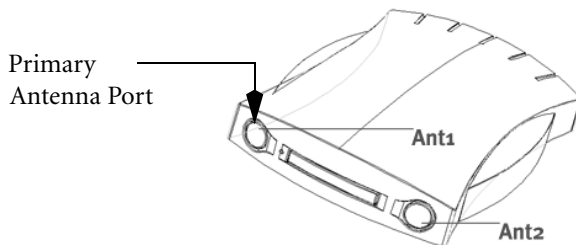
Note:

For better readability, the sequence of the discussed menus will be the same as in Chapter [ComPoint AccessPoint](#).



Note:

Always use the marked antenna port (see figure) for bridge links. This is the primary port of the device.



On the bottom of the device, there is a label with the names of both antennas. The primary antenna is called Ant 1.

Initiating the Telnet Connection, Login, and Setup of the User Interface

The initiation of a Telnet connection, the login, and the setup of the user interface are explained in [The ComPoint Enterprise User Interface](#) on page [Page 3–1](#) ff.

Activating the Bridge Mode

In order to activate the bridge mode, proceed as follows:

1. Go to the menu [Config > Ports > <Wireless Port>](#).
2. Select the option *BR* under *Operating Mode* .

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Ports wll_ap
                                Parameters
-----|-----
1 - Interface [ le0 ]           |
2 - OperatingMode [ AP ]       | operating mode
3 - RF settings [ -> ]         |
4 - Extended [ -> ]            |
5 - Service sets [ -> ]        |

                                Operating mode of this port.

Enter a number or name, "=" main menu, [ESC] previous menu.
3:07:55 [admin] >

```

3. Answer the question *Are you sure* with *y*.

The ComPoint can now be operated as bridge.



Note:

Ports operated in the bridge mode do not have any network name. Under Mode, the value BR for Bridge is displayed.

The Status Menu

The information on the ComPoint Bridge summarized in the *Status* menu can only be displayed but not configured by the user. You can find further information in [Section The Status Menu, Page 4–2](#).

Status > Summary

Ports operated in the bridge mode do not have any network name. Under *Mode*, the value *Bridge* is displayed. Moreover, these ports do not have any associated clients. This is why you cannot use an Access Control List (ACL) on a bridge port.

Bridge ports are displayed as port `wlx_br`.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Status
-----

Primary If  IP config      DHCP          SNMP Filter    Uptime
-----
IP address  010.010.000.009  in use       off Prot: macFlt  2:27:47
Subnet mask 255.255.000.000                Mflt: forward
Gateway     010.010.000.001                Sessions
                                                1

Port        MAC address    Speed         Mode Link      Info
-----
eth1        00:01:CD:0B:4F:66  10           HD +
eth2        00:01:CD:0B:4F:67  100          HD
w11_ap01    00:01:36:0B:6C:9C  --@06-2437* AP -          artem      0 Cl.
w12_br1     00:01:36:0B:6C:A0  --@11-2462* BR - S --- N --- dBm S/N -- dB

Enter [SPACE]refresh, [q]quit:

```

Status > Ports > wl1_br

Bridge ports do not have a NodeTable.

```
artem W2000 V5.0          artem WLAN products          by Funkwerk-EC )))
                        node0001CD0B4F66

                        Status Ports wl2_br1

-----
Command
-----
1 - MAC          [ 00:01:36:0B:6C:A0 ]
2 - Max speed    [ 54 ]
3 - Card type    [ -> ]
4 - Card firmware [ 2.12.11. ]
5 - Port stat
6 - Wireless stat

Show traffic statistics of this port.

Enter a number or name, "=" main menu, [ESC] previous menu.
4:36:37[admin]>
```

Port stat.

Via *Status > Ports > wl1_br > Port stat.*, you go to the following screen.

```

artem W2000 V5.0          artem WLAN products          by Funkwerk-EC ))))
                           node0001CD0B4F66

Parameters                Status Ports wl2_br1                Value
-----
Received frames since last reset          0
Transmitted frames since last reset      0
Average received signal strength         --- dBm
Average received signal noise            --- dBm
Filtered frames (on all ports) since last reset  6911

Enter [SPACE] refresh, [r] reset, [q] quit:
  
```

Parameter	Description
Average received signal strength	Reception strength of the signal at the receiver in dBm
Average received signal noise	Reception strength of the noise at the receiver in dBm

You can find further information in [Section Port stat, Page 4–11](#).

The Config Menu

In the *Config* menu, you can configure a variety of parameters of the ComPoint Bridge, depending on the user level on which you are logged on.



Note:

The following descriptions presume that the user is logged on on the *admin* user level.

Config > Ports

According to the device, there are up to 3 bridge ports: wl1_br, wl2_br, wl3_br.

Config > Ports > wl1_br

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Ports wl2_br
                                Parameters
-----|-----
1 - OperatingMode [ BR ]      operating mode
2 - RF settings [ -> ]
3 - Security [ -> ]
4 - Extended [ -> ]
5 - Bridge links [ -> ]

                                Operating mode of this port.

Enter a number or name, "=" main menu, [ESC] previous menu.
4:48:13[admin]>

```

The following table provides an explanation of the terms and options used in the menu.

Command	Meaning
Operating Mode	<p>This menu item allows you to select the desired <i>OperatingMode</i> of the port from a list or to enter it manually into the prompt.</p> <ul style="list-style-type: none"> • DBR (depending on the device used) Only devices purchased as double bridges. Allows channel bundling, i.e. a 22 Mbps link between two sides. Only possible on wl1, as wl2 follows automatically. This means that only one logical wireless port is left. • BR This port works in bridge mode. Wireless clients are not permitted to log on. The port can be used to interconnect two LANs. The preconditions are that there is a ComPoint Bridge in the other LAN segment, as well as the general preconditions (LOS) described on Page 5–5. • AP See Section ComPoint AccessPoint, page Page 4–1 ff.
RF settings	<p>Only contains the commands <i>Channel</i>, <i>Radio band</i> (only for devices operated with IEEE 802.11a technology) <i>Speed mode</i>, and <i>Tx power</i> (only for devices operated with IEEE 802.11g technology), and <i>Ant. diversity</i>. The commands are explained in Section Config > Ports > <Wireless Port>, Page 4–25.</p>
Security	<p>The configuration in the <i>Security</i> menu is described on Page 4–35 in this manual.</p>

Command	Meaning
Extended	Allows you to make specific settings as described on Page 4–28 in this manual.
Bridge Links	Allows you to configure a bridge link manually, as described in the manual on Page 5–21 ff.

Config > Ports > wl1_brx > Security

The configuration of the security settings is described on [Page 4–35](#) in this manual.

Config > Ports > wl1_brx > Extended

Allows you to make specific settings as described on [Page 4–28](#) in this manual.

Config > Ports > wl1_br > Bridge Links

Allows you to set up a new bridge link or configure an existing bridge link.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config Ports wl2_br Bridge_links
                                Submenu

-----|-----
Menu   |
-----|-----
1 - wl2 br1 [ -> ] | Interface [ le0 ]
2 - Add new link   | Link state [ disabled ]
                   | Alias name [ wl2_br1 ]
                   | Actual speed [ - ]
                   | Manual config [ -> ]
                   | Auto config [ -> ]

Select the bridge link you want to configure.

Enter a number or name, "=" main menu, [ESC] previous menu.
4:54:02 [admin]>

```

Menu	Submenu
wl1_br1 wl1_br2	Select the link you wish to configure.
Add new link	Adds a new bridge link. Up to 6 links can be set up.
Remove link	Removes a bridge link. The last link cannot be removed.

Config > Ports > wl1_br > Bridge Links <Port>

Here, you can make the configuration settings for the selected port.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66


      Config Ports wl2_br Bridge_links wl2_br1
      Command                Parameters
-----|-----
1 - Interface [ le0 ]                interface name
2 - Link state [ disabled ]
3 - Alias name [ wl2_br1 ]
4 - Actual speed [ - ]
5 - Manual config[ -> ]
6 - Auto config [ -> ]

      Interface assignment for this port.

Enter a number or name, "=" main menu, [ESC] previous menu.
5:00:41[admin]>

```

The following table provides an explanation of the terms and options used in the menu.

Command	Meaning
Interface	This option allows you to allocate an interface.
Link state	Enabling and disabling of the bridging function. Available values are: <ul style="list-style-type: none"> • enabled • disabled
Alias name	<p>Here you can assign a name to the link to simplify its identification. This name will replace the default name, e.g. w11_br1.</p> <p> Note: Alias names must not be assigned twice. If you wish to reset an alias name to the default name, select <i>Default</i>.</p>
Actual speed	Displays the current transmission rate.
Manual config	Allows you to configure a BridgeLink manually, as described on Page 5–29 of the manual.
Auto config	Allows you to configure a BridgeLink automatically, as described on Page 5–21 in this manual.
Link test	<p>The link test provides all data required to evaluate the quality of the bridge link.</p> <p>Moreover, the link test supports you when adjusting the antennas. This option is only displayed if the <i>Link state</i> is set to <i>enabled</i>.</p>

Config > Ports > wl1_br > Manual config

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

      Config Ports wl2_br Bridge_links wl2_br1 Manual_config
Command
-----|-----
1 - Local card [ 00:01:36:0B:6C:A0 ] |
2 - Remote MAC [ unconfigured ]      |
3 - Channel    [ Auto_DFS ]          |
4 - Actual speed [ - ]                |

      MAC address of the wireless card of this device.

View Only.
Enter a number or name, "=" main menu, [ESC] previous menu.
5:06:02 [admin] >

```

The table below explains the options used in the menu:

Option	Meaning
Local Card	MAC address of the WLAN card of the ComPoint.
Remote MAC	Enter the MAC address of the WLAN card of the partner device of the radio link.
Channel	Allows you to set the channel (frequency).
Actual Speed	Displays the current transmission rate.

Config > Ports > wl1_br > Auto config

```
artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

      Config Ports wl2_br Bridge_links wl2_br1 Auto_config
      Command                                Parameters
-----|-----
1 - Config state [ allowed ]                Config state
2 - Lock state  [ Unlocked ]
3 - Settings    [ -> ]

      Show current status of remote configuration process. Select
      'perform' to scan for available bridge partners.

Enter a number or name, "=" main menu, [ESC] previous menu.
5:09:50[admin]>
```

The table below explains the options used in the menu.

Command	Meaning
Config state	<p>Shows the current state of the configuration process. This parameter can have the following values:</p> <ul style="list-style-type: none"> • allowed Only available if no settings have been made or if the settings have been reset to the factory defaults by Control > Admin cmds > Reset config. The bridge may be configured from another bridge. • perform Enter perform in order to search for available bridges and perform an automatic configuration. • done The configuration has been performed. • failure The configuration has failed.
Lock state	<p>Indicates whether a bridge is locked for autoconfiguration (<i>locked</i>). A lock applies to all links of a multi-point bridge.</p>
Settings	<p>Allows to check, and, if necessary, to correct the following parameters:</p> <ul style="list-style-type: none"> • Channel (= frequency) • Radio band (change between the frequency bands 2.4 GHz and 5 GHz; subsequently, you can select a channel on one of these frequency bands). • Speed mode (transmission rate) • Privacy (authentication and encryption method) • State (indicates whether the selected authentication or encryption method has been activated)

Setting up a Bridge Link Automatically



Note:

The automatic bridge link setup for devices operated according to 802.11g will ignore 802.11b devices.

To set up a bridge link automatically, the following steps are required:

1. Under *Settings*, select the frequency (*Channel*), the transmission rate (*Speed Mode*), and the security settings (*Privacy*) for the link on one of the partner bridges and activate the selected encryption method (*State*). In the case of longer radio links (starting with approximately 900M) a value of 10 ms per bridged kilometer has to entered under ACK window.

```

artem W2000 V5.0                                artem WLAN products                                by Funkwerk-EC )))
                                                node0001CD0B4F66

          Config Ports w12_br Bridge_links w12_br1 Auto_config Settings
          Command                                           Parameters
-----|-----
1 - Channel      [ Auto_DFS ]                               state
2 - Radio band   [ 2.4GHz ]
3 - Speed mode   [ Auto_fallback ]
4 - Privacy      [ TKIP ]
5 - State        [ disabled ]

          Selected method for wireless privacy (authentication and
          encryption).

Enter a number or name, "=" main menu, [ESC] previous menu.
5:13:49[admin]>

```

The settings will be transferred to the partner bridge during configuration.

2. On the first bridge, set *Lock state* to *unlocked*.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

      Config Ports w12_br Bridge_links w12_br1 Auto_config
      Command                                     Parameters
-----|-----
1 - Config state [ allowed ]                   mode
2 - Lock state  [ Unlocked ]
3 - Settings    [ -> ]

      Bridge lock status. Locked bridge links cannot be accessed
      via remote configuration. This setting affects all links of
      a multi-point bridge.

Enter a number or name, "=" main menu, [ESC] previous menu.
5:16:25 [admin] >

```



Note:

The default setting for every ComPoint Bridge is *unlocked*.

3. Select the option *perform* for *Config state*.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

      Config Ports w12_br Bridge_links w12_br1 Auto_config
      Command                                     Config_state
-----|-----
- Config state [ allowed ]                   perform
- Lock state  [ Unlocked ]
- Settings    [ -> ]

      Show current status of remote configuration process. Select
      'perform' to scan for available bridge partners.

Select from list or enter 'Config state' in prompt. [ESC] break.
5:19:19 [admin] >

```

If the antennas are installed correctly on both sides, and the LOS is unhampered (see Section [Preconditions for Use of Links with ComPoint Bridges](#)), the bridge will be able to find available bridges and display them under *Scan results* :

```

                                artem WLAN products                by Funkwerk-EC )))
artem W2000 V5.0                node0001CD0B4F66
  Config Ports w11_br Bridge_links w11_br1 Auto_config
Link name      Name           Signal   State   Locked  MAC address
-----
  1  w12_br1  *  ace051 [jla]   -68 dBm  enabled  Unlocked  00:01:CD:0B:1E:84

Enter [SPACE]refresh, [q]quit:

```

If the partner bridge cannot be found, check the line of sight and the antenna installation. Subsequently, run *perform* once more. The partner should now be found.

4. Select the desired partner bridge.

The link between the two bridges will now be set up automatically. As soon as the configuration has been completed, the parameter *done* appears under *Config state*.

```

                                artem WLAN products                by Funkwerk-EC )))
artem W2000 V5.0                                node0001CD0B4F66
                                Config Ports wll_br Bridge_links wll_br1 Auto_config
                                Command
-----|-----
1 - Config state [ scan complete ] |
2 - Scan results [ 6 ]             |
3 - Lock state   [ Unlocked ]      |
4 - Settings     [ -> ]            |

                                Show table of results from scan for remote bridge link
                                partners. Select partner and press 'Enter' to establish
                                link.

Enter a number or name, "=" main menu, [ESC] previous menu.
0:42:22 [admin] >

```

5. For security reasons, you should set the *Lock state* of both partner bridges to *locked*. This will prevent the autoconfiguration of the two bridges.

Now, the bridge link is active, and the data is transmitted between the LAN segments.

Checking a Bridge Link (Link Test)

The link test provides all data required to evaluate the bridge link. Moreover, the link test supports you when adjusting the antenna.

Performing a Link Test



Prerequisite:

Before you perform a link test, you should reduce the display interval from 5 seconds to 1 second (see [Section The Refresh Command, Page 4–93](#)).

1. Log on to your local bridge via Telnet or http on the *admin* user level.
2. Select *Config > Ports > Wireless Port > Bridge Links > <Bridge Link> > Link test* to open the *Link test* menu.

```

                                artem WLAN products           by Funkwerk-EC )))
artem W2000 V5.0                node0001CD0B4F66
                                Config Ports wl2_br Bridge_links wl2_br1
                                Command
-----|-----
1 - Interface    [ le0 ]
2 - Link state   [ enabled ]
3 - Alias name   [ wl2_br1 ]
4 - Actual speed [ 54 ]
5 - Manual config[ -> ]
6 - Auto config  [ -> ]
7 - Link test

                                Continuously show connection quality of a configured bridge
                                link.

Enter a number or name, "=" main menu, [ESC] previous menu.

```

The data of the link test will be displayed.

Screen of a single bridge:

```

                                     artem WLAN products                by Funkwerk-EC )))
artem W2000 V5.0                               node0001CD0B4F66

Config Ports w12_br Bridge_links w12_br1
          Local Bridge                Remote Partner
-----
Link Quality
          excellent                    excellent
SNR:    56 dB                          SNR:    56 dB
Signal: -38 dBm                        Signal: -38 dBm
Noise : -94 dBm                        Noise : -94 dBm

Received at Rate
54 Mbps:    292                          54 Mbps:    294
48 Mbps:     3                          48 Mbps:     1
36 Mbps:     0                          36 Mbps:     0
1-24 Mbps:  0                          1-24 Mbps:  0

Frames Sent:                297
Frames Received:            295
Frames Lost:                 1

Enter [SPACE] refresh, [r] reset, [q] quit:

```

This display is updated at every refresh interval.

Per interval, test frames are sent to the partner and answered there. These responses will then be evaluated and the results will be displayed.

3. By pressing r(eset), you can reset the counters.

The table below explains the parameters displayed in the evaluation of the link test:

Parameter	Meaning										
Link quality	Constitutes the title of the parameters indicating the link quality.										
Evaluation of the quality	This parameter can have the following values: <ul style="list-style-type: none"> • excellent • good • marginal • poor 										
SNR	The Signal to Noise Ratio (in dB) is an indicator of the radio link quality. <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Values</th> <th style="text-align: left;">Evaluation</th> </tr> </thead> <tbody> <tr> <td>> 25 dB</td> <td>excellent</td> </tr> <tr> <td>15 – 25 dB</td> <td>good</td> </tr> <tr> <td>2 – 15 dB</td> <td>marginal</td> </tr> <tr> <td>0 – 2 dB</td> <td>poor</td> </tr> </tbody> </table>	Values	Evaluation	> 25 dB	excellent	15 – 25 dB	good	2 – 15 dB	marginal	0 – 2 dB	poor
Values	Evaluation										
> 25 dB	excellent										
15 – 25 dB	good										
2 – 15 dB	marginal										
0 – 2 dB	poor										
Signal	Reception strength of the signal at the receiver in dBm										
Noise	Reception strength of the noise at the receiver in dBm										
Received at rate	Constitutes the title of the parameters indicating the number of received frames.										
54 Mbps	Number of frames received at a transfer rate of 54 Mbps.										
48 Mbps	Number of frames received at a transfer rate of 48 Mbps.										
36Mbps	Number of frames received at a transfer rate of 36 Mbps.										
1 - 24 Mbps	Number of frames received at a transfer rate of 1 to 24 Mbps.										

Parameter	Meaning
11 Mbps	Number of frames received at a transfer rate of 11 Mbps.
5.5 Mbps	Number of frames received at a transfer rate of 5,5 Mbps.
2 Mbps	Number of frames received at a transfer rate of 2 Mbps.
1 Mbps	Number of frames received at a transfer rate of 1 Mbps.
Frames Sent	Number of frames sent by this device since the start of the LinkTest.
Frames received	Number of frames received by this device since the start of the LinkTest.
Frames lost	Number of frames lost in this link since the start of the LinkTest.

4. If you want to quit the link test, press <ESC> or <q> (telnet), or select <BACK> (web interface).

Setting up a Bridge Link Manually

We generally recommend you to select the automatic setup of a bridge link, since it is easier to implement and less error-prone. For manual configuration, proceed as follows:

1. Select *Config > Ports > <Wireless Port> > Bridge Links > <Wireless Port> Manual config*.
2. Determine the MAC address for each bridge under *Local card* and note it down.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC ))))
                                node0001CD0B4F66

      Config Ports w12_br Bridge_links w12_br1 Manual_config
      Command
-----|-----
1 - Local card [ 00:01:36:0B:6C:A0 ] |
2 - Remote MAC [ unconfigured ]     |
3 - Channel    [ Auto_DFS ]         |
4 - Actual speed [ - ]              |

      MAC address of the wireless card of this device.

View Only.
Enter a number or name, "=" main menu, [ESC] previous menu.
5:38:46 [admin] >

```

3. Enter the MAC address of the WLAN card of the respective partner bridge at every bridge under *Config > Ports > <Wireless Port> > Bridge Links > <Bridge Link> Manual config > Remote MAC*.

```

artem WLAN products                               by Funkwerk-EC )))
artem W2000 V5.0                                  node0001CD0B4F66

      Config Ports wl2_br Bridge_links wl2_br1 Manual_config
Command                                     Parameters
-----|-----
1 - Local card   [ 00:01:36:0B:6C:A0 ] | remote MAC addr
2 - Remote MAC   [ unconfigured ]     |
3 - Channel      [ Auto_DFS ]         |
4 - Actual speed [ - ]                 |

      MAC address of the wireless card of the remote device.

Enter a number or name, "=" main menu, [ESC] previous menu.
5:41:44 [admin] >

```

4. Set both bridges to the same radio band and the same channel. You can select the radio band under *Config > Ports > <Wireless Port> > RF Settings > Radio band* and the channel under *Config > Ports > <Wireless Port> > RF Settings > Channel*.

```

artem W2000 V5.0                                artem WLAN products                                by Funkwerk-EC )))
                                                node0001CD0B4F66

Config Ports wl2_br RF_settings
Command                                         channel
-----
- Channel [ 11-2462 ]                          Auto_DFS      09-2452
- Radio band [ 2.4GHz ]                       01-2412      10-2457
- Speed mode [ Auto_fallback ]                 02-2417      11-2462
- Tx power [ max ]                             03-2422      12-2467
- Ant diversity[ none ]                       04-2427      13-2472
                                                05-2432
                                                06-2437
                                                07-2442
                                                08-2447

Radio operating channel.

Select from list or enter 'channel' in prompt. [ESC] break.
5:47:15[admin]>

```

5. Set the *Link state* on both bridges to *enabled*.

```

artem W2000 V5.0                                artem WLAN products                                by Funkwerk-EC )))
                                                node0001CD0B4F66

Config Ports wl2_br Bridge_links wl2_br1
Command                                         Parameters
-----
1 - Interface [ le0 ]                          link state
2 - Link state [ enabled ]
3 - Alias name [ wl2_br1 ]
4 - Actual speed [ - ]
5 - Manual config[ -> ]
6 - Auto config [ -> ]
7 - Link test

Enable or disable bridge link.

Enter a number or name, "=" main menu, [ESC] previous menu.
9:39:39[admin]>

```

As soon as both ports are *enabled*, the link will be set up. The *Actual speed* indicates the current transmission rate.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

Command          Config Ports w12_br Bridge_links w12_br1
                  Parameters
-----|-----
1 - Interface    [ le0 ]                link state
2 - Link state   [ enabled ]
3 - Alias name   [ w12_br1 ]
4 - Actual speed [ 54 ]
5 - Manual config[ -> ]
6 - Auto config  [ -> ]
7 - Link test

        Enable or disable bridge link.

Enter a number or name, "=" main menu, [ESC] previous menu.
9:39:39[admin]>

```

As soon as you have set up a link by means of one of the procedures (automatically or manually), both LAN segments are connected. This means that computers from one segments can establish a connection with computers from the other segment.

Checking a Bridge Link (Link Test)

The link test provides all data required to evaluate the quality of the bridge link. Moreover, the link test supports you when adjusting the antenna.

You can learn how to perform a link test in Section [Performing a Link Test](#).



Installation note:

As a rule, one of both antennas has to be rotated by 90° during installation in order to achieve an optimum performance of the double bridge link.

Double Bridge

Only the following products which are no longer available support the double bridge:

- ComPoint BR2
- CPD-BR-b
- CPD-BR-b-PoE
- CPE-BR2-b



Note:

For details on the configuration of the double bridge, refer to your ComPoint Enterprise manual.

The difference between a double bridge and a normal bridge is that it uses 2 bridge ports simultaneously. Traffic arriving at the Ethernet is automatically distributed among both wireless ports, depending on the available capacity.



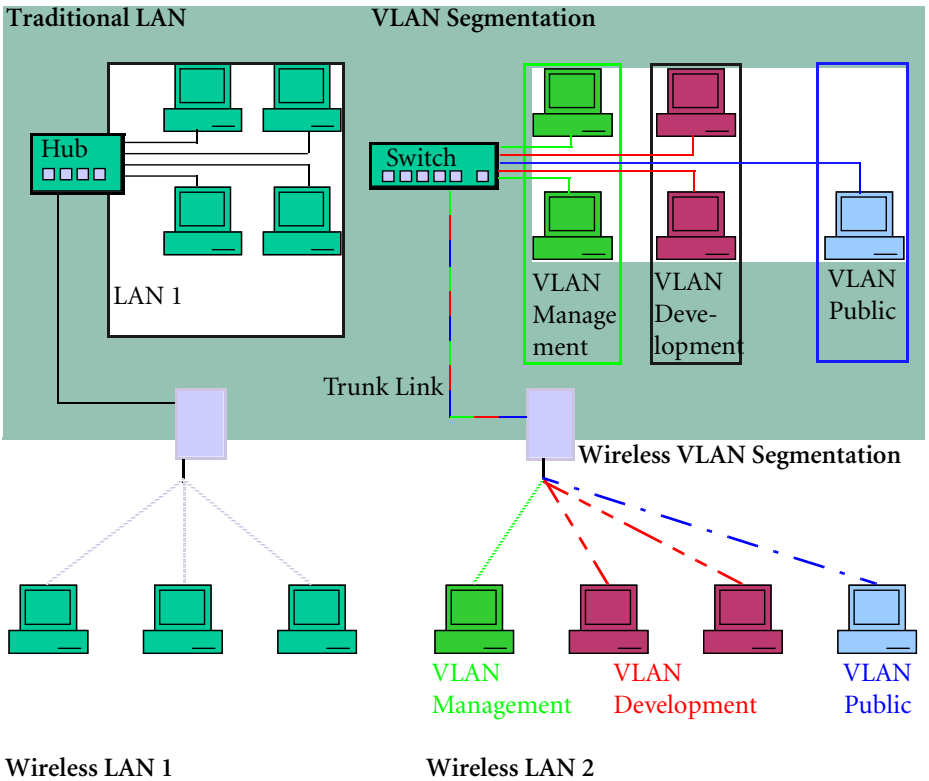
Note:

A supplementary upgrade to a ComPoint Double Bridge is not available. If you want to use this function, you need to acquire the corresponding devices right from the start.



VLAN Configuration

The implementation of the VLAN tagging/untagging functionality according to 802.1q allows the configuration of a VLAN on the ComPoint. The wireless ports of an access point are able to remove the VLAN tag of a frame sent to the clients and to tag received frames with a predefined VLAN ID. With this functionality, an access point is nothing less than a VLAN-aware switch with the extension of summarizing clients in groups.



To set up a VLAN, proceed as follows:

Setting up a VLAN

1. Select the menu *Config > VLAN > VLANs > Add*.
2. Enter a VLAN ID and click RETURN.
3. Enter a name for the VLAN and click RETURN.

The freshly created VLAN will now be displayed under *Show*.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

                                Config VLAN VLANs

Command
-----|-----
1 - Show [ 1 ] |
2 - Add  |
3 - Edit [ -> ] |
4 - Remove |

                                Show all defined VLANs

Enter a number or name, "=" main menu, [ESC] previous menu.
6:07:41 [admin] >

```

Adding a Port to a VLAN

1. Select the menu *Config > VLAN > VLANs > Edit > Select VLAN*.
2. Enter the VLAN ID of the VLAN to which you want to add a port. Subsequently, click RETURN.
3. Select the menu *Config > VLAN > VLANs > Edit > Add Port*.

4. Select the port you want to add to the VLAN and click RETURN.
5. If you want to remove the VLAN information from all frames transmitted via the port, select *Untag*.

```

artem W2000 V5.0                                artem WLAN products                                by Funkwerk-EC ))))
                                                node0001CD0B4F66

          Command                                Config VLAN VLANs Edit
          -----                                - - - - -
          - Select VLAN [ 1 ]                    | Untag
          - Add Port                               | Tag
          - Edit Port                             |
          - Del Port                              |

          Add a port to the selected VLAN and set the egress rule
          (Tag/Untag frames transmitted out of this port).

          Select from list or enter 'Tag/Untag' in prompt. [ESC] break.
1:20:05 [admin]>

```

If you do NOT want to remove the VLAN information from any frames transmitted via the port, select *Tag*.

6. Subsequently, click RETURN.

You have just added a port to the VLAN and defined its transmission mode. Under *Config > VLAN > VLANs > Edit > Edit Port*, you can modify the transmission mode for each port at a later point in time.

Viewing the VLAN Configuration

Under *Config > VLAN > VLANs > Show* you can view the defined VLAN configuration.

```

artem W2000 V5.0                artem WLAN products                by Funkwerk-EC )))
                                node0001CD0B4F66

```

VID	Name	Port	Config	VLAN	VLANs	Egress Rule
1	Management	eth1		Untag		
		eth2		Untag		
		wl1_ap01		Untag		
		wl2_br1		Untag		

Enter [SPACE]refresh, [q]quit:

Defining Rules for Receiving Frames on Individual Ports

1. Select the menu *Config > VLAN > PVID > Edit > Select Port*.
2. Select the port to be configured for receiving frames and click RETURN.

You can now make your settings for receiving frames:

```

artem W2000 V5.0                                artem WLAN products                                by Funkwerk-EC ))))
                                                    node0001CD0B4F66

          Config VLAN PVID Edit
          Command                               Parameters
-----|-----
1 - Select Port [ eth1 ]                       | Port VID
2 - PVID [ 1 ]                                  |
3 - Drop Untagged[ disabled ]                  |
4 - Drop NonMemb.[ enabled ]                   |

          Set the rx port's vlan identifier.

Enter a number or name, "=" main menu, [ESC] previous menu.
6:26:13[admin]>

```

If untagged frames are to be tagged by ComPoint:

3. Select the menu *Config > VLAN > PVID > Edit > PVID*.
4. Select the VLAN ID with which you want to tag any untagged frames and click RETURN.

If all untagged frames received via a port are to be dropped:

5. Select the menu *Config > VLAN > PVID > Edit > Drop untagged*.
6. Select *enable*.

If all frames tagged with the ID of a VLAN of which the selected port is not a member are to be dropped:

7. Select the menu *Config > VLAN > PVID > Edit > Drop NonMemb*.
8. Select *enable* and click RETURN.

Viewing the Receive Rules

Under *Config > VLAN > PVID > Show* you can view the defined receive rules.

```

artem W2000 V5.0          artem WLAN products          by Funkwerk-EC )))
                        node0001CD0B4F66

Port          PVID      Config VLAN PVID
Drop non members Drop untagged frame
-----
wl2_br1       1          enabled      disabled
wl1_ap01      1          enabled      disabled
eth2          1          enabled      disabled
eth1          1          enabled      disabled

Enter [SPACE] refresh, [q] quit:

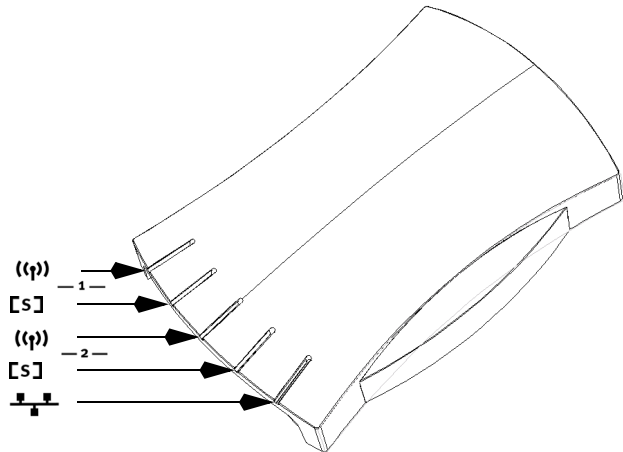
```

The LED States


By means of the five LEDs, you can determine the radio status, the radio activity, the Ethernet activity, and the LED states of the ComPoint. The LED states are displayed by means of LED combinations which will be discussed in detail in this chapter.

Assignment of LEDs to Ports


This figure shows the assignment of the LEDs on the ComPoint.



The following table describes the LEDs and their functions at the am Compoint Revision 1 (until 2003/01/31).

LED	— 1 —		— 2 —		
	((P))	[S]	((P))	[S]	
Color	Yellow	Green	Yellow	Green	Yellow
Wireless Port	This LED displays the activity of Wireless Port 1.	This LED displays the status of Wireless Port 1.	This LED displays the activity of Wireless Port 2.	This LED displays the status of Wireless Port 2.	This LED displays the Ethernet activity.
Display	This LED displays the quantity of wireless data. It flashes shortly if few data is being transmitted; with a high data stream it shines permanently.	This LED flashes if no wireless client is logged on to the ComPoint. As soon as a client logs in, it shines permanently.	This LED displays the quantity of wireless data. It flashes shortly if few data is being transmitted; with a high data stream it shines permanently.	This LED flashes if no wireless client is logged on to the ComPoint. As soon as a client logs in, it shines permanently.	This LED flashes shortly with low Ethernet activity and shines permanently if the activity is high.

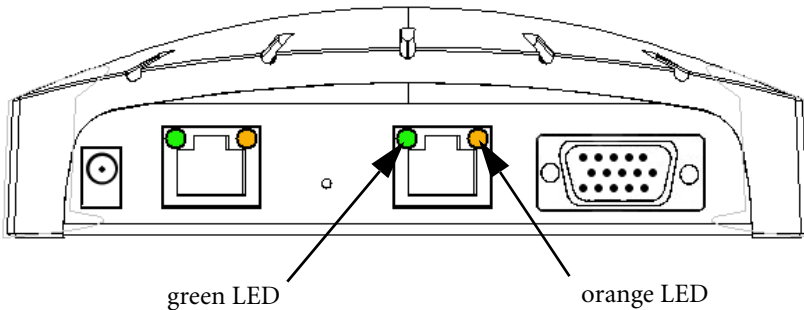
The following table describes the LEDs and their functions at the am Compoint Revision 2 (from 2003/02/01 onwards).

LED	— 1 —		— 2 —		
	((p))	[s]	((p))	[s]	
Color	Red	Green	Red	Green	Green / Red
Wireless Port	This LED displays the activity of Wireless Port 1.	This LED displays the status of Wireless Port 1.	This LED displays the activity of Wireless Port 2.	This LED displays the status of Wireless Port 2.	This LED displays the Ethernet activity.
Display	This LED displays the quantity of wireless data. It flashes shortly if few data is being transmitted; with a high data stream it shines permanently.	This LED flashes if no wireless client is logged on to the ComPoint. As soon as a client logs in, it shines permanently.	This LED displays the quantity of wireless data. It flashes shortly if few data is being transmitted; with a high data stream it shines permanently.	This LED flashes if no wireless client is logged on to the ComPoint. As soon as a client logs in, it shines permanently.	This LED flashes shortly with low Ethernet activity and shines permanently if the activity is high. Red refers to eth1, while green refers to eth2.

The LEDs of the Ethernet Jack

The Ethernet jack at the rear side of the ComPoint is also provided with two LEDs.

Revision 2 (from 2003/02/01 onwards)



If the orange LED shines permanently, the speed is 100 Mbps, whereas if the green LED shines permanently, the speed is 10 Mbps.

If both LEDs are turned off, the ComPoint does not detect any operable network connection.



Note:

The LEDs of both Ethernet ports work in the same way.






Note:

Please use merely one Ethernet port for connecting the device to your network. The second port serves for cascading.














LED States when Booting

With each booting process, you can determine which action is being performed by means of the LED activity. The following table, which displays the different LEDs as circles, provides an overview on this subject. The color code mentioned below is used:

-  The LED is turned off.
-  The green LED shines.
-  The red LED shines.

LED States in Wireless Operation

By means of the LED activity during the normal operation of the ComPoint, you are able to identify specific error conditions in the firmware. The following table provides an overview on this matter.

Error Status	— 1 —		— 2 —		
	((γ))	[S]	((γ))	[S]	
Program error has occurred: LED of the radio activity of Port 1 shines permanently.					
Operating system error has occurred: LEDs of the radio activity and status of Port 1 shine permanently.					
Fatal operating system error has occurred: The LEDs of the radio activity and status of Port 1 as well as the LED of the radio activity of Port 2 shine permanently.					

Technical Data and Specifications

Frequencies and Channels

Worldwide, there is a number of different approval regulations. Basically, the ETSI and FCC regulations apply. ETSI is mainly valid for Europe, FCC for the USA and Canada. Please observe the regulatory flyer (enclosed to the product and contained on the product CD), as well as the [Declaration of Conformity \(Page 1\)](#). These documents contain important information on the countries where the ComPoint Workgroup may be used.

Channel	Frequency (GHz)	ETSI	FCC	IL
1	2412	X	X	
2	2417	X	X	
3	2422	X	X	
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	-
10	2457	X ¹⁾	X	-
11	2462	X ¹⁾	X	-
12	2467	X ¹⁾	-	-
13	2472	X ¹⁾	-	-

¹⁾ If operated in France, limited to these 4 channels

Specifications

Standards	IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.3
Channels	11 channels (USA), 13 channels (Europe)
Antenna Port	RTNC jack
Transmission Capacity	max. 100 mW (20 dBm) eirp.
Receiver Sensitivity	<p>In the 5 GHz frequency band</p> <p>6Mbps -90 dBm, 9Mbps -88 dBm, 12Mbps -86 dBm, 18Mbps -84 dBm, 24Mbps -79 dBm, 36Mbps -76 dBm, 48Mbps -71 dBm, 54Mbps -69 dBm</p> <p>In the 2.4 GHz frequency band</p> <p>6Mbps -92 dBm, 9Mbps -90 dBm, 12Mbps -88 dBm, 18Mbps -86 dBm, 2 Mbps -82 dBm, 36Mbps -78 dBm, 48Mbps -73 dBm, 54Mbps -71 dBm, 1Mbps -98 dBm, 2Mbps -93 dBm, 5.5Mbps -92 dBm, 11Mbps -88 dBm</p>
Modulation	<p>IEEE802.11b and IEEE802.11g: DSSS: BPSK, QPSK, CCK</p> <p>IEEE802.11g: OFDM: BPSK, QPSK, QAM</p>
Network Port	2 10BaseT RJ45 ports
Monitor Button	1 monitor button
LEDs	<p>2 x radio, 1 x I/O jack</p> <p>2 x Ethernet</p>
Security Features	WEP, WPA, access control list, network name broadcast can be deactivated

WEP Key Lengths (Bits)	40 (64) or 104 (128)
Dimensions	145 mm x 208 mm x 37 mm (WxLxH)
Power supply	AC: 100–230 V, 47Hz-63Hz DC: 12V (+/- 1V), max. 1 A
Power Input	approximately 4 Watt
Approvals	CE
Operating Temperature	0 °C to +55 °C
Storage Temperature	-10 °C to +70 °C
Relative Air Humidity	0 % to +95 %, not condensing

Declaration of Conformity (Page 1)

Funkwerk Enterprise
Communications GmbH
Olgastr. 152
D-89073 Ulm
Tel: +49-180-300 91 91-0
Fax: +49-180-300 91 93-0
e-mail: info@funkwerk-ec.com
www.funkwerk-ec.com



Declaration of conformity for the following Artem products

ComCards:	CC-W54g-STD-PC	CC-W54g-PCI	CC-PC-b-H2-STD	CC-CF-b-H2-STD
ComPoints:	CPE-XT1-b CPE-XT2-b CPE-XT3-b CPE-BR1-b CPE-BR1-b-ActAnt	CPE-XT1-g CPE-XT2-g CPE-XT3-g CPE-BR1-g CPE-BR1-g-ActAnt	W1000 W2000 W3000	
ComPoint Workgroup:	CPW-b-EE	CPW-b-ES		

The Wireless LAN products are wireless network products that use Direct Sequence Spread Spectrum (DSSS) or Orthogonal Frequency Division Multiplexing (OFDM) radio technology. These products are designed to be interoperable with any other wireless DSSS/OFDM type product that complies with:

- The IEEE 802.11 Standard on Wireless LANs (Revision b / g), as defined and approved by the Institute of Electrical and Electronics Engineers.
- The Wireless Fidelity (Wi-Fi) certification as defined by the Wireless Fidelity Alliance.

European Union Notice

Radio products which contains radio transmitters are labeled with **CE 0560** **C**, **CE 0336** **D**, **CE 0470** **C**, or **CE** **D** and comply with the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community.

Compliance with this directive implies conformity to the following European norms (in brackets are the equivalent international standards).

EN 60950:2000 (IEC60950) - Product Safety

EN 300 328-1/2 V1.4.1:2003 Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2.4 GHz ISM band and using spread spectrum modulation techniques;

ETSI EN 301 489-1/17 Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services;

Part 1 V1.4.1:08/2002: Common technical requirements

Part 17 V1.2.1:08/2002: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

The following products are furthermore compliant to the following European norm: EN 60601-1-2:2001

ComPoint Enterprise CPE and it's variants

ComCard CC-W54g-STD-PC, CC-PC-b-h2-STD, CC-CF-b-H2-STD

Ulm, 18.04.2005

Dipl.-Ing. (FH) Torsten Urban
Chief Operations Officer

Wireless LAN and your health

Wireless LAN products, like other radio devices, emit radio frequency electromagnetic energy. The level of energy emitted by Wireless LAN devices however is far much less than the electromagnetic energy emitted by wireless devices like for example mobile phones.

Because Wireless LAN products operate within the guidelines found in radio frequency safety standards and recommendations, Artem believes Wireless LAN is safe for use by consumers. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature.

Declaration of Conformity (Page 2)

Regulatory information

This device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product.

For country-specific radio and telecommunications approvals, please consult page 2 of this flyer.

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. These situations may for example include:

Using the wireless equipment on board of airplanes, or in any other environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the policy that applies on the use of wireless equipment in a specific organization or environment (e.g. airports), you are encouraged to ask for authorization to use this device prior to turning on the equipment.

The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this kit, or the substitution or attachment of connecting cables and equipment other than specified by manufacturer.

The correction of interference caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.

Radio Approvals

To determine whether you are allowed to use your device in the countries listed below, please check the number of the transmitter number that is printed on the identification label of your device.

Approval Reference and Radio Type	Country	Remarks
R&TTE Directive 1999/5/EC :	France	Restricted frequency band: In France exist different regulatives, depending on departments (please contact ART for procedure to follow: http://www.art-telecom.fr).
CE 0336 Q ComCard CC-PC-b-H2-STD	Italy	a) within own ground (indoor and outdoor if no public soil is crossed): free use - no licence required b) across public ground: subject to "autorizzazione generale" (general authorization: notification to the Ministry of Communications, yearly fees). Please check with http://www.comunicazioni.it/it/ for more details.
CE Q CPE-XT1-b CPE-XT2-b CPE-XT3-b CPE-XT1-g CPE-XT2-g CPE-BR-g CPE-XT3-g CPE-XT1-g-PoE CPE-XT2-g-PoE CPE-BR-g-PoE CPE-XT3-g-PoE ComCard CC-W54g-STD-PC ComCard CC-W54g-PCI W1000 W2000 W3000		
CE 0470 Q ComPoint CPW-b-EE ComPoint CPW-b-ES		
CC-W54g-STD-PC: FCC-ID: M4Y-XG-300 CC-W54g-PCI: FCC-ID: M4Y-XG-900		

The Radio Type Number has the format CC-xx-b-H2-STD, resp. CC-W54g-STD:

CC-xx-b identifies the type of transmitter: a 2.4 GHz radio, compliant with the IEEE 802.11b Standard for Wireless LANs.

xx identifies the type of card:

PC: PC Card

CF: Compact Flash card

Antenna:

STD: internal antennas (PC Card: with additional proprietary ComCard connector.)

CC-W54-STD identifies the type of transmitter: a 2.4 GHz radio, compliant with the IEEE 802.11g Standard for Wireless LANs.

Internal antennas without additional antenna connector.

Glossary

- **802.11a/b/g**
See [IEEE802.11b](#) and [IEEE802.11a/g](#).
- **AAA**
Authentication, Authorization, Accounting
- **Accounting**
These services and resources have to be paid for by the user.
- **Ad-Hoc Network**
An ad-hoc network is the designation for a number of computers which form an independent wireless 802.11 WLAN together with a wireless adapter. Ad-hoc networks are operated independently, without access points on a peer-to-peer basis. The ad-hoc mode is also referred to as IBSS mode (Independent Basic Service Set). Its application makes sense in very small networks, e.g. if two notebooks are to be networked without an access point.
- **Authentication**
Checking the identity of the user (authentication).
- **Authorization**
On the basis of the identity (authentication), the user can be authorized to access specific services and resources.
- **Default Gateway**
Designates the address of the router to which the complete traffic is sent which is not intended to go over the proper network.
- **DHCP, Dynamic Host Configuration Protocol**
A protocol which performs the IP configuration for individual computers in the network automatically and centrally. If a networked computer is to be integrated into the network or the Internet via the Internet protocol (TCP/IP), it requires a number of basic settings which are essential for any communication. This process can be performed without the interaction of a user via a DHCP server, since the DHCP server knows the settings and forwards them to the clients. Without such a DHCP server, the user has to perform the settings manually. Each time he changes the network, e.g. when he takes his notebook from one location to another, he has to enter the settings

again. If a DHCP server is used, this process is automatically performed each time.

- **DNS**

DNS means Domain Name System and administrates the allocation of IP addresses to domain names. DNS is used, for instance, to allocate the corresponding IP address to the domain `www.funkwerk-ec.de`

- **DSSS**

Direct Sequence Spread Spectrum is a radio technology which was originally developed for the military sector and offers a high resistance against interferences, as the payload signal is spread over a wide sector. The signal is spread via a spread sequence or a chipping code, which consists of 11 chips on a bandwidth of 22 MHz. If one or several chips are disturbed during the transmission, the information can be reliably regained from the rest of the chips.

- **Dynamic IP Address**

In contrast to a static IP address, a dynamic IP address is temporarily assigned via DHCP. Network components, such as Web servers or printers, usually have static IP addresses. Clients, such as notebooks and workstations, normally receive dynamic IP addresses.

- **ESS**

The Extended Service Set refers to several BSS (several access points) which form a single virtual wireless network.

- **FHSS, Frequency Hopping Spread Spectrum**

Frequency spread is attained in a FHSS system by means of continuously changing frequencies, which are altered according to specific hopping patterns. In contrast to DSSS systems, there are no fixed frequencies, but definable hopping patterns. The frequency is often changed within one second.

- **Firmware**

Software code which contains all functions of a device. This code is written in a PROM (Programmable Read-Only Memory) and is stored there even after switching off the device. The firmware can be upgraded by the user if a new software version is available (firmware upgrade).

- **IEEE**
The Institute of Electrical and Electronics Engineers (IEEE). This is an international committee of engineers. It continuously improves standards to ensure the compatibility of the most diverse devices.
- **IEEE802.11b**
One of the IEEE standards for wireless network hardware. Products corresponding to the same IEEE standard are able to communicate with each other, even if they were produced by different hardware manufacturers. The IEEE802.11b Standard specifies data rates of 1, 2, 5.5, and 11 Mbps, a working frequency in the range of 2.4 to 2.4835 GHz, and WEP encryption. IEEE802.11 wireless networks are also referred to as Wi-Fi networks.
- **IEEE802.11a/g**
Specifies data rates of 54, 48, 36, 24, 18, 12, 9, and 6 Mbps as well as a working frequency in the range of 5 GHz (with IEEE802.11a) or 2.4 GHz (with IEEE802.11g). IEEE802.11 g can be configured in such a way that it additionally supports 11b or 11b and 11.
- **Infrastructure Mode**
A network in the infrastructure mode is a network which contains at least one access point as communications and control center. In a network in the infrastructure mode, all clients will exclusively communicate with each other over access points. There is no direct communication between the individual clients. Such a network is also referred to as BSS (Basic Service Set). A network which consists of several BSSs is called ESS (Extended Service Set). Most wireless networks are operated in the infrastructure mode to set up connections to the wired network.
- **IP Address**
The Internet Protocol (IP) in its most frequently used form has a 32-bit address which is used to identify the senders and receivers of packets unambiguously. You can send requests in the Web to remote servers or send e-mails, and the opposite terminal will know from where the request or the e-mail comes. There are public and private IP addresses. Private IP addresses are preferably assigned by routers if a group of computers is used in a private or corporate network. Such addresses may read, for instance, 192.168.0.1.

- **IPCONFIG**
This is an auxiliary program used by Windows computers to check or modify the proper IP settings.
- **ISP**
An Internet Service Provider (ISP) is a provider of Internet services or related services, such as the hosting of websites or website creation.
- **LAN**
A LAN (Local Area Network) is a local network which is usually set up within a building. Here, all computers involved share local services (e.g. DHCP or file server). With the help of a WLAN, a LAN may also comprise and network several buildings.
- **MAC address**
The MAC (Media Access Control) address is the unambiguous hardware address of a network interface. Each hardware manufacturer assigns his proper MAC addresses from his own number pool. As a result, manufacturers can be assigned on the MAC address level.
- **Mixed Mode**
The AP accepts WPA and WPA2.
WPA = TKIP, TKIP
WPA2 = TKIP, CCMP
- **NAT, Network Address Translation**
Translation of an IP address in one network into another IP address in another network. As a result, many computers in one network can be displayed to the outside with a single IP address. NAT is often used by SOHO routers or in ComPoint Workgroup ACs if several clients are connected via a switch.
- **Network Mask**
see [Subnet Mask](#)
- **PCMCIA**
The PCMCIA (Personal Computer Memory Card International Association) is an industrial association founded in 1989 which produces and sells I/O cards with the size of credit cards, e.g. WLAN cards.

- **Ping**
Ping means Packet INternet Grouper and is a tool which serves to check whether a computer is online. Ping is used to search for errors in a network (troubleshooting). The person who carries out the check waits for replies of other computers.
- **PVID, Port VLAN ID**
Also refer to [VLAN, Virtual Local Area Network](#). Default VLAN-ID of the corresponding port of the ComPoint. Each port of the system has to be assigned precisely one Port VLAN Identifier (PVID).
The PVID is necessary if a frame without VLAN identifier / a “VLAN-untagged” frame is received on this port.
The PVID setting of each port corresponds to the VLAN Management Identifier.
- **RJ-45**
A plug-in connector as it is also used for ISDN telephones. It serves to connect computers via Ethernet. In contrast to ISDN where only 4 pins are used, all 8 pins are used in the case of an Ethernet cable.
- **Roaming**
In WLANs with several cells, clients can move freely through the cells. When doing so, they can log out at one access point and log on to another without the user noticing it. This capacity is called roaming.
- **SOHO**
Small Office/Home Office
- **Static IP Address**
A permanently configured IP address, in contrast to dynamic IP addresses.
- **Subnet Mask**
A method to divide several IP networks into a number of subgroups or subnetworks. The mask is a binary pattern which has to correspond to the IP addresses in the network. By default, the subnet mask is 255.255.255.0. In this case, 254 different IP addresses could occur in a subnetwork, from x.x.x.1 to x.x.x.254.
- **TCP, Transmission Control Protocol**
A method used in the IP protocol to transfer messages as units (data-grams) between the network subscribers within a LAN or WLAN.

While IP is concerned with the packet transfer via IP addresses, TCP controls which packets belong together. TCP is a connection-oriented protocol which transfers acknowledgments on the receipt of the packets to the sender.

- **TCP/IP, Transmission Control Protocol / Internet Protocol**
TCP/IP is the basic protocol in the Internet. It does not consist of TCP and IP only, but also contains a number of protocols.
- **Temporal Key Integrity Protocol (TKIP)**
see [WPA, Wi-Fi-Protected Access](#)
- **UDP, User Datagram Protocol**
In contrast to TCP, UDP does not send receipts on received packets and is used in LANs and WLANs for the transmission of audio and video data. If a packet is lost, it is not resent, since it would already be obsolete by then.
- **WEP, Wired Equivalent Privacy**
Encryption mechanism standardized by the IEEE in the scope of passing the WLAN standard. Based on symmetrical encryption, i.e. both partners use the same key for encryption and decryption. The key length can be 64 bits (corresponds to a 40-bit-effective key) and 128 bits (corresponds to a 104-bit-effective key). As long as all used clients support 128-bit encryption, we recommend to select this encryption mechanism since it offers increased security.
- **WINIPCFG**
A graphic tool under Windows 95, 98, and Millennium, which uses the Win32 API to view and perform the address configuration of computers.
- **WLAN, Wireless Local Area Network**
A group of computers which is networked wirelessly (WLAN).
- **WPA, Wi-Fi-Protected Access**
The Wi-Fi Alliance (an alliance of several WLAN manufacturers) has developed its own encryption in order to enhance security in wireless LAN environments. The so-called WPA protocol (Wi-Fi-Protected Access) replaces the static encryption keys of the WEP by dynamic keys which are more difficult to crack. The Temporal Key Integrity Protocol (TKIP), which is part of standards 802.11i, is used for this purpose. Just like the WEP encryption procedure, the TKIP encryp-

tion is based on the RC4 algorithm. As a new feature, it is dynamic. For instance, TKIP can be configured either on the basis of the data volume or a time range. This means that the key is not valid long enough for being cracked by the familiar procedures.

- **WPA 2 - Enterprise**

Addresses the requirements of enterprises and offers secure encryption and authentication. Uses 802.1x and the Extensible Authentication Protocol (EAP) and therefore offers an efficient option to authenticate users.

It is not the ComPoint, but a central authentication server, such as RADIUS, which authenticates each client before granting access to the network. ComPoint merely serves as the initial contact for the clients. The actual decision with respect to the authentication is made on the authentication server.

After successful authentication, the server sends a shared key to the client and AP to transmit the data in the wireless network.

- **WPA 2 - PSK (Home, Personal)**

Addresses private users or small enterprises which do not operate a central authentication server. PSK stands for Pre-Shared Key and means that the AP and client use a fixed arbitrary sequence of characters (8 to 63 characters) known to all subscribers as the basis to calculate keys in wireless transmission.

TKIP and CCMP encryption are used for all transmission processes. In this mode, no authentication of the client is performed.

- **VLAN, Virtual Local Area Network**

Mapping of a logical structure to the actual physical structure of a LAN, as defined, among others, in standard IEEE 802.1Q1.

Networks are set up with the help of active components, switches, and routers. Sometimes, two or more independent networks are to be set up with identical physical components. These differing networks are to be set up in such a way that the users of the networks do not interfere with each other. Example: one network for the Finance Department and one for Production.

VLANs are the solution to this problem. Each VLAN is assigned an unambiguous number. This number is called VLAN ID. A device belonging to the VLAN with ID=1 can communicate with any other

device operated within the same VLAN, but not with a device belonging to one of the other VLANs ID=2,3,..

- **VID, VLAN ID**

See [VLAN, Virtual Local Area Network](#)

Index

A

AC [2-6](#)

AccessPoint [4-1](#)

Accounting [4-37](#)

ACK window [4-31](#)

ACL local [4-78](#)

ACL remote [4-79](#)

AclLocal [4-77](#)

AclRemote [4-77](#)

Actual speed [5-17](#), [5-18](#)

Actual value [1-16](#), [4-24](#)

Add port [4-64](#)

Add rule [4-53](#)

Add SSID [4-34](#)

Adding a device [2-7](#)

Admin [1-17](#), [4-65](#)

Admin cmds [4-91](#)

Admin password [4-74](#)

After commissioning [1-8](#)

Alias name [5-17](#)

Antenna diversity [4-27](#)

Antenna systems [1-1](#)

Ant. diversity [4-27](#)

AP [2-6](#), [5-14](#)

AP distance [4-29](#)

Application [2-6](#)

ARP cache [4-18](#)

artem ComPoint Manager [1-9](#), [1-10](#), [2-1](#)

Assoc_time [4-17](#)

Authenticate [4-76](#)

Authentication server [4-76](#)

Auth. cache [4-82](#)

Auth. passwd [4-88](#)

Auth. proto [4-88](#)

Auto config [5-17](#)

Auto neg mode [1-16](#), [4-24](#)

Available devices [2-4](#)

Average received signal noise [5-12](#)

Average received signal strength [5-12](#)

B

Basic configuration [1-10](#), [1-16](#), [2-1](#)

Bcst SSID [4-5](#), [4-33](#)

Beacon frames [4-29](#)

BLD [4-63](#)

BLD status [4-63](#)

BR [2-6](#), [5-14](#)

Bridge [4-23](#), [5-1](#)

Bridge link [5-15](#)

 Automatic setup [5-21](#)

 Check [5-25](#)

 Manual setup [5-29](#)

Bridge port [5-1](#)

Broken link detection [4-63](#)

Browser [1-9](#)

Browser-based user interface [3-5](#)

Buffer util. [4-19](#)

C

Cable ends [1-7](#)

Channel [4-26](#), [5-18](#), [5-20](#)

Channel frequency [1-15](#)

Channels [1-15](#)

Client ID [4-46](#)

Commissioning [1-4](#)

Communities [4-84](#), [4-85](#)

Comm. state [4-71](#), [4-79](#), [4-80](#)

Comm. table [4-85](#)

ComPoint

 Product package [1-1](#)

ComPoint AccessPoint [4-1](#)

ComPoint Bridge [5-1](#)

 Configuration [5-8](#)

 Use [5-1](#)

ComPoint Manager [2-1](#)

 Exit [2-20](#)

 Interface [2-2](#)

Config [4-20](#)

Config state [5-20](#)

Configuration reset [2-10](#)

Configuring the Ethernet port [1-16](#)

Contact [4-21](#)

Control [4-72](#)

Conventions for interface names [1-13](#)

Current date [4-90](#)

Current time [4-90](#)

Customize [4-41](#)

CW max [4-31](#)

CW min [4-31](#)

D

DBR [5-14](#)

Declaration of conformity [B-4](#)

Default rule [4-57](#)

DefaultMode [4-51](#)

Def. access [4-79](#), [4-81](#)

Def. action [4-43](#)

Delete [2-7](#)

 Configuration [2-10](#)

DES [4-88](#)

Description [4-21](#)

Desktop device [1-5](#)

Device

 Delete [2-7](#)

DHCP [2-5](#), [4-4](#), [4-46](#)

 Status [4-46](#)

Direct link [4-30](#)

Discovered [2-6](#)

Double bridge [4-23](#), [5-33](#)

Drop non Memb. [4-70](#)

Drop untagged frames [4-70](#)

Dst MAC [4-54](#)

DST ports [4-55](#)

DTIM period [4-29](#)

E

EAP [4-80](#)

EAPOL timeout [4-81](#)

ED threshold [4-31](#)

Edit rule [4-53](#)

Encapsulation [4-31](#), [4-41](#), [4-42](#)

Enc. passwd [4-88](#)

Enc. proto [4-88](#)

Entering the IP address [2-1](#)

Entering the name [2-1](#)

Entering the netmask [2-1](#)

Entering the standard gateway [2-1](#)

Enterprise [4-23](#)

Error

 Operating system [A-6](#)

 Software [A-6](#)

Ethernet [1-2](#), [1-16](#)

 Activity [1-13](#), [A-1](#)

 Connection to the [1-7](#)

 Jack [A-4](#)

 Port [1-14](#)

 Port Statistics [4-7](#)

eth1 [1-13](#)

Evaluation of the quality [5-27](#)

Example for multicast filtering [4-58](#)

Exceptions [4-42](#), [4-43](#)

Exit [4-93](#)

Exit command [4-93](#)

Exiting the ComPoint Manager [2-20](#)

Extended [4-27](#), [5-15](#)

F

Factory defaults [2-20](#), [4-91](#)

Fallback [2-5](#)

Features [4-23](#)

Filter [4-4](#)

 Discard [4-51](#)

 Forward [4-51](#)

Filter rules [4-55](#)

Filtered frames since last reset [4-8](#), [4-11](#)

Filtered frames (on all ports) since last reset [4-8](#), [4-12](#)

Filtering [4-47](#)
 ARP process [4-50](#)
 Protocol [4-50](#)

Firmware upgrades [2-14](#)

Firmware upgrading [2-1](#)

Flash date [4-22](#)

Floppy disk [1-10](#)

Frame compression [4-30](#)

Frame concatenation [4-30](#)

Frames lost [5-28](#)

Frames received [5-28](#)

Frames sent [5-28](#)

Frequencies and channels [1-20](#)

Frequency [1-15](#)

Fresnel zone [5-5](#)

Front view [1-1](#)

Functions
 ComPoint Manager [2-4](#)

G

Gateway [1-11](#), [1-16](#), [2-9](#), [4-44](#)

H

Hardware [4-21](#)

Help [4-93](#)

Help command [4-93](#)

I

IEEE802.1H [4-42](#)

IEEE802.1x [4-76](#), [4-77](#)

Input section [3-4](#)

Interface [1-13](#), [1-15](#), [1-16](#), [4-24](#), [4-25](#), [4-44](#), [5-17](#)

Interface names [1-13](#)

IP address [1-9](#), [1-10](#), [1-11](#), [1-16](#), [2-9](#), [4-17](#), [4-44](#), [4-71](#), [4-90](#)

IP mode [2-5](#)

K

Key 1-4 [4-38](#)

L

Lease IP [4-46](#)

Lease status [4-46](#)

Leave WLAN [4-71](#)

LED states [A-1](#)

LEDs

- Assignment to ports [A-1](#)
 - Bootup process [A-5](#)
 - Color [A-2](#), [A-3](#)
 - Display [A-2](#), [A-3](#)
 - Error conditions [A-6](#)
 - Wireless port [A-2](#), [A-3](#)
- Line of sight [5-5](#)
- Link [4-5](#)
- Link quality [5-27](#)
- Link state [5-17](#)
- Link status [4-63](#)
- Link test [5-17](#), [5-25](#)
 - Perform [5-25](#)
- LLC frame [4-41](#)
- LLC header [4-41](#)
- Load balancing [4-29](#)
- Local card [5-18](#)
- Location [4-21](#)
- Lock state [5-20](#)
- Logging [4-91](#)
- LOS [5-5](#)
- ## M
- MAC address [1-11](#), [2-9](#), [4-4](#), [4-17](#)
- MAC_filter [4-51](#)
- Main window [2-2](#)
- Manual config [5-17](#)
- Max. reauth [4-81](#)
- Max. requests [4-81](#)
- Mcast rate [4-27](#)
- MD5 [4-88](#)
- Medium distribution [4-31](#)
- Menu [2-3](#)
 - Config [4-20](#)
 - Control [4-72](#)
 - Status [4-2](#)
- Menu and command section [3-3](#)
- Mgmt VID [4-66](#)
- Microsoft Internet Explorer [3-5](#)
- Mixed mode [4-36](#)
- Mode [4-5](#), [4-41](#)
- Mode 802.11g [4-29](#)
- MPDU [4-14](#)
- MPDUs received without appropriate privacy configuration [4-16](#)
- MSDU [4-13](#)
- Multicast [4-53](#)
- MULTICAST filtered frames since last reset [4-8](#), [4-12](#)
- Multicast filtering [4-58](#)
- Multicast interface
 - Determine [2-19](#)
- MULTICAST received frames since last reset [4-8](#), [4-11](#)
- MULTICAST transmitted frames since

last reset [4-8](#), [4-12](#)

MW robustness [4-28](#)

N

Name [1-11](#), [2-9](#), [4-17](#)

Network [1-10](#), [2-1](#), [4-1](#)

Network address [4-44](#)

Network name [1-18](#), [4-33](#), [4-71](#)

Network parameters [4-3](#)

Nitro mode [4-30](#)

Nitro xm [4-30](#)

Node name [4-20](#)

Node table [4-16](#)

Noise [4-5](#), [5-27](#)

Not found [2-6](#)

Number of aborted frames [4-16](#)

Number of CTS frames received in response to an RTS [4-15](#)

Number of dropped received unicast and multicast MSDUs [4-16](#)

Number of duplicate received MSDUs [4-14](#)

Number of frame transmissions without ACK received [4-14](#)

Number of MPDUs received without required encryption [4-16](#)

Number of MPDUs which could not be

transmitted [4-16](#)

Number of MSDUs dropped before transmission [4-14](#)

Number of MSDUs successfully sent after more retries [4-14](#)

Number of MSDUs successfully sent after one retry [4-14](#)

Number of MSDUs that could not be transmitted [4-14](#)

Number of multicast MSDUs received successfully [4-14](#)

Number of multicast MSDUs transmitted successfully [4-13](#)

Number of partially or erroneously received MSDUs [4-16](#)

Number of PHY aborted frames [4-16](#)

Number of received frames without any filter [4-14](#)

Number of received MPDUs that could not be decrypted [4-15](#)

Number of received MPDUs without decryption key [4-15](#)

Number of rejected unencrypted MPDUs [4-16](#)

Number of RTS frames with no CTS received [4-15](#)

Number of transmitted MPDUs [4-14](#)

Number of unicast MSDUs received successfully [4-14](#)

Number of unsuccessfully received

frames [4-16](#)

O

Operating mode [4-25](#), [5-14](#)

P

PassPhrase [4-37](#)

Password [1-17](#), [2-11](#), [3-6](#)
Change [2-12](#)

Patch cable [1-7](#)

Path [3-3](#)

PC [1-10](#), [2-1](#), [4-1](#)

PHY settings [4-31](#)

Piggyback ack [4-30](#)

Plug-in power supply [1-3](#)

Point-to-multipoint topology [5-3](#)

Point-to-point topology [5-3](#)

Poll count [4-90](#)

Poll interval [4-90](#)

Poll timeout [4-90](#)

Port [4-4](#), [4-6](#), [4-24](#)

Port number [4-71](#), [4-79](#)

Port stat [4-7](#)

Wireless port [4-11](#)

Port state [4-33](#)

Power supply [1-2](#), [1-3](#), [1-6](#)

Preconditions for use of links with
ComPoint Bridges [5-5](#)

Primary if [4-3](#)

Prim. server [4-80](#)

Priority [4-91](#)

Privacy [4-36](#), [5-20](#)

Probe response [4-29](#)

Processing order of the rules [4-57](#)

Prompt [3-4](#)

PVID [4-65](#), [4-69](#), [4-70](#)

Q

Quiet period [4-81](#)

R

Radio activity [1-13](#), [A-1](#)

Radio band [5-20](#)

Radio card [1-13](#)
External [1-13](#)
Internal [1-13](#)
Lower [1-13](#)
Upper [1-13](#)

Radio status [1-13](#), [A-1](#)

Rate [4-17](#)

Rear view [1-2](#)

Reauth period [4-82](#)

Reauth. switch [4-82](#)

- Receive [4-43](#)
 - Received at rate [5-27](#)
 - Received frames since last reset [4-8](#), [4-11](#)
 - Refresh [4-93](#)
 - Refresh command [4-93](#)
 - Reg. domain [4-23](#)
 - Release date [4-22](#)
 - Remote MAC [5-18](#)
 - Remove port [4-64](#)
 - Remove rule [4-55](#)
 - Remove SSID [4-34](#)
 - Repeating [4-33](#)
 - Resetting
 - to factory defaults [2-20](#)
 - Resetting the password [1-20](#)
 - Restart [2-1](#), [2-20](#), [4-91](#)
 - Retries [4-64](#)
 - RF settings [4-26](#), [5-14](#)
 - RFC_1042 [4-42](#)
 - RFC_2886 [4-37](#)
 - RJ45 jack [1-2](#)
 - Rod antenna [1-1](#)
 - Screwing on [1-5](#)
 - RTS threshold [4-28](#)
 - Rule number [4-54](#)
 - Rule status [4-54](#)
 - Rule table [4-53](#)
- ## S
- Saving and loading a configuration [2-10](#)
 - SC [2-6](#)
 - Screwing on antenna [1-5](#)
 - Searching [2-4](#)
 - Security [4-34](#), [4-73](#), [4-87](#), [5-14](#)
 - Security level [1-19](#)
 - Sec. level [4-88](#)
 - Select port [4-70](#)
 - Selecting the frequency [1-15](#)
 - Sel. channel [4-26](#)
 - Server config [4-37](#), [4-80](#)
 - Service sets [4-27](#), [4-32](#)
 - Serv. timeout [4-81](#)
 - Session [4-4](#)
 - Setting the network name [1-18](#)
 - Setting up a Telnet connection [2-1](#)
 - Settings [5-20](#)
 - Shared secret [4-37](#), [4-80](#)
 - SHA1 [4-88](#)
 - Show ports [4-64](#)
 - Signal [5-27](#)
 - Signal strength [4-5](#)

SNMP [4-4](#), [4-83](#)
 Status [4-84](#)

SNR [5-27](#)

SNTP
 Status [4-90](#)

Software [4-22](#)

Specifications [B-2](#)

Speed [4-4](#), [A-4](#)

Speed mode [4-26](#), [5-20](#)

Src MAC [4-54](#)

SSID [1-18](#)

Standard patch cable [1-7](#)

State [2-6](#), [4-36](#), [5-20](#)

Static [2-5](#)

Statistical data [4-2](#)

Status [4-2](#)

Status bar [2-3](#)

Status section [3-4](#)

Subnet mask [1-16](#)

Subnetmask [1-11](#), [2-9](#)

Summary [4-3](#)

Summary view [4-2](#)

Supp. timeout [4-81](#)

Sync period [4-71](#), [4-79](#)

Syslog [4-91](#)

System [4-20](#)

T

Telnet [1-9](#), [3-1](#)

Telnet user interface [3-1](#)

Terminal program [1-9](#)

Test interval [4-64](#)

The LEDs of the Ethernet jack [A-4](#)

Time zone [4-90](#)

Timeout [4-64](#)

Title section [3-3](#)

Tool bar [2-3](#)

Transmit [4-42](#)

Transmitted frames since last reset [4-8](#), [4-11](#)

Traps [4-84](#)

Tx power [4-27](#)

Type [4-17](#)

U

Uptime [4-4](#)

Usage area [4-23](#)

User [1-17](#)

User info [4-73](#)

User interface [3-1](#)
 Browser [3-5](#)

User interface of the ComPoint Manager [2-2](#)

User level [1-17](#)

USM

 Security [4-87](#)

USM table [4-87](#)

USM users [4-85](#), [4-86](#), [4-87](#)

V

VACM table [4-89](#)

VACM views [4-88](#)

VID [4-66](#)

View [1-17](#)

View logs [4-91](#)

Virtual LAN [4-65](#)

VLAN [4-65](#)

 Configuration [6-1](#)

 Setting up [4-67](#)

VLAN cache [4-71](#)

VLAN Manager [4-71](#)

VLANs [4-65](#)

W

Wall mounting [1-4](#), [1-5](#)

Web connection [2-1](#), [2-13](#)

WEP [1-19](#), [4-36](#)

Wireless backbone [5-4](#)

Wireless bridge connected to wireless

clients [5-4](#)

Wireless Equivalent Privacy (WEP) [4-36](#)

Wireless network [1-8](#)

Wireless port [1-14](#)

Wireless stat [4-13](#)

WL VLAN [4-65](#), [4-70](#)

wlx_br [5-10](#)

wl1_ap01 [4-33](#), [4-71](#)

wl1_xxx [1-13](#)

wl2_xxx [1-13](#)

WPA2 Enterprise [1-19](#)

WPA2 enterprise [4-36](#)

WPA2 PSK [1-19](#), [4-36](#)