

# 9479-ET(G)-CSL

## CSL Intrinsically Safe Gigabit Ethernet WLAN AP / Bridge



## **DECLARATION OF CONFORMITY**

A printed version of the Declaration of Conformity has been provided separately within the original shipment of goods. However, you can find a copy of the latest version at -

<http://www.mtl-inst.com/certificates>

# CONTENTS

<b>1</b>	<b>FEATURE</b>	<b>1</b>
<b>2</b>	<b>DESCRIPTION</b>	<b>2</b>
<b>3</b>	<b>CONNECTIONS</b>	<b>3</b>
3.1	DATA & POWER TERMINALS	3
3.2	LAN (RJ45) 10/100/1000 BASE-T Ethernet	3
3.3	LED indicators	3
<b>4</b>	<b>ORDERING INFORMATION</b>	<b>4</b>
<b>5</b>	<b>DIMENSIONS</b>	<b>4</b>
<b>6</b>	<b>ENVIRONMENTAL</b>	<b>4</b>
<b>7</b>	<b>WASTE REMOVAL INFORMATION</b>	<b>4</b>
<b>8</b>	<b>INSTALLATION</b>	<b>5</b>
<b>9</b>	<b>ATEX &amp; IECEX CERTIFICATION INFORMATION</b>	<b>6</b>
<b>10</b>	<b>SPECIFICATION</b>	<b>8</b>
<b>11</b>	<b>APPROVALS</b>	<b>9</b>
<b>12</b>	<b>NETWORK SETUP</b>	<b>10</b>
12.1	Network Configuration	10
<b>13</b>	<b>WI_FI SETUP</b>	<b>12</b>
<b>14</b>	<b>DHCP SERVER</b>	<b>16</b>
<b>15</b>	<b>SYSTEM STATUS</b>	<b>18</b>
15.1	Device Information	18
15.2	Network Interfaces	18
<b>16</b>	<b>ROUTES</b>	<b>20</b>
<b>17</b>	<b>HTTP/HTTPS</b>	<b>21</b>
<b>18</b>	<b>FIRMWARE</b>	<b>22</b>
<b>19</b>	<b>PASSWORD</b>	<b>22</b>
<b>20</b>	<b>SYSTEM</b>	<b>23</b>
<b>21</b>	<b>SYSTEM LOG</b>	<b>24</b>
<b>22</b>	<b>NETWORK UTILITIES</b>	<b>26</b>
<b>23</b>	<b>SAVE CONFIG / RESET</b>	<b>26</b>

## GENERAL SAFETY INFORMATION

### Safety instructions for installation and operating personnel

The operating instructions provided here contain **essential safety instructions** for installation personnel and those engaged in the operation, maintenance and servicing of the equipment.



#### WARNING !

A 'WARNING' marked in this way is provided for operator and plant safety and **MUST** be followed.

#### CAUTION !

A Caution is provided to prevent damage to the instrument.

#### NOTE

These are used to guide the user in the operation of the instrument.

### Before commencing installation or commissioning:

- Read and understand the contents of this manual
- Ensure installation and operating personnel have received adequate training for this task
- Ensure that any operating instructions are fully understood by the personnel responsible.
- Observe national and local installation and mounting regulations (e.g. IEC 60079-14).



#### WARNING !

These assemblies may not be used in explosion-hazard area applications if they have been used previously in general electrical installations.



#### WARNING !

The responsibility for planning, installation, commissioning, operation and maintenance, particularly with respect to applications in explosion-hazard areas, lies with the plant operator.

### During operation:

- Make the relevant instructions available at all times to the operating personnel.
- Observe safety instructions.
- Observe national safety and accident prevention regulations.
- Operate the equipment within its published specification.
- Servicing, maintenance work or repairs not described in this manual must not be performed without prior agreement with the manufacturer.
- Any damage to this equipment may render its explosion protection null and void.
- No changes to any of the components that might impair their explosion protection are permitted.

### If any information provided here is not clear:

Contact **Eaton's MTL product line** or an authorised distributor or sales office.

#### NOTE

**Improper installation and operation of the enclosure can result in the invalidation of the guarantee.**

## 1 FEATURE

- Intrinsically Safe ATEX / IECEx Certification
- Dual Band 2.4GHz / 5GHz WLAN Support
- Dual Antenna 802.11n MIMO 2T2R
- Access Point (AP) Mode or Client/Bridge Mode
- Dual Port Switch 10/100/1000MB LAN (daisy-chain capability)
- Versions: 2x Gigabit LAN Ports (-ETG), or 2x 10/100 LAN/PoEx\* Ports (-ET)
- CPU Management Feature via Web Pages
- Compact dimensions (W: 42 x H: 160 x D: 140 mm)
- Ex ia IIB T4 Ga, Ex ia [ia Da] IIIC T135°C Db (non-mining),  
Ex ia I Ma (M1 mining)- ETG version
- Ex ia IIC T4 Ga, Ex ia [ia Da] IIIC T135°C Db (non-mining),  
Ex ia I Ma (M1 mining)- ET version
- Ta -40°C to 70°C
- Zone 1 / Zone 21 mounting
- (Zone 0 / Zone 20 with a suitable Ex ia Power Supply)

*\*Note – PoEx is a simple adaptation of the IEEE 802.3af Power over Ethernet (PoE) standard to bring the benefits to the 9400 Range of Hazardous Area devices. This allows two spare pairs in the existing Cat5e cable to distribute the power supply from a 9476 Ethernet Switch (Power Sourcing Equipment – PSE) to each of the devices connected to its five ports (PD – Powered Device). This adaptation is necessary due to restrictions for Hazardous Area use. It is not implied that the device conforms to the 802.3af (PoE) standard.*

## 2 DESCRIPTION

The 9479-ET(G)-CSL is an Intrinsically Safe (IS) WLAN AP/Bridge Module suitable for Zone 1 / Zone 21 mounting, (Zone 0 / Zone 20 with a suitable Ex ia Power Supply).

It may be configured as either an AP or Client/Bridge. Also supporting either 2.4GHz or 5GHz operation further extends its range of applications.

There are 2x RJ45 (LAN) ports that support 10/100/1000 IS Ethernet connections – these can allow 'daisy-chaining' of units together.

Power (12V DC) is supplied to the module either locally or using Power over Ethernet (PoEx) from the LAN port - This requires the PoEx output to be wired to the Supply Input terminals by the user (-ET version only).

The compact and cost effective design makes it the ideal choice for many applications:

### **Petrochem**

Process Monitoring & Control...

### **Mining**

Underground Communication Links, PLC and Machine Monitoring...

Electrical connections are via cage-clamp and/or screw type plug/socket terminals along with RJ45 type connectors for the Ethernet LAN ports.

### 3 CONNECTIONS

#### 3.1 DATA & POWER TERMINALS

##### Power + External IP Rated LEDs (CON1)

Pin	Function	Pin	Function
1	Power In +12V#	2	Power In 0V#
3	LAN1 PoEx +12V#	4	LAN1 PoEx 0V#
5	LAN2 PoEx +12V#	6	LAN2 PoEx 0V#
7		8	
9		10	
11	0V	12	0V
13	LAN1 LED	14	LAN2 LED
15	WLAN LED	16	
17		18	

#Connect LAN1 OR LAN2 PoEx terminals to Power In terminals to use this function

External IP66 rated LEDs wire down to 0V

Power  $U_i = 15.4V$

#### 3.2 LAN (RJ45) 10/100/1000 BASE-T Ethernet

Pin	10/100 Function	Gigabit Function
1	Tx +	BI_DA+
2	Tx-	BI_DA-
3	Rx +	BI_DB+
4	PoEx +12V*	BI_DC+
5	PoEx +12V*	BI_DC-
6	Rx-	BI_DB-
7	PoEx 0V*	BI_DD+
8	PoEx 0V*	BI_DD-

\*Note - PoEx only on LAN1-2 ports when 10/100 (-ET version only)

PoEx not available on Gigabit ports

#### 3.3 LED indicators

	OFF	FLASH	ON
<b>PWR (green)</b>	Power Fail	N/A	Power OK
<b>WDG (green)</b>	Fault	Green- Healthy (10Hz)	Fault
<b>STAT (green)</b>	Initialising or Fault	N/A	Healthy
<b>RJ45 ACT (yellow)</b>	Ethernet link disconnected	Ethernet link activity	Ethernet link connected
<b>RJ45 1000 (green)</b>	10/100Mbps	N/A	1000Mbps
<b>WLAN ACT (blue)</b>	No Link	Data	Linked
<b>LAN1 – LAN2 EXT LED</b>	Ethernet link disconnected	Ethernet link activity	Ethernet link connected
<b>WLAN EXT LED</b>	No Link	Data	Linked

## 4 ORDERING INFORMATION

Part Number	Description	Comments
<b>9479-ETG-CSL</b>	<b>Gigabit WLAN AP / Bridge</b>	<b>Standard</b>
9479-ET-CSL	WLAN AP / Bridge (10/100 PoEx)	Special Order (Subject to MOQ)

Note: 2x Antenna required (not included) these need to be ordered separately

### Accessories

Part Number	Description
<b>ANTSMA94</b>	<b>Antenna SMA Plug, length 150mm Gain, 3dBi</b>
<b>ANT94</b>	<b>Antenna TNC Plug, length 150mm Gain, 3dBi</b>
<b>ANT94RA</b>	<b>Stubby Antenna TNC 90° Plug, length 80mm, Gain 2dBi</b>
<b>CSL-RG316-SMA-1000</b>	<b>SMA Bulkhead Socket ⇔ SMA Plug, length 1000mm RG316 Cable Assembly</b>
<b>CSL-RG316-TNC-SMA-1000</b>	<b>TNC Bulkhead Socket ⇔ SMA Plug, length 1000mm RG316 Cable Assembly</b>

## 5 DIMENSIONS

Width	42mm
Height	160mm
Depth	140mm
Weight	1500g
Mounting	Din Rail

## 6 ENVIRONMENTAL

### Operating Temperature

-40°C...+70°C

### Storage Temperature

-40°C...+70°C

### Humidity

0...95% RH, non-condensing

### Ingress Protection

Select enclosure to suit application, see certificates for information

## 7 WASTE REMOVAL INFORMATION



The electronic equipment within must not be treated as general waste. By ensuring that this product is disposed of correctly you will be helping to prevent potentially negative consequences for the environment and human health, which could otherwise be caused by incorrect waste handling of this product. For more detailed information about the take-back and recycling contact Controlled Systems Ltd



## 8 INSTALLATION



### **WARNING !**

See Special Conditions of Safe Use in the following section regarding ATEX & IECEx Certification Information before installation

The 12V supply to the module connects via screw terminals 1 + 2 as shown above.

If the unit is being powered using Power over Ethernet (PoEx), it is required that you connect the relevant PoEx power terminals (Con1) to the main power supply pins (Con1), see connections section.

As the 9479 supports Auto MDI/MDI-X, a straight connected RJ45 Cat5e cable is used to connect to any device.

It is recommended that Cat5e cables for Hazardous Area Zone 1 use are 'Blue' in colour and are of good quality (see accessories section), the Safe Area cables being a colour other than blue to aid identification.

The operating parameters must not exceed those as detailed on the certificate.

This apparatus must only be installed or replaced by a competent person who must ensure that existing IS segregation is maintained.

## **9 ATEX & IECEx CERTIFICATION INFORMATION**

The following information is in accordance with the Essential Health and Safety Requirements (Annex II) of the EU Directive 2014/34/EU [the ATEX Directive- safety of apparatus] and is provided for those locations where the ATEX Directive is applicable.

### **General**

- a) This equipment must only be installed, operated and maintained by competent personnel. Such personnel shall have undergone training, which included instruction on the various types of protection and installation practices, the relevant rules and regulations, and on the general principles of area classification. Appropriate refresher training shall be given on a regular basis. [See clause 4.2 of EN 60079-17].
- b) This equipment has been designed to provide protection against all the relevant additional hazards referred to in Annex II of the directive, such as those in clause 1.2.7. This equipment has been designed to meet the requirements of intrinsically safe electrical apparatus in accordance with EN 60079-0, EN 60079-11 and EN 60079-26.

### **Installation**

- a) Reference to the IEC code of practice IEC 60079-14. In addition particular industries or end users may have specific requirements relating to the safety of their installations and these requirements should also be met. For the majority of installations the Directive 1999/92/EC [the ATEX Directive- safety of installations] is also applicable.
- b) Unless already protected by design this equipment must be protected by a suitable enclosure against
  - i) mechanical and thermal stresses in excess of those noted in the certification documentation and the product specification.
  - ii) aggressive substances excessive dust moisture and other contaminants
- c) This apparatus is intrinsically safe electrical apparatus and is normally mounted in a hazardous area.

### **Inspection and maintenance**

- a) Inspection and maintenance should be carried out in accordance with European, national and local regulations which may refer to the IEC standard IEC 60079-17. In addition specific industries or end users may have specific requirements which should also be met.
- b) Access to the internal circuitry must not be made during operation.

### **Repair**

This product cannot be repaired by the user and must be replaced with an equivalent certified product.

### Specific Conditions of Use (Special Conditions)

The following conditions relate to safe installation and/or use of the equipment.

**8.1** For Group I, the modules shall each be mounted within an enclosure providing a degree of protection of at least IP54.

This shall be in accordance with EN 60529, and the modules installed in a manner that does not impair the existing creepage and clearance distances. The enclosure shall also comply with the appropriate requirements of Clauses 7.4.2 and 7.5, or 8.2 of EN 60079-0.

**8.2** For Group II, the RJ45 connectors shall be fitted with either a plug or blanking plug. Alternatively, the module shall be mounted in an enclosure providing a degree of protection of at least IP20.

This shall be in accordance with EN 60529, and the modules installed in a manner that does not impair the existing creepage and clearance distances. The enclosure shall also comply with the appropriate requirements of Clauses 7.4.2 and 7.5, or 8.3 of EN 60079-0.

**8.3** For Group III, the module shall be mounted inside a suitably certified enclosure which provides a minimum degree of protection of at least IP54. The module shall be installed in a manner that does not impair the existing creepage and clearance distances.

**8.4** The supply to the modules must be derived from a suitably certified, intrinsically safe supply.

**8.5** The values of Co and Lo shall apply when one of the two conditions below is given:

- The total Li of the external circuit (excluding the cable) is < 1% of the Lo value, or
- The total Ci of the external circuit (excluding the cable) is < 1% of the Co value.

The above parameters are reduced to 50% when both of the two conditions below are given:

- The total Li of the external circuit (excluding the cable) > 1% of the Lo, and
- The total Ci of the external circuit (excluding the cable) > 1% of the Co.

Note: the reduced capacitance of the external circuit (including cable) shall not be greater than 1µF for Group I and IIB/III and 600 nF for IIC.

**8.6** The equipment shall be mounted on an earthed metal bracket or housing.

### Marking

Each device is marked in accordance with the Directive and CE marked with the Notified Body Identification Number.

#### 9479-ETG-CSL Product Label



Serial No.

Part No. **9479-ETG-CSL Gigabit WLAN AP/Bridge**

**CML 19ATEX2414X**

**IECEX CML 19.0150X**

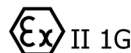
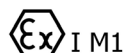
**IECEX ExTC 20.0019X**

Ex ia I Ma

Ex ia IIB T4 Ga

Ex ia [ia Da] IIIC T135°C Db

Ta=-40°C to +70°C



II 2(1)D



**SEE INSTRUCTION MANUAL**

**Controlled Systems Limited**  
**Swadlincote Derbyshire (UK)**



2813



## **10 Specification**

### **Power supplies**

12VDC IS Power Supply Input  
PoEx™ (Power over IS Ethernet)  
Typically 12V @ 300mA (Inrush < 400mA)  
Ui =15.4V  
9492-PS-PLUS recommended

### **Ethernet**

Intrinsically Safe 10/100/1000Base-T

### **Connector**

RJ45 (x2)

### **Cable Length**

Up to 100m Cat5e

### **WLAN**

#### **TX Output – 802.11n**

2.4GHz: 18 to 20.5 dBm  
5GHz: 15 to 18 dBm  
(per antenna output in 2T/2R mode)

#### **RX Sensitivity – 802.11n**

2.4GHz: -92 to -73 dBm  
5GHz: -96 to -72 dBm

### **Data Rates**

802.11n : up to 300Mbps (2T/2R)  
802.11a/h : 6 to 54Mbps  
802.11b : 1 to 11Mbps  
802.11g : 1 to 54Mbps

### **Security – AP Mode**

WEP, WPA-PSK, WPA2-PSK, WPA/WPA2,  
SSID visibility status

### **Security – Client/Bridge Mode**

WEP, WPA-PSK, WPA2-PSK, WPA/WPA2,  
AES/TKIP/WEP by hardware encryption

### **ANTENNA CONNECTIONS**

#### **Connector (Top Port MAIN, Bottom Port AUX)**

SMA (MAIN)

SMA (AUX)

## 11 APPROVALS

### Location of Unit

Zone 1, IIBT4 hazardous area (9479-ETG)

Zone 1, IICT4 hazardous area (9479-ET)

### Certification Code

Ex ia IIBT4 Ga (9479-ETG)

Ex ia IICT4 Ga (9479-ET)

Ex ia [ia Da] IIIC T135°C Db (non-mining)

Ex ia I Ma (M1 mining)

Ta = -40°C to +70°C

### Certificate numbers

ATEX (CML 19ATEX2414X)

IECEX (IECEX CML 19.0150X)

QLD (IECEX ExTC 20.0019X)


*See certificates for further information*



## 12 Network Setup

To begin configuring the unit, the Default IP Address is 192.168.1.253

The screenshot shows the 'SETUP' tab of the CSL 9479-ET(G) WLAN AP/Bridge configuration interface. On the left is a sidebar menu with options: PHYSICAL INTERFACES, VIRTUAL INTERFACES, NETWORK (selected), CU PORT, VPN, BRIDGING, ROUTING / FIREWALL, QOS, and SERVICES. The main area is titled 'NETWORK OVERVIEW' and contains a table with the following data:

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY (METRIC)	PERSISTENCE	ACTIONS
Cu Port	<input checked="" type="checkbox"/>	192.168.0.175	255.255.255.0		Enabled	

Below the table is an 'Add network' button.

This page displays the current network configuration.

Click the **ADD NETWORK** button to create a new IP network.

Click the **REMOVE** button under the 'action' heading to remove the selected network.

Click the **EDIT** button under the 'action' heading to open the network configuration page.

### 12.1 Network Configuration

The screenshot shows the 'NETWORK - CU PORT' configuration page. The sidebar menu is the same as in the previous screenshot. The main area has a title 'NETWORK - CU PORT' and a description: 'On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.'

The 'COMMON CONFIGURATION' section has three tabs: 'General Setup' (selected), 'Interfaces Settings', and 'Advanced Settings'. It contains the following fields:

- Enable interface:** ☒
- Network description:** Cu Port
- Protocol:** static (dropdown menu)
- IPv4-Address:** 192.168.0.175
- IPv4-Netmask:** 255.255.255.0 (dropdown menu)
- Default IPv4 gateway:** (empty field)
- Default gateway metric:** 0
- DNS server(s):** (empty field)

Below these fields is a section titled 'IP ALIASES' with a warning: 'NATed VRRP networks warning. The following applies to NATed networks which use the VRRP protocol:'

- Public-side NAT MUST NOT define IP aliases; else the NAT might use the alias IP as public address instead of the VRRP IP
- Conversely, Private-side NAT SHOULD define a private IP alias to allow connection tracking replication

Below the warning is a note: 'This section contains no values yet' and an 'Add' button.

At the bottom of the page are three buttons: 'Reset', 'Save', and 'Save & Apply'.

Once you have clicked the EDIT button, you will see the network configuration page, here you can set all the information about your network.

### General Setup:

**Enable Interface:** Tick this box to enable the selected network interface.

**Network Description:** This entry is to provide an identification to your network

**Protocol:** Choose DHCP if you have a DHCP server in the network and you want to assign an IP address to the AP. Choose Static if you do not have a DHCP server in the network or if you need a fixed address to the interface.

**\*Note** – You cannot choose DHCP if you have enabled the DHCP server option on the DHCP page; the AP cannot be both a DHCP client and a DHCP server.

**IPv4 Address:** Only available in static mode. The IP address of the AP on the local network. Assign any unused IP address in the range of IP addresses available for the LAN

**IPv4 Netmask:** The subnet mask of the LAN

**Default IPv4 gateway:** The IP address of the router on the local area network.

**DNS Server(s):** The IP addresses of the DNS server(s) you want to use.

If you selected the DHCP protocol, you can choose to use the value defined in the menu TOOLS/System, or you can define a new HOSTNAME, specific to this network.

### Interfaces Setting:

The screenshot shows the 'COMMON CONFIGURATION' window with the 'Interfaces Settings' tab selected. The 'Bridge Interfaces' section has a checked box for 'creates a bridge over specified interface(s)'. The 'Enable STP/RSTP' section has an unchecked box, with a warning message: 'WARNING: Some cautions must be taken with wireless interfaces, please see user guide'. The 'Enable LLDP forwarding' section has an unchecked box. The 'Bridge VLAN' section has an unchecked box with a note: 'Enable VLAN management in bridge. You must configure the bridge VLANs before enabling this option (setup->bridging)'. The 'Interface' list shows four interfaces: 'WiFi adapter: WiFi 1 - acksys (lan)', 'WiFi adapter: WiFi 2 (currently disabled) - acksys (lan)', 'Ethernet adapter: LAN 1 (lan)', and 'Ethernet adapter: LAN 2 (lan)'. The 'MTU' field is set to 1500.

**Bridge Interfaces:** If checked, all interfaces in this network are linking with the software equivalent of an Ethernet switch.

**Enable STP/RSTP:** If checked the STP/RSTP will be activated on this bridge. If you choose to not use STP/RSTP, you have to set up your devices to avoid network loops, by yourself.

**Enable LLDP Forwarding:** Check this box if the internal bridge must forward the LLDP multicast frame.

**Bridge VLAN:** Enable VLAN management in the bridge.

**Interface:** This is the list of available network interfaces. Disabled (greyed) interfaces are already used in another network. For Bridge networks, select all the interfaces you want to bridge together in to the LAN being configured. For simple networks, select the one interface to configure.

### Advanced Settings:

The screenshot shows the 'COMMON CONFIGURATION' window with the 'Advanced Settings' tab selected. The 'Network persistence' dropdown menu is set to 'Enabled', with a sub-note: 'Avoid the network deletion after a link down.'

Network Persistence: When this option is enabled, the IP setting (routes, gateway, virtual interfaces) remains persistent when the physical interface loses its connection. Default value is enabled for static IP, and disabled for DHCP.

## 13 Wi-Fi Setup

**9479-ET(G) WLAN AP/Bridge**

SETUP TOOLS STATUS

PHYSICAL INTERFACES  
VIRTUAL INTERFACES  
NETWORK  
VPN  
BRIDGING  
ROUTING / FIREWALL  
QOS  
SERVICES

### WIRELESS INTERFACES OVERVIEW

You can set up to 8 simultaneous roles (wifi interface types) per radio card, among the following combinations:

Combination	Channel selection		Can use DFS	Max number of interfaces			
	Multiplicity			Access point	Infrastructure client	Mesh point	Ad-hoc
Multiple access points	single, auto, multiple		yes	8			
Portal	single		no	8		1	
Client / bridge	single, auto, multiple, roaming		yes		1		
Other / repeater	single		no	8	1 (non-roaming)	1	1

When using several roles, they all use the same shared channel; in this case, the client role must not be set to multichannel roaming. Repeater mode is a combination of two roles: access point + client.

### Wi-Fi 4 (802.11n) Wireless interface

CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
10	802.11g+n	acksys10024	Access Point (infrastructure)	WPA2-PSK (Personal)	[EDIT] [REMOVE]

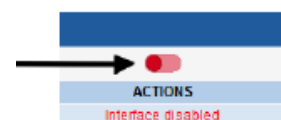
### GLOBAL PARAMETERS

#### RADIO REGULATION AREA

Country: United Kingdom

[Save] [Save & Apply]

This page allows the user to configure the wireless network settings, by default the radio will be disabled and you will need to turn it on.



**Country:** The regulation rules of the selected country will determine the channels and transmission powers you can use. Additionally, in the client role, the product will use the country provided by the AP in its beacons.

Under the 'actions' heading, you can click the buttons 'EDIT' and 'REMOVE'.

Click REMOVE to remove the selected SSID.

Click EDIT to open the radio windows and edit this SSID's Properties.



## Device Configuration:

The screenshot shows the 'WIRELESS SETTINGS : WIFI' configuration page. On the left is a sidebar with navigation links: PHYSICAL INTERFACES, WIFI, LAN, VIRTUAL INTERFACES, NETWORK, VPN, BRIDGING, ROUTING / FIREWALL, QOS, and SERVICES. The main content area has tabs for SETUP, TOOLS, and STATUS. Under 'WIRELESS SETTINGS : WIFI', there's a note about the Device Configuration section covering physical settings. Below this are two main sections: 'DEVICE CONFIGURATION' and 'INTERFACE CONFIGURATION'. The 'DEVICE CONFIGURATION' section has tabs for General Setup, 802.11n Mcs, and Advanced Settings. The 'General Setup' tab is selected, showing '802.11 mode' as '802.11g+n (2.4 GHz)', 'HT mode' as '20MHz', and 'Channel' as '5'. The 'INTERFACE CONFIGURATION' section has tabs for General Setup, Wireless Security, Advanced Settings, MAC Filter, and Frame Filter. The 'General Setup' tab is selected, showing 'Role' as 'Access Point (infrastructure)', 'ESSID' as 'jacksys10024', 'Maximum simultaneous associations' as 'Max allowed by radio card', 'Hide ESSID' checked, and 'Network' as 'Cu Port'. At the bottom are buttons for 'Back to Overview', 'Reset', 'Save', and 'Save & Apply'.

### General Setup:

This selection gathers all the settings that are common to each SSID you may create on this radio.

**Enable Device:** If this box is checked, the radio card is enabled and is able to communicate. Uncheck it to disable the radio.

#### 802.11 Mode:

The 802.11g+n mode operates in the 2.4GHz band and is compatible with 802.11g and 802.11n devices.

The 802.11a+n mode operates in the 5GHz band and is compatible with 802.11a/h and 802.11n devices.

The 802.11ac+n mode operates in the 5GHz band and is compatible with 802.11ac, 802.11a/h and 802.11n devices.

\*Note – A unit configured in 802.11ac+n/802.11a+n cannot communicate with another one configured in 802.11g+n mode because they are using different frequency ranges.

**HT (high throughput) mode:** In HT mode, you can aggregate adjacent channels (2 in 802.11n, 2 or 4 in 802.11ac) in order to increase bandwidth. One of the channels is the one selected in the channel section (see below). The second one may be the one directly below or directly above. If you choose 20MHz, only one channel will be used at a time.

**Automatic channel select (ACS):** Depending on the unit role, the channel can be selected automatically;

AP Role: At start up, the AP will select the channel among all the ones allowed in your country. In order to limit the choice to specific channels, do not check ACS, but use the channels multi-selection box instead.

Client Role: The client will scan all channels allowed in your country. In order to limit the channel scan list, do not check ACS, but use the channels multi-selection box instead. If the client is set in roaming mode, this channel list is superseded by the one in the roaming tab.

Other Roles: The other roles, (mesh portal, ad-hoc) support only one channel, this parameter is not available and you must select a channel in the dropdown box.

**Channel:** According the selected 802.11 mode and the regulation rules of the selected country, a list of channels is available for selection. This is not used for infrastructure client modes, as they use all the allowed channels for scanning.

In some cases, a single radio card can handle multiple Wi-Fi roles simultaneously. In this case and 'client' function must be set to only scan the common channel.

You can select several channels so that the AP will select the cleanest one and will be able to switch to another if a radar is detected on the current one. To select multiple channels, use Ctrl + click.

## Advanced Settings

The screenshot shows the 'Advanced Settings' tab within a 'DEVICE CONFIGURATION' window. The interface includes several configuration fields with their respective units and descriptions:

- Max Transmit Power:** A text input field with a help icon and the text 'dBm - leave empty to use max value allowed by your country and your radio card'.
- Antennas:** A dropdown menu currently set to 'All'.
- QoS Profile:** A dropdown menu currently set to 'Default'.
- Distance Optimization:** A text input field with a help icon and the text 'Distance to farthest network member in meters'.
- Beacon interval:** A text input field with a help icon and the text 'In multiple of 1024us. Used by AP, ad-hoc and mesh modes'.
- Fragmentation Threshold:** A text input field.
- RTS/CTS Threshold:** A text input field.
- Retry settings:** A checkbox that is checked.
- Short retry:** A text input field set to '7' with a help icon and the text 'Retry for frame sent without RTS/CTS'.
- Long retry:** A text input field set to '2' with a help icon and the text 'Retry for frame sent with RTS/CTS'.
- Aggregate retry:** A text input field set to '30' with a help icon and the text 'Retry for aggregate frame (802.11n only)'.

**Max Transmit Power:** The transmit power is normally set automatically based on the regulation rules for the given channel and the capabilities of the radio card. This option sets an upper bound on the transmit power. The transmit power is distributed between the configured antennas.

**Antennas: NOTE: Improved RX signal strength and full TX power is achieved only buy using two antennas** and selecting "All" for this option. Both are also required for 802.11n MIMO mode. For single antenna use select "Only #1" and connect the antenna to the AUX socket, however performance will be reduced with a single antenna.

**Qos Profile:** This option allows choosing between the two Qos profiles.

**Distance optimization:** Use this option if your link covers a long distance, it will update the internal timeouts.

**Beacon interval:** This option allows configuring the interval between two beacon frames.

**Fragmentation threshold:** This option configures the maximum 802.11 frame size in 802.11a/b/g mode in bytes. Frames that exceed this threshold are fragmented.

**RTS/CTS threshold:** The Wi-Fi standard uses the RTS/CTS protocol to avoid collision in the air; this option defines the size of the frames subject to this protection. Use RTS/CTS when you have interference on your channel or a poor performance on the Wi-Fi.

**Retry settings:** Unicast data frames are normally acknowledged. If the transmitter does not receive the acknowledgment, it must resend the frame. In 802.11n mode, several frames can be aggregated into one big frame called an A-MPDU. Independent frames are acknowledged by an individual ACK frame, while A-MPDU frames are acknowledged by a single 'Block acknowledge' frame containing one acknowledgment for each subframe in the A-MPDU. When you check this option, you can set the number of retries.

Short Retry: This is the number of retries for a physical data frame.

Long Retry: This is the number of retries for a physical data frame sent with the RTS/CTS protocol

Aggregate Retry: This option configures the number of retries for a frame aggregated into an A-MPDU.

### **Interface Configuration:**

This section is duplicated for each SSID; settings only apply to the selected SSID.

#### **General setup:**

**Role:** The unit has the following supported roles;

- Access Point
- Isolating access point
- Client (connecting at an access point)
- Mesh 802.11s
- Point to multipoint station (ad-hoc)
- SRCC

**ESSID:** This is the Wireless network name.

**Maximum association:** Specifies the maximum number of clients allowed to connect on the Access Point.

**Hide ESSID:** This option allows you to not broadcast the SSID on the network. This means that your clients will need to know the SSID beforehand, since scanning will not reveal this SSID on the AP.

**Network:** This option allows selecting the network where the interface is added.

**Mesh ID (only in mesh mode):** This option replaces the ESSID when the Mesh mode is selected.

#### **General setup client mode:**

**Multiple ESSIDs:** When this is checked, a multi-selection field, (Wireless network nicknames), replaces the single ESSID field. You can select several SSIDs with their security parameters and the client will associate to any AP advertising one of the combination. In case several matching APs are in range, you can prioritize the SSIDs.

When using multiple ESSIDs, the roaming features are not available; the security is defined together with the corresponding ESSID in a separate menu.

#### **Wireless Security:**

This menu allows you to choose the type of wireless security you want to apply on this SSID. The different security schemes are;

- No Encryption
- WEP Open System
- WEP Shared Key
- WPA-PSK
- WPA2-PSK
- WPA-PSK/WPA2-PSK Mixed Mode
- WPA-EAP
- WPA2-EAP
- WPA-LEAP
- WPA2-LEAP

Depending on which security option you choose, a range of options will appear that you must configure.

## 14 DHCP Server

PHYSICAL INTERFACES

VIRTUAL INTERFACES

NETWORK

VPN

BRIDGING

ROUTING / FIREWALL

QOS

SERVICES

ALARMS/EVENTS

CONN. TRACKING

COUNTERS GRAPHS

DHCP / DNS RELAY

DISCOVER AGENT

SNMP AGENT

VRRP

WEB SERVER

SETUP

TOOLS

STATUS

DHCP / DNS RELAY

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

INTERFACE SETTINGS : CU PORT

General Setup

Ignore interface

☒
☐ Disable DHCP for this interface.

STATIC LEASES

Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.

HOSTNAME	MAC-ADDRESS	IPv4-ADDRESS
This section contains no values yet		

Add

DHCP RELAY

Use the Add Button to add a new DHCP relay entry. The Relayed interface must have a static IP address. The DHCP Server/Relay must be able to reach back the network where the initial client's request originated from.

RELAYED INTERFACE	DHCP SERVER IPv4-ADDRESS	TRUSTED INTERFACE	SORT
Where DHCP request are received (from clients)	Where DHCP requests are sent (to server)	Where DHCP replies are received (from server)	
This section contains no values yet			

Add

DNS RELAY

Rebind protection

☒
☐ Enable DNS rebind attack protection. Block the DNS response if the IP address is on the private IP range (according to RFC1918).

Rebind localhost

☒
☐ Allow DNS response with IP address in 127.0.0.0/8 range.

Reset

Save

Save & Apply

### General Setup:

INTERFACE SETTINGS : LAN

General Setup

Advanced Settings

Ignore interface

☐
☒ Disable DHCP for this interface.

DHCP pool first address

100

☐ Lowest leased address as offset from the network address.

DHCP pool size

150

☐ Maximum number of leased addresses.

Lease time

12h

☐ Expiry time of leased addresses, minimum is 2 Minutes (2m).

**Ignore interface:** If checked, the DHCP server will be disabled on the selected interface.

**DHCP pool first address (if enabled):** First IP Address of the DHCP pool. This is interpreted as an offset relative to network address.

**DHCP pool size (if enabled):** Maximum number of leased addresses.

**Lease time (if enabled):** This represents the time during which a given IP Address remains valid. After that time, the client needs to renew his lease.

## Advanced Settings

INTERFACE SETTINGS : LAN

General Setup | **Advanced Settings**

**Dynamic DHCP** ☒ Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

**Force** ☐ Force DHCP on this network even if another server is detected.

**IPv4-Netmask**

**DHCP-Options**

Define additional DHCP options, for example "5,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

**Dynamic DHCP:** If unchecked, only static leases will be authorized.

**Force:** By default, the DHCP service doesn't start if it detects the presence of another DHCP server on the network. If this option is checked, the DHCP server won't check for another server before start.

**IPv4 Netmask:** This option overrides the default netmask value sent to DHCP clients.

**DHCP Options:** This field allows you to enter an additional DHCP option (enclosed into quotes). Syntax depends on the option itself.

## Static Lease:

STATIC LEASES

Use the *Add* button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

HOSTNAME	MAC-ADDRESS	IPV4-ADDRESS
test	5c:d9:98:44:a3:3a (192.168.1.188)	192.168.1.188

This option allows to always give the same predefined IP Address according to the MAC address.

## 15 System Status

### 15.1 Device information

The screenshot shows the web interface for the CSL 9479-ET(G) WLAN AP/Bridge. The top navigation bar includes 'SETUP', 'TOOLS', and 'STATUS' (selected). A left sidebar contains links for 'DEVICE INFO', 'NETWORK', 'WIRELESS', 'SERVICES', and 'LOGS'. The main content area is titled 'DEVICE INFORMATION' and contains two sections: 'FIRMWARE INFORMATION' and 'DEVICE INFORMATION'.

FIRMWARE INFORMATION	
WaveOs version:	4.4.4.1
Boot loader version:	3.0.7.1
Firmware ID:	E2148.AC.1

DEVICE INFORMATION	
Host name:	Acksys
Model:	EmbedAir100/R
Product version:	V1
Motherboard ID:	00001ad3c230
Product serial number :	16295497

The Device Information page allows a quick overview of the unit's useful information and the currently installed firmware information.



### 15.2 Network Interfaces

The screenshot shows the web interface for the CSL 9479-ET(G) WLAN AP/Bridge. The top navigation bar includes 'SETUP', 'TOOLS', and 'STATUS' (selected). A left sidebar contains links for 'DEVICE INFO', 'NETWORK', 'BRIDGES', 'MULTICAST ROUTES', 'ROUTES', 'WIRELESS', 'SERVICES', and 'LOGS'. The main content area is titled 'INTERFACES' and contains a section for 'CU PORT'.

IP CONFIGURATION  
IPv4: 192.168.0.175 Netmask: 24 MTU: 1500

GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	LAN	00:09:90:01:0a:cd	119446	307367	Negotiated 100 baseTX FD, link ok	1500
	WiFi	00:09:90:01:0a:cc	298578	0	Role: Access Point (infrastructure) SSID: acksys10024 Channel: 10	1500

This Page shows a summary of the currently configured network interfaces and displays the transmitted and received packets.

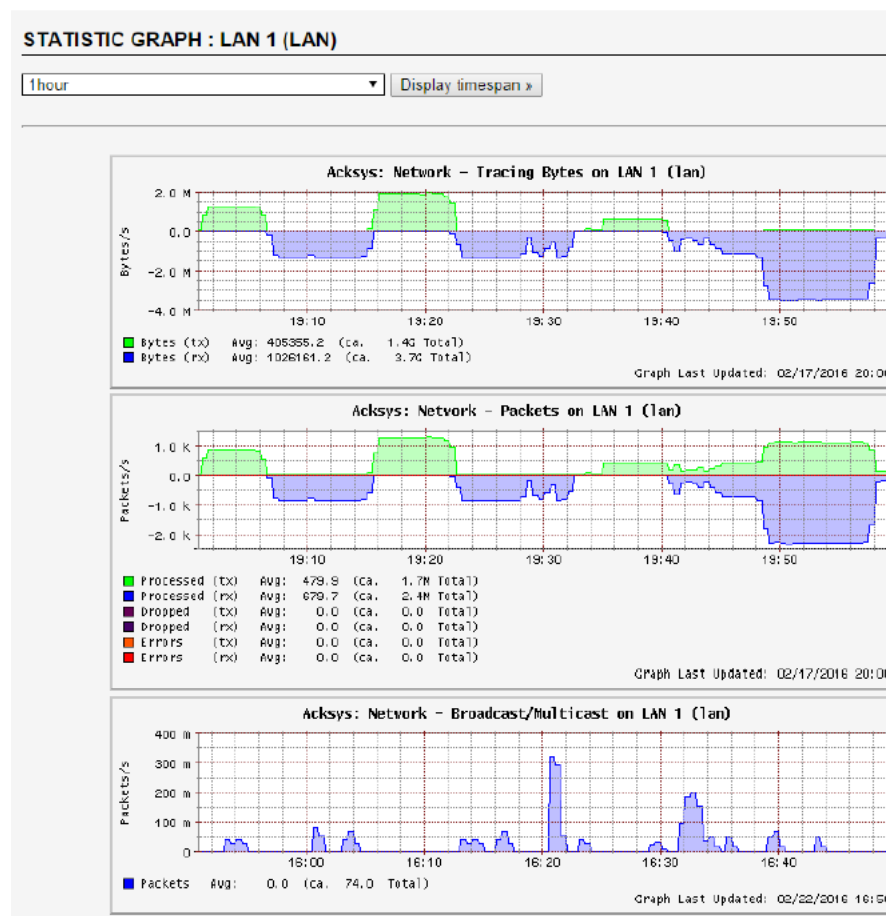
GRAPH	PHYSICAL INTERFACE	
	LAN	
	WiFi	

Pressing the Graph button will present a history graph of the selected interface, the following information will be available;

**Tracing Bytes graph:** Displays the number of bytes of transmission and reception on the interface

**Packets graph:** Displays the number of processed, dropped and error packets of transmission and reception on the interface

**Broadcast/Multicast graph:** Displays the number of Broadcast/Multicast Packets on the interface



You can also configure the display duration to the following; 10 minutes, 1 hour, 1 day, 1 week and 1 month.



## 16 Routes

The screenshot shows the CSL 9479-ET(G) WLAN AP/Bridge STATUS page. The left sidebar contains a menu with options: DEVICE INFO, NETWORK, BRIDGES, MULTICAST ROUTES, ROUTES, WIRELESS, SERVICES, and LOGS. The main content area is titled 'ROUTES' and displays the following rules currently active on the system:

ACTIVE IPV4-ROUTES				
NETWORK	TARGET	IPV4-NETMASK	IPV4-GATEWAY	METRIC
Cu Port	192.168.0.0	255.255.255.0	local	0

This Page shows all of the active IPV4 Routes on the unit.

The screenshot shows the CSL 9479-ET(G) WLAN AP/Bridge STATUS page. The left sidebar contains a menu with options: DEVICE INFO, NETWORK, BRIDGES, MULTICAST ROUTES, ROUTES, WIRELESS, SERVICES, and LOGS. The main content area is titled 'MULTICAST ROUTING' and displays the following information:

The "network interfaces" table displays network interface states related to multicasting.  
The "multicast routes" table displays active routes.  
The "rendezvous points" table displays candidate and elected rendezvous points.

NETWORK INTERFACES									
INTERFACE	LOCAL ADDRESS	SUBNET	THRESHOLD	EN	UP	DR	NEIGHBOR MC ROUTERS	MULTICAST GROUPS	IGMP REPORTS
Cannot upload multicast status information									

MULTICAST ROUTES						
ROUTE TYPE	MULTICAST SOURCE	MULTICAST GROUP	IN USE	RENDEZVOUS POINT	INGRESS I/F	EGRESS I/F

RENDEZVOUS POINTS				
Current BSR address: (The BSR is the coordination server which chooses among redundant RP candidates)				
RP ADDRESS	INGRESS I/F	MULTICAST GROUP	PRIORITY	HOLD TIME

This page displays all the available information about the running instance of the PIM multicast router.

### **Network interface:**

**Interface:** The Network number referred to in the ingress/egress columns.

**Local Address:** Unicast IP address assigned to the network in the setup/Network Page

**Subnet:** The subnet that this interface connects to and the number of subnet bits.

**Threshold:** Minimum TTL required to forward data to this interface.

**EN:** Multicasting is enabled on this interface.

**UP:** This interface is available (e.g the RJ45 connector is plugged in)

**DR:** This router is designated for this network.

**Neighbour MC Router:** Other PIM routers directly connected to this network.

**Multicast Groups:** PIM-SSM groups handled on this interface.

**IGMP reports:** list of groups for which receivers send join request on this local network.



### **Multicast routes section:**

**Route type:** (\*,G) for any source to group, (S,G) for specific source to group.

**Multicast source:** Source requested by the receiver: any or a specific IP Address.

**Multicast group:** The group concerned by the route entry.

**In Use:** This entry is actively used to forward data.

**Rendezvous Point:** The IP Address that was computed for the group.

**Ingress I/F:** Interface where the multicast data is expected to arrive.

**Egress I/F:** Interface list where the multicast data must be forwarded.

### **Rendezvous Point:**

**RP Address:** The IP Address of the rendezvous point for this block of groups

**Ingress I/F:** Interface toward the RP, where data comes in.

**Multicast Group:** The block of groups associated to this RP.

**Priority:** Priority of the RP for elections. Locally configured groups have a priority of 1.

**Hold Time:** The delay after which this entry will become invalid if not refreshed in the meantime.

\*Note – There will always be an entry for the IP Address 169.254.0.1, which is used internally to manage the SSM Routing.

## **17 HTTP/HTTPS**

The screenshot shows the 'WEB SERVERS' configuration page for a CSL 9479-ET(G) WLAN AP/Bridge. The page has a blue header with the CSL logo and the device name. Below the header is a navigation bar with 'SETUP', 'TOOLS', and 'STATUS' tabs. On the left is a sidebar menu with categories: PHYSICAL INTERFACES, VIRTUAL INTERFACES, NETWORK, VPN, BRIDGING, ROUTING / FIREWALL, QOS, and SERVICES. The 'SERVICES' category is expanded, showing sub-items: ALARMS/EVENTS, CONN. TRACKING, COUNTERS GRAPHS, DHCP / DNS RELAY, DISCOVER AGENT, SNMP AGENT, VRRP, and WEB SERVER. The main content area is titled 'WEB SERVERS' and contains a sub-section 'HTTP & HTTPS CONFIGURATION'. It includes a text box with instructions: 'In this page you will be able to enable, disable and configure HTTP & HTTPS servers. When you apply after switching between HTTP/HTTPS, remember to change http/https in the browser address bar'. Below this are two fields: 'Web server security level' set to 'HTTP (clear text)' and 'HTTP TCP port number' set to '80'. At the bottom right are three buttons: 'Reset', 'Save', and 'Save & Apply'.

The screenshot shows the 'WEB SERVERS' configuration page for a CSL 9479-ET(G) WLAN AP/Bridge, specifically the 'HTTPS' configuration section. The layout is identical to the previous screenshot, but the 'Web server security level' is set to 'HTTPS (encrypted)' and the 'HTTPS TCP port number' is set to '443'. There is an additional section titled 'Upload a new HTTPS certificate' with a 'Choose file' button and the text 'No file chosen'. Below this, a note states: 'Must be a PEM file containing both the certificate and its unencrypted private key. A default low security self-signed certificate is used if you do not provide one'. The 'Reset', 'Save', and 'Save & Apply' buttons are at the bottom right.

These pages allow you to configure whether the web pages use HTTP or HTTPS. HTTPS offers a more secure encrypted option. If you choose to use HTTPS, you can upload a web certificate file. If you choose not to, it will default to a low security self-signed certificate but this may not be accepted by all browsers

**We strongly recommend the use of HTTPS so that the data between browser and 9479 is encrypted**

## 18 Firmware

The screenshot shows the web interface for the CSL 9479-ET(G) WLAN AP/Bridge. The top navigation bar includes 'SETUP', 'TOOLS', and 'STATUS'. The left sidebar lists menu items: 'FIRMWARE UPGRADE', 'PASSWORD SETTINGS', 'SYSTEM', 'NETWORK', 'SAVE CONFIG / RESET', and 'LOG SETTINGS'. The main content area is titled 'SYSTEM FIRMWARE UPGRADE'. It contains a description: 'The Firmware Upgrade section can be used to update to the latest firmware code to improve functionality and performance. Please select the firmware file, and click on upgrade button.' Below this, it says 'Please do not turn off the product's power supply or push the reset button before the upgrade completes.' There is a 'Firmware image:' label followed by a 'Choose file' button and the text 'No file chosen'. At the bottom right, there is an 'Upgrade' button with a green arrow icon.

This page allows you to upgrade the firmware in the unit. All previous configuration changes will be left unchanged.

## 19 Password

The screenshot shows the 'ROOT PASSWORD SETTINGS' section of the web interface. The top navigation bar and left sidebar are the same as in the previous screenshot. The main content area is titled 'ROOT PASSWORD SETTINGS' and includes the text: 'The password settings section can be used to change the product root password'. Below this, there are two input fields: 'password' and 'confirmation', each with a yellow key icon and a strength indicator (A ●). At the bottom right, there are 'Reset' and 'Submit' buttons.

The screenshot shows the 'USER PASSWORD SETTINGS' section of the web interface. The top navigation bar and left sidebar are the same as in the previous screenshots. The main content area is titled 'USER PASSWORD SETTINGS' and includes the text: 'The password settings section can be used to change the product user password'. Below this, there are two input fields: 'password' and 'confirmation', each with a yellow key icon and a strength indicator (A ●). At the bottom right, there are 'Reset' and 'Submit' buttons.

These Pages allow you to change the Password on both the Root and the user accounts.

**On initial power up, both passwords are set empty, this will allow you to enter the unit and configure the unit, as you require.**

**It is recommended that a strong password be set to prevent unauthorised access**

**CSL** 9479-ET(G) WLAN AP/Bridge

SETUP **TOOLS** STATUS

FIRMWARE UPGRADE  
PASSWORD SETTINGS  
**SYSTEM**  
NETWORK  
SAVE CONFIG / RESET  
LOG SETTINGS

**SYSTEM**

The time configuration option allows you to configure, update, and maintain the correct time on the internal system clock

**DEVICE LOCAL SETTINGS**

Host name: Acksys  
This device's name.  
Warning: This value can be changed by dhcp settings from dhcp server.

System time: 12/14/2019 10:25  
format MM/DD/YYYY hh:mm

Time zone: UTC

**MIB-2 SYSTEM SETTINGS**

Device location: User-definable  
this will appear in the MIB-2 'sysLocation' OID

**NETWORK TIMER SERVER**

server name: 0.europe.pool.ntp.org  
server port: 123

Reset Save & Apply

**Host Name:** This is a user definable Host Name for the device.

**System Time:** This is the current system time. Local time is lost on a reboot, use an NTP server if required


**Time Zone:** This allows you to set the time zone you are in.

**Device Location:** This is a user definable device location field.

**Server name:** If there is a NTP server reachable on the network, the unit can use it to configure its local time. You can use either an IP Address or the domain name, but the domain name requires configuring one or more DNS server addresses.

**Server Port:** This entry is for the port number of the NTP Server

## 21 System Log



9479-ET(G) WLAN AP/Bridge

SETUP TOOLS STATUS

DEVICE INFO  
NETWORK  
WIRELESS  
SERVICES  
LOGS  
SYSTEM LOG  
KERNEL LOG  
ROAMING LOG  
CONFIG LOG

SYSTEM LOG

Save logs to file

Sat Dec 14 10:00:07 2019 user.err kernel: [ 12.433084] block: unable to load configuration (fstab: Entry not found)  
Sat Dec 14 10:00:07 2019 user.err kernel: [ 12.440058] block: no usable configuration  
Sat Dec 14 10:00:07 2019 user.err kernel: [ 13.033787] block: unable to load configuration (fstab: Entry not found)  
Sat Dec 14 10:00:07 2019 user.err kernel: [ 13.040765] block: no usable configuration  
Sat Dec 14 10:00:12 2019 daemon.err block: /dev/ubi0\_2 is already mounted on /overlay  
Sat Dec 14 10:00:16 2019 daemon.err modprobe: xt\_multiport is already loaded  
Sat Dec 14 10:00:16 2019 daemon.err modprobe: xt\_connmark is already loaded  
Sat Dec 14 10:00:16 2019 daemon.err modprobe: xt\_comment is already loaded  
Sat Dec 14 10:00:16 2019 daemon.err modprobe: xt\_length is already loaded  
Sat Dec 14 10:00:19 2019 daemon.err modprobe: xt\_multiport is already loaded  
Sat Dec 14 10:00:19 2019 daemon.err modprobe: xt\_connmark is already loaded  
Sat Dec 14 10:00:19 2019 daemon.err modprobe: xt\_comment is already loaded  
Sat Dec 14 10:00:19 2019 daemon.err modprobe: xt\_length is already loaded  
Sat Dec 14 10:00:20 2019 daemon.crit netifd: cannot read /sys/class/net/br-lan/bridge/group\_fwd\_mask, using 0 instead  
Sat Dec 14 10:00:22 2019 daemon.err uhttpd[2324]: socket(): Address family not supported by protocol  
Sat Dec 14 10:00:29 2019 user.err acksys\_event\_handler: acksys-status: hostapd connect failed  
Sat Dec 14 10:00:29 2019 user.err acksys\_event\_handler: acksys-status: hostapd connect failed  
Sat Dec 14 10:00:29 2019 user.err acksys\_event\_handler: acksys-status: hostapd connect failed  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: MIB search path: //.snmp/mibs:/usr/share/snmp/mibs  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (NET-SNMP-EXTEND-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (SNMPv2-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (IF-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (IP-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (TCP-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (UDP-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (HOST-RESOURCES-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (NOTIFICATION-LOG-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (DISMAN-EVENT-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (DISMAN-SCHEDULE-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (SNMP-VIEW-BASED-ACM-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (SNMP-COMMUNITY-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (SNMP-FRAMEWORK-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (SNMP-MPD-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (SNMP-USER-BASED-SH-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (TUNNEL-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (IPV6-FLOW-LABEL-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (UCD-DLMOD-MIB): At line 0 in (none)  
Sat Dec 14 10:00:33 2019 daemon.err snmpd[3140]: Cannot find module (NET-SNMP-PASS-MIB): At line 0 in (none)  
Sat Dec 14 10:00:34 2019 daemon.err snmpd[3140]: NET-SNMP version 5.8  
Sat Dec 14 10:00:36 2019 daemon.err snmpd[3140]: No pgpgin line in /proc/vmstat  
Sat Dec 14 10:00:36 2019 daemon.err snmpd[3140]: No pgpgout line in /proc/vmstat  
Sat Dec 14 10:00:36 2019 daemon.err snmpd[3140]: No psupin line in /proc/vmstat  
Sat Dec 14 10:00:36 2019 daemon.err snmpd[3140]: No psupout line in /proc/vmstat  
Sat Dec 14 10:10:36 2019 daemon.err uhttpd[2324]: WebUI: accepted login on /status/interface for root from 192.168.4

This panel allows for the visualization of the units logs.

**Config Log:** This log displays a summary of the units configuration

**Kernel Log:** This log displays messages from the Linux kernel only.

**System Log:** This log displays messages from both the kernel and from the running services. The messages in this log are limited to the importance levels configured in the Log Settings page.

SETUP

TOOLS

STATUS

FIRMWARE UPGRADE

PASSWORD SETTINGS

SYSTEM

NETWORK

SAVE CONFIG / RESET

LOG SETTINGS

### LOG SETTINGS

You can configure the log parameters on this page.

**General settings:**  
This section is about configuring the system log, which filters and and dispatches the log messages to the user. The "System Log Output Level" acts as a final filter for the log messages from various components. Set it to the highest level you want to see from any component. So, please make sure the system log output level is high enough to display all required messages.

**Wireless log settings:**  
These sections configure wireless logging for access points and clients. The messages are sent to the system log.

**VRRP service log settings:**  
This section configures logging of VRRP activities. Messages are sent to the system log.

#### GENERAL SETTINGS

System Log Output Level

Error

System Log Buffer Size

16

KiB

External System Log Server

0.0.0.0

External System Log Server Port

514

#### WIRELESS ACCESS POINT LOG SETTINGS (WIFI)

Wireless Log Level

Info

#### VRRP SERVICE LOG SETTINGS

VRRP log level

Error

#### OPENVPN SERVERS LOG SETTINGS

	NAME	MODE	VERBOSITY LEVEL
VPN1	vpn1		Errors
VPN2	vpn2		Errors

Reset

Save & Apply

This is the log settings page, it allows you to configure the system logs.

**Systems Log Out Level:** This sets the minimum level of a message to allow its insertion in the system log.

**External System Log server and port:** Optional remote log server configuration. IP Address and UDP port where the log messages will be sent using the syslog protocol. Leave empty to disable.

**Log Settings:** These sections are used to configure logging for various services, the messages are sent to the system log if their seriousness is above the configured level. The messages go through two rounds of filtering: once in the specific service and one in the syslog service. Please make sure the system log output level is high enough to display all required messages.



## 22 Network Utilities

The screenshot shows the web interface for the 9479-ET(G) WLAN AP/Bridge. The top navigation bar includes 'SETUP', 'TOOLS', and 'STATUS'. The left sidebar lists various settings: 'FIRMWARE UPGRADE', 'PASSWORD SETTINGS', 'SYSTEM', 'NETWORK', 'SAVE CONFIG / RESET', and 'LOG SETTINGS'. The main content area is titled 'NETWORK UTILITIES' and contains two sections: 'LINK DIAGNOSTIC' and 'BANDWIDTH TEST'. The 'LINK DIAGNOSTIC' section has two input fields, both containing 'www.example.com', with 'Ping' and 'Traceroute' buttons below them. The 'BANDWIDTH TEST' section features a table with columns for 'MODE', 'PROTOCOL', 'DELAY (S)', and 'DISPLAY (S)'. The 'MODE' dropdown is set to 'Server' and 'PROTOCOL' is set to 'TCP'. A 'Run Test' button is located below the table.

MODE	PROTOCOL	DELAY (S)	DISPLAY (S)
Server	TCP		1

This panel provides two standard UNIX tools: ping and traceroute. Place the argument in the text field above the corresponding button and then click the button. The results will be displayed in a frame below.

## 23 Save Config / Reset

The screenshot shows the web interface for the 9479-ET(G) WLAN AP/Bridge, specifically the 'CONFIGURATION MANAGEMENT' section. The top navigation bar includes 'SETUP', 'TOOLS', and 'STATUS'. The left sidebar lists various settings: 'FIRMWARE UPGRADE', 'PASSWORD SETTINGS', 'SYSTEM', 'NETWORK', 'SAVE CONFIG / RESET', and 'LOG SETTINGS'. The main content area is titled 'CONFIGURATION MANAGEMENT' and contains two sections: 'SAVE AND RESTORE CONFIGURATION' and 'RESET AND REBOOT'. The 'SAVE AND RESTORE CONFIGURATION' section has a 'Configuration file' input field with a 'Choose file' button and a 'No file chosen' status. Below this are 'Restore configuration from file' and 'Backup settings to file' buttons, each with a corresponding 'Restore' or 'Backup' button. The 'RESET AND REBOOT' section has 'Reset to factory settings' and 'Reboot your device' buttons, each with a corresponding 'Reset' or 'Reboot' button.

The Save and restore configuration section allows you to backup the units current settings to a file. You are then able to restore the previously saved file, back into the unit. This will load up all of its previous settings

**Reset:** Clicking this button will restore its factory default settings. There is also a hardware push button that can be accessed through the small hole in front panel near the LEDs, its operation is as follows -

- Short push, anytime (Reboot)
- Long push (>2secs)
  - while operating (Restore factory defaults)
  - while in Emergency Upgrade mode (Restore factory settings)
  - at startup (Enter Emergency Upgrade mode)

**Reboot:** Click this button to reboot the unit

**This page is left intentionally blank**

## AUSTRALIA

Eaton Electrical (Australia) Pty Ltd,  
10 Kent Road, Mascot, New South Wales, 2020, Australia  
Tel: +61 1300 308 374 Fax: +61 1300 308 463  
E-mail: mtl@salesanz@eaton.com

## BeNeLux

MTL Instruments BV  
Ambacht 6, 5301 KW Zaltbommel  
The Netherlands  
Tel: +31 (0) 418 570290 Fax: +31 (0) 418 541044  
E-mail: mtl.benelux@eaton.com

## CHINA

Cooper Electric (Shanghai) Co. Ltd  
955 Shengli Road, Heqing Industrial Park  
Pudong New Area, Shanghai 201201  
Tel: +86 21 2899 3817 Fax: +86 21 2899 3992  
E-mail: mtl-cn@eaton.com

## FRANCE

MTL Instruments sarl,  
7 rue des Rosieristes, 69410 Champagne au Mont d'Or  
France  
Tel: +33 (0)4 37 46 16 53 Fax: +33 (0)4 37 46 17 20  
E-mail: mtlfrance@eaton.com

## GERMANY

MTL Instruments GmbH,  
Heinrich-Hertz-Str. 12, 50170 Kerpen, Germany  
Tel: +49 (0)22 73 98 12-0 Fax: +49 (0)22 73 98 12-2 00  
E-mail: csckerpen@eaton.com

## INDIA

MTL India,  
No.36, Nehru Street, Off Old Mahabalipuram Road  
Sholinganallur, Chennai- 600 119, India  
Tel: +91 (0) 44 24501660 /24501857 Fax: +91 (0) 44 24501463  
E-mail: mtlindiasales@eaton.com

## ITALY

MTL Italia srl,  
Via San Bovio, 3, 20090 Segrate, Milano, Italy  
Tel: +39 02 959501 Fax: +39 02 95950759  
E-mail: chmninfo@eaton.com

## JAPAN

Cooper Industries Japan K.K.  
MT Building 3F, 2-7-5 Shiba Diamon, Minato-ku  
Tokyo, Japan 102-0012  
Tel: +81 (0)3 6430 3128 Fax: +81 (0)3 6430 3129  
E-mail: mtl-jp@eaton.com

## NORWAY

Norex AS  
Fekjan 7c, Postboks 147,  
N-1378 Nesbru, Norway  
Tel: +47 66 77 43 80 Fax: +47 66 84 55 33  
E-mail: info@norex.no

## RUSSIA

Cooper Industries Russia LLC  
Elektrozavodskaya Str 33  
Building 4  
Moscow 107076, Russia  
Tel: +7 (495) 981 3770 Fax: +7 (495) 981 3771  
E-mail: mtlrussia@eaton.com

## SINGAPORE

Eaton Electric (Singapore) Pte Ltd  
100G Pasir Panjang Road  
Interlocal Centre  
#07-08 Singapore 118523  
#02-09 to #02-12 (Warehouse and Workshop)  
Tel: +65 6 645 9888 ext 9864/9865  
Fax: 65 6 645 9811  
E-mail: sales.mtl@eaton.com

## SOUTH KOREA

Cooper Crouse-Hinds Korea  
7F. Parkland Building 237-11 Nonhyun-dong Gangnam-gu,  
Seoul 135-546, South Korea.  
Tel: +82 6380 4805 Fax: +82 6380 4839  
E-mail: mtl-korea@eaton.com

## UNITED ARAB EMIRATES

Cooper Industries/Eaton Corporation  
Office 205/206, 2nd Floor SJ Towers, off. Old Airport Road,  
Abu Dhabi, United Arab Emirates  
Tel: +971 2 44 66 840 Fax: +971 2 44 66 841  
E-mail: mtlgulf@eaton.com

## UNITED KINGDOM

Eaton Electric Limited,  
Great Marlings, Butterfield, Luton  
Beds LU2 8DL  
Tel: +44 (0)1582 723633 Fax: +44 (0)1582 422283  
E-mail: mtl@enquiry@eaton.com

## AMERICAS

Cooper Crouse-Hinds MTL Inc.  
3413 N. Sam Houston Parkway W.  
Suite 200, Houston TX 77086, USA  
Tel: +1 800-835-7075 Fax: +1 866-298-2468  
E-mail: mtl-us-info@eaton.com