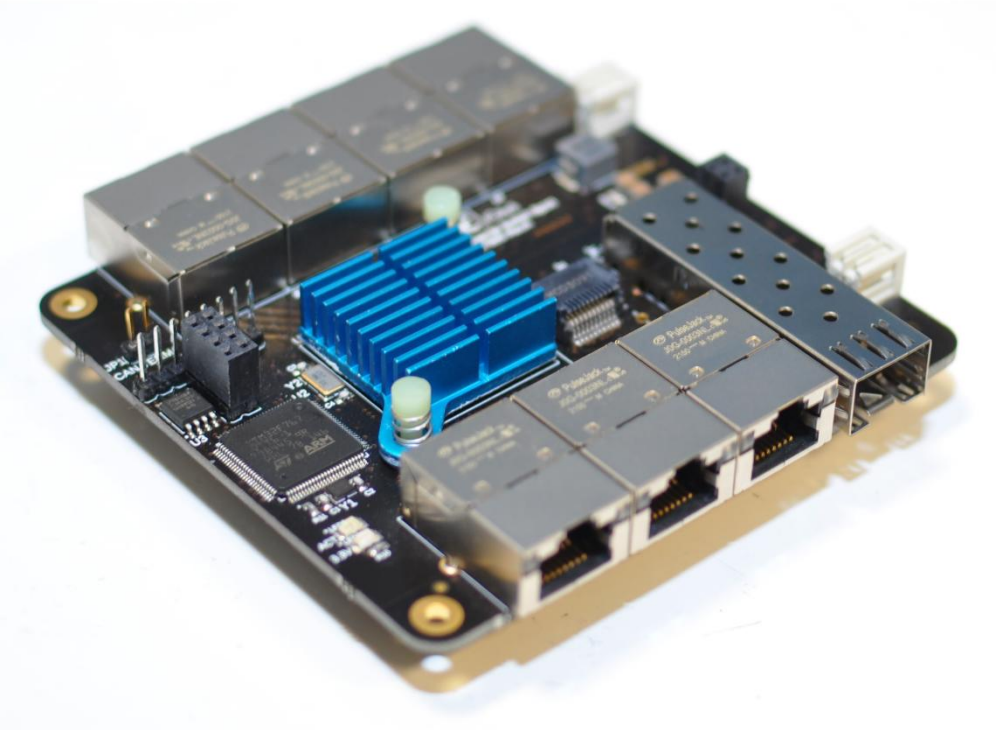
USER MANUAL



8-PORT ETHERNET SWITCH

REVISION D

REVISIONS

PUBLISHED	REVISION	NOTES	REVISED BY
27.05.2025	D	Updated template, reworked structure, added Functional description	OMH
14.08.2024	C	Changed type ID to new	FTO
05.10.2023	B	Added default values	VHA
30.05.2023	A	Issued for release	VHA

CONTENT

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

This document outlines and defines the installation, operation, and maintenance procedures for the Ixys Ethernet Switch PCB. The manual will contain all relevant data and methods to be able to use and maintain the device for its intended purpose.

The manual includes technical specifications, installation information, description of the various switch features, as well as troubleshooting suggestions.

1.2 ABBREVIATIONS

ABBREVIATION	DESCRIPTION
DHCP	Dynamic Host Configuration Protocol
ESD	Electrostatic Discharge
IP	Internet Protocol
UDP	User Datagram Protocol
PCB	Printed Circuit Boards
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network

1.3 SUPPLIER CONTACT INFORMATION

Ixys AS
Langmyra 11
4344 Bryne
Norway

+47 51 42 22 22
post@ixys.no
https://ixys.no

1.4 DOCUMENT REFERENCES

DOCUMENT NUMBER	DESCRIPTION
117995-ICS-PD-DAS-0001	Datasheet
ICS-SW-PRT-0005	Register list expansion PCBs

See ixys.no for the latest revisions of these documents.

2 HEALTH, SAFETY AND ENVIRONMENT

2.1 GENERAL

Safety Notes and General Precautions shall be presented to all personnel concerned prior to testing, operation, maintenance, and repair. The operations shall be performed by the responsible engineer/supervisor. The personnel using this equipment must have knowledge of this type of equipment and have familiarized themselves with the applicable procedures and manuals for this product.

2.2 SAFETY MESSAGE LEVELS

Safety message level		Indication
	**DANGER:**	A hazardous situation which, if not avoided, will result in death or serious injury
	**WARNING:**	A hazardous situation which, if not avoided, could result in death or serious injury
	**CAUTION:**	A hazardous situation which, if not avoided, could result in minor or moderate injury or damage to equipment
	**Electrical Hazard:**	The possibility of electrical risks if instructions are not followed in a proper manner
Note:		A potential situation which, if not avoided, could result in an undesirable result or state. A practice not related to personal injury

3 TECHNICAL INFORMATION AND DATA

3.1 TECHNICAL DESCRIPTION

The Ethernet Switch is a PCB with 8 ports for connecting multiple network devices together. The PCB optionally has 1 or 2 SFP slots, which can be used with optical fibers for long-distance high-speed communication (up to 2.5 Gbps).

The switch is capable of being an Ixys Control System (CS) master, stacked physically together with any boards from the Ixys CS range to form a complete control system for any application.

All data is available over Modbus and FINS for usage from VJU or other systems, and all features of the switch can be configured through a user-friendly web-interface. The board has built-in monitoring of supply voltage, ambient temperature, switch core temperature and water detection.

3.2 TECHNICAL DATA

Manufacturer	Ixys AS
Ixys part number	117996 / 117997 / 117998
Description	PCB CS Ethernet Switch 8-port
Weight	~ 120 g
Dimensions	96 x 90 x 13 mm (PC/104 format)
Supply voltage	8-30 V DC
Power consumption	< 3 W
Copper ports	10/100/1000 Mbps
Fiber ports	Up to 2.5 Gbps

3.3 WARRANTY CONDITIONS AND GUARANTEE

- Improper use of equipment where use is not reflected in what it was intended to.
- Where general maintenance is not performed leading to defective parts or other types of defects.
- Incorrect handling or use of equipment.
- Packing not carried out in an ESD protective way.

3.4 ORDERING

Ixys Part Number	Description
117996	PCB CS Ethernet Switch 8-port
117997	PCB CS Ethernet Switch 8-port with SFP
117998	PCB CS Ethernet Switch 8-port with Dual SFP

3.5 ACCESSORIES

Ixys Part Number	Description
100040	Connector – 2-way cable contact Wago 733-102
107847	SFP 1 Gbps single-fiber TX 1310 nm RX 1550 nm
109060	SFP 1 Gbps single-fiber TX 1550 nm RX 1310 nm
118780	SFP 2.5 Gbps single-fiber TX 1490 nm RX 1550 nm
118781	SFP 2.5 Gbps single-fiber TX 1550 nm RX 1490 nm

4 HARDWARE DESCRIPTION

4.1 DRAWING

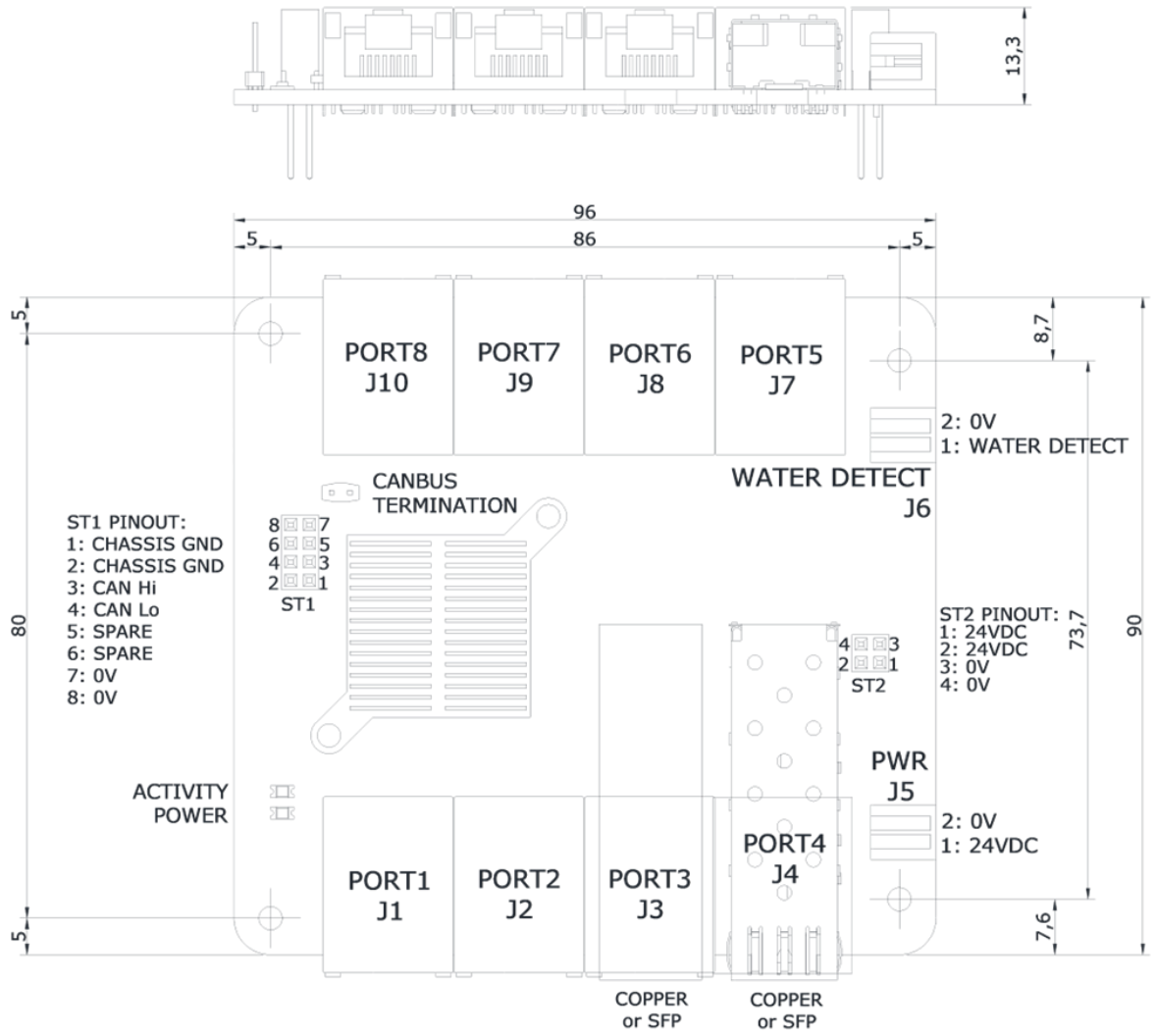


Figure 1 - Dimensions and pinout

4.2 LEDS

The POWER LED will light up as soon as the board is powered correctly. The ACTIVITY LED will blink once per second when the application is running correctly.

Each copper port has two LEDs. The green LED is a combined link/activity LED. When it's lit, a link has been established on this port, and blinking indicates acitivy on this port. The yellow LED is lit when the port is connected to a 1000 Mbps device.

Each SFP has a LED on the underside of the PCB, indicating whether fiber link has been established.

4.3 CONNECTIONS

The switch should be powered by connecting supply voltage on J5.

J6 is usable for water detection. If pin 1 of J6 is shorted to pin 2, the switch will detect this, and indicate it as described in section 6.2.

Any Ixys CS PCB can be stacked underneath or on top of this PCB through ST1 and ST2 headers. If the switch is used as a stack master, jumper JP1 must be installed to terminate the internal CAN bus.

Note: If the switch is used as a stack master, it's recommended to solder the ST1 and ST2 connectors to ensure connectivity in high-vibration scenarios.

See chapter 5.3 for details on the stack master functionality.

5 FUNCTIONAL DESCRIPTION

5.1 GENERAL

By default, this product works as a normal Ethernet switch, connecting all ports together. The following sections describe all additional features available.

The switch has a water detect input, which can be used to indicate water intrusion. It also includes temperature and supply voltage measurement. See section 6.2 for details on how to read out these values.

The default IP of the switch is 10.0.37.239/24.

5.1.1 WEB INTERFACE

All features of the switch can be configured from a user-friendly web interface. The web interface is accessible by opening the switch's IP address in any modern browser.

The About page shows the switch's firmware version, serial number and hardware revision. It's also possible to perform a Factory reset to return all settings to default, and to reboot the switch.

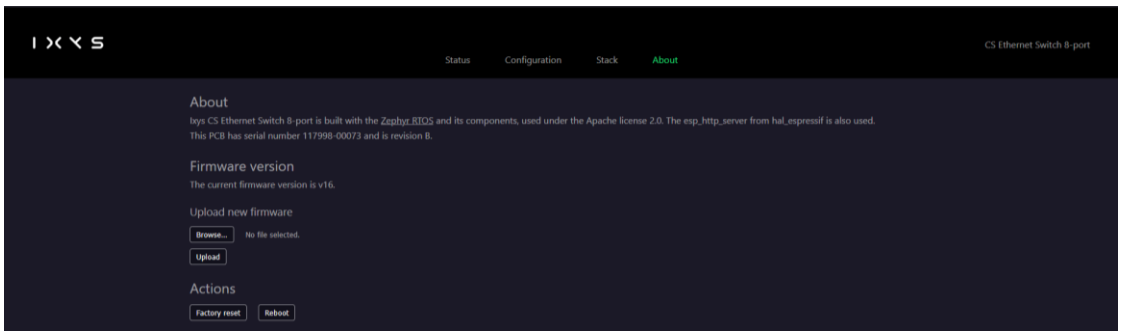


Figure 2 About page

The Status page shows the current state of all network ports, supply voltage, water detect input, data transfer counters and more.

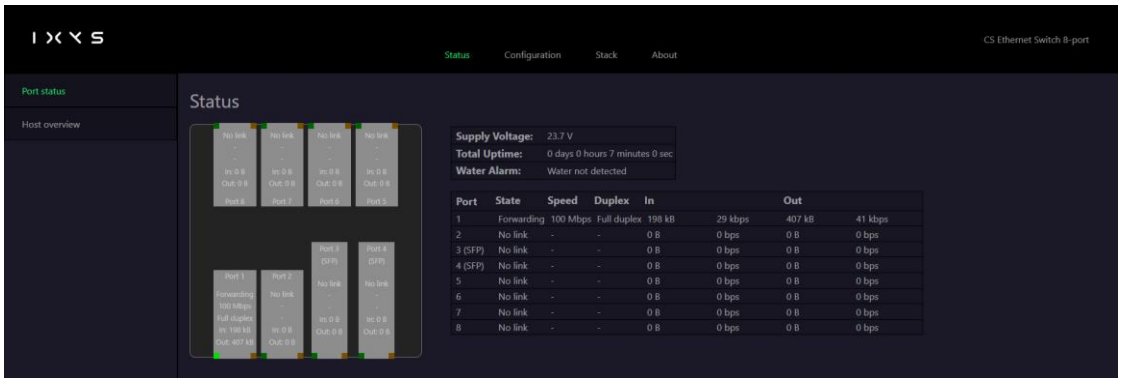


Figure 3 Status page

All configuration is available on the Configuration tab, including the ability to change the switch's IP address.

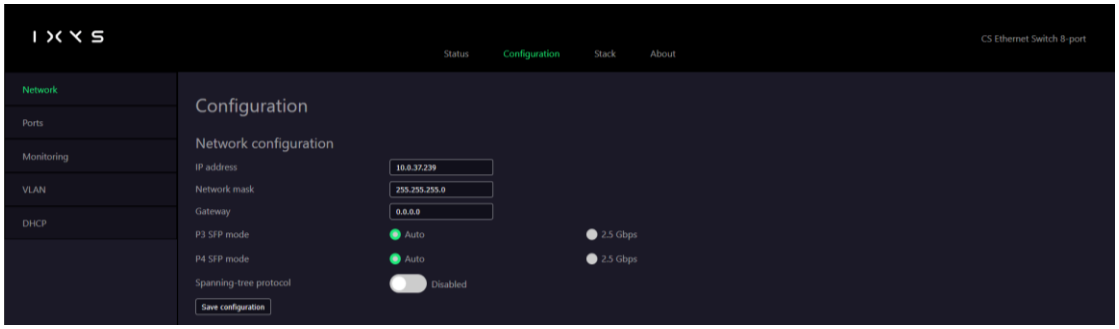


Figure 4 Basic configuration

5.1.2 COMMUNICATION FAILURE

When used as part of a control system, it is usually expected that another device in the system will write desired output states to the switch periodically. Should such writes not happen for a given period, this often indicates a system problem.

The switch therefore monitors writes, and can be configured to set all outputs to pre-defined states if no further writes occur a given period. This period is called the Communication Failure timeout, and can be set from the web interface, or in a Modbus register.

By default, the switch is set up to leave all outputs as-is when the Communication Failure timeout triggers. For each output, there are two settings that can be configured: enable or disable communication failure feature, and communication failure value.

If communication failure is enabled for an output, the switch will set the output to the communication failure value on timeout. If communication failure is disabled for an output, the output will be left with the current value on timeout.

Communication Failure can be enabled or disabled per output both through registers as described in section 0, and in the web interface, in the Stack section.

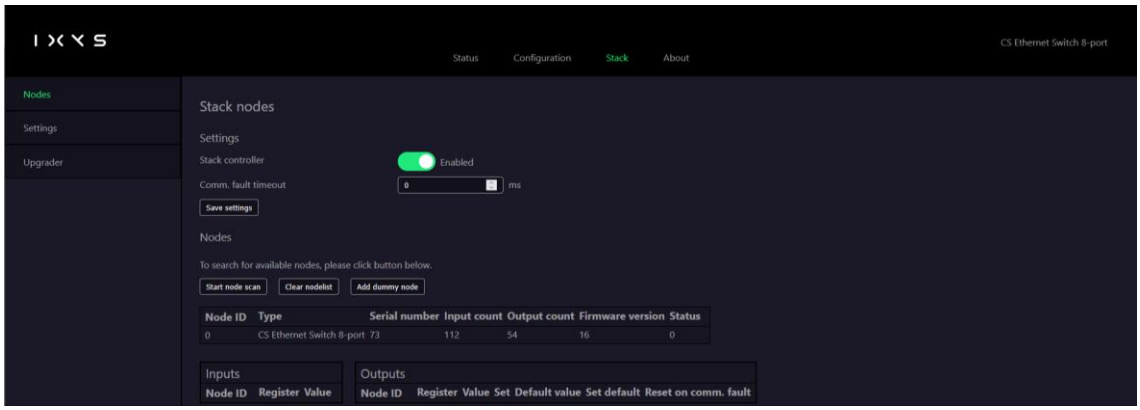


Figure 5 Setting up communication failure feature

5.1.3 HEARTBEAT BROADCAST

Every 5 seconds, the device sends a UTF-8 encoded JSON object in a UDP packet to the broadcast IP 255.255.255.255 on port 65000. This message includes the device's IP address, firmware version, serial number, and allows easy identification.

Ixys VJU Studio software will use this to automatically identify the device, but it can also be found manually for instance with Wireshark, or by other applications.

5.1.4 MODBUS TCP/UDP

The switch supports the Modbus protocol over TCP and UDP for reading and writing all registers described in section 6.

All registers are readable with Function Code Read Holding Registers and Read Input Registers. All registers are writable with both Write Single Register and Write Multiple Registers.

5.1.5 FINS

The switch supports Omron's FINS protocol for reading and writing all registers described in section 6.

5.1.6 FIRMWARE UPGRADE

Firmware upgrades will be made available on an ongoing basis on ixys.no. Upgrades are provided as a zip archive of an updater-application. The updater application will upgrade both the actual firmware and the included web interface.

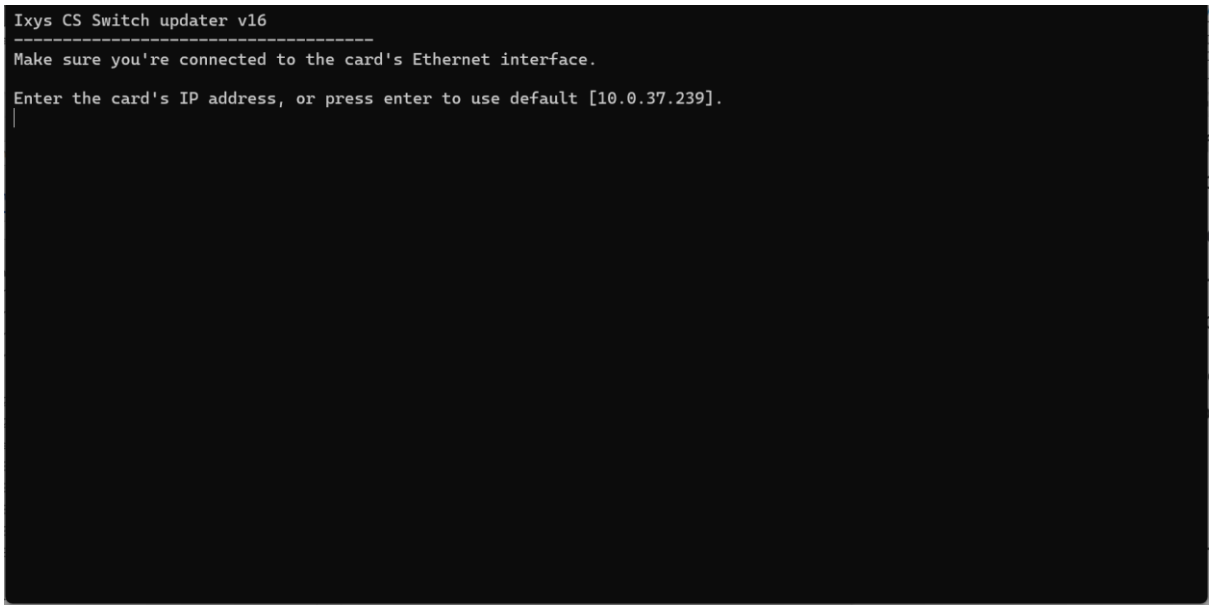


Figure 6 Switch updater application

After an upload has been completed, the switch should be kept powered for a couple of minutes to allow the upgrade to finalize.

5.2 NETWORKING FUNCTIONS

5.2.1 PORT CONFIGURATION

By default, all network ports are set up with auto-negotiation, advertising 10/100/1000 Mbps. For each port, it's possible to limit the modes that port will advertise, for instance if there are cable or equipment limitations. If two-pair cables are used, it is important not to advertise 1000 Mbps, since this speed requires a four-pair cable.

Port speed and duplex mode can be set to fixed values for each port. Beware that forcing 1000 Mbps is not possible. Also avoid using fixed speed on a port connected to equipment in auto-negotiate mode, as that will cause a duplex mismatch, and give performance issues.

It's also possible to disable a port temporarily, for instance for isolating a network segment.

Note: Port disabling is not saved, and after a power-cycle all ports are always enabled.

Changing egress mode allows you to prevent multicast and/or broadcast data to be sent to ports that don't need it. This can be useful to avoid overwhelming old or slow devices with data they don't care about.

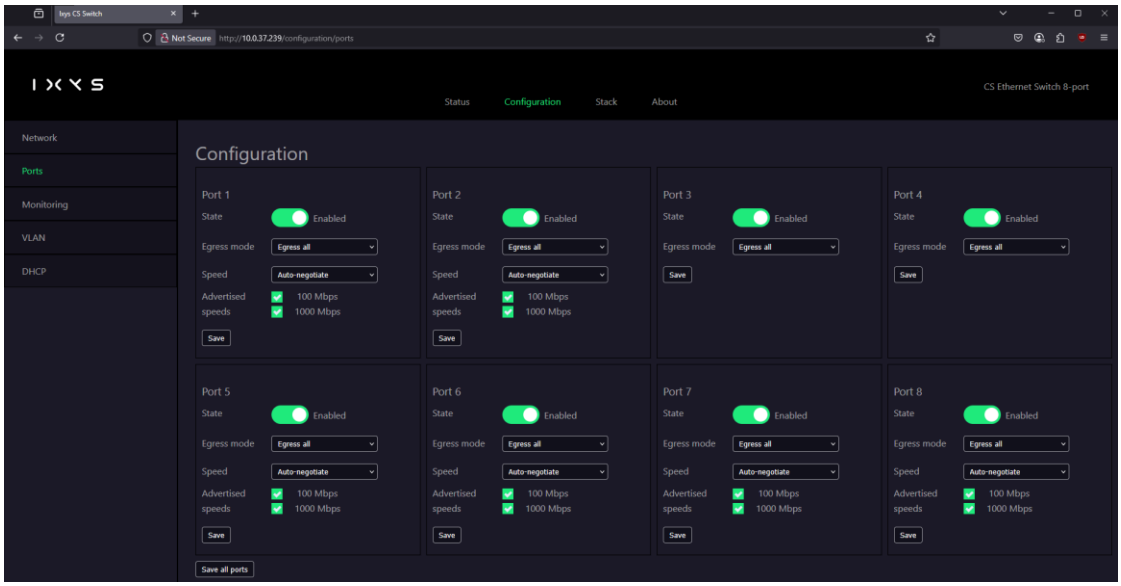


Figure 7 Port settings

5.2.2 SFPS

The switch is available in variants that supports one or two SFPs in addition to copper ports. SFPs can be used to communicate over fiberoptic cables instead of copper, which enabled longer range, and optionally higher bandwidth.

It's possible to use both two- and single-fiber SFPs. When using two-fiber SFPs, the same SFP can be used in both ends of the link, but will need to cross the fibers. When using a single-fiber SFP, it's required to use different SFPs in each end, so that one SFP will transmit on the wavelength the other SFP will receive on and vice-versa.

Beware that 2.5 Gbps SFPs requires manual configuration, by enabling the 2.5 Gbps mode in the web interface, under Configuration and Network.

It's possible to read out additional status data from SFPs, both in the web interface, and in Modbus registers, for instance signal strength, transmission and receive wavelengths, temperature and more.

5.2.3 VIRTUAL LANS (VLANS)

Virtual LANs is a feature that enables isolating network traffic. Traffic on different VLANs is treated separately, and devices on VLAN A will not be able to connect to or see traffic from devices in VLAN B.

VLANs in an Ixys switch is set up with a name and an ID. The ID is compatible with network equipment from other vendors, so a VLAN ID configured on an Ixys switch can be used on equipment from other vendors as well.

On a given network port, there can be either Untagged or Tagged VLAN traffic. One port can have a single Untagged VLAN, but can have multiple Tagged VLANs. A non-VLAN aware device connected to a network port will see only the Untagged VLAN. Only equipment that supports VLANs will see Tagged VLAN traffic.

In multi-switch setups it's likely desirable to send multiple VLANs Tagged on any switch-to-switch connections, but to have different VLANs Untagged on the different ports. This can for instance allow isolating video traffic from other equipment, or isolate equipment from different vendors.

By default, all ports are Untagged members of VLAN ID 1. This means that devices that are connected to these ports will see all traffic from VLAN ID 1 with no further configuration.

The web interface is available only on VLAN ID 1, so it's important to ensure that at least one port is a member of this VLAN to keep the ability to configure the switch itself.

VLANs can be configured on a separate page on the Configuration tab in the web interface.

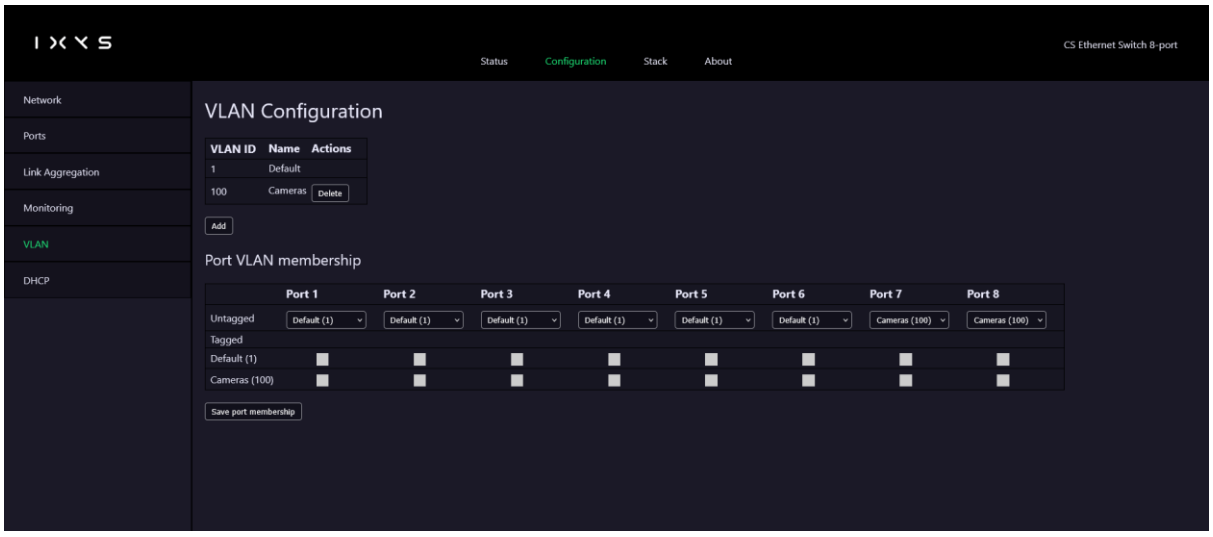


Figure 8 VLAN configuration

5.2.4 LINK AGGREGATION

By using Link aggregation, two or more network links can be used together as one link. This can be used to connect two switches with multiple cables, either fiber or copper, and in that way get double bandwidth between them, as well as redundancy – if one cable is lost, connectivity will be kept using the remaining one.

Link aggregation is configured by adding a Link Aggregation group with an ID, and then adding any number of ports to that group. Those ports can then all be connected to the same number of ports on another switch.

Beware that Link aggregation must be set up on both switches for it to work correctly.

This is often a simpler way to achieve redundancy in smaller systems than using STP, as it doesn't incur any increase in startup time, or any change in behavior when the network topology changes or links go up or down.

Link Aggregation can be configured on a separate page on the Configuration tab in the web interface.

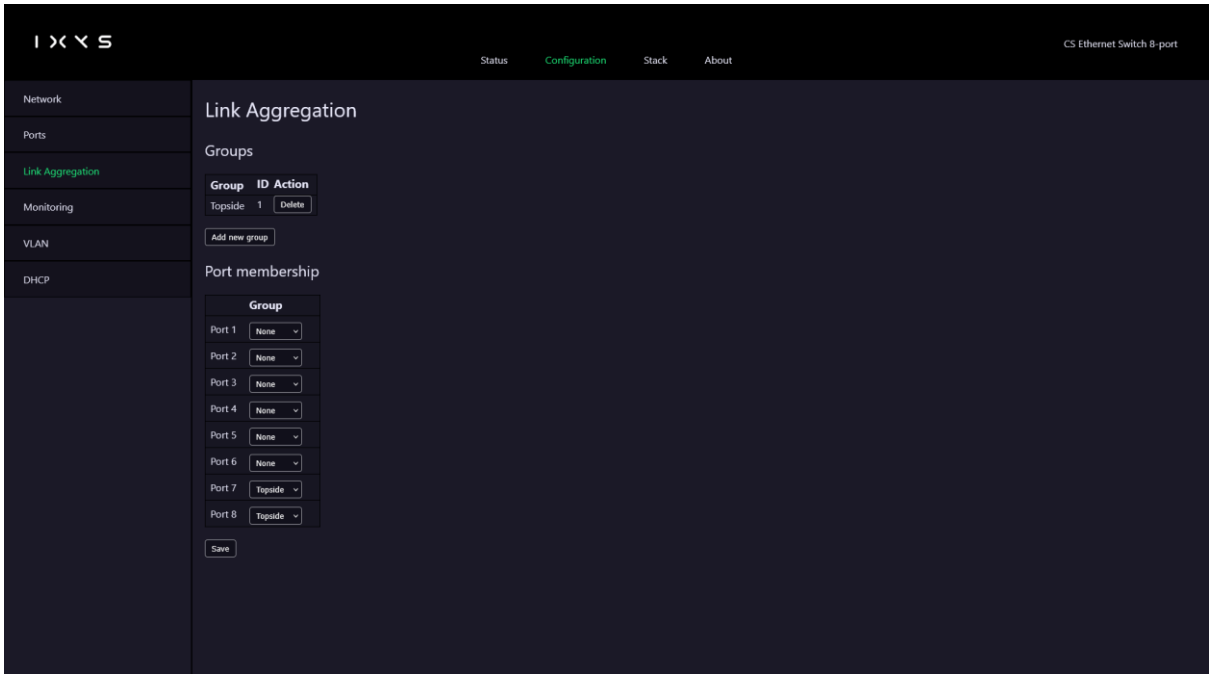


Figure 9 Link Aggregation configuration

5.2.5 SPANNING TREE PROTOCOL

It's possible to enable support for the Spanning Tree Protocol (STP) in the switch. This can be useful in cases where there are loops in the network topology, for instance to support redundancy.

STP is a standardized protocol, and if it is enabled, the switch will participate in any ongoing negotiation to find the root bridge.

Beware that enabling STP will cause the switch to take additional time before passing through data after startup, since the negotiation processes need to complete before normal data flow can start.

STP can be enabled on the Network page under Configuration.

5.2.6 HOST OVERVIEW

The switch keeps track of the MAC address of all devices that have communicated with it. This overview allows seeing what MAC address is connected to which physical port on the switch, and can be very useful to ensure configuration is applied to the correct port, and for debugging.

The Host overview is available under the Status tab in the web interface.

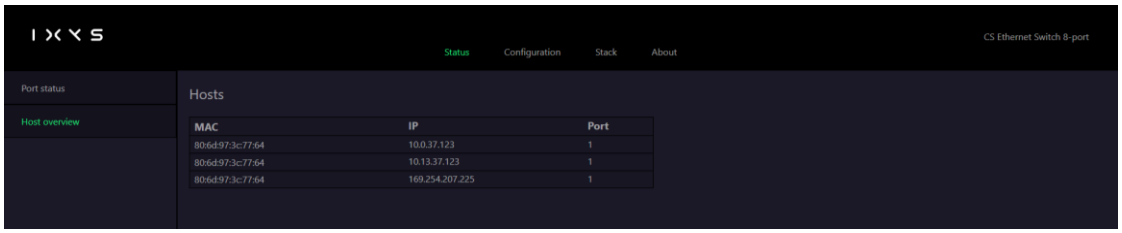


Figure 10 Host overview

5.2.7 DHCP SERVER FUNCTION

A DHCP server is a server that gives out IP addresses to other equipment, so that IPs don't always have to be set statically. DHCP serving functionality is built into the switch. If enabled, IPs are assigned from a pool of addresses, but specific IPs can be reserved per port, so that any DHCP client connecting to a certain port would get a specific IP address. This can be useful to ensure that spare equipment once put in use gets the same configuration as the equipment it is replacing.

The DHCP server can be enabled or disabled, and the start address for the pool can be set. The server uses a pool of 32 addresses. It's further possible to assign a specific IP, either inside or outside the pool, to each port of the network switch.

For DHCP server functionality to be effective, clients connected must also have a DHCP client enabled. DHCP server configuration is available on the DHCP page on the Configuration tab.

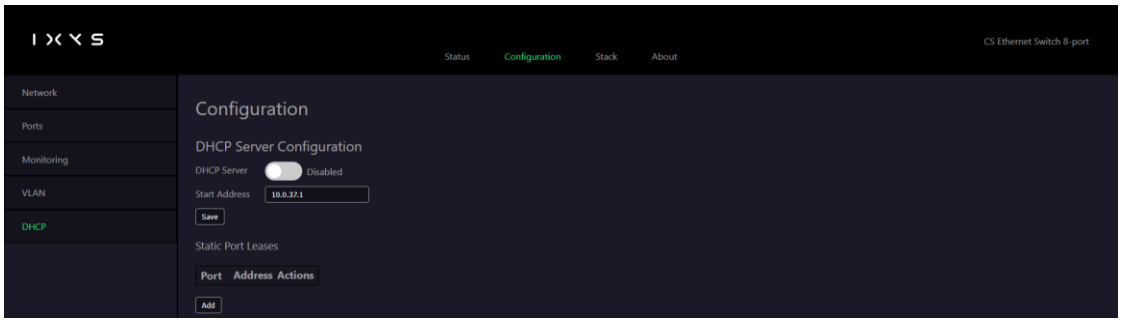


Figure 11 DHCP server configuration

5.2.8 MONITORING FUNCTION

When debugging or investigating systems, it is sometimes useful to see other devices' network traffic. A switch tries to not data only to devices that need it, so it's not normally possible for a client connected to port A to see traffic flowing between ports B and C. Port monitoring changes this.

It's possible to set a given port as the monitoring port, and then to select which other ports ingress or egress traffic should be monitored. When this feature is enabled, the switch will make a copy of all frames coming in (ingress) or going out of the port (egress) being monitored, and send that copy out on the monitoring port. To see all data between two devices, it's possible to enable monitoring of ingress on the ports where the two devices are connected, and then designate the investigators device's port as the monitoring port.

The device connected to the monitoring port can then use a network monitoring application, for instance Wireshark, to investigate the traffic between the other two devices.

Port monitoring is not saved across reboots, and defaults to off. It can be configured on the Port monitoring page on the Configuration tab.

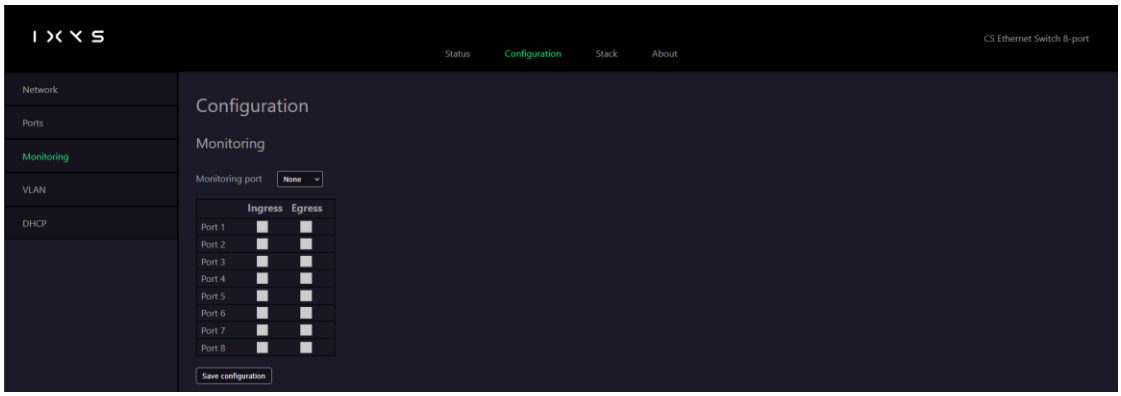


Figure 12 Port monitoring configuration

5.3 STACK MASTER FUNCTION

5.3.1 GENERAL

It's possible to use the Ethernet switch as the master device of an Ixys Control System stack. This makes it possible to build a system of multiple CS PCBs in a stack, which uses the stack headers for communication and power between them. All inputs and outputs of the stack is usable over network via the Ethernet switch.

The stacked PCBs use an internal CAN bus for communication, and it's important to terminate this bus. When the switch is used as a stack master, the CAN bus jumper should therefore be installed. See section 4.3.

Each CS PCB has a number of outputs, inputs and settings available, making it possible to build a control system for almost any application. Multiple PCBs of the same type can be used in a stack, to get the desired features. See the product list on ixys.no for details on available PCBs.

All stack outputs can be used with the communication failure feature, described in section 5.1.2, and the communication failure timeout should be set according to the system requirements.

The main stack functionality is available on the Nodes page on the Stack tab of the web interface.

5.3.2 NODE SCAN

For the stack functionality to function, the Ethernet switch needs to know which PCBs are stacked underneath it. This is determined when a node scan is performed.

When the node scan is done, the switch will establish communication with all stacked PCBs, and add them to its list of stack nodes. This list is shown both in the web interface and in Modbus registers (see section 6.5). A node scan ends when there no further PCBs are found.

Each PCB in a stack must have a unique node ID, which is typically set by adjusting a physical wheel on the PCB when assembling the stack. If duplicate IDs are discovered during a node scan, an error will be shown in the web interface, and Modbus registers for node ID 19 populated with data for the duplicate node.

Should a stack node stop communicating after having been identified during a node scan, its serial number will be shown as 0.

It's possible to clear the node list manually, without performing a new node scan.

Note: If having multiple Ethernet Switches on top of a stack, it's important to perform a node scan on only one of the switches, since there can only be a single stack master. If a node scan is performed on both switches, the node list must be cleared on the one that is not supposed to be the master.

5.3.3 INPUTS AND OUTPUTS

The number and type of inputs and outputs available in a CS stack is dependent on the type and number of PCBs stacked. The number of inputs and outputs for each scanned stack node can be viewed in the web interface and in the stack node information registers (see section 6.5), and the document ICS-SW-PRT-0005 explains what the inputs and outputs values represent.

Stack node inputs and outputs have designated sections in the register list of the Ethernet switch. Inputs and outputs are sorted by node ID, so the inputs for node ID 1 will come before inputs for node ID 2 and so on. For example, if node ID 1 has 8 inputs, inputs for node ID 2 will start at the register 130 (base stack node input register is 122, plus 8).

The web interface shows live data for all inputs and outputs. For each output, it's also possible to set the current value, as well as controlling the communication failure behavior and value.

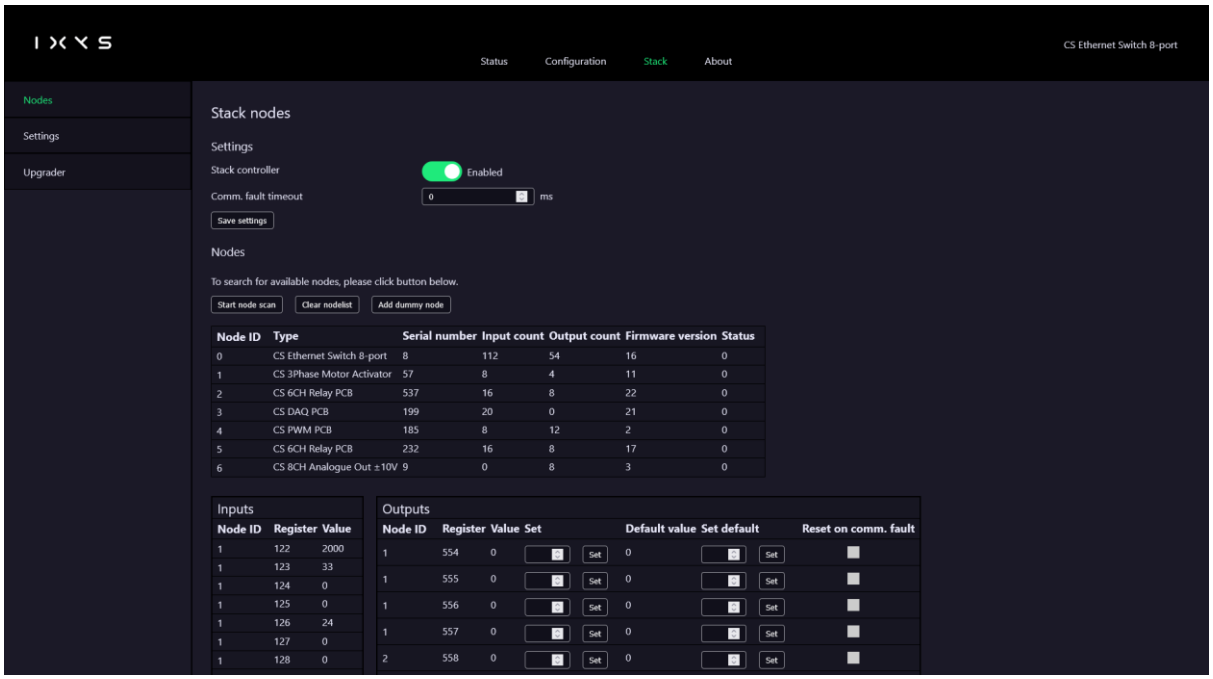


Figure 13 Stack configuration

5.3.4 DUMMY NODES

Since the exact address of a given stack node's registers is dependent on what other nodes are in the stack, it can occasionally be useful to add dummy nodes to a stack. This can be used to achieve a consistent register structure across stacks which don't necessarily have the same PCBs.

It's possible to add a dummy node both in the web interface, and by writing the input/output count register over Modbus (see section 6.5).

5.3.5 SETTINGS

Each stack node has settings that can be changed. Each setting is identified by an index, and has a 16-bit value. What each setting controls is given per type of stack node in ICS-SW-PRT-0005.

It's possible to read or write settings either from the web interface, or through Modbus registers (see section 0).

Stack node settings are available on the Settings page on the Stack tab of the web interface.

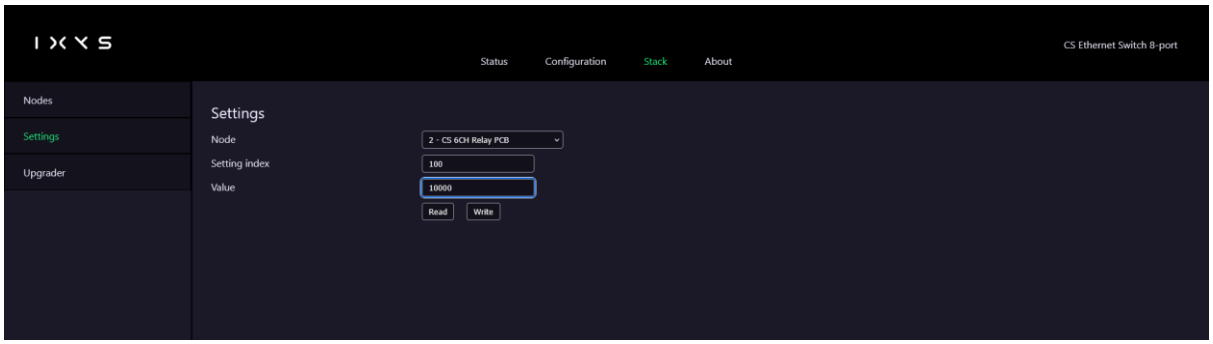


Figure 14 Stack node settings

5.3.6 UPGRADE

It's possible to upgrade the firmware of stack nodes via the Ethernet Switch's web interface. The stack node information will show the current firmware version of all nodes.

If a firmware file has been provided by Ixys, upgrading a stack node is possible on the Upgrader page on the Stack tab. First select the node to be upgraded from the drop-down, and then browse to find the firmware file. Finally press Start upgrade.

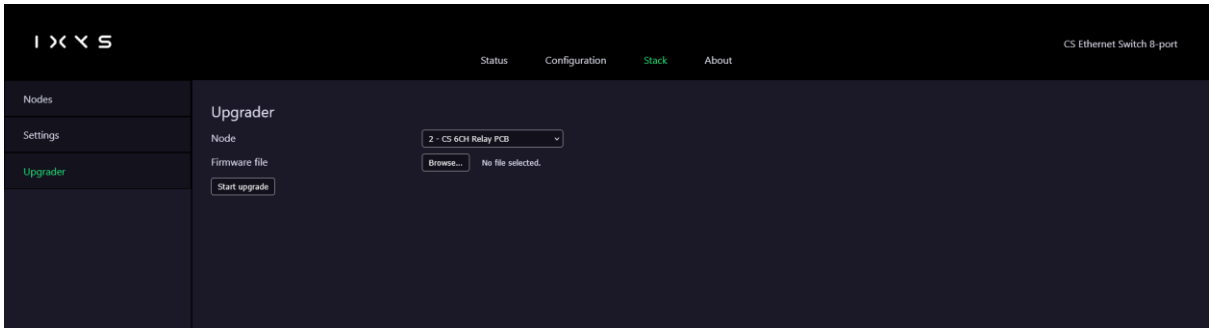


Figure 15 Stack node upgrading

Note: Should a stack node upgrade fail, it's important to not power cycle the system before the upgrade has been retried until it succeeds.

6 REGISTERS

The following sections describe all registers that can be read or written either over Modbus or over FINS.

6.1 DATA TYPES

The following table describes the data types used. For 32-bit values two Modbus registers are used, where the first is the most significant.

Name	Size	Value Range
INT16	2 bytes	-32,768 to 32,767
UINT16	2 bytes	0 to 65,535
INT32	4 bytes	-2,147,483,648 to 2,147,483,647
UINT32	4 bytes	0 to 4,294,967,295
REAL32	4 bytes	1.2E-38 to 3.4E+38

6.2 HEADER REGISTERS

Address	Description	Default	Note	Data Type
0	PCB Type	45	Ethernet Switch Type = 45	UINT16
1	Serial Number	N/A	Last part of the serial number	UINT16
2	Firmware Version	N/A	Numeric part of firmware version	UINT16
3	Status	N/A	Bit0 = Reserved Bit1 = Water Alarm	UINT16
4	Modbus Port	502		UINT16
5	Supply Voltage	N/A	Unit = 0.1 V	UINT16
6	Timeout	1000	Milliseconds without communication before Com Fail is triggered. Changes to this register will be stored.	UINT16
7	Node Address	1	Modbus Node Address	UINT16
8	Heartbeat	N/A	1 Hz counter. Rolls over to zero after 65535	UINT16
9	Reserved	N/A		UINT16

6.3 INPUT REGISTERS

Input registers are not writable.

Address	Description	Note	Data Type
10	Switch Core Temperature	Unit = 1 °C	UINT16
11	Switch Ambient Temperature	Unit = 1 °C	UINT16
12	Reserved		UINT16
13	Reserved		UINT16
14	Port 1 State	0=No link, 1=Disabled/Blocked, 2=Listen, 3=Learning, 4=Forwarding	UINT16
15	Port 1 Spare		UINT16
16	Port 1 Speed	Speed in Mbps + 1 if Full Duplex	UINT16
17	Port 1 InBytes LSB	Successful RX Bytes LSB	UINT32
18	Port 1 InBytes MSB	Successful RX Bytes MSB	
19	Port 1 OutBytes LSB	Successful TX Bytes LSB	UINT32
20	Port 1 OutBytes MSB	Successful TX Bytes MSB	
21-23	Port 1 Reserved		UINT16
24-93	Port 2-8 Equal to port 1		
94	SFP Port 3 Wavelength	Unit = 1 nm	UINT16
95	SFP Port 3 Temperature	Unit = 0.1 °C	UINT16
96	SFP Port 3 Voltage	Unit = 1 mV	UINT16
97	SFP Port 3 Tx Bias	Unit = 10 µA	UINT16
98	SFP Port 3 Tx Power	Unit = 0.01 dBm	INT16
99	SFP Port 3 Rx Power	Unit = 0.01 dBm	INT16
100-103	Reserved		UINT16
104-109	SFP Port 4 Equal to SFP Port 3		
110-121	Reserved		UINT16
122-499	Additional stack node inputs	See section 5.3.3 and ICS-SW-PRT-0005	

6.4 OUTPUT REGISTERS

All Output registers from 500 to 553 and 800 to 1399 are non-volatile and stored on change except for Port Monitoring and Port Disable that are both reset to default on reboot.

Address	Description	Default	Note	Data Type
500	Monitor Port	0	Port number for monitoring ingress or egress frames on other ports	UINT16
501	Port 1 Disable	0	Bit 0 => Port Disable Bit 1 => Ingress Monitoring Bit 2 => Egress Monitoring	UINT16
502	Port 1 Rate	0	0 => Auto-negotiate (all speeds) 1 => Auto-negotiate (advertising 10/100 Mbps) 2 => Auto-negotiate (advertising 10/1000 Mbps) 3 => Auto-negotiate (advertising 10 Mbps) 10 => Fixed 10 Mbps 100 => Fixed 100 Mbps 1000 => Fixed 1000 Mbps	UINT16
503	Port 1 Egress Multicast Enable	3	0 => Block unknown multicast and unicast 1 => Block multicast 2 => Block unknown unicast 3 => Egress all	UINT16
504	Port 1 Reserved	0		UINT16
505	Port 1 Duplex	0	0 => Half-Duplex, 1 => Full Duplex	UINT16
506-540	Port 2-8 Equal as port 1	N/A		
541-553	Spare	N/A		UINT16
554-799	Additional stack node outputs	N/A	See section 5.3.3 and ICS-SW-PRT-0005	
800-1099	Com-fail States	0	These registers define the value to be set in the corresponding output register (500-799) in the event of a communication timeout if the Com-fail Config register (1100-1399) is set to 1.	

1100-1399	Com-fail Config	0	These registers define the behavior of each output register (500-799) in the event of a communication timeout. 0=Stay as is 1=Set to the value defined in Com-fail State Register (800-1099)	

6.5 STACK NODE INFORMATION

The switch itself is always node 0, so the maximum number of additional stack nodes is 17.

Address	Description	Note	Data Type
1400-1419	Node Type	Type number of node	UINT16
1420-1439	Node Serial Number	Resets to zero if lost connection with Node	UINT16
1440-1459	Node Inputs/Outputs	Byte 0 = Number of input registers Byte 1 = Number of output registers Zero until “Node Scan” performed	UINT16
1460-1479	Node Firmware Version		UINT16

If a new node with Node ID outside the range of 1-18 or same Node ID as existing node, its information will be available as Node ID 19 (e.g. at 1419, 1439 and 1479). A new Node ID can be sent to the board by writing to setting index 0 as described in section 0.

Note: Stack node PCBs with jumpers or rotary hex switch set to any Node ID except 0 will be overridden at power reset to the physically set Node ID.

6.6 STACK NODE SETTINGS

Write to registers 1480-1486 first and then trigger the command by increasing register 1487 by one. Completion of command will be indicated by register 1488 set equal to register 1487.

Address	Description	Note	Data Type
1480	Setting Write Command	Set to 1 to prepare write command	UINT16
1481	Setting Read Command	Set to 1 to prepare read command	UINT16
1482	Setting Type	Type number used for Read/Write Command	UINT16
1483	Setting Node-ID	Node-ID used for Read/Write Command	UINT16
1484	Setting Serial	Serial number used for Read/Write Command	UINT16
1485	Setting Index	Setting Index used for Read/Write Command	UINT16
1486	Setting Value	Value used for Write Command or feedback from Read command	UINT16
1487	Setting Trigger	Write or read command is performed when this is unequal to 1488	UINT16
1488	Setting Completion	Write or read command is completed when this is equal to 1487	UINT16

7 TROUBLESHOOTING / FAULTFINDING

Symptom	Possible cause	Remedy
Power LED not lit, or Activity LED not blinking	Not powered	• Verify power connections are according to specifications in section 3.2 and connected as in section 4.3
	Faulty PCB	• Contact Ixys support
No link LED	Linked device not powered	• Verify linked device is powered
	Faulty cabling	• Try different network cable • Verify cable used with other equipment
Intermittent link LED	Poor cabling	• Try different network cable • Verify cable used with other equipment
	Wrong configuration	• Verify that linked device is correctly powered • Try using fixed speed and duplex on both devices
Not able to access web interface	Wrong IP address being used	• Use VJU Device Discovery or read broadcast messages to identify IP. See section 5.1.3 for details.
	Client device in wrong subnet	• Verify the client is in the same subnet as the PCB
Unstable detection and communication with stack nodes	No termination on CAN bus between the boards	• Add jumper to the CAN bus termination header pins.