ernitec

USER MANUAL · MANAGED SWITCH

ELECTRA-M12-10GB-FIBER

12 × 10 Gigabit SFP managed switch – installation, configuration and web interface reference

12	192.168.1.254	admin / admin	Web · CLI
10G SFP PORTS	DEFAULT IP	DEFAULT LOGIN	MANAGEMENT

Manual contents

01 Foreword
02 Accessing the switch
03 Status
04 Network
05 Port
06 VLAN
07 MAC address table
08 Spanning tree
09 ERPS
10 Loopback detection
11 Discovery (LLDP)
12 DHCP
13 Multicast
14 Routing
15 Security
16 ACL
17 QoS
18 Diagnostics
19 Management

Version 1.0 · Specifications and features are subject to change without notice.

Contents

1 Foreword 5
1.1 Target audience 5
1.2 Manual conventions 5
2 Accessing the switch 5
2.1 Web interface 5
2.2 Console port (CLI) 6
2.3 Telnet and SSH 6
2.4 Changing the management IP address 6
2.5 The web interface 6
3 Status 7
3.1 System information 7
3.2 Port statistics 7
3.3 Link aggregation and logging 7
3.4 MAC address table 7
3.5 Reboot 7
4 Network 7
4.1 DNS 7
4.2 System time 8
5 Port 9
5.1 Port setting 9
5.2 Error disabled 9
5.3 Link aggregation 9
5.4 Jumbo frame 10
5.5 Port security 10
5.6 Protected port 10
5.7 Storm control 11
5.8 Mirroring 11
6 VLAN 11
6.1 Creating VLANs 11
6.2 Assigning ports to VLANs 12
6.3 Port VLAN settings 12
6.4 Surveillance VLAN 12
6.5 Voice VLAN 13
6.6 Protocol VLAN 13
6.7 MAC VLAN 13
6.8 GVRP 14
7 MAC address table 15
7.1 Dynamic addresses 15
7.2 Static addresses 15
7.3 Filtering addresses 15
7.4 Port security addresses 15
8 Spanning tree 16
8.1 Global properties 16
8.2 Port settings 16
8.3 MST instances 17
8.4 MST port settings 17
8.5 Example: MSTP load sharing 17

9 ERPS 18
9.1 Property 18
9.2 ERPS instance 18
10 Loopback detection 18
11 Discovery (LLDP) 19
11.1 LLDP properties 19
11.2 Port settings 19
11.3 LLDP-MED 19
11.4 Monitoring 20
12 DHCP 21
12.1 Property 21
12.2 IP pool setting 21
12.3 VLAN interface address group 21
12.4 Client list and static bindings 21
13 Multicast 22
13.1 General settings 22
13.2 IGMP snooping 22
13.3 MLD snooping 23
13.4 MVR 23
14 Routing 23
14.1 IPv4 interfaces 23
14.2 IPv4 static routes and ARP 24
14.3 IPv6 24
14.4 RIP 24
14.5 OSPF 24
15 Security 26
15.1 RADIUS and TACACS+ 26
15.2 AAA 26
15.3 Management access 27
15.4 Authentication manager (802.1X, MAC and web) 27
15.5 DoS protection 28
15.6 Dynamic ARP inspection 28
15.7 DHCP snooping 28
15.8 IP source guard 29
16 ACL 29
16.1 MAC ACL 29
16.2 IPv4 and IPv6 ACL 30
16.3 ACL binding 30
17 QoS 31
17.1 Property 31
17.2 Queue scheduling 31
17.3 Priority mapping 31
17.4 Rate limiting 32
18 Diagnostics 32
18.1 Logging 32
18.2 Ping and traceroute 32
18.3 Fiber module 32
18.4 UDLD 32
19 Management 33

19.1 User accounts 33
19.2 Firmware 33
19.3 Configuration files 33
19.4 SNMP 33
19.5 RMON 34

Index 35

ELECTRA-M12-10GB-FIBER · CHAPTERS 1–4

Getting started, status and network

Accessing the switch, the web interface, status pages and basic network settings

1 Foreword

1.1 Target audience

This manual is written for installers and system administrators who install, configure and maintain networks. It assumes familiarity with network protocols and terminology, and experience with web-based management, command-line interfaces (CLI) and SNMP.

1.2 Manual conventions

Convention	Meaning
Note	Explains an operation or adds useful information.
Caution	Warns that an incorrect operation may cause data loss or damage to the equipment.

2 Accessing the switch

The switch can be managed in three ways: through the web interface, through the console port (CLI), or remotely via Telnet/SSH. All methods use the same default login.

Setting	Default
Default IP address	192.168.1.254 / 255.255.255.0
Username	admin
Password	admin
Console settings	115200 baud, 8 data bits, no parity, 1 stop bit

2.1 Web interface

1. Connect the PC to a switch port. All ports are SFP, so insert an SFP module first (e.g. a copper RJ45 SFP).
2. Give the PC a fixed IP address in the same subnet: **192.168.1.x** (x = 1–253), subnet mask **255.255.255.0**.
3. Open a browser and go to **http://192.168.1.254**.
4. Log in with username **admin** and password **admin**, then click **Log in**.

NOTE Use a current version of Chrome, Firefox or Edge.

2.2 Console port (CLI)

Console access works regardless of the IP configuration and is the best option if the IP address is unknown.

1. Connect a serial console cable (USB-to-RJ45) from the switch's **Console** port to a USB port on the PC.
2. Find the COM port number in Windows Device Manager under Ports (COM & LPT).
3. Open a terminal program such as PuTTY or SecureCRT, select **Serial** and the COM port.
4. Set **115200 baud, 8 data bits, no parity, 1 stop bit**. Turn off flow control if there is no response.
5. Press Enter until the Username prompt appears, then log in with admin / admin.

2.3 Telnet and SSH

1. In the web interface, enable Telnet or SSH under **Security › Management Access › Management Service** (see chapter 15).
2. Connect to the switch IP address with PuTTY or another client and log in with admin / admin.

2.4 Changing the management IP address

In the web interface, the management address is set under **Routing › IPv4 Management and Interfaces › IPv4 Interface** (see chapter 14). From the CLI, enter privilege mode and run (adjust to your network):

```
ip address 192.168.1.10 mask 255.255.255.0
ip default-gateway 192.168.1.1
```

CAUTION Change the default password after the first login (Management › User Account).

2.5 The web interface

The web interface consists of a navigation bar on the left, the configuration area in the centre and toolbar buttons at the top right, including Save and Reboot. Main menus: Status, Network, Port, VLAN, MAC Address Table, Spanning Tree, ERPS, Loopback, Discovery, DHCP, Multicast, Routing, Security, ACL, QoS, Diagnostics and Management. Each main menu is described in its own chapter.

NOTE Settings take effect when you click **Apply**, but are lost at reboot unless saved. Click **Save** at the top right, or use **Management › Configuration › Save Configuration** (chapter 19).

3 Status

3.1 System information

MENU Status › System Information

Shows a live view of the front panel with port states, plus product information and device status. Hover over a port to see port number, type, speed and state. Click **Edit** to change System Name, Location and Contact, then **Apply**.

3.2 Port statistics

MENU Status › Port › Statistics

Shows detailed traffic counters per port. Click **Clear** to reset the counters for the selected port. Under the same menu, **Error Disabled** lists ports shut down by a protection feature and **Bandwidth Utilization** shows the load on each port.

3.3 Link aggregation and logging

Status › Link Aggregation shows the state and members of each aggregation group. **Status › Logging Message** shows the device's run-time and operation log.

3.4 MAC address table

MENU Status › MAC Address Table

Field	Description
MAC	Destination MAC address
VLAN	VLAN ID the address belongs to
Port	Port on which the address was learned
Type	**Dynamic**: learned automatically and removed after the aging time. **Static**: configured manually, never ages. **Management**: the switch's own management address.

3.5 Reboot

Click **Reboot** at the top right of the interface. Save the configuration first, or unsaved changes are lost.

4 Network

4.1 DNS

MENU Network › DNS

DNS translates host names to IP addresses, so the switch can use names (e.g. for SNTP, ping or log servers).

Parameter	Description

DNS State	Enable or disable DNS lookup
DNS Default Name	Default domain name appended to host names

1. Set DNS State and the default name.
2. Click **Add** to enter one or more DNS server addresses.
3. Click **Apply**.

Network › Hosts shows and configures static host-name mappings and the dynamic host table.

4.2 System time

MENU Network › System Time

Parameter	Description
Time Source	SNTP, PC (copy from the browser) or manual
Time Zone	Local time zone
Address Type	Host name or IPv4 address of the SNTP server
Server Address / Port	SNTP server and UDP port (SNTP only)
Date / Time	Set manually (manual mode only)
Daylight Saving Type	None, recurring, non-recurring, USA or Europe
Offset	Time added during daylight saving
Recurring / Non-recurring	Start and end of daylight saving for custom modes

ELECTRA-M12-10GB-FIBER · CHAPTERS 5–6

Port and VLAN

Port settings, link aggregation, port protection, mirroring and VLANs

5 Port

5.1 Port setting

MENU Port › Port Setting

Select one or more ports and click **Edit** to configure them.

Parameter	Description
Description	Port name or alias
State	Enable or disable the port
Speed	Auto-negotiation, or fixed 100 Mbps, 1000 Mbps or 10 Gbps
Duplex	Auto-negotiation, full or half duplex
Flow Control	Sends PAUSE frames during congestion so the link partner pauses transmission. **Disable**, **Enable** or **Auto** (negotiated with the link partner). Must be enabled at both ends.

5.2 Error disabled

MENU Port › Error Disabled

When the switch detects certain error events on a port, it shuts the port down automatically to protect the network. This page enables or disables this protection and its recovery settings. Affected ports are listed under Status › Port › Error Disabled.

5.3 Link aggregation

Link aggregation bundles several physical ports into one logical link (LAG). The bandwidth equals the sum of the member links, and the links back each other up: if one fails, traffic is shared across the remaining members. The switch supports **8 LAGs** with up to **8 member ports** each.

Mode	Description
Static (manual)	Members are added manually without LACP. All links forward traffic and share the load. Use when the link partner does not support LACP.
LACP (dynamic)	IEEE 802.3ad. The switches exchange LACPDUs and agree automatically which ports join the group. Members must connect to the same device with the same speed, duplex and basic configuration.

MENU Port › Link Aggregation › Group

1. Select the load-balancing algorithm and click **Apply**.
2. Select a LAG (1–8) and click **Edit**.
3. Enter a name, choose **Static** or **LACP**, move the member ports to the selected list and click **Apply**.
4. Configure the link partner identically.

Parameter	Description
LAG	Group number 1–8
Name	Description of the group
Type	Static or LACP
Member	Up to 8 member ports

Port › Link Aggregation › Port Setting sets the attributes of member ports. **Port › Link Aggregation › LACP** sets the LACP parameters:

Parameter	Description
System Priority	Decides which device is active in the negotiation
Port Priority	Decides which ports become active members
Timeout	How often LACP messages are sent (long or short)

CAUTION Remove all members from a LAG before changing its type. The mode must be the same at both ends.

5.4 Jumbo frame

MENU Port › Jumbo Frame

Sets the maximum frame size (MTU) the switch forwards.

5.5 Port security

MENU Port › Port Security

Port security limits which MAC addresses may use a port. Frames from other addresses are blocked. This stops unauthorised devices from connecting and protects the MAC table against flooding. Enable the function globally, then select ports and click **Edit** to set the limit and action per port. Learned addresses are shown under MAC Address Table › Port Security Address.

5.6 Protected port

MENU Port › Protected Port

Protected (isolated) ports cannot exchange traffic with each other, including broadcast and multicast, but can still reach unprotected ports such as the uplink. Select the ports, click **Edit**, enable protection and click **Apply**.

5.7 Storm control

MENU Port › Storm Control

Limits broadcast, unknown multicast and unknown unicast traffic, which would otherwise flood all ports in the VLAN and could cause a broadcast storm. The switch compares the received rate with the configured threshold and drops traffic above it.

1. Set the global mode (e.g. packets or bits per second) and click **Apply**.
2. Select a port and click **Edit**.
3. Enable control and enter rates for broadcast, unknown multicast and unknown unicast, then click **Apply**.

5.8 Mirroring

MENU Port › Mirroring

Copies traffic from one or more source ports to a monitor port, where a network analyser can be connected for monitoring and troubleshooting. Four sessions are available.

Parameter	Description
Session ID	Session 1–4
State	Enable or disable the session
Monitor Port	Destination port. One physical port only; cannot be a LAG or a source port.
Ingress Port	Traffic received on these ports is mirrored
Egress Port	Traffic transmitted on these ports is mirrored

6 VLAN

A VLAN divides one physical network into separate logical networks (broadcast domains). Devices in different VLANs cannot communicate without a router or Layer 3 switch. VLANs limit broadcast traffic, improve security and let users be grouped regardless of physical location.

The switch supports 802.1Q, port-based, protocol-based and MAC-based VLANs. 802.1Q is the default. Each port has a PVID (port VLAN ID): untagged frames received on the port are assigned to this VLAN.

6.1 Creating VLANs

MENU VLAN › VLAN › Create VLAN

1. Enter the VLAN IDs in the available list and move them to the list on the right. IDs 1–4094 are valid, e.g. 1-3,5,7,9. Up to 256 VLANs can be created.
2. Click **Apply**. The VLANs appear in the VLAN table.
3. Click **Edit** to give a VLAN a name.

NOTE VLAN 1 is the default VLAN and exists already. All ports are untagged members of VLAN 1 from the factory.

6.2 Assigning ports to VLANs

Ports can be assigned in two ways: many ports to one VLAN (VLAN Configuration), or one port to many VLANs (Membership).

MENU VLAN › VLAN › VLAN Configuration – select the VLAN, then set each port

MENU VLAN › VLAN › Membership – select a port, click Edit, then set each VLAN

Membership	Meaning
Excluded	The port is not a member of the VLAN
Tagged	The port sends frames of this VLAN with an 802.1Q tag
Untagged	The port sends frames of this VLAN without a tag
PVID	This VLAN is the port's native VLAN
Forbidden	Frames of this VLAN are never forwarded on the port

6.3 Port VLAN settings

MENU VLAN › VLAN › Port Setting

Tagged frames carry a 4-byte 802.1Q tag containing the VLAN ID (1–4094) and a priority (0–7). Trunk ports between switches normally carry tagged frames for several VLANs.

Parameter	Description
Mode	**Access**: member of one VLAN only (end devices). **Trunk**: untagged in the PVID, tagged in other VLANs (switch links). **Hybrid**: tagged and untagged in any VLANs. **Tunnel**: Q-in-Q.
PVID	Native VLAN of the port
Accept Frame Type	All, Tag Only or Untag Only
Ingress Filtering	Drops frames for VLANs the port is not a member of
Uplink	Marks the port as an uplink
TPID	Tag protocol identifier (normally 0x8100)

6.4 Surveillance VLAN

MENU VLAN › Surveillance VLAN › Property / Surveillance OUI

Surveillance VLAN gives video streams from IP cameras higher priority than ordinary traffic. The switch recognises camera traffic by the first 24 bits of the source MAC address (the OUI) and places it in the surveillance VLAN automatically.

Parameter	Description
State	Enable surveillance VLAN globally
VLAN	Surveillance VLAN ID (1–4094)
CoS / 802.1p Remarking	Rewrite the priority of surveillance traffic
Aging Time	How long learned entries are kept
Port State / Mode	Enable per port, in **auto** or **manual** mode
QoS Policy	Which traffic the QoS policy applies to

1. Create the surveillance VLAN (6.1) and set the camera ports to Hybrid mode (6.3).
2. Under **Surveillance OUI**, add the OUI (first three bytes of the camera MAC address, e.g. 00:11:22) and click **Apply**.
3. Under **Property**, enable the function, select the VLAN, then edit the camera ports, enable them in auto mode and click **Apply**.

6.5 Voice VLAN

MENU VLAN › Voice VLAN › Property / Voice OUI

Works like surveillance VLAN, but for IP telephones: voice traffic is recognised by OUI and given higher priority to reduce delay and packet loss. The settings are the same as in 6.4.

NOTE In auto mode, the port forwards voice VLAN traffic even if it is not a static member of the voice VLAN.

6.6 Protocol VLAN

MENU VLAN › Protocol VLAN › Protocol Group / Group Binding

Assigns untagged frames to a VLAN based on protocol type, e.g. IPv4 to one VLAN and IPv6 to another.

Parameter	Description
Group ID	Protocol group number
Frame Type	Ethernet II, LLC or RFC 1042
Protocol Value	EtherType 0x0600–0xFFFE (e.g. 0x0800 for IPv4, 0x86DD for IPv6)

Under **Group Binding**, click **Add** to bind a port and protocol group to a VLAN. The port must be in Hybrid mode.

6.7 MAC VLAN

MENU VLAN › MAC VLAN › MAC Group / Group Binding

Assigns untagged frames to a VLAN based on source MAC address, so devices keep their VLAN when moved to another port. Useful where only known devices may reach a network.

Parameter	Description
Group ID	MAC group number
MAC Address	MAC address to match
Mask	Number of bits to match; 48 = exact match

Under **Group Binding**, click **Add** to bind a Hybrid port and MAC group to a VLAN.

6.8 GVRP

MENU VLAN › GVRP › Property / Membership / Statistics

GVRP lets switches exchange VLAN information over 802.1Q trunks, so VLANs created on one switch are learned dynamically by the others and unused VLANs are pruned from trunks.

Setting	Description (cs = 1/100 s)
State	Enable GVRP globally
Join	Join timer, 20 cs (2–16375)
Leave	Leave timer, 60 cs (45–32760)
LeaveAll	LeaveAll timer, 1000 cs (65–32765)
Port State	Enable GVRP on the port
VLAN Creation	Allow VLANs to be created dynamically
Registration	**Normal**: dynamic and static VLANs. **Fixed**: static VLANs only. **Forbidden**: no dynamic VLANs; only VLAN 1 is kept.

Membership lists the dynamically learned VLANs and ports. **Statistics** shows GVRP message counters per port.

ELECTRA-M12-10GB-FIBER · CHAPTERS 7–11

MAC table, spanning tree and ring protection

MAC addresses, STP/RSTP/MSTP, ERPS, loopback detection and LLDP discovery

7 MAC address table

The switch forwards frames using its MAC address table, which links each MAC address and VLAN to a port. If the destination address is in the table, the frame is sent only to that port (unicast). If it is unknown or a broadcast address, the frame is sent to all ports in the VLAN except the receiving port.

7.1 Dynamic addresses

MENU MAC Address Table › Dynamic Address

Learned entries are removed when they have not been refreshed within the aging time. Too short an aging time causes unnecessary flooding; too long keeps outdated entries. The recommended value is **300 seconds** (default). Enter the MAC Aging Time and click **Apply**. The table itself is shown under Status › MAC Address Table (section 3.4).

7.2 Static addresses

MENU MAC Address Table › Static Address

Static entries are configured manually and never age.

Parameter	Description
MAC	MAC address, format HH:HH:HH:HH:HH:HH (required)
VLAN	VLAN ID (required)
Port	Port (required). Must be a member of the VLAN.

7.3 Filtering addresses

MENU MAC Address Table › Filtering Address

Frames matching a filtering entry (MAC address and VLAN) are discarded.

7.4 Port security addresses

MENU MAC Address Table › Port Security Address

Lists secure MAC addresses with VLAN and port. On a port with port security, only frames from its secure addresses are forwarded; all others are discarded (see 5.5).

8 Spanning tree

Redundant links improve reliability but create loops, which cause broadcast storms and an unstable MAC table. Spanning tree blocks redundant links to remove loops and reactivates them if the active path fails.

Protocol	Characteristics
STP (802.1D)	Loop-free tree; slow convergence. One tree for all VLANs.
RSTP (802.1w)	As STP, with rapid convergence.
MSTP (802.1s)	Rapid convergence and several trees (instances), so VLANs can follow different paths for load sharing. Compatible with RSTP and STP.

8.1 Global properties

MENU Spanning Tree › Property

Parameter	Description
State	Enable spanning tree (enabled by default)
Operation Mode	STP, RSTP or MSTP
Path Cost	Long or short path cost method
BPDU Handling	How BPDUs are handled when spanning tree is disabled
Priority	Bridge priority; lowest value becomes root
Hello Time	Interval between BPDUs
Max Age	Maximum age of BPDU information
Forward Delay	Time spent in listening and learning states
Tx Hold Count	Maximum BPDUs sent per second
Region Name	MST region name (default: the switch MAC address)
Revision	MSTP revision number
Max Hop	Hops within an MST region before a BPDU is discarded

NOTE Switches belong to the same MST region only if region name, revision and VLAN-to-instance mapping are identical.

8.2 Port settings

MENU Spanning Tree › Port Setting

Parameter	Description
State	Enable spanning tree on the port

Path Cost	0–200,000,000 (IEEE 802.1t); 0 = automatic
Priority	Port priority; lower value = higher priority
Edge Port	For ports connected directly to end devices (e.g. cameras, PCs). Goes straight to forwarding.
BPDU Filter	Stop sending and receiving BPDUs on the port
BPDU Guard	Shut down the port if a BPDU is received. Disabled by default. The port must be re-enabled manually.
Point-to-Point	Auto, Enabled or Disabled

8.3 MST instances

MENU Spanning Tree › MST Instance

MSTP maps groups of VLANs to instances (MSTI 0–15). Each instance has its own tree, so traffic for different VLANs can use different links.

Parameter	Description
MSTI	Instance number 0–15
VLAN	VLANs mapped to the instance
Priority	Bridge priority for the instance, a multiple of 4096 (0–61440). Default 32768.

8.4 MST port settings

MENU Spanning Tree › MST Port Setting

Select the instance at the top left, then a port, and set **Path Cost** and **Priority** for that instance. The page also shows the port role (root, designated, alternate, backup, disabled), state (discarding, forwarding, disabled), mode and type (boundary or internal).

8.5 Example: MSTP load sharing

1. On all switches, create VLAN 10 and 20 and add them tagged to the ring ports.
2. Set the mode to **MSTP** under Spanning Tree › Property.
3. Under MST Instance, map VLAN 10 to MSTI 1 and VLAN 20 to MSTI 2.
4. On switch A set MSTI 1 priority 0 and MSTI 2 priority 4096. On switch B set the opposite. A is root for VLAN 10, B for VLAN 20, and each backs up the other.

Spanning Tree › Statistics shows BPDU counters per port.

9 ERPS

ERPS (Ethernet Ring Protection Switching, G.8032) prevents loops in a ring and restores traffic within milliseconds when a link fails. One port on the ring, the RPL owner port, is blocked in normal operation and opened if another link fails.

NOTE Recovery below 20 ms applies to fibre ports. Only a main ring is supported.

9.1 Property

MENU ERPS › Property

Enables or disables ERPS globally.

9.2 ERPS instance

MENU ERPS › ERPS Instance

Each ring instance is a logical ring with its own control channel, data channels and owner node. Click **Apply** to create an instance, then select it and click **Edit**.

Parameter	Description
Ring Status	Enable or disable the ring
MEL	Maintenance entity level 0–7
Protected Instance	MST instance holding the data and control VLANs. VLANs not mapped here may cause a broadcast storm.
Control VLAN	VLAN that carries the ERPS (R-APS) messages
WTR Time	Wait-to-restore time before the owner port is blocked again after recovery (revertive mode)
Guard Time	Ignores old R-APS messages after a link recovers, to avoid oscillation
Work Mode	Revertive or non-revertive
Ring ID	Ring number
Ring Type	0 = main ring
Port0 / Port1	The two ring ports
Port Role	Normal, Owner, Neighbour or Next-neighbour

10 Loopback detection

MENU Loopback › Loopback Config

Loopback detection finds loops in the network and blocks the affected port to prevent loop storms. Enable it globally and per port, and set the detection interval and the automatic recovery time. Detection can run automatically or manually.

11 Discovery (LLDP)

LLDP (IEEE 802.1AB) lets devices advertise their identity, management address and port information to directly connected neighbours. The information is stored in MIBs for network management and topology mapping. LLDP-MED extends LLDP with network policy, location and inventory information.

11.1 LLDP properties

MENU Discovery › LLDP › Property

Parameter	Description
State	Enable or disable LLDP
LLDP Handling	When LLDP is disabled: Filtering, Bridging or Flooding of received LLDP frames
TLV Advertise Interval	30 s (5–32768 s)
Hold Multiplier	Default 4; interval × multiplier must not exceed 65535
Reinitializing Delay	2 s (1–10 s)
Transmit Delay	2 s (1–8191 s)
Fast Start Repeat Count	3 (1–10), LLDP-MED ports

11.2 Port settings

MENU Discovery › LLDP › Port Setting

Parameter	Description
Mode	**Normal** (default): send and receive. **Transmit** only, **Receive** only, or **Disable**.
Optional TLV	Which optional information to advertise
802.1 VLAN Name	VLAN names to advertise

11.3 LLDP-MED

MENU Discovery › LLDP › MED Network Policy

Parameter	Description
Policy ID	Policy number
Application	Application type for the network policy TLV
VLAN / VLAN Tag	VLAN ID, tagged or untagged

Priority / DSCP	CoS and DSCP values for the application

MENU Discovery › LLDP › MED Port Setting

Per port: enable LLDP-MED and choose whether to advertise the network policy, location and inventory TLVs.

11.4 Monitoring

Packet View shows the LLDP frames per port. **Local Information** shows the switch's own LLDP data and port status. **Neighbor** lists discovered neighbouring devices. **Statistics** shows sent and received LLDP frames per port.

ELECTRA-M12-10GB-FIBER · CHAPTERS 12–14

DHCP, multicast and routing

DHCP server, IGMP/MLD snooping, MVR, IP interfaces and RIP/OSPF routing

12 DHCP

DHCP assigns IP addresses and network settings to clients automatically. The switch can act as a DHCP server (or relay) for connected devices. Clients receive addresses in four steps: discover, offer, request and acknowledge. A client renews its lease when half the lease time has passed.

Allocation	Description
Manual	The administrator binds a fixed IP address to a specific client
Automatic	Addresses are assigned with unlimited lease time
Dynamic	Addresses are assigned for a limited lease time (most common)

12.1 Property

MENU DHCP › Property

Sets the global DHCP mode (server or relay) and static bindings. Select ports and click **Edit** to enable DHCP on them.

NOTE When DHCP server or relay mode is enabled, it must also be enabled on the relevant ports.

12.2 IP pool setting

MENU DHCP › IP Pool Setting

Click **Add** to create an address pool with start address, end address and related settings.

CAUTION The pool range must not include the gateway address.

12.3 VLAN interface address group

MENU DHCP › VLAN IF Address Group Setting

In the **DHCP Server Group Table**, click **Add** to create a server group. In the **VLAN Interface Address Pool Table**, select a VLAN interface and a server group and click **Apply** to bind them.

12.4 Client list and static bindings

DHCP › Client List shows the clients that have received an address. **DHCP › Client Static Binding Table**: click **Add** to reserve a fixed IP address for a client. The address must lie within the assigned pool range.

13 Multicast

Multicast sends one stream to many receivers, which is typical for video from IP cameras. Without control, a switch floods multicast to all ports in the VLAN. IGMP snooping (IPv4) and MLD snooping (IPv6) let the switch forward each multicast group only to the ports that have requested it.

13.1 General settings

MENU Multicast › General

Page	Description
Property	Global multicast settings
Group Address	Static multicast groups: VLAN, IP version, multicast address and member ports. Click **Add** or **Edit**.
Router Port	Ports connected to multicast routers
Forward All	Ports that receive all multicast traffic
Throttling	Maximum number of multicast groups per port
Filtering Profile	Profiles that allow or deny multicast groups, and their binding to ports

13.2 IGMP snooping

MENU Multicast › IGMP Snooping › Property

IGMP snooping is disabled by default and must be enabled globally. Then select a VLAN and click **Edit**.

Parameter	Description
State	Enable IGMP snooping in the VLAN
Router Port Auto Learn	Learn router ports automatically
Immediate Leave	Remove a port from a group as soon as a leave message is received
Query Robustness	Tuning for expected packet loss
Query Interval	Interval between general queries
Query Max Response Interval	Maximum response time for queries
Last Member Query Counter	Number of group-specific queries before a group is removed
Last Member Query Interval	Interval between group-specific queries

MENU Multicast › IGMP Snooping › Querier

If there is no multicast router in the VLAN, enable the switch as IGMP querier. Settings: VLAN, State, Version and Querier Address; the operational status is shown. **Statistics** shows IGMP counters.

NOTE In camera networks without a multicast router, enable IGMP snooping and the querier in the video VLAN so multicast streams are not flooded to all ports.

13.3 MLD snooping

MENU Multicast › MLD Snooping › Property / Statistics

The IPv6 counterpart of IGMP snooping, with the same per-VLAN settings. Disabled by default.

13.4 MVR

MENU Multicast › MVR

Multicast VLAN Registration delivers one multicast stream from a dedicated multicast VLAN to receivers in different VLANs, so the stream is not duplicated per VLAN. Disabled by default.

Parameter	Description
State / VLAN	Enable MVR and select the multicast VLAN
Mode	**Compatible**: join messages are not forwarded to the router port, so the router must be configured statically. **Dynamic**: join messages are forwarded, so the router learns groups dynamically.
Group Start / Count	First multicast address and number of groups
Query Time	Group query time
Port Role	**Receiver**: port with multicast receivers. **Source**: port towards the multicast source.
Immediate Leave	Fast removal of leaving members

Group Address shows the MVR groups with VLAN and members.

14 Routing

The switch supports Layer 3 VLAN interfaces (VLANIF) with IP addresses, so it can route between VLANs and communicate with other network-layer devices. Create the VLAN before creating its interface.

14.1 IPv4 interfaces

MENU Routing › IPv4 Management and Interfaces › IPv4 Interface

This is also where the management IP address is changed (default 192.168.1.254).

Parameter	Description
VLAN	VLAN of the interface
Loopback	Loopback interface
Address Type	**Static** (manual) or **Dynamic** (DHCP)

IP Address / Mask	Address and subnet mask of the interface

14.2 IPv4 static routes and ARP

MENU Routing › IPv4 Management and Interfaces › IPv4 Routes

Parameter	Description
IP Address / Mask	Destination network
Next Hop Router IP	Next hop; must be in the same subnet as an interface
Metric	Route cost (hops)

MENU Routing › IPv4 Management and Interfaces › ARP

Shows and configures static ARP entries: VLAN interface, IP address and MAC address.

14.3 IPv6

MENU Routing › IPv6 Management and Interfaces › IPv6 Interface

Parameter	Description
VLAN / Loopback	Interface
Auto Configuration	Enable address autoconfiguration
DAD Attempts	Neighbour solicitations sent for duplicate address detection
Stateless	Stateless autoconfiguration
Information Refresh Time	Refresh time (and minimum) for autoconfiguration information

IPv6 Address: interface, type (global or link-local), address, prefix length and EUI-64. **IPv6 Routes**: prefix, prefix length, next hop and metric. **Neighbors**: static IPv6 neighbour entries (interface, IPv6 address, MAC address).

14.4 RIP

MENU Routing › Rip Routes Management › Rip Routes Setting

RIP is a simple distance-vector routing protocol for small networks. It uses hop count as metric (maximum 15 hops), sends updates every 30 seconds on UDP port 520 and has administrative distance 120. RIPv2 supports CIDR and VLSM and uses multicast 224.0.0.9.

In the **Network Setting** table, click **Add** to advertise a network.

14.5 OSPF

MENU Routing › Ospf Routes Management › Ospf Routes Setting

OSPF is a link-state routing protocol for larger networks within one autonomous system. Routers exchange link-state advertisements and calculate the shortest path. OSPF supports areas and authentication.

In **Area Network Setting**, click **Add** to add a network to an area.

NOTE Before advertising networks with RIP or OSPF, configure the interface IP address and make sure the interface is up.

ELECTRA-M12-10GB-FIBER · CHAPTERS 15–16

Security and ACL

Authentication servers, management access, 802.1X, attack protection and access control lists

15 Security

15.1 RADIUS and TACACS+

MENU Security › RADIUS / Security › TACACS+

Add external authentication servers for logins and network access control. The settings are the same for both server types.

Parameter	Description
Address Type	Host name, IPv4 or IPv6
Server Address	Address of the server
Server Port	Service port
Priority	Order in which servers are used
Key String	Shared secret between server and switch
Retry	Number of retransmissions
Timeout	Time to wait for a reply before retransmitting
Usage	What the server is used for (RADIUS only)

15.2 AAA

MENU Security › AAA › Method List / Login Authentication

A method list defines how logins are authenticated, with up to four methods tried in order. **Login Authentication** assigns method lists to the different login types.

Method	Description
Empty	Method not used
None	No authentication; the user is accepted
Local	Local user accounts on the switch
Enable	Local enable password
RADIUS	Remote RADIUS server
TACACS+	Remote TACACS+ server

15.3 Management access

MENU Security › Management Access › Management Service

Enables or disables the management services: **Telnet**, **SSH**, **HTTP/HTTPS** and **SNMP**, with their related settings. Telnet or SSH must be enabled here before the CLI can be reached over the network (see 2.3).

NOTE For better security, use SSH and HTTPS and disable services that are not needed.

MENU Security › Management Access › Management ACL / Management ACE

A management ACL restricts which hosts may manage the switch. Create the ACL, then add rules (ACEs):

Parameter	Description
ACL Name	Name of the management ACL
Priority	Rule order
Service	Management service the rule applies to
Action	Permit or deny
Port	Port the rule applies to
IP Version / Address	IPv4 or IPv6 source address

CAUTION Make sure the ACL permits your own management PC before activating it, or you may lock yourself out.

15.4 Authentication manager (802.1X, MAC and web)

MENU Security › Authentication Manager

Controls network access per port, using 802.1X, MAC-based or web-based authentication. **Property** enables the authentication types globally and sets them per port:

Parameter	Description
Authentication Type / Method	Types enabled on the port and the order they are tried
Host Mode	**Multiple Authentication**: each client authenticates separately. **Multiple Hosts**: once one client is authenticated, all get access. **Single Host**: one client only.
Guest VLAN	VLAN for clients that are not authenticated
VLAN Assign Mode	**Reject**: client is refused if RADIUS sends no VLAN. **Static**: client keeps its original VLAN if no VLAN is sent.

MENU Security › Authentication Manager › Port Setting

Parameter	Description

Port Control	**Force Authorized**: all clients get access. **Force Unauthorized**: no clients get access. **Auto**: clients must authenticate.
Reauthentication / Period	Enable periodic reauthentication and its interval in seconds
Max Hosts	Maximum clients in multiple-authentication mode
Inactive / Quiet	Inactivity timeout and quiet period after a failed attempt
TX Period / Supplicant Timeout / Server Timeout / Max Request	802.1X EAP timers and retries
Max Login	Maximum web login attempts

MAC-Based Local Account and **WEB-Based Local Account** hold local accounts for MAC and web authentication. **Sessions** lists active authentication sessions.

15.5 DoS protection

MENU Security › DoS › Property / Port Setting

Protects the switch against common denial-of-service attacks. Enable the protection types globally under Property, then select ports and click **Edit** to enable protection per port.

15.6 Dynamic ARP inspection

MENU Security › Dynamic ARP Inspection

Checks ARP packets against trusted IP-to-MAC bindings to prevent ARP spoofing. Enable it under **Property**; **Statistics** shows inspected and dropped packets per port.

15.7 DHCP snooping

MENU Security › DHCP Snooping › Property

DHCP snooping stops unauthorised DHCP servers from handing out wrong addresses. Ports are either **trusted** (towards the legitimate DHCP server) or **untrusted**. DHCP offers and acknowledgements arriving on untrusted ports are dropped. The switch also records which IP address each client received.

Parameter	Description
State	Enable DHCP snooping
VLAN	VLANs where snooping is active
Trust	Mark the port as trusted
Client Address Inspection	Check that the client MAC address in the DHCP message matches the source
Rate Limit	Limit DHCP packets per second on the port

1. Enable DHCP snooping and select the VLANs.
2. Edit the port connected to the DHCP server and set it as **Trust**.
3. Leave client ports untrusted. Click **Apply**.

Statistics shows DHCP packet counters per port.

MENU Security › DHCP Snooping › Option82 Property / Option82 Circuit ID

Option 82 adds information about the client's location (switch and port) to DHCP requests, so the server can apply address policies. Sub-option 1 (Circuit ID) carries VLAN and port; sub-option 2 (Remote ID) carries the switch MAC address or a custom string. The option is removed from replies before they reach the client.

Parameter	Description
Remote ID	Custom Remote ID string
Port	Enable Option 82 on the port
Untrust Port Action	For requests that already contain Option 82: **Keep**, **Drop** or **Replace**
Circuit ID	Custom Circuit ID per port (Option82 Circuit ID page)

15.8 IP source guard

MENU Security › IP Source Guard

IP source guard filters traffic by source IP (and optionally MAC) address, preventing devices from spoofing addresses. Bindings come from DHCP snooping or are added manually.

Parameter	Description
State	Enable IP source guard on the port
Verify Source	**IP**: check source IP. **IP-MAC**: check source IP and MAC.
Max Entry	Maximum bindings on the port

Under **IMPV Binding**, click **Add** to create a static binding of port, VLAN, MAC address and IP address (IP-MAC-port-VLAN or IP-port-VLAN). **Save Database** stores the binding table.

16 ACL

Access control lists filter traffic. Each list contains rules (ACEs) that match fields in the frame and permit, deny or shut down the port. ACLs are also used by other functions, such as QoS classification. Create the ACL, add rules to it, then bind it to ports.

Type	Matches
MAC ACL	Matches Layer 2 fields: MAC addresses, EtherType, VLAN, 802.1p
IPv4 ACL	Matches IPv4 addresses, protocol, ports, ToS and more
IPv6 ACL	As IPv4, for IPv6 traffic

16.1 MAC ACL

MENU ACL › MAC ACL / ACL › MAC ACE

Parameter	Description
Sequence	Rule order, 1–2147483647
Action	Permit, Deny or Shutdown
Source / Destination MAC	Address and mask, or Any
EtherType	0x0600–0xFFFF, or Any
VLAN	1–4094, or Any
802.1p	Priority and mask 0–7, or Any

16.2 IPv4 and IPv6 ACL

MENU ACL › IPv4 ACL / IPv4 ACE · ACL › IPv6 ACL / IPv6 ACE

Parameter	Description
Sequence	Rule order, 1–2147483647
Action	Permit, Deny or Shutdown
Protocol	ICMP, TCP, UDP etc., or Any
Source / Destination IP	Address and mask, or Any
Type of Service	DSCP 0–63 or IP precedence 0–7, or Any
Source / Destination Port	Single port or range 0–65535, or Any
TCP Flags	URG, ACK, PSH, RST, SYN, FIN: Set, Unset or Don’t care
ICMP Type / Code	ICMP message type and code, or Any

16.3 ACL binding

MENU ACL › ACL Binding

Select ports and bind a MAC ACL and an IPv4 **or** IPv6 ACL to them. IPv4 and IPv6 ACLs cannot be bound to the same port.

ELECTRA-M12-10GB-FIBER · CHAPTERS 17–19

QoS, diagnostics and management

Traffic priority, rate limiting, troubleshooting tools, firmware, configuration, SNMP and RMON

17 QoS

QoS (Quality of Service) gives time-critical traffic, such as video and voice, priority over other traffic when the network is congested. Traffic is classified by its priority field and placed in one of the port's output queues. VLAN frames carry an 802.1p priority (CoS, 0–7) in the 802.1Q tag; IP packets carry a DSCP value (0–63) or IP precedence (0–7) in the ToS byte. In all cases a higher value means higher priority.

17.1 Property

MENU QoS › General › Property

Parameter	Description
State	Enable QoS globally
Trust Mode	Which priority field to trust: CoS, DSCP, CoS-DSCP or IP precedence
CoS (port)	Default CoS 0–7 for untagged traffic on the port
Port Trust Mode	Enable trust on the port
Remark CoS / DSCP / IP Priority	Rewrite the priority field on outgoing traffic

17.2 Queue scheduling

MENU QoS › General › Queue Scheduling

Parameter	Description
Strict Priority (SP)	Higher queues are always served first
WRR	Queues share bandwidth by weight
Weight	Share of the bandwidth for each queue in WRR mode

17.3 Priority mapping

These tables decide which queue each priority value is placed in. Change the mapping and click **Apply**.

Page (QoS › General)	Maps
CoS Mapping	802.1p priority 0–7 → queue
DSCP Mapping	DSCP 0–63 → queue

IP Precedence Mapping	IP precedence 0–7 → queue

17.4 Rate limiting

MENU QoS › Rate Limit › Ingress / Egress Port

Limits the bandwidth received (ingress) or sent (egress) on a port. Select ports, click **Edit**, enable the limit and enter the rate: **16–1,000,000 kbps**. **Egress Queue** sets rate limits per output queue.

18 Diagnostics

18.1 Logging

MENU Diagnostics › Logging › Property / Remote Server

Property enables logging and sets aggregation, aging and severity levels. Under **Remote Server**, click **Add** to send log messages to a remote syslog server. Logged messages are shown under Status › Logging Message.

18.2 Ping and traceroute

MENU Diagnostics › Ping / Diagnostics › Traceroute

Enter a host name or IP address and click **Ping** to test whether the device is reachable. **Traceroute** shows each hop on the path to the destination and its response time.

18.3 Fiber module

MENU Diagnostics › Fiber Module

Select a port to view the DDM (digital diagnostic monitoring) values of the SFP module, such as temperature, voltage and transmit/receive optical power. Useful when troubleshooting fibre links.

18.4 UDLD

MENU Diagnostics › UDLD › Property / Neighbor

UDLD (Unidirectional Link Detection) detects fibre or copper links that only work in one direction, which can otherwise cause spanning tree loops. UDLD must be supported at both ends of the link.

Mode	Description
Disabled	UDLD off on the port
Normal	Detects one-way links, marks the port as undetermined and logs the event
Aggressive	Detects one-way links and tries to re-establish the link for 8 seconds. If there is no echo, the port is error-disabled.

Neighbor lists UDLD neighbours: device ID and name, port ID, state, expiration time, and message and timeout intervals.

19 Management

19.1 User accounts

MENU Management › User Account

Add users and change user names, passwords and privilege levels.

> **CAUTION** Change the default admin password during commissioning.

19.2 Firmware

MENU Management › Firmware › Manual Upgrade / Active Image

The switch holds two firmware images. A new firmware file is uploaded to the inactive image and only used after it has been activated.

1. Under **Manual Upgrade**, choose the transfer method and select the firmware file. Start the upgrade.
2. Under **Active Image**, select the new image and click **Apply**.
3. Save the configuration and reboot the switch. The new image is used after the restart.

> **CAUTION** Do not power off the switch during a firmware upgrade.

19.3 Configuration files

MENU Management › Configuration › Manual Upgrade

Upload (**Upgrade**) or download (**Backup**) configuration files and logs via TFTP or HTTP. Keep a backup of the configuration after commissioning.

MENU Management › Configuration › Save Configuration

Copies configurations between running, startup and backup. To keep changes after a reboot, save the **running configuration** as the **startup configuration**. The **Save** button at the top right of the interface does the same.

File	Description
Running configuration	Active settings; lost at reboot unless saved
Startup configuration	Loaded when the switch starts
Backup configuration	Spare copy that can be restored to running or startup

Click **Factory Reset** to restore the factory settings, then restart the device.

> **NOTE** A factory reset restores the default IP address 192.168.1.254 and the login admin / admin.

19.4 SNMP

MENU Management › SNMP

SNMP lets a network management system (NMS) monitor and configure the switch. The switch runs an SNMP agent that answers requests and sends traps when events occur. SNMPv1, v2c and v3 are supported. SNMP must also be enabled under Security › Management Access › Management Service.

Page	Description
View	MIB views: name, OID subtree, Included or Excluded
Group	Groups: version (v1, v2c, v3), security level and read, write and notify views
Community	v1/v2c communities: group or view, and read-only or read-write access
User	v3 users: group, security level, authentication and privacy (encryption) method
Engine ID	Local and remote SNMP engine IDs
Trap Event	Which events send traps: authentication failure, link up/down, cold start, warm start
Notification	Trap receivers: address, version, Trap or Inform, community or user, security level, UDP port (162), timeout (15 s, 1–300) and retries (3, 1–255)

19.5 RMON

MENU Management › RMON

RMON (Remote Monitoring) collects traffic statistics on the switch itself and can raise alarms, reducing the load on the management system. The switch supports the statistics, history, event and alarm groups.

Group	Description
Statistics	Per-port counters (collisions, CRC errors, undersize/oversize frames, broadcast/multicast, bytes and packets). **Clear**, **Refresh** and **View**; automatic refresh can be set.
History	Periodic samples per port: interval 1–3600 s (1800 s default), up to 50 samples (default 50)
Event	What happens when an alarm triggers: log, trap, log and trap, or nothing. Community, description and owner.
Alarm	Monitors a counter on a port: interval (100 s default), absolute or delta sampling, rising and falling thresholds and the events they trigger

Index

A

AAA 26
Access port 12
Accessing the switch 5
ACL 29
ACL binding 30
Admin password 33, 5
ARP 24, 28
Assigning ports to VLANs 12
Authentication manager (802.1X, MAC and web) 27

B

Backup configuration 33
Baud rate 6
BPDU guard / filter 16
Broadcast storm 11

C

Changing the management IP address 6
Circuit ID (Option 82) 28
Client list and static bindings 21
COM port 6
Configuration files 33
Console port 6
Console port (CLI) 6
CoS mapping 31
Creating VLANs 11

D

Daylight saving time 8
DDM (optical diagnostics) 32
Default IP address 5, 33
Default login 5
DHCP 21
DHCP relay 21
DHCP server 21
DHCP snooping 28
Diagnostics 32
Discovery (LLDP) 19
DNS 7
DoS protection 28
DSCP 31, 31
Dynamic addresses 15
Dynamic ARP inspection 28

E

Edge port 16
ERPS 18
ERPS instance 18
Error disabled 9, 7
Example: MSTP load sharing 17

F

Factory reset 33
Fiber module 32
Filtering addresses 15
Firmware 33
Firmware upgrade 33
Flow control 9, 6
Foreword 5

G

General settings 22
Global properties 16
Guest VLAN 27
GVRP 14

H

Hybrid port 12

I

IGMP querier 22
IGMP snooping 22
IP camera traffic 12, 22
IP pool setting 21
IP source guard 29
IPv4 and IPv6 ACL 30
IPv4 interfaces 23
IPv4 static routes and ARP 24
IPv6 24, 30
Isolation (protected port) 10

J

Jumbo frame 10

L

LACP 9
LAG 9
Link aggregation 9
Link aggregation and logging 7
LLDP properties 19
LLDP-MED 19
Logging 32
Loopback detection 18

M

MAC ACL 29
MAC address table 7, 15
MAC VLAN 13
Management 33
Management access 27
Management IP address 6, 23
Manual conventions 5
Mirroring 11
MLD snooping 23
Monitoring 20
MST instances 17
MST port settings 17
MSTP 16, 17
MTU 10
Multicast 22
MVR 23

N

Network 7

O

Option 82 28
OSPF 24

P

802.1p (CoS) 31, 29
Password 33, 5
Ping and traceroute 32
Port 9
Port mirroring 11
Port security 10
Port security addresses 15
Port setting 9
Port settings 16, 19
Port statistics 7
Port VLAN settings 12
Priority mapping 31
Property 18, 21, 31
Protected port 10
Protocol VLAN 13
PuTTY 6, 6
PVID 12, 11

Q

802.1Q 12
QoS 31
Queue scheduling 31

R

RADIUS 26
RADIUS and TACACS+ 26
Rate limiting 32
Reboot 7
RIP 24
RMON 34
Routing 23
RSTP 16

S

Save configuration 33, 6
Security 26
SFP module 5, 32
SNMP 33
SNTP 8
Spanning tree 16
SSH 6, 27
Static addresses 15
Static route 24
Status 7
Storm control 11
STP 16
Surveillance VLAN 12
Syslog server 32
System information 7
System time 8

T

TACACS+ 26
Target audience 5
Telnet 6, 27
Telnet and SSH 6
The web interface 6
Trap (SNMP) 33
Trunk port 12

U

UDLD 32
User accounts 33

V

VLAN 11
VLAN interface (VLANIF) 23, 23
VLAN interface address group 21
Voice VLAN 13

W

Web interface 5, 6

X

802.1X 27