

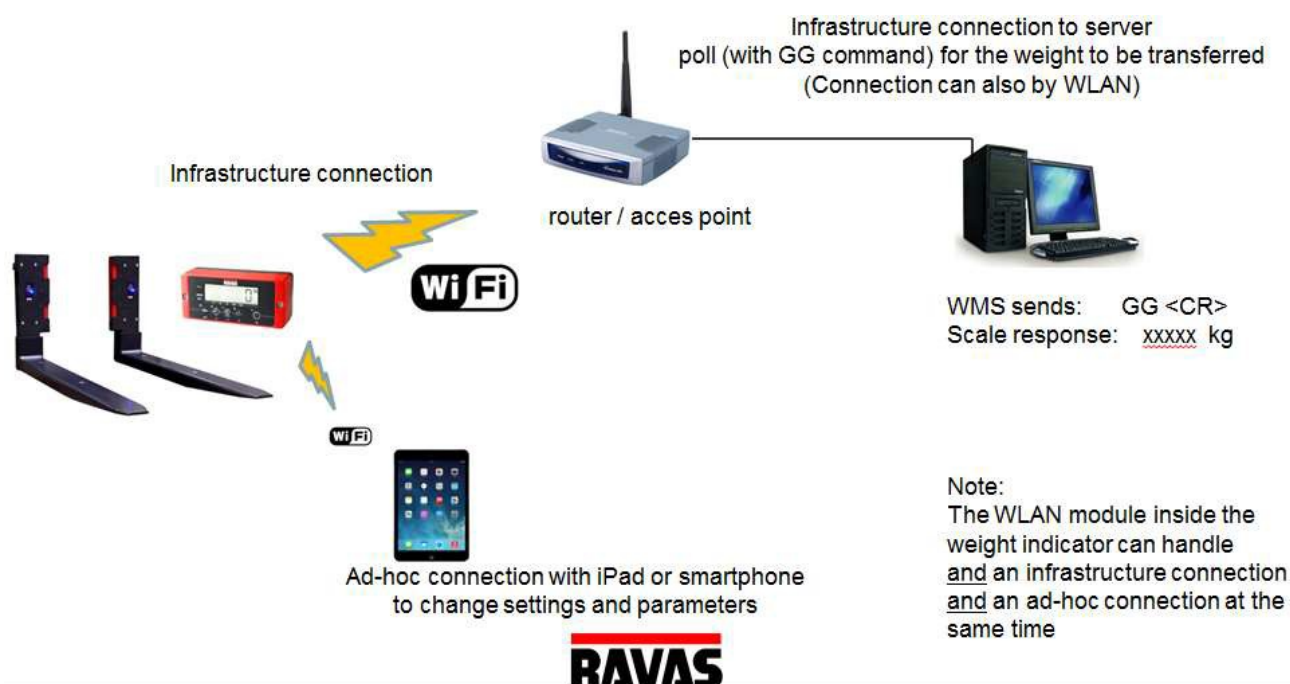
Manual

XPICO240 WLAN module inside RAVAS indicators

RAVAS indicators can be equipped (option) with a WLAN module – this to respond to IT systems which poll for weight information. The RAVAS indicator will get a dedicated IP address.

Customer has to provide a full WLAN coverage in the warehouse using Access Points

The operator gives a command to the main application on the server to poll for the weight at a certain RAVAS weight indicator (using GG command) - The weight indicator responds by sending the actual display value.



Configuring the WLAN connection with the Xpico using a laptop

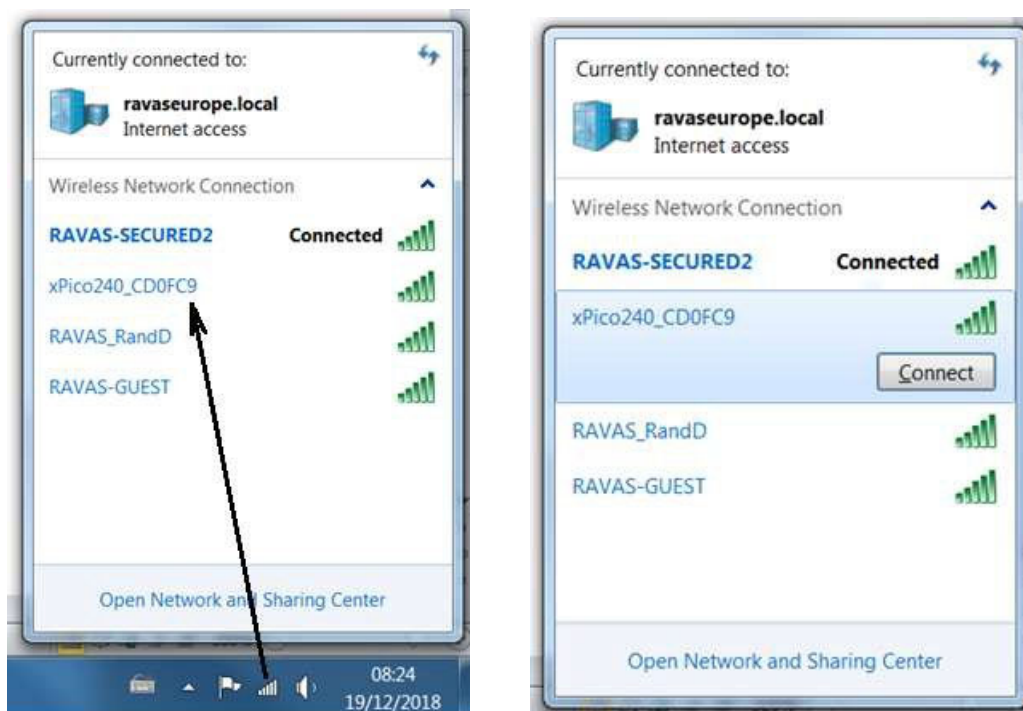
Important note:

You will see the name of the Xpico SSID in your list of WLAN signals
There are two models of Xpico

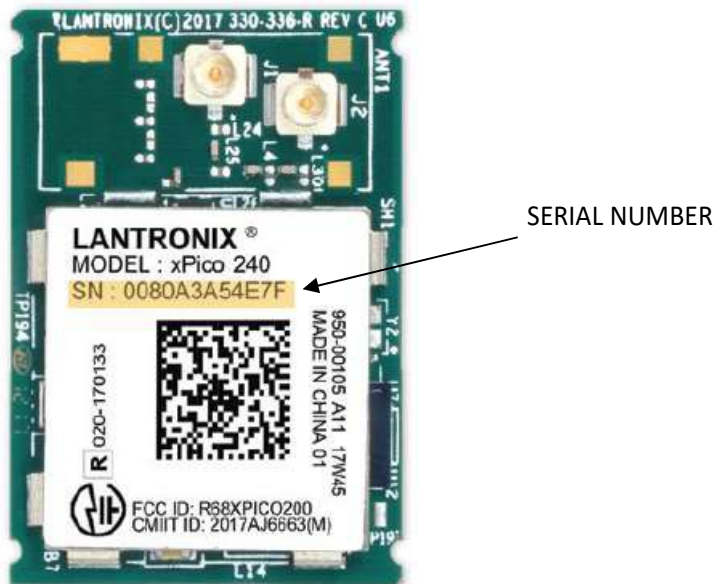
- XpicoWiFi_xxxxxxx
- Xpico240_xxxxxxx

Please make sure you also use the correct manual !!

Step 1: select the WLAN connection manager.



Step 2: connect to the xPico240_CD0FC9 (last six digits depend on the address of the Xpico installed). By default the SoftAP mode is enabled with a default SSID of xPico240_xxxxxx. Where xxxxxx are the last six characters of the unique xPico 240 serial number. This number is available on the module label. For example if the serial number on label were 0080A54E7F then the SSID would be Xpico240_A54E7F.



Step3: Using the Wi-Fi Connection Manager of your connecting device the above SSID should be presented as an available connection choice. Select the SSID and follow the device connection manager instructions to continue to connect.

The default security for xPico 240 SoftAP is WPA2 and the passphrase is **PASSWORD**. These defaults can be changed through the configuration web manager after the initial connection has been established.

When prompted enter the passphrase to complete the Wi-Fi connection authentication process. With a Wi-Fi client set to the above parameters, your device can connect directly to the xPico 240 Soft AP. In the WLAN manager you will see the connection being established.



Step 4: Open a standard browser (E.g. Internet Explorer®, Firefox®, Chrome™, Safari® etc.) and in the address field of the browser enter the following URL; xPico200.lantronix.com or alternatively use 192.168.0.1 as the IP Address.

When prompted enter the username of **admin** and password **PASSWORD** to access the Configuration and Management Web pages as shown below.

QuickConnect

Status

AES Credentials

Bridge

CLI Server

Clock

CPM

Device

Diagnostics

Discovery

File System

HTTP Server

Line

MACH10

Modem Emulation

Monitor

Network

NTP

Power

Radio

SPI

TLS Credentials

Tunnel

User

WLAN Profiles

Product Information

Product Type: xPico240

Firmware Version: 2.0.0.4R11

Serial Number: 0080A3CD0FC9

Uptime: 17 minutes 14 seconds

Permanent Config: Saved

Network Settings

Interface ap0

MAC Address: 02:80:A3:CD:0F:CA

State: Up

SSID: xPico240_CD0FC9

Security Suite: WPA2

IP Address: 192.168.0.1/24

Interface eth0

MAC Address: 00:80:A3:CD:0F:C9

State: Down

Interface wlan0

MAC Address: 00:80:A3:CD:0F:CA

Connection State: Disconnected

Line Settings

Line 1: RS232, 9600, None, 8, 1, None
Protocol: Tunnel

Line Virtual_1: Protocol: None

Line Virtual_2: Protocol: None

MACH10

State: Registering

Tunneling

Accept Mode

Connect Mode

Tunnel 1: Waiting

Tunnel Virtual_1: Inhibited

Tunnel Virtual_2: Inhibited

Logout

Copyright © Lantronix, Inc. 2007-2018. All rights reserved.

By clicking Network > Network 1 > Link to get to the Configuration page, the SSID, Security Suite Type and Security and passphrase can be modified. Modification to any of these parameters requires a reset/power cycle of the module in order to take effect.



xPico 240 LANTRONIX

QuickConnect

Status [ap0](#) [eth0](#) [wlan0](#)

Interface [Link](#)

Status [Configuration](#)

Access Point ap0 Configuration

SSID:

Guest: ☒ Enabled ☐ Disabled

Channel:

Auto Channel Scan Interval:

Suite:

Encryption: ☒ CCMP ☐ TKIP

Passphrase:

Mode:

DNS Redirect:

[Logout](#)

These settings pertain to the Access Point in the device. Changes take effect immediately. After saving the changes, re-establish any connections to the Access Point.

Copyright © Lantronix, Inc. 2007-2018. All rights reserved.

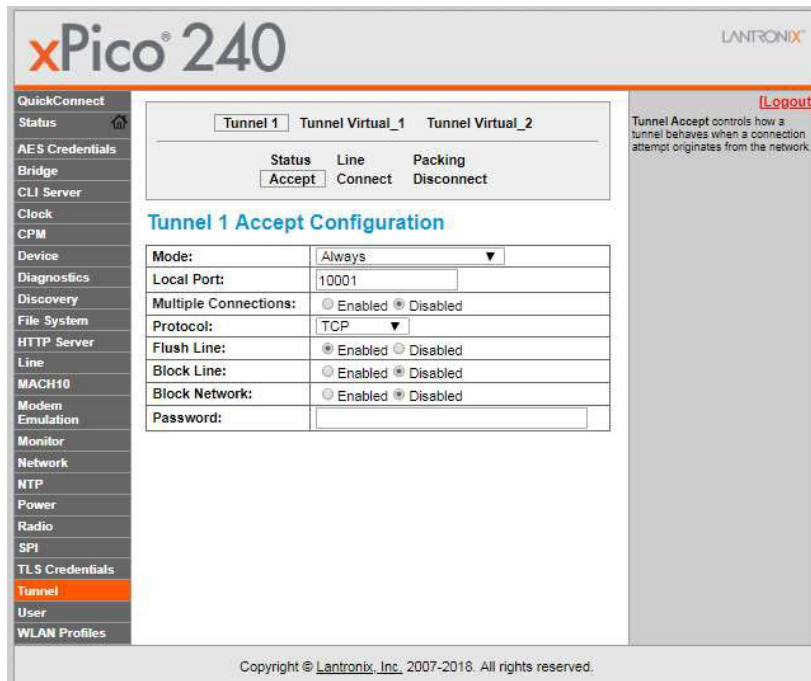
It is recommended that you record any changes you make.

SSID: _____

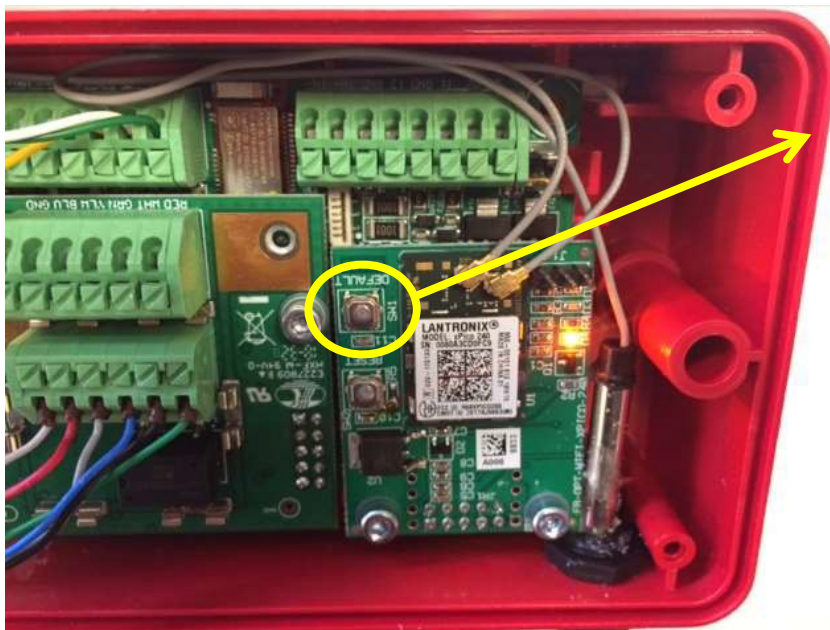
Security Suite: _____

Encryption: _____

Passphrase: _____



In 'Tunnel'/'Accept' set 'Flush Line' to Enable this can be useful when operating in a busy area where many devices share the same Access Point.




TIP when needed – you can use the default button for a total reset of the unit (press and hold for more than 6 s.) The internal red LED will start flashing when default cycle is finished

Important to have the coax cable installed not parallel with other cables - -this to prevent interference.

QuickConnect (WLAN 0 - infrastructure)

QuickConnect offers the ability to configure the WLAN Client interface on xPico 240 to establish connection to an active Access Point. QuickConnect learns most of the connection properties from the available Access Points and prompts the user only for the security parameters and saves the settings under a corresponding new/existing WLAN profile for future autonomous operation of the WLAN Client interface.



xPico 240 LANTRONIX

QuickConnect [Status](#) [WLAN Link Scan](#) [Logout](#)

Network name:


☐ Refresh scan results every 60 seconds

Network Name	BSSID	Ch	RSSI	Security Suite
<u>XpicoWiFi AE0CE2</u>	00:80:A3:AE:0C:E2	1	-45	WPA2-CCMP
<u>RAVAS_RandD</u>	64:7D:02:5D:A7:FB	1	-46	WPA2-TKIP
<u>RAVAS-GUEST</u>	00:1A:8C:D5:06:4E	11	-51	WPA2-CCMP
<u>RAVAS-SECURED2</u>	00:1A:8C:D5:06:4D	11	-52	WPA2-CCMP-EAP
<u>RAVAS-SECURED2</u>	00:1A:8C:D5:06:80	6	-60	WPA2-CCMP-EAP
<u>RAVAS-GUEST</u>	00:1A:8C:D5:06:81	6	-61	WPA2-CCMP
<u>RAVAS-SECURED2</u>	00:1A:8C:D5:06:3C	1	-67	WPA2-CCMP-EAP
<u>RAVAS-SECURED2</u>	00:1A:8C:D5:06:5E	4	-72	WPA2-CCMP-EAP
<u>RAVAS-GUEST</u>	00:1A:8C:D5:06:5F	4	-72	WPA2-CCMP

This page shows a scan of the wireless devices within range of the device.

It reports:

- Network name (Service Set Identifier)(SSID)
- Basic Service Set Identifier (BSSID)
- Channel
- Received Signal Strength Indication (RSSI)
- Security Suite

The  icon indicates the active profile.

Click on a network name for QuickConnect configuration.

Copyright © Lantronix, Inc. 2007-2018. All rights reserved.

Upon selection of the QuickConnect option, the xPico 240 scans and displays up to 20 wireless devices in order of strongest signal strength at the top. Click on a network name to view the connection to that desired Access Point.

When the selected Access Point profile displays, enter the password and click Submit to directly connect to the Access Point and to add the profile and configuration details to the WLAN profiles.

QuickConnect

Status

AES Credentials

Bridge

CLI Server

Clock

CPM

Device

Diagnostics

Discovery

File System

HTTP Server

Line

MACH10

Modem Emulation

Monitor

Network

NTP

Power

Radio

SPI

TLS Credentials

Tunnel

User

WLAN Profiles

WLAN Profile "RAVAS-GUEST"

Connect To

Network Name (SSID):	RAVAS-GUEST
BSSID:	00:1A:8C:D5:C6:4E
Security Suite:	WPA2-CCMP
Signal Strength:	-51

Security

WPAx IEEE 80211r:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Key Type:	<input checked="" type="radio"/> Passphrase <input type="radio"/> Hex
Password:	<input type="password"/>

Advanced

Apply

Test Connection

Submit

Logout

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to update the WLAN settings and save them to Flash.

Use the **Test Connection** button to test connecting to the network using this profile.

xPico® 240

LANTRONIX™

QuickConnect

Status

AES Credentials

Bridge

CLI Server

Clock

CPM

Device

Diagnostics

Discovery

File System

HTTP Server

Line

MACH10

Modem Emulation

Monitor

Network

NTP

Power

Radio

SPI

TLS Credentials

Tunnel

User

WLAN Profiles

WLAN Profile "RAVAS-GUEST"

The changes have been saved permanently.

Basic

Network Name (SSID):

RAVAS-GUEST

State:

☒ Enabled
 ☐ Disabled

Security

Suite:

WPA2 ▼

WPAX IEEE 80211r:

☐ Enabled
 ☒ Disabled

Authentication:

PSK ▼

Key Type:

☒ Passphrase
 ☐ Hex

Password:

Encryption:

☒ CCMP
 ☐ TKIP

Advanced

TX Power Maximum:

17

dBm

Power Management:

☐ Enabled
 ☒ Disabled

Test Connection

[Logout]

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to update the WLAN settings and save them to Flash.

Use the **Test Connection** button to test connecting to the network using this profile.

Copyright © Lantronix, Inc., 2007-2018. All rights reserved.

Once added, the Quick Connect profile is connected and is accessible and configurable through WLAN Profiles.

WLAN Profile Management

View or Edit

Delete


RAVAS-GUEST 

Create new WLAN Profile

[\[Logout\]](#)

This page allows view, edit, delete or creation of a WLAN Profile on the device.

Select a profile for editing by clicking its name; this takes you to the Configuration web page.

The  icon indicates the active profile.

Delete one or more profiles by checking their delete checkboxes.

Create a new profile by entering a name in the text box. The new profile initially has default parameter values. Up to 4 profiles may be created.

When you name a new profile or check a box, the **Apply** and **Submit** buttons will appear.


Use the **Apply** button to try out the changes without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to update the profiles and save them to Flash.

Copyright © Lantronix, Inc. 2007-2018. All rights reserved.

TIP: Delete all other profiles except the one you want to work with

SETTINGS RDC protocol!!


LANTRONIX®

QuickConnect

Status

AES Credentials

Bridge

CLI Server

Clock

CPM

Device

Diagnostics

Discovery

File System

HTTP Server

Line

MACH10

Modem Emulation

Monitor

Network

NTP

Power

Radio

SPI

TLS Credentials

Tunnel

User

WLAN Profiles

[\[Logout\]](#)

Tunnel Connect controls how a tunnel behaves when a connection attempt originates locally.

Tunnel 1
Tunnel Virtual_1
Tunnel Virtual_2

Status	Line	Packing
Accept	<input type="button" value="Connect"/>	Disconnect

Tunnel 1 Connect Configuration

Mode:	Always ▼	
Host 1:	192.168.0.150:5555, TCP	<input type="button" value="[Edit]"/>
Host 2:	<None>	<input type="button" value="[Edit]"/>
Connections:	Sequential ▼	
Reconnect Time:	15 seconds	
Flush Line:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Block Line:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Block Network:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	

Copyright © Lantronix, Inc., 2007-2018. All rights reserved.

Weight information is sent by the indicator using the PRINT key and using Wi-Fi.

The Xpico inside the RAVAS 3200 or 5200 indicator has to send the data to the RDC server. Therefore the Xpico needs to know the static IP address of the RDC server.

To do this, go to:

Tunnel / Tunnel 1 / Connect / Host 1 >> click on [edit]

Tunnel 1 Connect Configuration

Mode:	Disable
Local Port:	<Random>
Host 1 [Summary]	
Address:	192.168.0.50
Port:	5555
Protocol:	TCP
Initial Send:	

Address: > enter server static IP address
Port: > enter 5555

Click on Submit / confirm to store this entries permanently

Configuration methods

For the unit to operate correctly on a network, it must have a unique IP address on the network. There are three basic methods for logging into the device server to assign an IP address and configure the unit:

- * Device Installer: Assign an IP address and view the current xPico configuration using a Graphical User Interface (GUI) on a PC attached to a network. (See 3 Using Device Installer.)
- * Web-Manager: Through a web interface, configure the xPico and its settings using the xPico's Web-Manager. (See 4 Configuration Using Web Manager)
- * Serial & Telnet Ports: There are two approaches to accessing Serial Mode. Make a Telnet connection to the network port (9999) or connect a terminal (or a PC running a terminal emulation program) to the unit's serial port. (See 5 Configuration via Telnet or Serial Port (Setup Mode))

Reference Documentation

For more information on the use and operation of the xPico 240Device Server please refer to the latest product documents which are available on the Product Website.

www.lantronix.com and key in the Site Search box 'Xpico200'

Technical data xPico 240

Network

Wireless LAN Specifications

- IEEE 802.11 a/b/g up to 54 Mbps; 802.11 n (1x1) up to 150 Mbps
- 20 and 40 MHz channel width with optional SGI
- Dual Band 2.4 GHz and 5 GHz, Channels 1-13, UNII-1, 2a, 2e and 3
- Supports IEEE 802.11 d/h/i

Data Communication

- TruPort® Serial Technology— TCP and UDP Server Mode, TCP and UDP Client Mode, Multi-host Connect; TLS Client and Server
- TruPort® Socket— Multi-host Client and Server Modes, HTTP(S), Sockets, TLS
- Authenticated SMTP Support— Send email directly from device

Security and Authentication

- TruPort® Security Software
 - Secure Boot, Secure Firmware-Over-the-Air (FOTA) Updates
 - Secure Key Storage, Encrypted Configuration
 - Secure Connections with SSL/TLS, HTTPS
 - Software Controlled Network Service Ports Enable/Disable
 - Role Based Access Control
- AES/CCMP and TKIP encryption, WPA/WPA2 Personal
- WPA2 Enterprise (EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-FAST)
- SSLv3/TLS 1.2 with PKI and X.509 Certificates (up to 4096-bit Keys)
- AES Algorithm, 256-bit, 192-bit, 128-bit

Management Interfaces

- Lantronix MACH10™ IoT Software Platform, REST, MQTT,
- Lantronix Discovery Protocol (77FE)
- Serial Port, Internal Web Server (HTTP/HTTPS)
- XML Configuration and XML Status (CLI, API)
- Secure Firmware Upgrade via HTTP; MACH10 Gateway Manager
- Remote management with Lantronix Gateway Central™

Protocol Support

- DHCP Client, Server (Soft AP), HTTP Server/Client
- IPv4, TCP/IP, UDP/IP, ARP, ICMP, Auto-IP, DNS

Wireless Features

- Concurrent Soft AP + STA (Client), Client, Soft AP
- Up to 6 simultaneous client connections to Soft AP interface
 - Up to 4 in Concurrent Mode
- Connect to multiple WLAN networks, WLAN QuickConnect
- Ethernet to Wi-Fi Client Bridge (Single Host Mode), Auto-MAC ID

Certifications & Compliance

- Type Approvals: USA (FCC Part 15), Canada (IC RSS), EU (RED), Japan (MIC), China (SRRC), AU/NZS
- Safety: IEC 62368, EN 62368, EN 62311, UL 60950
- RoHS, REACH