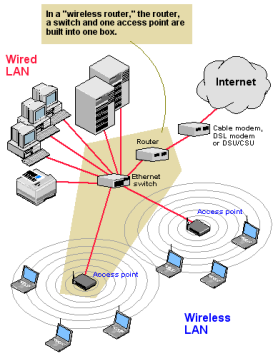
CoNeT Mobile Lab
Wireless Communication

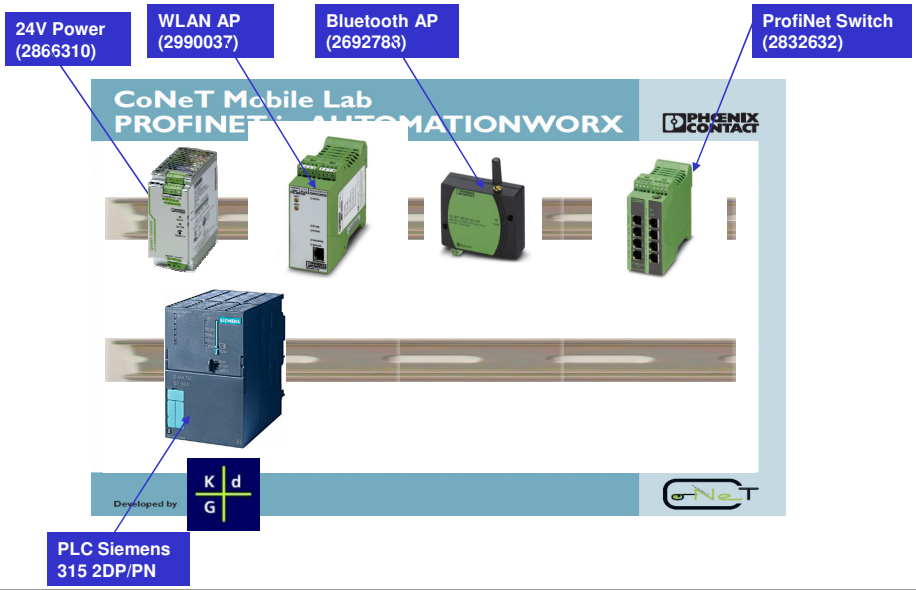


(Version 2)

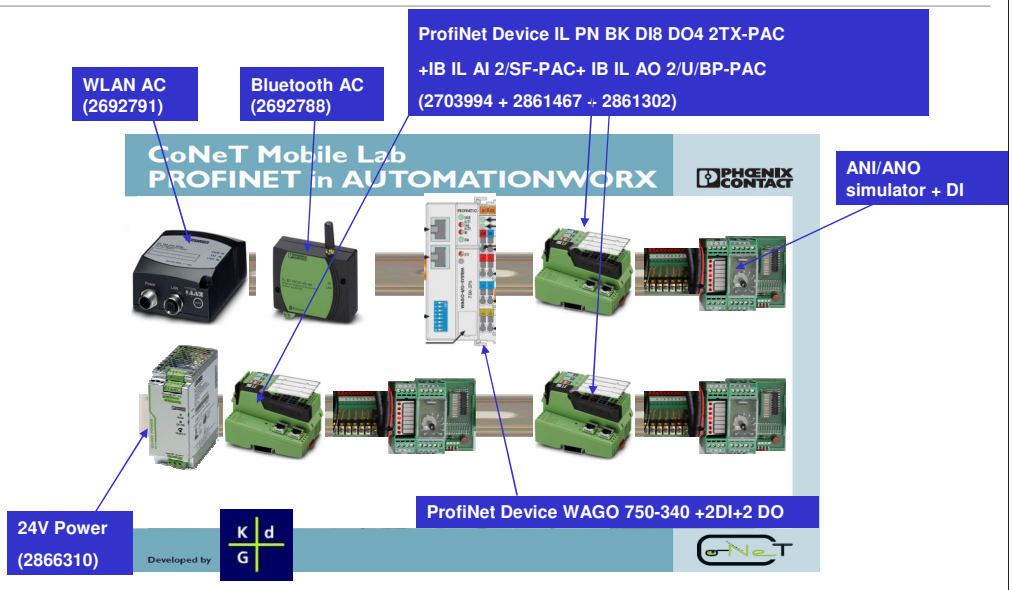
CoNeT Mobile Lab
Wireless Communication

PART 2: Practical Aspects of Wireless Communication

1. Overview of the Components in the Wireless CML(1)



1. Overview of the Components in the Wireless CML(2)



2. Description functionalities of the Wireless components

2.1 FL WLAN 24 AP 802-11 XDB

- wireless transceiver that can function as:
  - ✓ Access Point (AP)
  - ✓ Bridge
  - ✓ Access Client (AC)
- The transceivers can send Ethernet data with the option of adding serial data over the wireless link.
- Conforms to IEEE 802.11a/b/g standards
- Security Mechanism
  - ✓ WEP Encryption (shared or open authentication)
  - ✓ WPA with TKIP/AES-CCMP Encryption
  - ✓ WPA-EAP-TLS, and WPA2-EAP-TLS
  - ✓ MAC Address Filtering
  - ✓ Bridge encryption (AES)

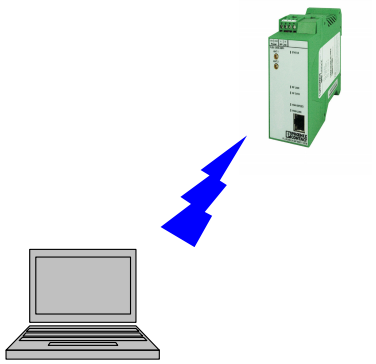
2. Description functionalities of the Wireless components

2.1 FL WLAN 24 AP 802-11 XDB transceiver

There are two antenna connectors on the transceiver. This is for the purpose of antenna diversity. The transceiver may be operated using a single antenna; however, in some environments you may experience multi-path problems (null spots). If using a single antenna, it must be connected to the **ANT 1** port.

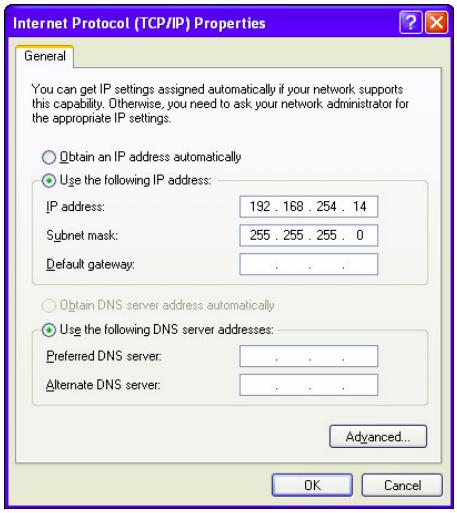
The transceiver can use either the 2.4 or 5 GHz ISM band. However, the antenna must be specific to the frequency. There are dual band antennas available, if using both frequency ranges. **802.11a** uses the 5 GHz band, whereas **802.11b** and **802.11g** use the 2.4 GHz band.

Exercise 1: Wireless communication between a PC with WLAN interface and the FL WLAN 24 AP 802-11 XDB



2.2 Configuring the WLAN transceiver (FL WLAN 24 AP)

2.2.1 Configuring a PC to communicate with the WLAN AP



2.2.1 Configuration PC to communicate with the WLAN AP

1. Select the “Start… Settings… Network” menu and click the “Dial up Connections” button. Right-click the “Local Area Connection” button that the transceiver is connected to and click the “Properties” button.

2. Highlight Internet Protocol (TCP/IP) and click the “Properties” button.

3. Select Use the following IP address and enter the following IP address: 192.168.254.xxx (xxx can be 1-253)

4. Set the Subnet mask to 255.255.255.0.

5. Click the ‘OK’ button to enable the connection

2.2.2 Configuring the WLAN Transceiver as Access Point (AP)

To configure the WLAN transceiver to function as an Access Point:

1. Apply power to the WLAN transceiver and open a web browser, such as Internet Explorer, on the computer.
2. Enter the following IP address into the “Address” field of the browser:

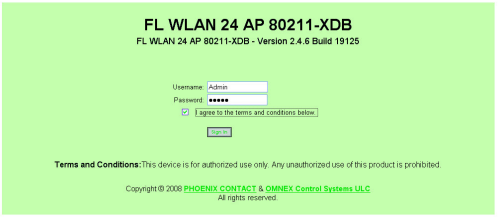
https://192.168.254.254

3. Enter the default case-sensitive credentials:

Username: Admin

Password: admin

4. Agree to the terms and conditions and click the “Sign In” button.



https://192.168.254.254

Username: Admin
Password: admin

2.1.2 Configuration WLAN Transceiver as Access Point (AP)

To configure the WLAN transceiver to function as an Access Point:

1. Apply power to the WLAN transceiver and open a web browser on the computer, such as Internet Explorer.
2. Enter the following IP address into the “Address” field of the browser:

https://192.168.254.254

3. Enter the default case-sensitive credentials:

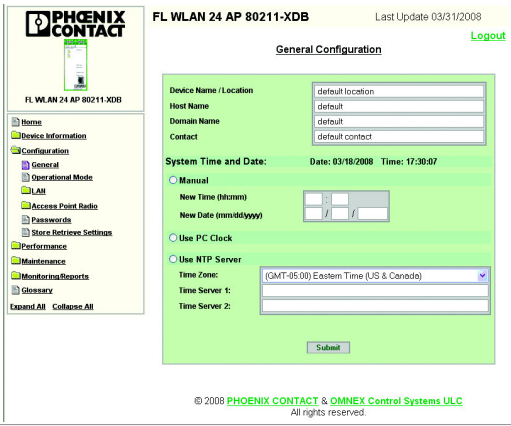
Username: Admin

Password: admin

4. Agree to the terms and conditions and click the “Sign In” button.

• The “Configuration… General” menu

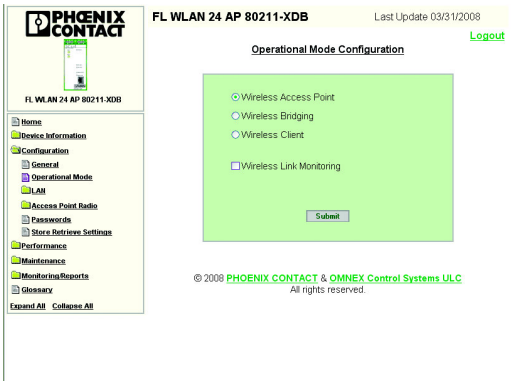
5. Click the “Expand All” button at the bottom of the menu to open all of the folders.
6. Click the “Configuration… General” menu
7. Click the “Submit” button to make the settings active.



• If desired, enter a Device Name/Location, Host Name, Domain Name, and Contact. These are not necessary for proper operation but make troubleshooting large networks easier.
• Click the appropriate radio button for the desired time keeping method. Time keeping can be done by
– manually entering the time.
– using the connected PC clock.
– connecting to an NTP (Network Time Protocol) server (requires an Internet connection).

•The “Configuration… Operation Mode” menu

8. Click the “Configuration… Operational Mode” menu.
9. Click the “Wireless Access Point” button. Then, click the Submit” button. The radio will reboot.



A reboot may take up to one minute and requires the user to log in again.

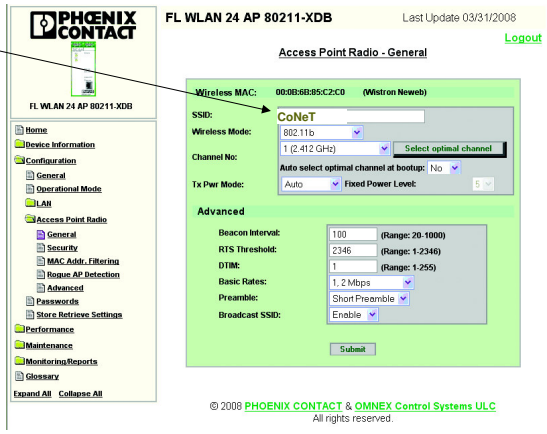
• The “Configuration..Access Point Radio..General” menu

11. Enter a new value (eg. CoNeT) in the “SSID” field. All Client transceivers in the same network must have the same SSID.

CoNeT

12. Click the “Submit” button to save the settings**.**

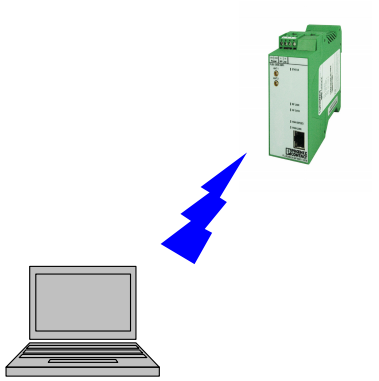
To maintain security, the SSID should be changed to something other than the default. Eg. CoNeT



• The “Configuration..Access Point Radio..General” menu

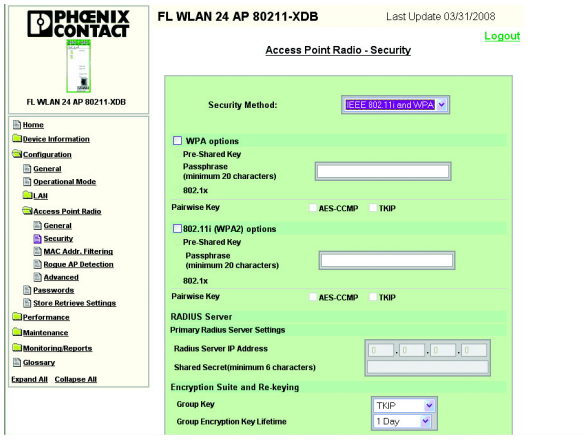
- Enter a mode using the “Wireless Mode” drop-down menu. All transceivers in the same network must operate in the same mode. Modes b and g can be mixed if 802.11b and 802.11g clients exist in the network.
- Enter a channel using the “Channel No:” drop-down menu. If 802.11b/g mode is used, Channels 1, 6 and 11 have the least amount of overlap to allow for the least amount of interference from other 802.11 wireless networks. 802.11a has no overlapping channels. The Channel No. must be the same for all transceivers. If unsure about the channel, select “Yes” from the “Auto select optimal channel at bootup” drop-down menu.
- Select a value other than “Off” from the “Tx Pwr Mode” drop-down menu. If “Off” is selected, radio transmission is disabled. Select “Auto” to allow the radio to adjust power to a level optimized for the network structure. Auto mode is recommended, but the power level can be fixed to one of five levels with “5” the highest power setting.
- Select “Disable” from the “Broadcast SSID” drop-down menu. This is a minimum security setting that prevents other 802.11 transceivers from easily entering the network.

TEST of the Wireless communication between PC and the FL WLAN 24 AP 802-11 XDB



• The “Configuration..Access Point Radio..Security” menu

13. Click the “Access Point Radio… Security” menu.
14. Enter the desired method of security and appropriate settings.
15. Enter the desired security settings.



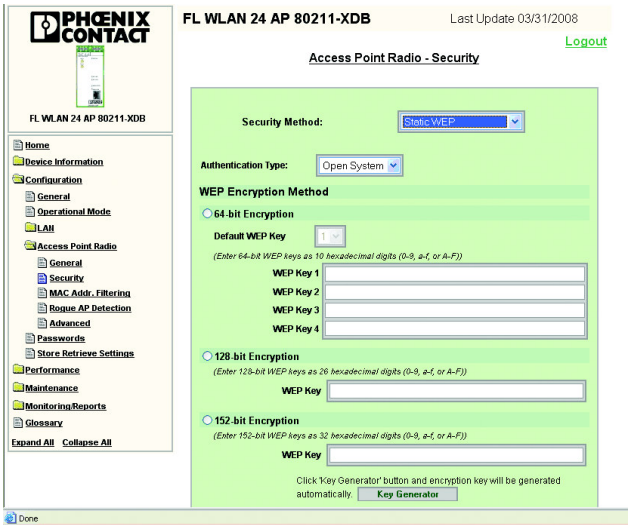
Static WEP is an older method of encryption that can be easily broken by determined individuals. WPA and 802.11i (WPA2) are more advanced encryption methods and are recommended over WEP; however, all transceivers in the network must have this capability.

Most devices available today support WPA.

• WEP security Settings for AP

1. Click the “Access Point Radio… Security” menu.

- The “Authentication Type” drop-down menu allows selection of “open”, “shared” or “open/shared” (clients may employ either)
- WEP Encryption Method selects one of three sizes of keys that can be used by WEP
- WEP Keys 1-4 (64-bit encryption) selects one of four possible keys that can be used with 64-bit encryption



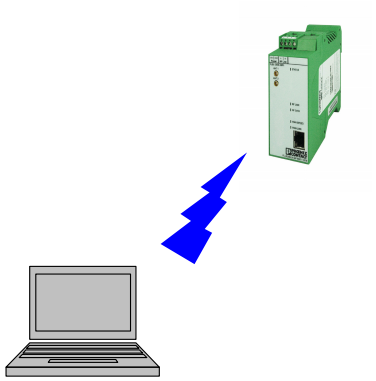
The buttons and fields in the WEP window are:

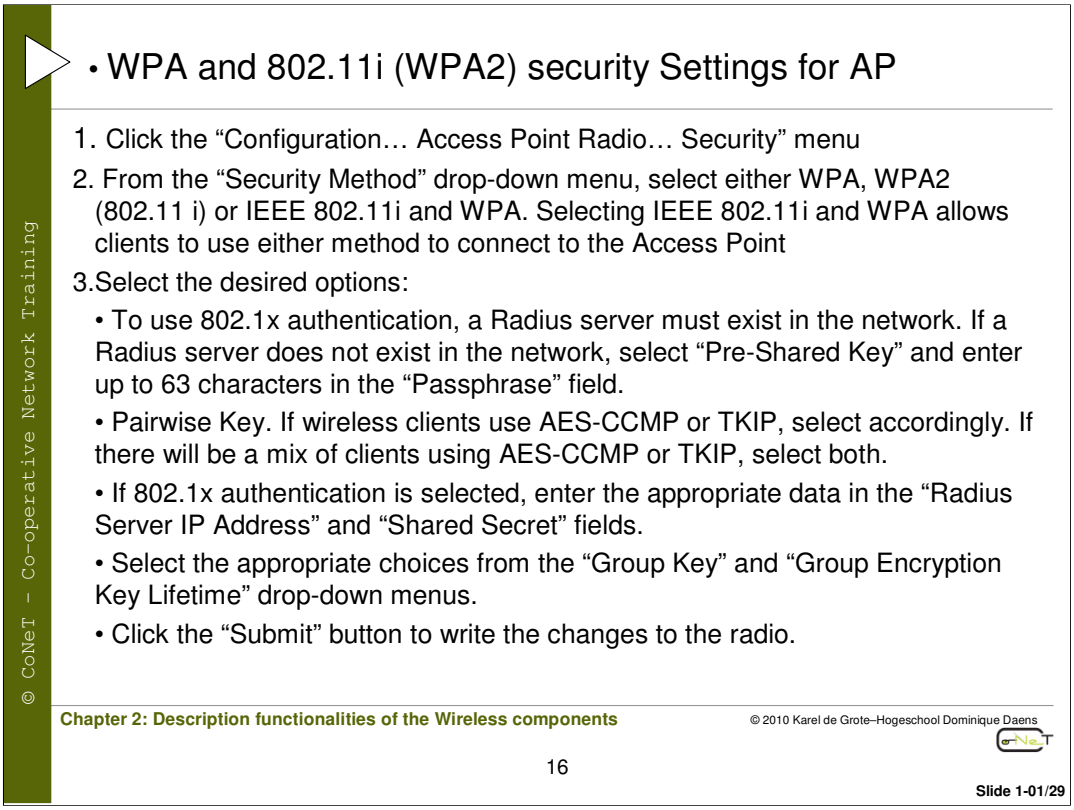
– The “Authentication Type” drop-down menu allows selection of “open”, “shared” or “open/shared” (clients may employ either). “Shared” provides slightly higher security; however, all clients must also have “Shared” selected as well.

– WEP Encryption Method selects one of three sizes of keys that can be used by WEP. Larger keys provide a higher level of security. Select the size of key and enter a key using only hexadecimal characters and no spaces (0-9 and A-F). Make a note of this key as it must be entered in all client radios. Click the “Key Generator” button to have the program automatically generate a key. Copy the key into other radios this unit must communicate with.

– WEP Keys 1-4 (64-bit encryption) selects one of four possible keys that can be used with 64-bit encryption. This serves the purpose of allowing periodic rotation of the WEP key by the operator. Simply select which key is desired. The same key must be selected in the access point and all client radios for successful operation. Only one key will be used at a time. Copy the key into other radios this unit must communicate with.

TEST of the WEP security





Security Mechanism

Wi-Fi Protected Access, or WPA, was designed to enable use of wireless legacy systems employing WEP while improving security.

WPA uses improved data encryption through the temporal key integrity protocol (TKIP) which mixes keys using a hashing algorithm, and adds an integrity-checking feature to ensure that the keys aren’t tampered with.

TKIP also incorporates re-keying, so the key is periodically changed to prevent old keys from being captured and used for unauthorized network access.

In addition, user authentication is enabled using the extensible authentication protocol (EAP).

Finally, a message integrity check (MIC) is used to prevent an attacker from capturing and altering or forging data packets. It can also employ a form of AES (Advanced Encryption Standard) called AES-CCMP.

TKIP: temporal key integrity protocol

Protocol which mixes keys using a hashing algorithm, and adds an integrity-checking feature to ensure that the keys aren’t tampered with. TKIP also incorporates re-keying, so the key is periodically changed to prevent old keys from being captured and used for unauthorized network access.

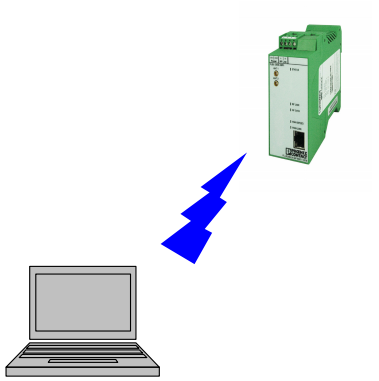
AES: Advanced Encryption Standard

AES is currently approved for military use, and utilizes a 128-bit block cipher algorithm and encryption technique for protecting computerized information.

AES-CCMP: AES-Counter Mode CBC-MAC Protocol

AES-Counter Mode CBC-MAC Protocol (AES-CCMP) is an encryption algorithm used in the 802.11i security protocol. It uses the AES block cipher, but restricts the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) and adapts them to Ethernet frames to provide a robust security protocol between the mobile client and the access point. AES itself is a very strong cipher, but counter mode makes it difficult for an eavesdropper to spot patterns, and the CBC-MAC message integrity method ensures that messages have not been tampered with.

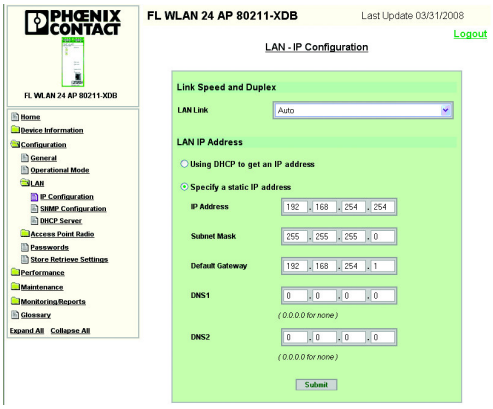
TEST of the WPA security



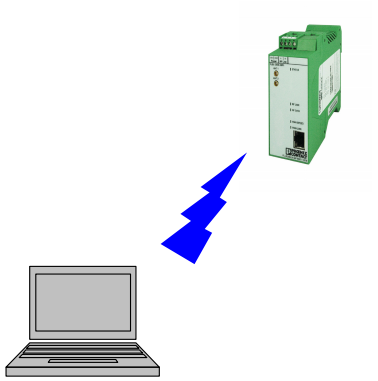
• The “Configuration...LAN...IP Configuration” menu

1. Click the “Configuration… LAN… IP Configuration” menu
- Select the speed of the LAN or select Auto from the “LAN Link” dropdown menu. If Auto is selected, the radio automatically determines network speed.
- If the network does not support DHCP (Dynamic Host Configuration Protocol), click the “Specify a static IP Address” radio button and enter the data in the “Subnet Mask” and “Default Gateway” fields.

2. Click the “Submit” button to activate the new LAN settings.



Test out your configuration !!!!



2.3 The Phoenix Contact FL WLAN EPA

2.3.1 Properties

- The Ethernet port adapter (FL WLAN EPA) is a high-performance, industrial WLAN interface for Ethernet or Profinet-compatible automation equipment (Higher priority for Profinet data)
- A transparent protocol is used for data transmission on Layer 2 level, which ensures easy integration in Industrial Ethernet networks such as Profinet, Modbus/TCP or Ethernet/IP.
- The FL WLAN EPA meets the Profinet requirements of conformance class A and the Profisafe profile for failsafe communication.
- compatibility with WLAN standard IEEE 802.11 b/g
- High level of security with WEP, WPA, and IEEE 802.11i encryption mechanisms
- Easy configuration with standard web browsers via Ethernet, SNMP or AT commands. The "Phoenix SPA EPA Toolbox" software package can be downloaded free of charge at www.phoenixcontact.com

The Ethernet port adapter (FL WLAN EPA) is a high-performance, industrial WLAN interface for Ethernet or Profinet-compatible automation equipment. A WLAN access point or another FL WLAN EPA can be used as the access point to the Ethernet control network. A transparent protocol is used for data transmission on Layer 2 level, which ensures easy integration in Industrial Ethernet networks such as Profinet, Modbus/TCP or Ethernet/IP.

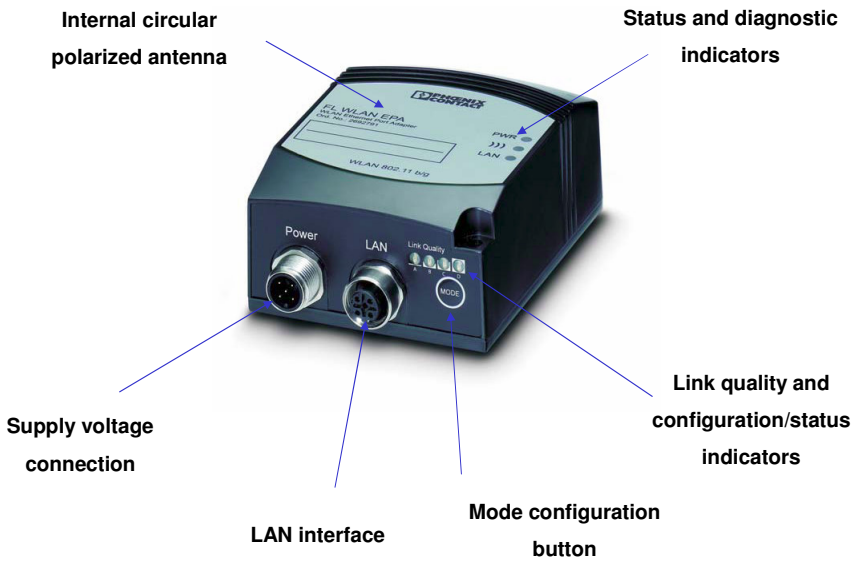
The FL WLAN EPA meets the Profinet requirements of conformance class A and the Profisafe profile for failsafe communication.

The FL WLAN EPA has certified compatibility with WLAN standard IEEE 802.11 b/g. This means it can connect any WLAN module to the Ethernet network, provided the module also supports standard IEEE 802.11 b/g.

Industrial devices with WLAN interface include, for example, (industrial) PCs or notebooks, PDAs (personal digital assistants), industrial

barcode scanners, RFID readers, and weighing systems.

2.3.2 FL WLAN EPA interface



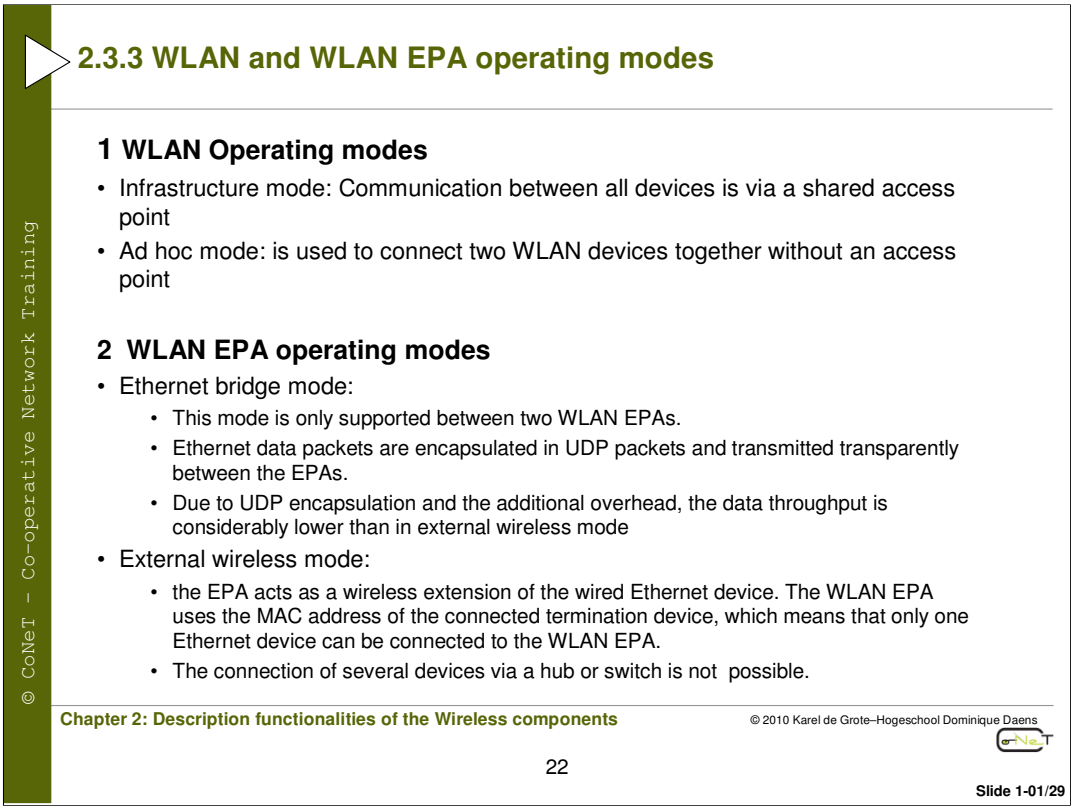
– Antenna

The device is supplied with an **internal** circular polarized 5 dB panel antenna. The internal antenna cannot be replaced.

– The supply voltage is connected via the 5-pos. M12 female connector (connector on the device).

– Network connection: Copper interface in M12 format (female connector on the device) with 10/100 Mbps with auto negotiation.

– Status and diagnostic indicator: The LEDs indicate the status of the Ethernet and WLAN interfaces or act as configuration indicators.



Infrastructure mode

Infrastructure mode is the simplest form of a wireless network. Communication between all devices is via a shared access point. In this mode, all available transmission bandwidths up to 54 Mbps can be used. The user can set the authentication and encryption methods.

Ad hoc mode

This mode is used to connect two WLAN devices together without an access point. Ad hoc mode only offers the transmission bandwidth according to 802.11 b (11 Mbps) and encryption according to the WEP standard.

Ethernet bridge mode

This mode is only supported between two WLAN EPAs. In this mode, Ethernet data packets are encapsulated in UDP packets and transmitted transparently between the EPAs. For the termination devices at both ends of the WLAN connection, the wireless transmission is "invisible". Due to UDP encapsulation and the additional overhead, the data throughput is considerably lower in this operating mode than in external wireless mode.

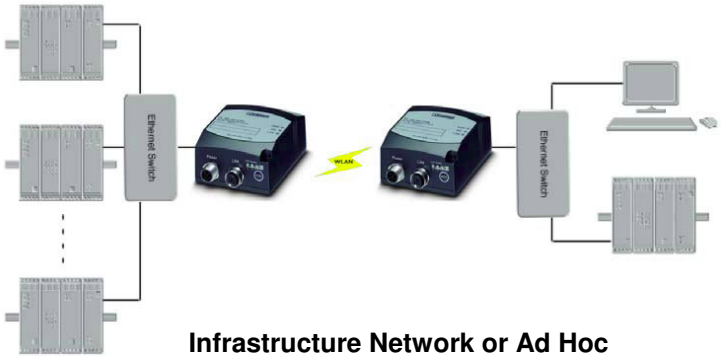
External wireless mode

In this mode, the EPA acts as a wireless extension of the wired Ethernet device. The WLAN EPA uses the MAC address of the connected termination device, which means that only one Ethernet device can be connected to the WLAN EPA. The connection of several devices via a hub or switch is not possible.

2.3. 4 Examples of FL WLAN EPA Configurations

Example 1: Two WLAN EPAs form an Ethernet bridge (option 1)

- several devices are connected to both EPAs
- The data from the connected devices is transmitted via the UDP tunnel.
- This mode can be used both in ad hoc mode and in infrastructure mode.



Infrastructure Network or Ad Hoc

The configuration can be set using the SMART button.

Sequence in ad hoc mode

1. Switch on the first device and set it to Smart mode. Then select configuration mode 4 "Wait for auto configuration" (LED C).

2. Switch on the second device and set it to Smart mode. Then select configuration mode 5 "Initiate auto configuration via WLAN, EPA to EPA bridge" (LED A+C).

3. Wait until the devices have connected to one another and then restart the devices.

4. The first device can now be accessed under IP address 10.0.0.99 and the second device under IP address 10.0.0.100. Both devices are now operating in ad hoc mode.

Sequence in managed (infrastructure) mode

To use automatic configuration in managed mode, either use default values or adapt the settings for SSID and security (encryption, authentication, user name, and key) manually. The settings can be adapted via WBM or AT commands.

1. Switch on the first device and set it to Smart mode. Then select configuration mode 8 "Wait for automatic configuration by another WLAN EPA in infrastructure mode“ (LED D).

2. Switch on the second device and set it to Smart mode. Then select configuration mode 9 "Initiate connection to another EPA in infrastructure mode" (LED A+D).

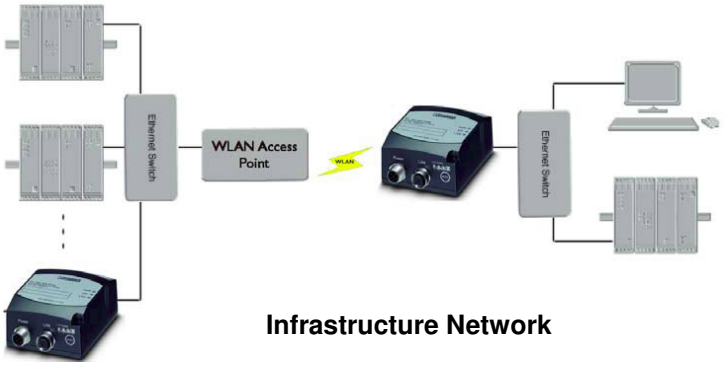
3. Wait until the devices have connected to one another and then restart the devices.

4. The first device can now be accessed under IP address 10.0.0.99 and the second device under IP address 10.0.0.100. Both devices are now operating in managed mode

2.3.4 Examples of FL WLAN EPA Configurations

Example 2: Two WLAN EPAs form an Ethernet bridge (option 2)

- Two EPAs in "Ethernet bridge" mode. One of the EPAs is connected to a wired network and not via the wireless interface.
- In this case, only infrastructure mode can be used.



Infrastructure Network

2.3.4 Examples of FL WLAN EPA Configurations

Example 3: Two WLAN EPAs in external wireless mode (option 1)

- This example shows two EPAs in "External wireless" mode. One Ethernet device is connected to each EPA.
- This operating mode has a considerably higher data throughput than "Ethernet bridge" because there is no UDP data encapsulation.

Ad Hoc Network

The configuration can be set using the SMART button and uses ad hoc mode.

Sequence in ad hoc mode

1. Switch on the first device and set it to Smart mode. Then select configuration mode 4 "Wait for auto configuration" (LED C).

2. Switch on the second device and set it to Smart mode. Then select configuration mode 5 "Initiate auto configuration via WLAN, EPA to EPA bridge" (LED A+C).

3. Wait until the devices have connected to one another and then restart the devices.

4. Set both devices to Smart mode 11 "Configure external wireless as a wireless extension" (LED A+B+D), so that each of the EPAs learns the MAC address of the relevant connected device.

For this operating mode, the Ethernet device must transmit Ethernet frames spontaneously. If the Ethernet device is unable to do so, the MAC address of the Ethernet device can be entered manually in WBM for the EPA.

2.3.4 Examples of FL WLAN EPA Configurations

Example 4: Two WLAN EPAs in external wireless mode (option 2)

- One Ethernet device is connected to each EPA. The EPAs are connected together via a WLAN access point.
- This operating mode has a considerably higher data throughput than "Ethernet bridge" because there is no UDP data encapsulation

Infrastructure Network

Sequence in managed (infrastructure) mode

Both EPAs must be in "External wireless" mode.

1. Connect a PC to one EPA.
2. Specify the WLAN connection parameters. The following parameters are required:

- Operational Mode: Managed
- WLAN Channel: Select the channel on which the WLAN access point transmits
- WLAN Data Rate: This is the maximum possible data rate
- Link Adaptation: Yes/No
- Encryption: Select the encryption method required for the access point
- Authentication: Select the authentication method required for the access point
- User Name and Key: Select the settings required for the access point
- SSID: SSID of the WLAN network
- WLAN Address: The MAC address of the device connected to the EPA or set the address using the SMART button
- UDP Receiver: Off

3. Instead of entering the MAC address of the connected device manually, you can also use Smart mode 11.

2.3.4 Examples of FL WLAN EPA Configurations

Example 5: WLAN connection between PC and EPA (option 1)

- In this example, the EPA must be in "External wireless" mode.

Ad Hoc Network

Sequence in ad hoc mode

The EPA must be in "External wireless" mode.

1. Connect a PC to one EPA.
2. Specify the WLAN connection parameters. The following parameters are required:

- Operational Mode: Ad Hoc
- WLAN Channel: Select the channel on which the WLAN access point transmits
- WLAN Data Rate: The maximum possible data rate is 11Mbps. If a higher value is selected, 11 Mbps is used.
- Link Adaptation: No This is not supported in ad hoc mode
- Encryption: WEP Only WEP is supported in ad hoc mode.
- Authentication: Open
- Key: Select a WEP key
- SSID: SSID of the WLAN network
- WLAN Address: The MAC address of the device connected to the EPA or set the address using the SMART button
- UDP Receiver: Off

3. Instead of entering the MAC address of the connected device manually, you can also use Smart mode 11.
4. Please note that the corresponding settings must also be made on the PC.

2.3.4 Examples of FL WLAN EPA Configurations

Example 6: WLAN connection between PC and EPA (option 2)

- an Ethernet device is connected to the EPA. The PC uses Ethernet protocols to access the Ethernet device (e.g., http for WBM or Modbus/TCP).
- Since both the PC and the EPA are connected to one access point, it is possible to use managed (infrastructure) mode.

Infrastructure Network

Sequence in managed (infrastructure) mode

The EPA must be in "External wireless" mode.

1. Connect a PC to the EPA.
2. Specify the WLAN connection parameters. The following parameters are required:

- Operational Mode: Managed
- WLAN Channel: Select the channel on which the WLAN access point transmits
- WLAN Data Rate: This is the maximum possible data rate
- Link Adaptation: Yes/No
- Encryption: Select the encryption method required for the access point
- Authentication: Select the authentication method required for the access point
- User Name and Key: Select the settings required for the access point
- SSID: SSID of the WLAN network
- WLAN Address: The MAC address of the device connected to the EPA or set the address using the SMART button
- UDP Receiver: Off

3. Instead of entering the MAC address of the connected device manually, you can also use Smart mode 11.
4. Please note that the corresponding settings must also be made on the PC.

2.3.4 Examples of FL WLAN EPA Configurations

Example 7: Several Ethernet devices connected in external wireless mode (option 1))

- three or even more Ethernet devices are connected via EPAs in ad hoc mode.

Ad Hoc Network

Sequence in ad hoc mode

The EPA must be in "External wireless" mode.

1. Connect a PC to each EPA.
2. Specify the WLAN connection parameters. The following parameters are required:

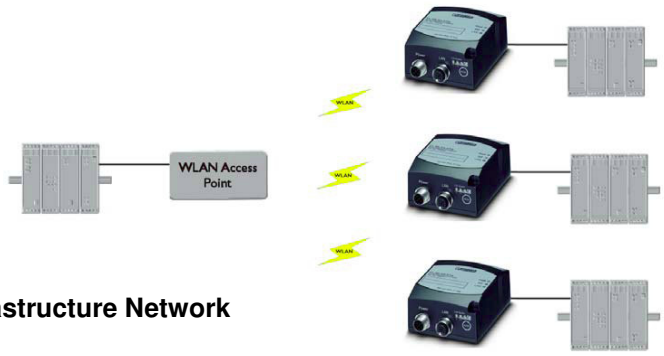
- Operational Mode: Ad Hoc
- WLAN Channel: Select the channel. This channel must be set on all EPAs.
- WLAN Data Rate: The maximum possible data rate is 11Mbps. If a higher value is selected, 11 Mbps is used.
- Link Adaptation: No This is not supported in ad hoc mode
- Encryption: WEP Only WEP is supported in ad hoc mode.
- Authentication: Open
- Key: Select a WEP key
- SSID: SSID of the WLAN network identical for all EPAs
- WLAN Address: The MAC address of the device connected to the EPA or set the address using the SMART button
- UDP Receiver: Off

3. Instead of entering the MAC address of the connected device manually, you can also use Smart mode 11.

2.3.4 Examples of FL WLAN EPA Configurations

Example 8: Several Ethernet devices connected in external wireless mode (option 2)

- three or even more Ethernet devices are connected via EPAs in managed mode via a WLAN access point



Infrastructure Network

Sequence in managed (infrastructure) mode

The EPA must be in "External wireless" mode.

1. Connect a PC to each EPA.
2. Specify the WLAN connection parameters. The following parameters are required:

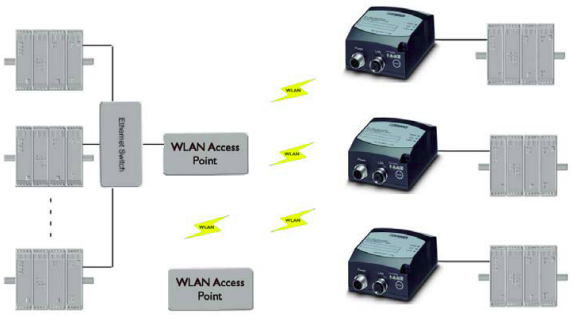
- Operational Mode: Managed
- WLAN Channel: Select the channel on which the WLAN access point transmits
- WLAN Data Rate: This is the maximum possible data rate
- Link Adaptation: Yes/No
- Encryption: Select the encryption method required for the access point
- Authentication: Select the authentication method required for the access point
- User Name and Key: Select the settings required for the access point
- SSID: SSID of the WLAN network
- WLAN Address: The MAC address of the device connected to the EPA or set the address using the SMART button
- UDP Receiver: Off

3. Instead of entering the MAC address of the connected device manually, you can also use Smart mode 11.

2.3.4 Examples of FL WLAN EPA Configurations

Example 9: Several EPAs connected via WLAN to a wired infrastructure

- three or even more EPAs are connected via WLAN access points to the Ethernet infrastructure.
- Other WLAN clients can operate at the WLAN access point at the same time.



Infrastructure Network

Sequence in managed (infrastructure) mode

The EPA must be in "External wireless" mode.

1. Connect a PC to each EPA.
2. Specify the WLAN connection parameters. The following parameters are required:

- Operational Mode: Managed
- WLAN Channel: Select the channel on which the WLAN access point transmits
- WLAN Data Rate: This is the maximum possible data rate
- Link Adaptation: Yes/No
- Encryption: Select the encryption method required for the access point
- Authentication: Select the authentication method required for the access point
- User Name and Key: Select the settings required for the access point
- SSID: SSID of the WLAN network
- WLAN Address: The MAC address of the device connected to the EPA or set the address using the SMART button
- UDP Receiver: Off

3. Instead of entering the MAC address of the connected device manually, you can also use Smart mode 11.

2.3.4 Examples of FL WLAN EPA Configurations

Example 10: External WLAN client connected to EPA

- a WLAN client is connected to an EPA.

Ad Hoc Network

Sequence in ad hoc mode

The EPA must be in "External wireless" mode.

1. Connect a PC to the EPA.
2. Specify the WLAN connection parameters. The following parameters are required:

- Operational Mode: Ad Hoc
- WLAN Channel: Select the same that the external WLAN device uses.
- WLAN Data Rate: The maximum possible data rate is 11Mbps. If a higher value is selected, 11 Mbps is used.
- Link Adaptation: No This is not supported in ad hoc mode
- Encryption: WEP Only WEP is supported in ad hoc mode.
- Authentication: Open
- Key: Select a WEP key as the external WLAN device
- SSID: Select the same SSID as the external WLAN device
- WLAN Address: The MAC address of the device connected to the EPA or set the address using the SMART button
- UDP Receiver: Off

3. Instead of entering the MAC address of the connected device manually, you can also use Smart mode 11.

2.4 Startup and Configuration of the FL WLAN EPA

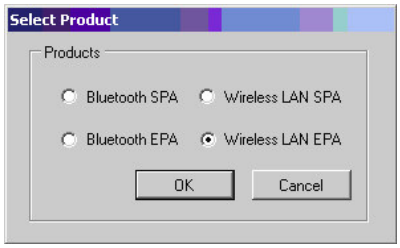
- Configuration using the “Mode” Button
- Web-Based management (WBM)
- Configuration using the Phoenix SPA/EPA Configuration Tool "Toolbox" software

Phoenix SPA EPA Toolbox.exe

2.4.1 Configuration of the FL WLAN EPA FL by SPA/EPA Toolbox

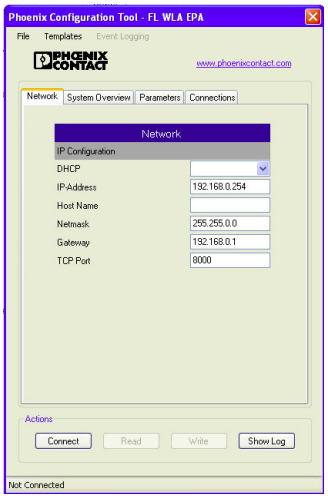
- Start the "Toolbox" software by double-clicking on the program icon

- Select the device: FL WLAN EPA = Wireless LAN EPA



2.4.1 Configuration of the FL WLAN EPA FL by SPA/EPA Toolbox

- Confirm the device selection with "OK". The following window opens:



IP# 192.168.0.254 (default)

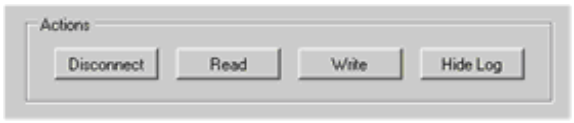
SM# 255.255.0.0

TCPport: 8000

- Click "Connect" to establish a connection to the module

2.4.1 Configuration of the FL WLAN EPA FL by SPA/EPA Toolbox

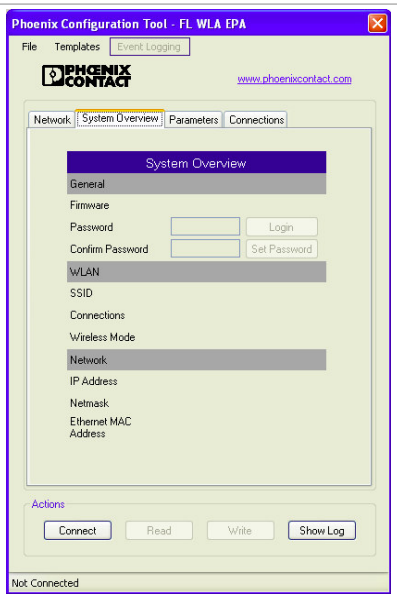
- After connection is established, the "Connect" button changes to "Disconnect" and "Read" and "Write" are activated.



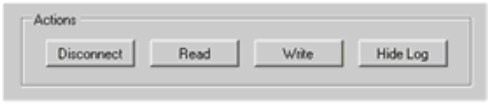
  - Read = Read the device configuration
    - The password for this must be entered in the "System Overview" tab. In order to read the configuration, the password for device access must first be entered.
    - Switch to the "System Overview" tab. Enter the password under "Password" and confirm with "Login".

Pasword (default): admin

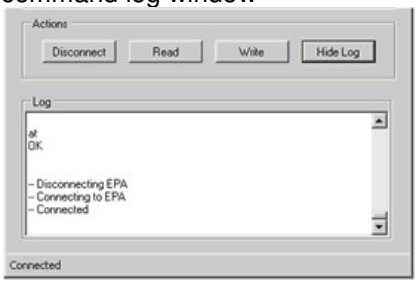
„System Overview“ tab



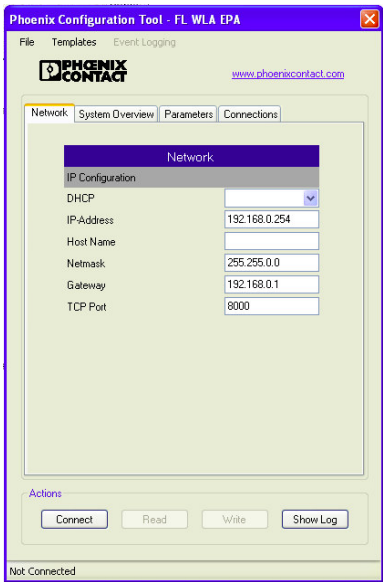
- Write = "Write" to transmit all modifications to the device.



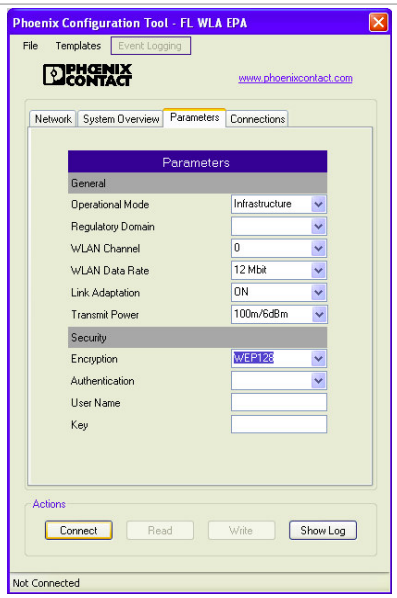
- Show/Hide Log: to show or hide the command log window



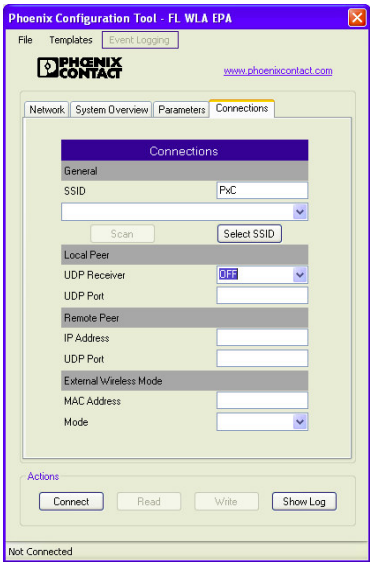
„Network“ tab



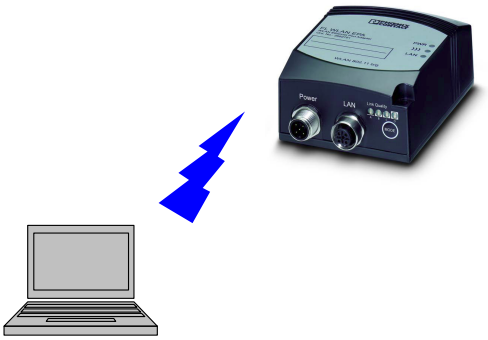
• „Parameters“ tab



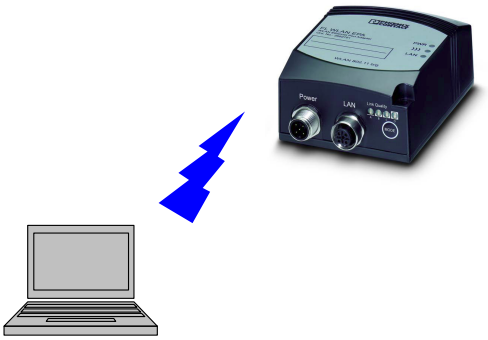
• „Connections“ tab



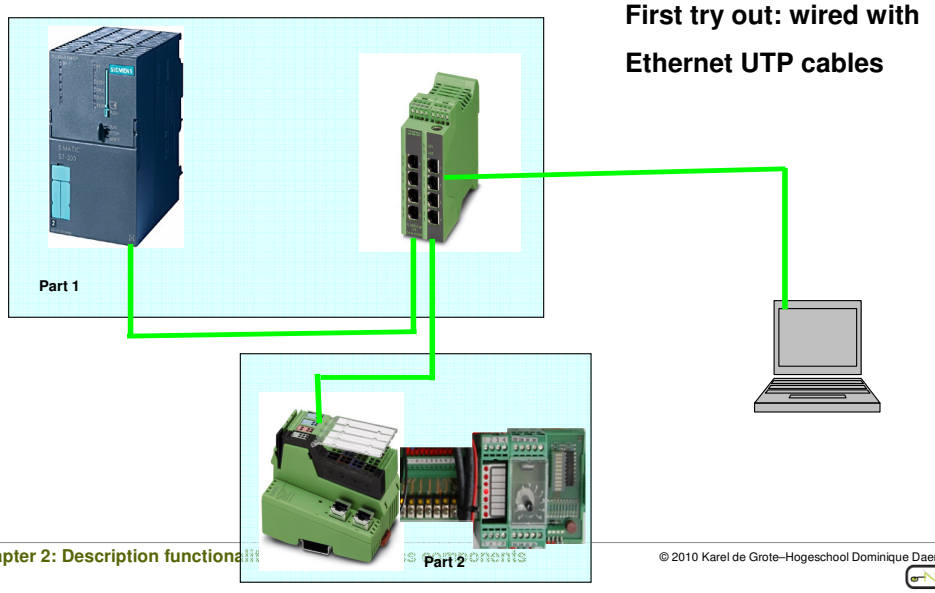
Exercise 2: Wireless communication between a PC with WLAN interface and the FL WLAN EPA (cf. configuration example 5)



Exercise 3: WLAN between PC, Access Point XDB and FL WLAN EPA (cf. configuration example 6)

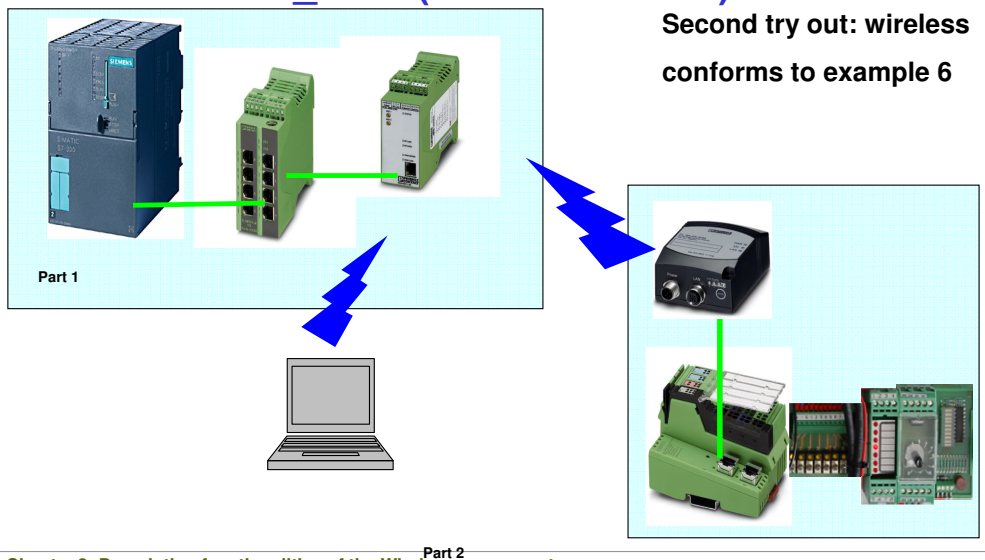


Exercise 4: Configuration of PROFINET Siemens S7 315-2DP/PN and IL PN BK 2TX_PAC (see also CML2)



See also CML2

Exercise 5: Configuration of PROFINET Siemens S7 315-2DP/PN and IL PN BK 2TX_PAC (see also CML2)



See also CML2

3. Real-time aspects of WLAN

Exercise 6: Research the maximum update rate of a PROFINET device

Exercise 7: Influence of 'other' TCP/IP traffic

4. Bluetooth (IEEE802.15.1)

- Bluetooth is a wireless technology used widely in the consumer sector.
- Currently, more effectively than Bluetooth wireless chipsets sold, [this doesn't make sense]
- mainly attributable to the application of this technology in mobile phones, headsets, etc.
- The basic technology is standardized in IEEE 802.15.1.
- Above the standard in places the Bluetooth SIG (Special Interest Group), an association of producers (Bluetooth chipsets and products), various application [this isn't quite right]
- profiles, eg for voice transmission, serial communications or wireless Ethernet connection in the so-called Personal Area Networks (PAN).

References for part 2

Phoenix Contact.: Quick Start Guide UM QS EN FL WLAN AP XDB Radios, order No: 2751762

Phoenix Contact.: User Manual UM EN...XDB, order No: 2751760

Phoenix Contact.: User Manual UM EN FL WLAN EPA, order No: 7901_en_01 06/2010