Weidmüller

Industrial Ethernet Training 32

Accessing local area network wirelessly with WiFi Access Point

Abstract:
Accessing a Local Area Network (LAN) wirelessly is facilitated by a WiFi Access Point. This enables seamless and flexible connectivity for devices, such as sensors, controllers, or HMIs, allowing them to be part of the network without the need for physical cables. This wireless access enhances mobility and simplifies the deployment of devices within the industrial setting in the factory.

Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	IE-Training Kit-01	2874670000	1.1.2 (Build 125086)
2	Wireless Access Point/Client	2536600000	1.16.18 (Build 18081617)
3			

IE-Training Kit Content

No.	Component name	Article No.	Hardware / Firmware version
1	IE-SR-4TX	2751270000	1.4.7
2	IE-SW-AL08M-8TX	2682280000	1.08
3	IE-SW-AL05M-5TX	2682250000	1.14
4	IE-CS-MBGW-2TX-1COM	2682600000	3.11

Software reference

No.	Software name	Article No.	Software version
1			
2			
3			

File reference

No.	Name	Description	Version
1			
2			

Contact
Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
www.weidmueller.com

For any further support please contact your local sales representative:
https://www.weidmueller.com/countries

Content

1 Warning and Disclaimer

Warning
Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer
This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

Note
The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

Security notes
In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

2 Prerequisites

You need to have the following hardware and documentation

- Via Ethernet connected Industrial Ethernet Training Kit
- Via Ethernet to the Industrial Ethernet Training Kit connected PLC
- Application Note Industrial Ethernet Training 01 "*Setting up default configuration of IE Training Kit*" for applying default IP address configuration
- Application Note Industrial Ethernet Training 24 "Setting up a Weidmueller WiFi access point"
-

Note: *The mentioned Prerequisites are only mandatory for performing the exact use case we are exemplifying in this Application Note. These are optional, if you only want to understand the functionality of the following Application and implement it by yourself.*

Note: *Additional information and tutorial videos to this Application Note can be found in the Weidmueller support center (*Weidmüller - Support Center (weidmueller.com)). These videos can also be found by searching for "*Industrial Ethernet tutorials"* in the support center.

3 Configuring the Access Point

The Weidmueller access point is, besides being a signal repeater and converter for a wired signal, also capable of running in client mode. This means that the Access Point can connect wirelessly to another network and then transmit the signal via an Ethernet cable to your router. By this means, we are still able to manage all our local devices with our router and our local devices can connect to the other network via the router without being in the other network. For example, your machine which is connected locally to your router via Ethernet cable is now able to communicate with a machine in another network via the router's connection to the access point and the access point connecting to the external network.

1. To switch the access point into client mode, we have to access the web interface. We can connect to the web interface via an Ethernet cable running between our device and the access point and using our IP *"192.168.1.60"* to get a connection.

2. First, we must change the operation mode. This can be done in the menu tree by selecting *"Wireless LAN Setup"* and then choose *"Operation Mode"*. Now, we want to change the operation mode in the drop-down menu from *"AP"* to *"Client"* as shown below. After changing our operation mode, we need to *save and restart* the device.

Figure 1: Operation Mode

3. After successfully restarting our device and logging back in, we are now in client mode. The access point is now acting as a WiFi client device, i.e., it does not host an own WiFi network other devices can connect to. Instead, it is now able to connect to another network wirelessly as a WiFi client. To do that, we must navigate the menu tree to *"Wireless LAN Setup"* then select *"WLAN"* and lastly choose *"Basic WLAN Setup"*. In this menu, we can now manually enter the WiFi's name (SSID) we want to connect to or use the button *"Site Survey"* to find the WiFi signal we are searching in our area. After submitting the changes, *do not* restart the device yet.

Figure 2: Basic WLAN Setup

4. To finally connect the access point to the WiFi, we must type in the WiFi's password for a successful connection. We can do this in the same menu path but instead of clicking on *"Basic WLAN Setup"*, we select *"WLAN Security Settings".* Type your password in the passphrase field and adapt the *security mode* settings if needed. Now, we can *submit* our changes and *save and restart* our router.

Figure 3: WLAN Security Settings

5. We are now successfully connected to the external network with our Access Point. Our last step is to configure our IP Settings. Since our access point is connected to the other network, it needs to activate the automatic IP configuration DHCP (Dynamic Host Resolution Protocol). With DHCP, the access point automatically gets a known IP address from the external network to communicate with it and it also applies a standard gateway and DNS-server (Domain name system) for our access point. We can apply these settings by navigating to *"General Setup"* and then *"Network Settings"*. Once in the menu, we select DHCP in the drop-down menu for *"IP address assignment"* and submit our settings. Do not forget to restart your access point to save the settings.

   We have now successfully configured the access point into client mode and established a connection to an external network.

Figure 4: configuring DHCP setting

4 Configuring the router

To get a working connection to an external network, we need our router to be configured correctly. To use our local devices, which are connected to the router in the external network, we must use our router's WAN port.

1. First, connect the LAN port of the access point with your router's WAN port via an Ethernet cable. Keep in mind to have your computer connected to the router via LAN in order to access the router's web interface.

2. We can access our router's web interface as usual with the following IP: *"192.168.1.10"* and the user credentials.

3. After logging into the interface, we can go to the WAN settings of the router. Since our router is connected to the access point via WAN, we must adapt our *WAN network settings* in the router's web interface. This means, that we must use *DHCP* for our WAN port again so our router can communicate with the external network by having its network settings automatically applied.
   We first want to navigate in the menu to *"Configuration"* and then select *"IP configuration"*. Next, find the WAN settings and select DHCP in the drop-down menu *"IP assignment".* Furthermore, check the *"DNS via DHCP"* and *"Gateway via DHCP"* checkboxes. Lastly, it is important to also check the *NAT Masquerading* option. *NAT masquerading* changes the sender's IP address. This means, that our router sends our internet traffic in the name of the router's IP even though it comes from our computer. This is important for the external network to know whom to send your internet traffic in form of packets back as our computer is not part of the external network, but our router is. Thus, our router gets the packets back and can redirect them to our computer. Lastly, we *apply* the settings and *save* them.

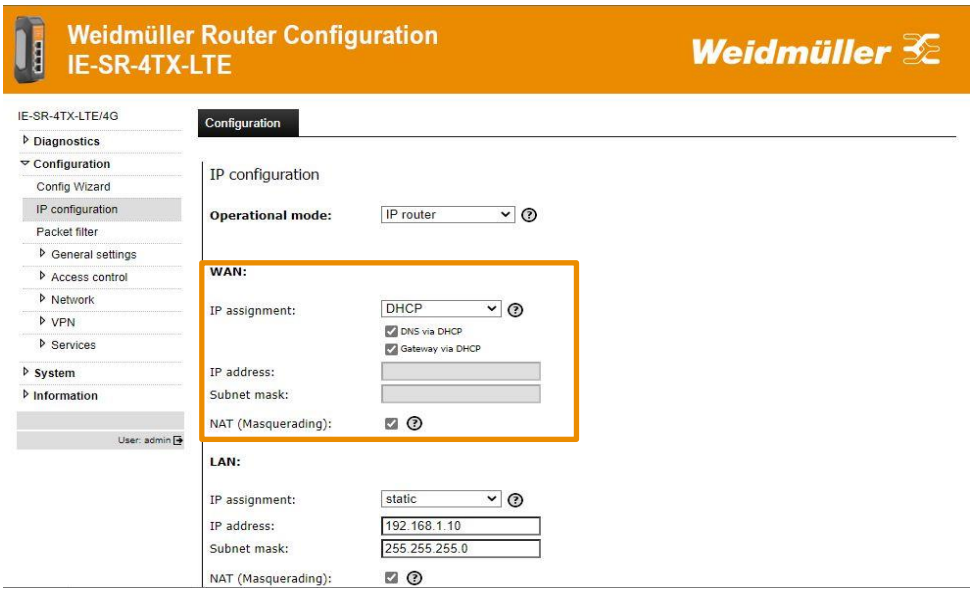

Figure 5: WAN DHCP settings

5 Configuring the computer

We have now successfully configured our access point and our router to work properly with the external network. Now, any device connected to it only needs a few more steps to configure to work properly with our own network. In our example, we are going to set up our computer to work with the network.

1. First, we must go into our ethernet properties and then go to our IPv4 settings. If you do not know where to find the ethernet properties and the IPv4 settings, please refer to *Application Note Industrial Ethernet Training 01 "Setting up default configuration of IE Training Kit" for applying default IP address configuration*

2. Once we are in properties dialogue, we must change the following two settings: standard gateway and DNS (Domain Name System) server.
   Currently, our computer is in the network *192.168.1.15* meaning that an IP address out of this range (e.g., "10.10.10.10") cannot be found and the packets get lost. A standard gateway can help us to redirect such undeliverable packets to our router, that then can redirect the packets via WAN to the access point and then to the external network we are trying to get to. Hence, we must set our *standard gateway* to our router's IP, which is *"192.168.1.10"*. Type it into the standard gateway field as shown:

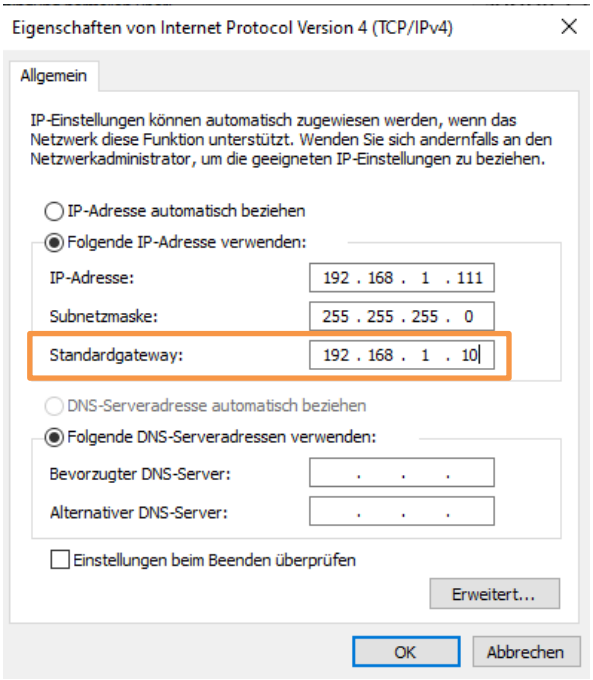

Figure 6: Standard gateway computer

3. We can now redirect unknown IP addresses to our router who can then redirect them to the external network to find the IP addresses we are searching. But as of now, a Domain Name System (DNS) like https://weidmueller.com cannot be found, as it is not an IP address. For that, we want to implement a DNS server that can resolve the DNS into a valid IP. If our external network we are connecting to has access to the internet, we can use the external network's router as a DNS server because the router will redirect it to its own DNS server. But we can also use a publicly available DNS server such as Cloudflare's 1.1.1.1 or Google's 8.8.8.8 server. We used the external network's router IP as a primary DNS server and Cloudflare's as the secondary DNS server.

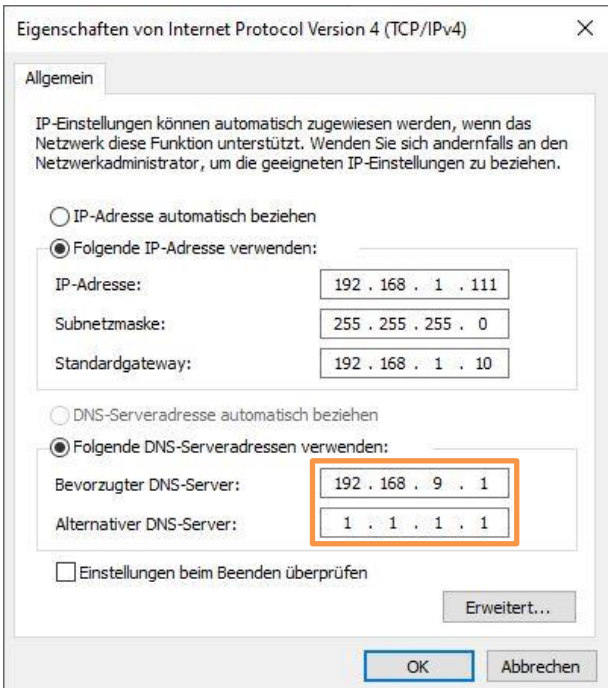

Figure 7: DNS computer settings

6 Results

We are now able to connect our own network with the help of the access point to an external network. Furthermore, we understand how to use the access point’s client mode and we understand how to properly set up our router and computer to work with our two connected networks. In fact, we can now connect many devices to our local router and we only need to configure our router for the external network instead of having to configure every device from our local network. This can be helpful for managing a lot of devices in our production hall when there is only one router available with internet connectivity.