



# KSwitch D10 MMT Managed Time Sensitive Ethernet Switch

Doc. User Guide, Rev. 1.7

Doc. ID: 1069-3835

This page has been intentionally left blank



# KSWITCH D10 MMT MANAGED TIME SENSITIVE ETHERNET SWITCH - USER GUIDE

## Disclaimer

Kontron would like to point out that the information contained in this user guide may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the user guide or any product characteristics set out in the user guide. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this user guide are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this user guide only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

This user guide is protected by copyright. All rights are reserved by Kontron. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron. Kontron points out that the information contained in this user guide is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this user guide only reflects the technical status of the products by Kontron at the time of publishing.

Brand and product names are trademarks or registered trademarks of their respective owners.

©2023 by Kontron Europe GmbH

Kontron Europe GmbH

Gutenbergstraße 2  
85737 Ismaning  
Germany  
[www.kontron.com](http://www.kontron.com)

## Intended Use

THIS DEVICE AND ASSOCIATED SOFTWARE ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE FOR THE OPERATION OF NUCLEAR FACILITIES, THE NAVIGATION, CONTROL OR COMMUNICATION SYSTEMS FOR AIRCRAFT OR OTHER TRANSPORTATION, AIR TRAFFIC CONTROL, LIFE SUPPORT OR LIFE SUSTAINING APPLICATIONS, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION IN A HAZARDOUS ENVIRONMENT, OR REQUIRING FAIL-SAFE PERFORMANCE, OR IN WHICH THE FAILURE OF PRODUCTS COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE (COLLECTIVELY, "HIGH RISK APPLICATIONS").

You understand and agree that your use of Kontron devices as a component in High Risk Applications is entirely at your risk. To minimize the risks associated with your products and applications, you should provide adequate design and operating safeguards. You are solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning your products. You are responsible to ensure that your systems (and any Kontron hardware or software components incorporated in your systems) meet all applicable requirements. Unless otherwise stated in the product documentation, the Kontron device is not provided with error-tolerance capabilities and cannot therefore be deemed as being engineered, manufactured or setup to be compliant for implementation or for resale as device in High Risk Applications. All application and safety related information in this document (including application descriptions, suggested safety measures, suggested Kontron products, and other materials) is provided for reference only.

---

**NOTICE**

You find the most recent version of the "General Safety Instructions" online in the download area of this product.

---

## Revision History

Revision	Brief Description of Changes	Date of Issue	Author /Editor
1.0	Initial version	2022-Oct-11	CW
1.1	Change CA UK to UKCA and removed 19" rack mount kit 2U/4U.	2022-Nov-07	CW
1.2	Included Configuration examples in Chapter 8.3.5, relocated TSN Chapter, included default information in Chapter 8.1.1, Serial Consol Setup information uses Putty.	2022-Nov-10	CW
1.3	Included new front & introduction page photos, hot surface warning in Ch. 4.4 with new hot surface symbol, updated Figure 13 and updated Example 6 in Ch. 8.3.5.	2023-Jan-26	CW
1.4	Included chapter 8.5.1. IEEE 802.1AS Configuration Added "switchport access vlan" command	2023-May-24	CD
1.5	Added a Wall Mount Direction Caution (horizontal only with heatsink facing upwards) and Alarm Relay Contact Caution (max. 30 VAC, 42 VDC and 37 VA). Increased altitude to 3000 m. New Fig. 2 Type label. New Figures 7, 11 and 12 with new ground symbol.	2024-Mar-12	CW
1.6	Changed Alarm Relay Contact Caution (max. 30 VAC, 42 VDC and 1 A).	2024-Mar-13	CW
1.7	Changed IEEE802.1as PTP description and configuration Some header changes (8.7.7, 8.7.8)	2025-Jan-27	CD

## Terms and Conditions

Kontron warrants products in accordance with defined regional warranty periods. For more information about warranty compliance and conformity, and the warranty period in your region, visit <https://www.kontron.com/terms-and-conditions>.

Kontron sells products worldwide and declares regional General Terms & Conditions of Sale, and Purchase Order Terms & Conditions. Visit <https://www.kontron.com/terms-and-conditions>.

For contact information, refer to the corporate offices contact information on the last page of this user guide or visit our website [CONTACT US](#).

## Customer Support

Find Kontron contacts by visiting: <https://www.kontron.de/support-and-services>.

## Customer Service

As a trusted technology innovator and global solutions provider, Kontron extends its embedded market strengths into a services portfolio allowing companies to break the barriers of traditional product lifecycles. Proven product expertise coupled with collaborative and highly-experienced support enables Kontron to provide exceptional peace of mind to build and maintain successful products.







For more details on Kontron's service offerings such as: enhanced repair services, extended warranty, Kontron training academy, and more visit <https://www.kontron.de/support-and-services>.

## Customer Comments

If you have any difficulties using this user guide, discover an error, or just want to provide some feedback, contact Kontron Support. Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised user guide on our website.

## Symbols

The following symbols may be used in this user guide

<b>⚠ DANGER</b>	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
<b>⚠ WARNING</b>	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
<b>NOTICE</b>	NOTICE indicates a property damage message.
<b>⚠ CAUTION</b>	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
	<p><b>Electric Shock!</b></p> <p>This symbol and title warn of hazards due to electrical shocks (&gt; 60 V) when touching products or parts of products. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.</p>
	<p><b>ESD Sensitive Device!</b></p> <p>This symbol and title informs that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.</p>
	<p><b>HOT Surface!</b></p> <p>Do NOT touch! Allow to cool before servicing.</p>
	<p><b>Laser!</b></p> <p>This symbol informs of the risk of exposure to laser beam and light emitting devices (LEDs) from an electrical device. Eye protection per manufacturer notice shall review before servicing.</p>
	<p>This symbol indicates general information about the product and the user guide.</p> <p>This symbol also indicates detail information about the specific product configuration.</p>
	<p>This symbol precedes helpful hints and tips for daily use.</p>

## For Your Safety

Your new Kontron product was developed and tested carefully to provide all features necessary to ensure its compliance with electrical safety requirements. It was also designed for a long fault-free life. However, the life expectancy of your product can be drastically reduced by improper treatment during unpacking and installation. Therefore, in the interest of your own safety and of the correct operation of your new Kontron product, you are requested to conform with the following guidelines.

### High Voltage Safety Instructions

As a precaution and in case of danger, the power connector must be easily accessible. The power connector is the product's main disconnect device.

#### **⚠ CAUTION**

##### **Warning**

All operations on this product must be carried out by sufficiently skilled personnel only.

#### **⚠ CAUTION**



##### **Electric Shock!**

Before installing a non hot-swappable Kontron product into a system always ensure that your mains power is switched off. This also applies to the installation of piggybacks. Serious electrical shock hazards can exist during all installation, repair, and maintenance operations on this product. Therefore, always unplug the power cable and any other cables which provide external voltages before performing any work on this product.

Earth ground connection to vehicle's chassis or a central grounding point shall remain connected. The earth ground cable shall be the last cable to be disconnected or the first cable to be connected when performing installation or removal procedures on this product.

### Optical Safety Instructions



##### **Laser!**

This symbol informs of the risk of exposure to laser beam and light emitting devices (LEDs) from an electrical device. Eye protection per manufacturer notice shall review before servicing.

When a connector is removed during installation, testing, or servicing, or when an energized fiber is broken, a risk of ocular exposure to optical energy that may be potentially hazardous occurs, depending on the laser output power.

The primary hazards of exposure to laser radiation from an optical-fiber communication system are:

- ▶ Damage to the eye by accidental exposure to a beam emitted by a laser source
- ▶ Damage to the eye from viewing a connector attached to a broken fiber or an energized fiber



## Special Handling and Unpacking Instruction

### NOTICE



#### ESD Sensitive Device!

Electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times.

### CAUTION

Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled. Follow the "General Safety Instructions for IT Equipment" supplied with the product.

Do not handle this product out of its protective enclosure while it is not used for operational purposes unless it is otherwise protected.

Whenever possible, unpack or pack this product only at EOS/ESD safe work stations. Where a safe work station is not guaranteed, it is important for the user to be electrically discharged before touching the product with his/her hands or tools. This is most easily done by touching a metal part of your system housing.

It is particularly important to observe standard anti-static precautions when changing piggybacks, ROM devices, jumper settings etc. If the product contains batteries for RTC or memory backup, ensure that the product is not placed on conductive surfaces, including anti-static plastics or sponges. They can cause short circuits and damage the batteries or conductive circuits on the product.

### Lithium Battery Precautions

If your product is equipped with a lithium battery, take the following precautions when replacing the battery.

### CAUTION

Danger of explosion if the battery is replaced incorrectly.

- ▶ Replace only with same or equivalent battery type recommended by the manufacturer.
- ▶ Dispose of used batteries according to the manufacturer's instructions.

## General Instructions on Usage

In order to maintain Kontron's product warranty, this product must not be altered or modified in any way. Changes or modifications to the product, that are not explicitly approved by Kontron and described in this user guide or received from Kontron Support as a special handling instruction, will void your warranty.

This product should only be installed in or connected to systems that fulfill all necessary technical and specific environmental requirements. This also applies to the operational temperature range of the specific board version that must not be exceeded. If batteries are present, their temperature restrictions must be taken into account.

In performing all necessary installation and application operations, only follow the instructions supplied by the present user guide.

Keep all the original packaging material for future storage or warranty shipments. If it is necessary to store or ship the product, then re-pack it in the same manner as it was delivered.

Special care is necessary when handling or unpacking the product. See Special Handling and Unpacking Instruction.

## Quality and Environmental Management

Kontron aims to deliver reliable high-end products designed and built for quality, and aims to complying with environmental laws, regulations, and other environmentally oriented requirements. For more information regarding Kontron's quality and environmental responsibilities, visit <http://www.kontron.com/about-kontron/corporate-responsibility/quality-management>.

### Disposal and Recycling

Kontron's products are manufactured to satisfy environmental protection requirements where possible. Many of the components used are capable of being recycled. Final disposal of this product after its service life must be accomplished in accordance with applicable country, state, or local laws or regulations.

### WEEE Compliance

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to:

- ▶ Reduce waste arising from electrical and electronic equipment (EEE)
- ▶ Make producers of EEE responsible for the environmental impact of their products, especially when the product become waste
- ▶ Encourage separate collection and subsequent treatment, reuse, recovery, recycling and sound environmental disposal of EEE
- ▶ Improve the environmental performance of all those involved during the lifecycle of EEE



---

Environmental protection is a high priority with Kontron.  
Kontron follows the WEEE directive  
You are encouraged to return our products for proper disposal.

---

## Table of Contents

Symbols .....	7
For Your Safety .....	8
High Voltage Safety Instructions .....	8
Optical Safety Instructions .....	8
Special Handling and Unpacking Instruction .....	9
Lithium Battery Precautions .....	9
General Instructions on Usage .....	9
Quality and Environmental Management .....	10
Disposal and Recycling .....	10
WEEE Compliance .....	10
Table of Contents .....	11
List of Tables .....	13
List of Figures .....	14
1/ Introduction .....	15
2/ General Safety Instructions .....	16
2.1. Laser .....	18
2.2. Electrostatic Discharge (ESD) .....	18
2.3. Grounding Methods .....	18
3/ Shipment and Packaging .....	19
3.1. Packaging .....	19
3.2. Unpacking .....	19
3.3. Scope of Delivery .....	19
3.4. Accessories .....	21
3.4.1. Mounting Kits .....	21
3.4.2. SFP Modules .....	21
3.5. Product Identification Type Label .....	21
4/ Switch Features .....	22
4.1. Faceplate Features .....	23
4.1.1. RJ45 Copper Ethernet Ports .....	23
4.1.2. SFP Fiber Ethernet Ports .....	24
4.1.3. Indicator LEDs (P1, P2, ALM and Ethernet Ports) .....	27
4.2. Top Side Features .....	28
4.2.1. DC Terminal Block .....	28
4.2.2. Alarm Contacts .....	29
4.2.3. Serial Console Port .....	29
4.2.4. Reset Button .....	30
4.2.5. Ground Stud .....	30
4.3. Rear Side Features .....	31
4.3.1. DIN-Rail Clip .....	31
4.3.2. Wall Mounting .....	31
4.4. Side Features .....	33
5/ Mounting .....	34
5.1. DIN-Rail Mounting .....	34
5.2. DIN-Rail Removal .....	35
5.3. Wall Mounting .....	35
6/ Starting Up .....	37
7/ Technical Specification .....	39
7.1. Technical Specification .....	39
7.2. Environmental Specification .....	40

7.3. Mechanical Specification .....	40
7.4. Power Specification .....	44
7.5. Compliance .....	45
8/ Software Interface .....	47
8.1. Accessing the Switch .....	47
8.1.1. Accessing the IP address .....	47
8.1.2. Accessing the Switch NOS using the Web UI .....	47
8.1.3. Accessing the Switch NOS CLI using Telnet from a Remote Computer .....	48
8.1.4. Accessing the Operating System .....	53
8.1.5. Help Tools .....	53
8.2. Managing the KSwitch D10 MMT Using the Web Interface .....	54
8.3. Using the CLI .....	55
8.3.1. Completing a Partial Command .....	55
8.3.2. Command History .....	55
8.3.3. Using the Backspace Key in NOS CLI .....	55
8.3.4. 'no' Commands .....	56
8.3.5. Configuration Examples using the CLI .....	56
8.4. General Maintenance Commands .....	59
8.4.1. Configure Terminal .....	59
8.4.2. Interface .....	59
8.4.3. Exit .....	60
8.4.4. End .....	60
8.4.5. Show Running-Config .....	60
8.4.6. Show Running-Config All-Default .....	61
8.4.7. Dir .....	61
8.4.8. Copy Running-Config Startup-Config .....	61
8.4.9. Copy Running-Config Flash:<file-name> .....	62
8.4.10. Del Flash:<file-name> .....	62
8.4.11. Reload Cold .....	62
8.4.12. Reload Defaults .....	63
8.4.13. Reload Defaults Keep-IP .....	63
8.4.14. Show Version .....	63
8.5. TSN Features .....	64
8.5.1. IEEE 802.1AS Configuration .....	64
8.5.2. Using TSN Functions with PTP Time Synchronisation .....	64
8.5.3. Credit Based Shaper .....	65
8.5.4. Time Aware Shaper (TAS) .....	67
8.5.5. Configuration Considerations .....	69
8.5.6. Frame Preemption .....	73
8.6. Network .....	75
8.6.1. Ethernet Ports - Configuration Commands .....	75
8.6.2. Ethernet Port View Commands .....	78
8.6.3. IPv4, IPv6 - Configuration Commands .....	79
8.6.4. IPv4, IPv6 - View Commands .....	81
8.6.5. NTP (Network Time Protocol) - Configuration Commands .....	82
8.6.6. NTP (Network Time Protocol) - View Commands .....	82
8.6.7. Time Zone - Configuration Commands .....	83
8.6.8. Clock Summer-Time - Daylight Savings Time Configuration .....	84
8.6.9. Time Zone - View Commands .....	85
8.6.10. SysLog Report - Configuration Commands .....	86
8.6.11. SysLog Report - View Commands .....	87

8.6.12. MAC Table Learning - Configuration Commands .....	88
8.6.13. MAC Table Learning - View Commands .....	90
8.6.14. Routing - View Commands .....	91
8.7. Access Control .....	92
8.7.1. Local Users - Configuration Commands .....	92
8.7.2. Local Users - View Commands .....	93
8.7.3. Web Server - Configuration Commands .....	94
8.7.4. Web Server - View Commands .....	95
8.7.5. Telnet/SSH/Web - Configuration Commands .....	95
8.7.6. Telnet/SSH/Web - View Commands .....	98
8.7.7. Access Management - Configuration Commands .....	98
8.7.8. Access Management - View Commands .....	99
8.8. VLAN .....	100
8.8.1. VLAN Configuration Commands and Port Types .....	100
8.8.2. VLAN Ethertype S-Custom-Port .....	101
8.8.3. Switchport Mode .....	103
8.8.4. View VLAN Members .....	109
8.8.5. View VLAN Ports .....	109
8.9. Spanning Tree .....	110
8.9.1. STP Bridge Configuration Commands .....	110
8.9.2. STP Bridges View Commands .....	115
8.10. Port Mirroring .....	116
8.10.1. Port Mirroring Configuration .....	116
8.11. System Information .....	118
8.11.1. Read LAN9668 Temperature .....	118
8.11.2. Read Phy Temperature .....	118
8.11.3. Interface Status .....	118
8.11.4. Interface Capabilities .....	118
8.11.5. Interface Statistics .....	118
8.12. Managing the Switch Using SNMP .....	120
9/ Maintenance .....	121
9.1. Hardware Maintenance .....	121
9.2. Software Maintenance .....	121
9.2.1. Reset and Restore Switch .....	121
9.2.2. Switch Configuration .....	122
9.2.3. Software Update .....	125
10/ Technical Support .....	126
10.1. Returning Defective Merchandise .....	126
11/ Warranty .....	128
11.1. Limitation/Exemption from Warranty Obligation .....	128
List of Acronyms .....	129
About Kontron .....	130

## List of Tables

Table 1: Scope of Delivery .....	19
Table 2: Mounting Kit Accessories .....	21
Table 3: Ethernet Ports (RJ45) Pin Assignment .....	23
Table 4: 2.5G SFP Ethernet Port .....	26
Table 5: Indicator LEDs .....	27
Table 6: Serial Console Port (RJ45) .....	29
Table 7: Mounting with Wall Mount Plates (vertical and horizontal) .....	35

Table 8: Technical Specification .....	39
Table 9: Environmental Specification .....	40
Table 10: Mechanical Specification .....	40
Table 11: Electrical Specification .....	44
Table 12: CE Compliance .....	45
Table 13: International Compliance .....	45
Table 14: List of Acronyms .....	129

## List of Figures

Figure 1: KSwitch D10 MMT 8-Port Ethernet Switches .....	15
Figure 2: Type Label Example .....	21
Figure 3: Switch Variants .....	22
Figure 4: RJ45 Ethernet Ports .....	23
Figure 5: SFP Ethernet Ports .....	24
Figure 6: Indicator LEDs .....	27
Figure 7: Top Side Features .....	28
Figure 8: Rear Side Features .....	31
Figure 9: Left Side Features .....	33
Figure 10: DIN-Rail Clip Upper Position .....	34
Figure 11: Mechanical Dimensions KSwitch D10 MMT 8G (mm) .....	42
Figure 12: Mechanical Dimensions KSwitch D10 MMT 6G-2GS (mm) .....	42
Figure 13: Serial Consol Port .....	49

## 1/Introduction

This user guide focuses on describing the special features of Kontron's KSwitch D10 MMT 8-port managed time sensitive industrial DIN Rail Ethernet switch, also referred to as switch within this user guide

This user guide provides an overview of the switch's features and available accessories to help users to set up, mount, operate, manage and maintain the switch properly. Managed switches help users to prioritize partition and organize their network to provide reliable and good quality services.

To ensure you have the latest version of this user guide, visit Kontron's [KSwitch Industrial Ethernet Switches](#).

For safety reasons Kontron recommends that new users to study the instructions within this user guide before switching on the power.

Figure 1: KSwitch D10 MMT 8-Port Ethernet Switches



Key features are:

- ▶ Industrial fully managed
- ▶ 8-port Ethernet switch
  - ▶ 6x 10BASE-T/100BASE-TX/1000BASE-T
  - ▶ 2x 2.5GBASE-X/1000BASE-X or 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T
- ▶ Copper and fiber connectivity
- ▶ Time Sensitive Network (TSN) features
- ▶ Trigger In/Out
- ▶ IP 30 protection
- ▶ Rugged fanless design
- ▶ Dual redundant power supply (12 VDC to 58 VDC)
- ▶ -40°C to 70°C operating temperature
- ▶ Flexible mounting option
  - ▶ DIN-Rail
  - ▶ Wall mount (horizontal and vertical)

## 2/General Safety Instructions

Please read this passage carefully and take careful note of the instructions, which have been compiled for your safety and to ensure to apply in accordance with intended regulations. If the following general safety instructions are not observed, it could lead to injuries to the operator and/or damage of the product; in cases of non-observance of the instructions Kontron Europe is exempt from accident liability, this also applies during the warranty period.

The product has been built and tested according to the basic safety requirements for low voltage (LVD) applications and has left the manufacturer in safety-related, flawless condition. To maintain this condition and to also ensure safe operation, the operator must not only observe the correct operating conditions for the product but also the following general safety instructions:

- ▶ The product must be used as specified in the product documentation, in which the instructions for safety for the product and for the operator are described. These contain guidelines for setting up, installation and assembly, maintenance, transport or storage.
- ▶ The on-site electrical installation must meet the requirements of the country's specific local regulations.
- ▶ If a power cable comes with the product, only this cable should be used. Do not use an extension cable to connect the product.
- ▶ To guarantee that sufficient air circulation is available to cool the product, please ensure that the ventilation openings are not covered or blocked. If a filter mat is provided, this should be cleaned regularly. Do not place the product close to heat sources or damp places. Make sure the product is well ventilated.
- ▶ Only connect the product to an external power supply providing the voltage type (AC or DC) and the input power (max. current) specified on the Kontron Product Label and meeting the requirements of the Limited Power Source (LPS) and Power Source (PS2) of UL/IEC 62368-1 .
- ▶ Only products or parts that meet the requirements for Power Source (PS1) of UL/IEC 62368-1 may be connected to the product's available interfaces (I/O).
- ▶ Before opening the product, make sure that the product is disconnected from the mains.
- ▶ Switching off the product by its power button does not disconnect it from the mains. Complete disconnection is only possible if the power cable is removed from the wall plug or from the product. Ensure that there is free and easy access to enable disconnection.
- ▶ The product may only be opened for the insertion or removal of add-on cards (depending on the configuration of the product). This may only be carried out by qualified operators.
- ▶ If extensions are being carried out, the following must be observed:
  - ▶ all effective legal regulations and all technical data are adhered to
  - ▶ the power consumption of any add-on card does not exceed the specified limitations
  - ▶ the current consumption of the product does not exceed the value stated on the product label.
- ▶ Only original accessories that have been approved by Kontron Europe can be used.
- ▶ Please note: safe operation is no longer possible when any of the following applies:
  - ▶ the product has visible damages or
  - ▶ the product is no longer functioning
 In this case the product must be switched off and it must be ensured that the product can no longer be operated.
- ▶ Handling and operation of the product is permitted only for trained personnel within a work place that is access controlled.
- ▶ CAUTION: Risk of explosion if the battery is replaced incorrectly (short-circuited, reverse-poled, wrong battery type). Dispose of used batteries according to the manufacturer's instructions.
- ▶ This product is not suitable for use in locations where children are likely to be present

### Additional Safety Instructions for DC Power Supply Circuits

- ▶ To guarantee safe operation, please observe that:
  - ▶ the external DC power supply must meet the criteria for LPS and PS2 (UL/IEC 62368-1)
  - ▶ no cables or parts without insulation in electrical circuits with dangerous voltage or power should be touched directly or indirectly
  - ▶ a reliable protective earthing connection is provided
  - ▶ a suitable, easily accessible disconnecting device is used in the application (e.g. overcurrent protective device), if the product itself is not disconnectable



- ▶ a disconnect device, if provided in or as part of the product, shall disconnect both poles simultaneously
- ▶ interconnecting power circuits of different products cause no electrical hazards
- ▶ A sufficient dimensioning of the power cable wires must be selected - according to the maximum electrical specifications on the product label - as stipulated by EN62368-1 or VDE0100 or EN60204 or UL61010-1 regulations.

## 2.1. Laser




---

### **Laser!**

When a connector is removed, or when an energized fiber is broken, a risk of ocular exposure to optical energy that may be potentially hazardous occurs, depending on the laser output power.

Primary hazards of exposure to laser radiation from an optical-fiber communication system are:

- damage to the eye by accidental exposure to a beam emitted by a laser source
  - damage to the eye from viewing a connector attached to a broken fiber or an energized fiber
- 

## 2.2. Electrostatic Discharge (ESD)




---

A sudden discharge of electrostatic electricity can destroy static-sensitive devices or micro-circuitry.

---

Therefore, proper packaging and grounding techniques are necessary precautions to prevent damage. Always take the following precautions:

1. Transport ESD sensitive parts in ESD safe containers such as boxes or bags, until they arrive at an ESD safe workplace.
2. Always be properly grounded when touching sensitive components, or assembly.
3. Store ESD sensitive components in protective packaging or on antistatic mats.

## 2.3. Grounding Methods

By adhering to the guidelines below, electrostatic damage to the product may be avoided:

1. Cover workstations with approved antistatic material/mat. Always wear a wrist strap connected to workplace or heel straps.
2. Use properly grounded tools and equipment such as field service tools that are conductive.
3. Always handle ESD sensitive components by their edge or by their casing.
4. Avoid contact with pins, leads, or circuitry.
5. Switch off power and input signals before inserting and removing connectors or connecting test equipment.
6. Keep work area free of non-conductive materials such as ordinary plastic assembly aids and Styrofoam.

## 3/ Shipment and Packaging

### 3.1. Packaging

All parts are delivered together in a switch specific cardboard package designed to provide adequate protection to absorb shock. Kontron recommends keeping the packaging to store or transport the switch.

### 3.2. Unpacking

To unpack the switch, perform the following:

1. Remove packaging.
2. Do not discard the original packaging. Keep the original packaging for future transportation or storage.
3. Check the delivery for completeness by comparing the delivery with the original order.
4. Keep the associated paperwork. It contains important information for handling the switch.
5. Check the contents for visible shipping damage.

If you notice any shipping damage or inconsistencies between the contents and the original order, contact your Kontron representative for help and information.

### 3.3. Scope of Delivery

Check that your delivery is complete, and contains the items listed below. If you discover damaged or missing items, contact your dealer.

Table 1: Scope of Delivery

Delivered Items	Quantity	Description
KSwitch D10 MMT 6G-2GS	1	8 port managed industrial Ethernet switch: 6x RJ45 Copper 10BASE-T/100BASE-TX/1000BASE-T 2x SFP slot Fiber 2.5GBASE-X/1000BASE-X
DC Terminal Block	1	6-pin DC terminal block
DIN-Rail Mounting Kit	1	DIN-Rail clip and three screws
General Safety Instructions Sheet	1	Important general safety instructions for set up and operation



Delivered Items	Quantity	Description
KSwitch D10 MMT 8G	1	8 port managed industrial Ethernet switch: 6x RJ45 Copper 10BASE-T/100BASE-TX/1000BASE-T 2x RJ45 Copper 10BASE-T/100BASE-TX/1000BASE-T/ 2.5GBASE-T
DC Terminal Block	1	6-pin DC terminal block
DIN-Rail Mounting Kit	1	DIN-Rail clip and three screws
General Safety Instructions Sheet	1	Important general safety instructions for set up and operation



### 3.4. Accessories

#### 3.4.1. Mounting Kits

Table 2: Mounting Kit Accessories

Product Name/Product Group		Description
		WK25
		Wall Mount Kit includes two wall mount plates and four (M3x5) screws to attach the plates to the switch.

**CAUTION**

Horizontal mounting is only permitted with the heatsink facing upwards.

#### 3.4.2. SFP Modules

For information regarding reference SFP modules, contact [Kontron Support](#).

### 3.5. Product Identification Type Label

Figure 2: Type Label Example



- |                                   |                            |
|-----------------------------------|----------------------------|
| 1 Model full name                 | 5 Production date          |
| 2 Kontron Material Number         | 6 Electrical specification |
| 3 Revision number                 | 7 Compliance information   |
| 4 Serial Number (SN) with barcode | 8 QI Code                  |

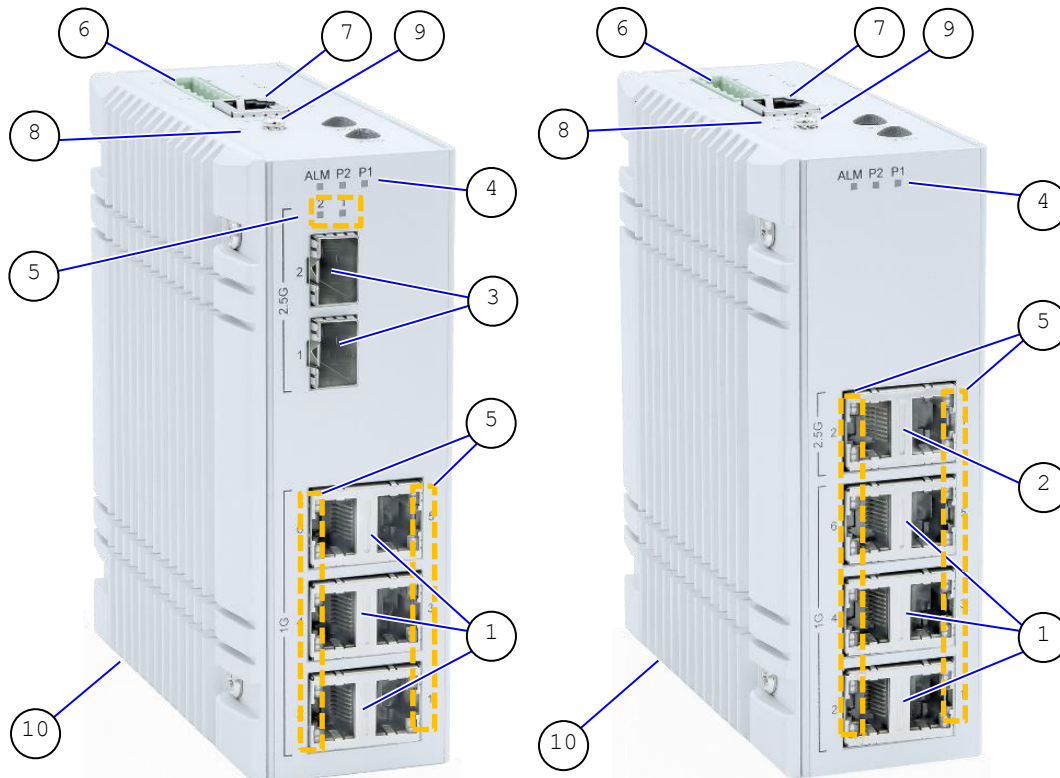
## 4/Switch Features

Before working with the switch, Kontron recommends users to take a few minutes to learn about the switch's various features and to observe the instructions and warning notices within this user guide.

Figure 3: Switch Variants

KSwitch D10 MMT 6G-2GS

KSwitch D10 MMT 8G



- |   |   |    |                        |
|---|---|----|------------------------|
| 1 | 6x RJ45 copper Ethernet ports<br>10BASE-T /100BASE-TX/1000BASE-T            | 6  | 1x DC terminal block   |
| 2 | 2x RJ45 copper Ethernet ports<br>10BASE-T /100BASE-TX/1000BASE-T/2.5GBASE-T | 7  | 1x Serial console port |
| 3 | 2x SFP slot fiber Ethernet ports<br>(2.5GBASE-X/1000BASE-X)                 | 8  | 1x Reset button        |
| 4 | Indicator LEDs (P1, P2, ALM)  | 9  | 1x Ground stud         |
| 5 | Indicator LEDs (Speed, Link/Activity)                                       | 10 | 1x Heatsink            |

## 4.1. Faceplate Features

The faceplate supports eight Ethernet ports (cooper and fiber) and indication LEDs.

### 4.1.1. RJ45 Copper Ethernet Ports

The RJ45 copper ports labelled 1G '1' to '6' are 10BASE-T/100BASE-TX/1000BASE-T Ethernet ports and the RJ45 copper ports labelled 2.5G '1' to '2' are 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T Gigabit Ethernet ports.

To achieve the specified Ethernet port performance use Category 5 twisted pair cables with 10BASE-T/100BASE-TX and Category 5E, 6 or 6a or better with 1000BASE-T/2.5GBASE-T Ethernet networks.

When connecting the switch to a PC use a straight-through or a cross-over Ethernet cable and when connecting the switch to another Ethernet device use UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair) Ethernet cables (for connections up to 100 m/328 ft.).

Figure 4: RJ45 Ethernet Ports



Table 3: Ethernet Ports (RJ45) Pin Assignment

Pin	Signal
1, 2	T/Rx+, T/Rx-
3, 6	R/Tx+, R/Tx-
4, 5	T/Rx+, T/Rx-
7, 8	R/Tx+, R/Tx-



#### Supported Ethernet Cables:

Use either UTP or STP Cat 5 twisted pair cables with 10BASE-T/100BASE-TX/1000BASE-T and Cat 5E, 6 or 6a or better with 1000BASE-T/2.5GBASE-T Ethernet networks for connections up to 100 m/328 ft.

### 4.1.2. SFP Fiber Ethernet Ports

The SFP ports labelled 2.5G '1' and '2' are 2.5GBASE-X/1000BASE-X SFP fiber Ethernet ports. SFP modules are hot swappable and plug into the SFP port to enable connection to other devices or the networks, using either fiber optic or copper network cables. When a SFP module with optical ports plugs into a SFP port, fiber patch cables are required for data transmission. When a SFP module with electrical ports plugs into a SFP port, Ethernet copper cables are required for data transmission.

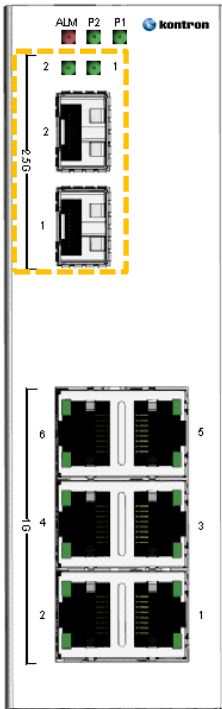
For each port there is a transmit (TX) and receive (RX) signal. When making connections ensure that the transmit (TX) port of the switch connects to the receive (RX) port of the other device, and the receive (RX) port of the switch connects to the transmit (TX) port of the other device.

For fiber SFP, the SFP port accepts 2.5GBASE-X/1000BASE-X SFP plug in fiber modules with LC type connector and depending on the SFP module multimode, single mode, long-haul (for connectors up to 80+ km).

For copper SFP the user must set the speed negotiated between the Copper SFP and the link partners in the switch.

For information on reference SFP modules, contact [Kontron Support](#).

Figure 5: SFP Ethernet Ports




---

**Supported Ethernet Cables:**



- Fiber: Fiber patch cables with LC connector
- Copper: Direct Attached Cables

Refer to the SFP module's datasheet regarding supported optical or copper cables.

---



**Laser!**

To avoid ocular exposure and a possible eye injury:

---



- Do not attempt to view optical connectors that might be emitting laser energy
  - Do not power up the laser without connecting the laser to the optical fiber and putting the cover in position, as laser outputs will emit infrared laser light at this point.
-

Table 4: 2.5G SFP Ethernet Port

Pin	Function	Signal
1	GND	Transmitter ground
2	TX_FAULT	Transmitter fault indication
3	TX_DIS	Optical output
4	SDA	Data serial ID
5	SCL	Clock serial ID
6	MOD_ABS	SFP present
7	RS0	Rate0 select
8	RX_LOS	Loss of signal
9	RS1	Rate1 select
10	GND	Receiver ground
11	GND	Receiver ground
12	RD+	Receiver data
13	RD-	Inverted receiver ground
14	GND	Receiver ground
15	V_VCCR	Receiver power (3.3 V)
16	V_VCCT	Transmitter power (3.3 V)
17	GND	Transmitter ground
18	TD+	Transmitter data
19	TD-	Inverted transmitter data
20	GND	Transmitter ground

### 4.1.3. Indicator LEDs (P1, P2, ALM and Ethernet Ports)

The LEDs indicate the normal operation of the switch and in the case of failure may be used for faultfinding.

Figure 6: Indicator LEDs

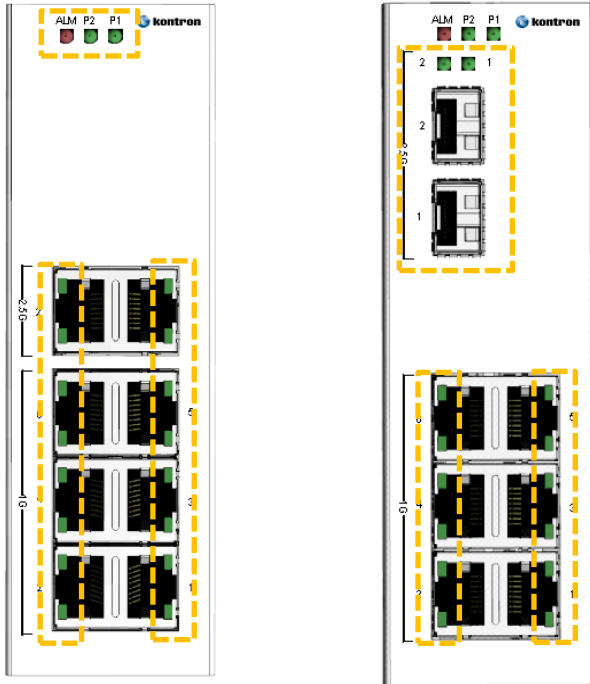


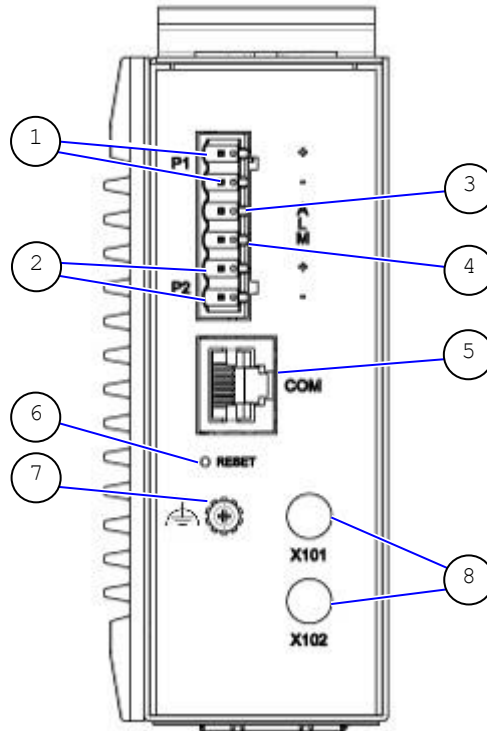
Table 5: Indicator LEDs

LED Name	Indicator /Color	Condition
P1/P2	Off	P1/P2 power line disconnect or does not have supply power
	On Green	P1/P2 power line has power
ALM	Off	No power failure alarm
	On Red	One of the two power rails is not active
Ethernet Port (RJ45 Copper) Link/Act- Left	Off	Ethernet link down
	On Green	Ethernet link up and no activity
	Flashing Green	Ethernet link up and activity
Ethernet Port (RJ45 Copper) Speed -Right	Off	10BASE-T/100BASE-TX
	On Green	1000BASE-T
	On Yellow	2.5G BASE-T
Ethernet Port (SFP) Link/Act LEDs	Off	Ethernet link down
	ON Green	Ethernet link up and no activity
	Flashing Green	Ethernet link up and activity

## 4.2. Top Side Features

The top side supports connectors to apply power and manage the switch.

Figure 7: Top Side Features



- |   |                 |   |   |
|---|-----------------|---|---|
| 1 | P1 +/- contacts | 5 | Serial console port                       |
| 2 | P2 +/-contacts  | 6 | Reset button                              |
| 3 | Alarm + contact | 7 | Ground stud                               |
| 4 | Alarm - contact | 8 | X101 and X102 are reserved for future use |

### 4.2.1. DC Terminal Block

The removable DC terminal block enables the connection of dual external (12 VDC to 58 VDC) power supplies using the P1+/- and P2+/- contacts (Figure 7, pos. 1 and 2). When dual power sources are connected to the switch, the switch utilizes the power supply with the higher voltage or the most stable power supply.

#### **CAUTION**

When connecting the power follow the polarity indicated for P1 +/- and P2+/-.



When attaching power wires to P1+/- and P2+/- on the DC terminal block consider:

- DC terminal block pitch, 5.08 mm (0.2 inch)
- Wire strip length 7 mm (0.28 inch)
- Wire size range: Solid wire: 12~24 AWG and Stranded wire: 12~24 AWG

- 
- Wire length 3 m (9.84 ft.) maximum
- 

#### 4.2.2. Alarm Contacts

The alarm contacts are available on the DC terminal block (Figure 7, pos. 3 and 4) and support fault alarm notification for power by detecting a power supply fail.

The default setting is Alarm Contact 'Normal Open'. To change the default setting to 'Normal Close' users are required to alter internal jumper settings. For more information, contact [Kontron Support](#).

#### **CAUTION**

---

When connecting the alarm contacts the maximum voltage must not exceed 30 VAC or 42 VDC at a maximum current of 1 A.

---




---

When attaching wires to the alarm contacts on the DC terminal block consider:

- DC terminal block pitch, 5.08 mm (0.2 inch)
  - Wire strip length 7 mm (0.28 inch)
  - Wire size range: Solid wire: 12~24 AWG and Stranded wire: 12~24 AWG
  - Wire length 3 m (9.84 ft.) maximum
- 

#### 4.2.3. Serial Console Port

The serial console port (Figure 7, pos. 5) enables local management of the switch. The serial console port features the RS232 serial management interface with TX and RX signals only and no hardware flow control. For more information, contact [Kontron Support](#).




---

The serial console port requires only the serial baud rate 115200 to be set up. Hardware flow control is not supported.

---

Table 6: Serial Console Port (RJ45)

Pin	Direction	Signal
1	Out/High	RTS <sup>[1]</sup>
2		NC
3	Out	TXD#
4		GND
5		GND
6	In	RXD#
7		NC
8	In	CTS

<sup>[1]</sup> Static active by resistor strapping

#### 4.2.4. Reset Button

The reset button (Figure 7, pos. 6) performs a warm reset. Pressing the reset button briefly performs a reboot without powering down. Pressing the reset button for a prolonged period-of-time (five seconds approximately) indicates a special event defined by the software, for future use.

The reset button is located within a small opening to avoid accidental activation. To press the reset button, use an instrument with a diameter of approximately 1 mm (0.04 inch), to enter the small opening and press the reset button.

#### 4.2.5. Ground Stud

The ground stud (Figure 7, pos. 7) connects to ground. The switch must be grounded properly for optimum system performance. Connect the switch to ground before connecting the power.

---

**▲ CAUTION**

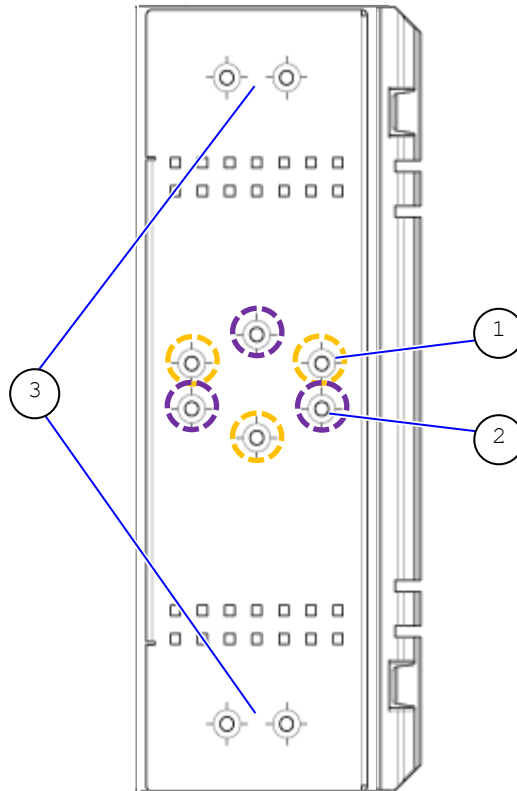
Ground properly using a ground that meets the ground requirements specified in your local, national and international region.

---

### 4.3. Rear Side Features

The rear side supports two installation methods.

Figure 8: Rear Side Features



- |  |  |
|--|--|
| <p>1 3x threaded screw openings for DIN-Rail clip (orange)</p> | <p>2 3x threaded screw openings for DIN-Rail clip (purple)</p> |
|  | <p>3 2x wall mount threaded screw openings</p>                 |

#### 4.3.1. DIN-Rail Clip

The mounting holes for the DIN-Rail clip (Figure 8, pos. 1 and pos. 2) changes the orientation of the DIN-Rail clip by 180°. For further mounting information, see Chapter 5.1: DIN-Rail Mounting.

#### 4.3.2. Wall Mounting

The set of mounting holes at the top and bottom (Figure 8, pos. 3) enable the installation of two wall mount plates. For further mounting information, see Chapter 5.3: Wall Mounting.

**⚠ CAUTION**

Horizontal mounting is only permitted with the heatsink facing upwards.

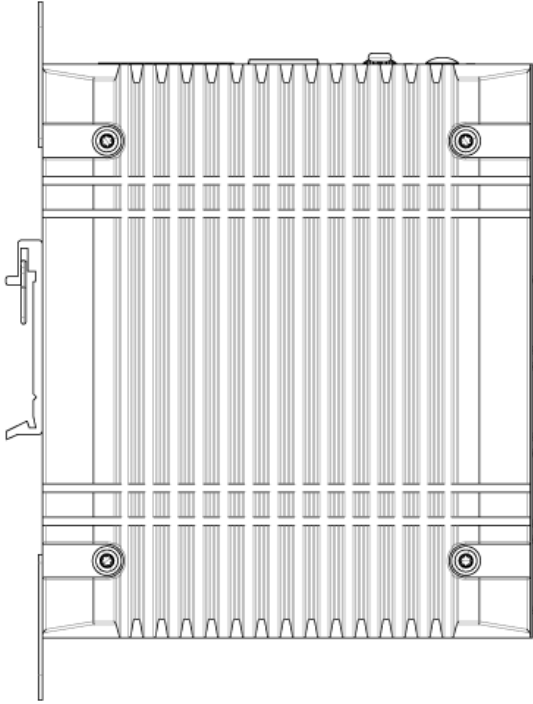
---



#### 4.4. Side Features

The switch is fanless and passively cooled by one heatsink positioned on the left side of the switch. The right side has no functional parts.

Figure 9: Left Side Features



---

##### **Hot Surface**

Heatsinks can get very hot. To avoid burns and personal injury:

- Do not touch the heatsink when the product is in operation
  - Allow the heatsink to cool before handling the product
  - Wear protective gloves
-

## 5/Mounting

Before installing or removing the switch read and observe the instructions within this user guide, including Chapter 2/: General Safety Instructions. Kontron assumes no responsibility for any damage resulting from failure to comply with these requirements.

### ⚠ CAUTION

Install the switch in the power off state only.

### ⚠ CAUTION

Horizontal mounting is only permitted with the heatsink facing upwards.



Before installing the switch consider the required orientation of the switch within the installation environment and access to connectors

The switch is fanless and passively cooled by a heatsink positioned on the left side of the switch. When installing the switch consider the ambient temperature in the installation environment around the switch. To allow for adequate heat dissipation without obstructions ensure a clearance of at least 20 mm around the switch.

### ⚠ CAUTION

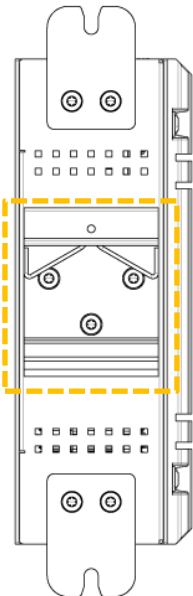
#### Prevent Overheating

Mount leaving a clearance of at least 20 mm around the switch, to ensure proper operation and prevent the switch from overheating.

### 5.1. DIN-Rail Mounting

The DIN-Rail clip enables easy installation or removal of the switch.

Figure 10: DIN-Rail Clip Upper Position



To install the switch on a DIN-Rail, perform the following:

1. Fasten the DIN-Rail clip on the switch in the upper position (Figure 10) using the three screws (M3x5) provided with the DIN-Rail clip.
2. Hook the top of the DIN-Rail clips over the DIN-Rail and push down slightly while moving the bottom of the switch towards the DIN-Rail until the DIN-Rail clip snaps into place.
3. Check the switch is securely attached to the DIN-Rail.

## 5.2. DIN-Rail Removal

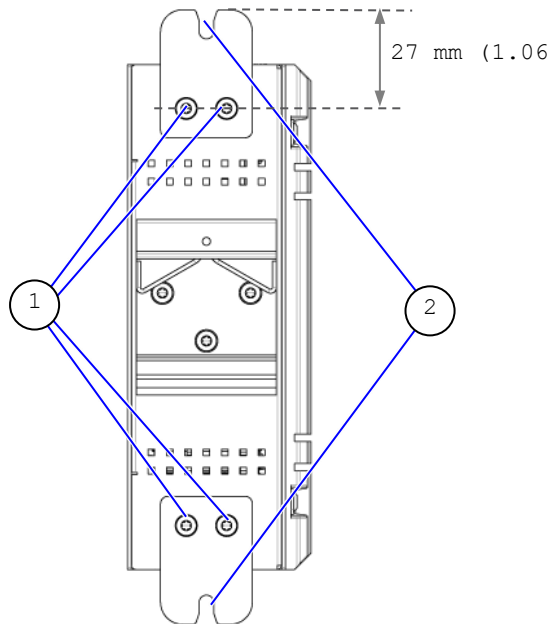
To remove the switch from a DIN-Rail, perform the following:

1. Push the switch down to free the bottom of the DIN-Rail clip from the DIN-Rail.
2. Rotate the bottom of the switch away from the DIN-Rail.
3. Unhook the top of the DIN-Rail clip from the DIN-Rail by lifting upwards.
4. Remove the DIN-Rail clip by loosening and removing the three screws (M3x5). Retain the three screws with the removed DIN-Rail clip.

## 5.3. Wall Mounting

To mount on a flat surface or wall use the Wall Mount Kit containing two wall mount plates and four (M3x5) screws, see Table 2: Mounting Kit Accessories. The switch may be mounted vertically and horizontally. Horizontal mounting is only permitted with the heatsink facing upwards.

Table 7: Mounting with Wall Mount Plates (vertical and horizontal)



- |   |                        |   |   |
|---|------------------------|---|---|
| 1 | 2 threaded screws hole | 2 | Grove to mount with screw on a wall or flat surface |
|---|------------------------|---|---|

**CAUTION**

Horizontal mounting is only permitted with the heatsink facing upwards.

**CAUTION**

**Secure Switch Properly**

Secure the wall mount plates using all four screws (M3x5) provided and mount on a wall or flat surface using two screws that match the mounting surfaces length requirements.

---



The distance from the wall mount plate's mounting holes to the top of the wall mount plate is 27 mm.

---

To install on a wall or flat surface, perform the following:

1. Make sure the mounting surface is clean and smooth and meets the screw's thickness requirement.
2. Fasten the wall mount plates to the switch (top and bottom) using the two screws (M3x5) provided. (Figure 7, pos. 1).
3. Insert two screws (top and bottom) into the wall mount plate's groves (Figure 7, pos. 2) and fasten firmly.  
Note: The two screws are not included in the Wall Mount Kit as their length depends on the mounting surface thickness.
4. Check the switch is attached to the mounting surface securely.
5. If installed horizontally, check that the heatsink faces upwards.

## 6/Starting Up

Before connecting the switch to power and starting up, read and observe the instructions within this user guide, including Chapter 2/: General Safety Instructions. Kontron assumes no responsibility for any damage resulting from failure to comply with these requirements.

### ⚠ CAUTION

Only connect the switch to an external power supply providing the voltage type (DC) and the input power (max. current) specified on the Kontron Product Label and meeting the requirements of the Limited Power Source (LPS) and Power Source (PS2) of UL/IEC 62368-1 .

### ⚠ CAUTION

Before connecting to power, first connect the ground cable to the ground stud and ensure that the installation sites ground meets the grounding requirements specified in your local, national and international region.

### ⚠ CAUTION

Ensure easy access to the power cable. If the operating environment restricts power cable access, guarantee disconnection using a separate cut-off fixture.

### ⚠ CAUTION

When connecting the power follow the indicated polarity P1+/- and P2+/-.

### ⚠ CAUTION

When connecting the alarm contacts the maximum voltage must not exceed 30 VAC or 42 VDC at a maximum current of 1 A.

### NOTICE

To protect the switch and any connected devices, a sufficient dimensioning of the power cable wires must be selected - according to the maximum electrical specifications on the product label - as stipulated by EN62368-1 .

When attaching power wires to the DC terminal block's power contacts consider:



- DC terminal block pitch, 5.08 mm (0.2 inch)
- Wire strip length 7 mm (0.28 inch)
- Wire size range: Solid wire: 12~24 AWG and Stranded wire: 12~24 AWG
- Wire length 3 m (9.84 ft.) maximum



With multiple power sources connected to the switch, the switch utilizes the power supply with the higher voltage or the most stable power supply.

To connect the switch to an external DC power supply and start up, perform the following:

1. Turn off the external DC power supplies via a disconnecting device (fuse/circuit breaker), to ensure that no power flows during the connection procedure.
2. Connect the ground stud to an appropriate earth connection.

3. Insert the positive and negative wires of the first external DC power supply to the P1+/-, contacts on the DC terminal block and tighten the wire-clamp screws to prevent the wires from loosening.
4. Insert the positive and negative wires of the second external power supply to the P2+/- contacts on the DC terminal block and tighten the wire-clamp screws to prevent the wires from loosening.
5. Insert the DC terminal block into the switch's power connector.
6. Turning-on the external DC power supplies automatically activates the switch.

## 7/Technical Specification

### 7.1. Technical Specification

Table 8: Technical Specification

Network	
Operating	Store and forward, full wire-speed/non-blocking Gigabit switch core
RJ45 Copper Ports	
Speed	Up to 6x 10BASE-T/100BASE-TX/1000BASE-T ports Up to 2x 10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T ports
MDI/MDIX Auto-crossover	Support straight or cross wired cables
Auto-Negotiation/Duplex	10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-T speed auto-negotiation; full & half duplex
Fiber Ports	
Port Types	Up to 2x 2.5GBASE-X/1000BASE-X SFP slots
Optimal Fiber Cable	Typical 50 or 62.5/125 $\mu\text{m}$ for multi-mode (mm) Typical 8 or 9/125 $\mu\text{m}$ for single mode (sm)
Protocols and Standards	
IEEE 802.1AS rev2011, IEEE 802.1Qci, IEEE 802.1Qav, IEEE 802.1Qbv, IEEE 802.1Qbu & IEEE 802.3br, 802.1CB, IEEE 802.1D/w, IEEE 802.1Q/p, IEEE 802.1ab, IEEE802.1X, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x, IEEE 802.3ad, LLDP, IPv4/IPv6, SNMP v1/v2c, TFTP, ARP, RARP, Telnet, Syslog, Flow Control, Back Pressure, ICMP, UDP, TCP, IEEE 1588 Rev 2	
Network Redundancy	
Spanning Tree Protocol	IEEE 802.1D/1w/1S, STP/RSTP/MSTP
Port Trunk / LACP	Static Trunk or LACP
Bridge, VLAN, Protocols	
Flow Control	IEEE 802.3x (full duplex) and Back-Pressure (half-duplex)
Max. VLANs	4095
VLAN Types	Port-based VLAN, IEEE 802.1Q tag-based VLAN
Multicast Protocols	IGMP v1, v2, up to 255 multicast groups
	IGMP snooping, querying
LLDP	IEEE 802.1ab LLDP
Traffic Management & QoS	
Priority	IEEE 802.1p QoS
Number of queues per port	8
Scheduling schemes	SPQ, DWRR
Security	
Port Security	IP and MAC-based Access Control/Filter, Auth. User / Privilege Level Control, IEEE 802.1X
Storm Control	Multicast / Broadcast / Flooding Storm Control / Port Access Control / Limiters
Management	
User Management	Web-based management, Command Line Interface
Interfaces	SNMP v1/v2c/v3, Trap, Telnet (5 sessions)
Management Security	HTTPs, SSH, Access Management, Loop Protection

Upgrade & Restore	TFTP/HTTP for configuration import / export TFTP/HTTP for firmware upgrade
Management	
Diagnostic	Syslog, Level Info / Warning / Error
	Port Mirror, Per VLAN mirroring, CPU Load Monitor, Traffic Counter, ICMP Ping
DHCP	Client Mode, Server Mode, Relay Mode, Snooping
SNTP	Supported
System Status	Device info/status; Ethernet port status
Green Ethernet	Port power savings
Indicators	
Power Status Indication	Power input status
Ethernet Port Indication	Link/Activity & speed
Relay Output	Default Setting Normal Open (1 A 30 V, 0.3 A 125 VAC)

## 7.2. Environmental Specification

Table 9: Environmental Specification

Environmental	
Operating Temperature	-40°C to +70°C (-40°F to 167°F )
Storage Temperature	-40°C to +85°C (-40°F to 185°F)
Humidity	93% RH at 40°C (non-condensing)
Shock (according to IEC 60068-2-27)	15 g, 9 ms half sine, Shock Count: 3/direction, total 18
Vibration (according to IEC 60068-2-6)	10 Hz to 300 Hz, 2 g
MTBF	>85000 h @ 30°C ground benign (according to MIL-HDBK-217)
Altitude	3000 m max. (6560 ft.)

## 7.3. Mechanical Specification

Table 10: Mechanical Specification

Mechanical		KSwitch D10 MMT 8G	KSwitch D10 MMT 6G-2GS
Dimensions (H x D x W) (without heatsink)		138 mm x 117.3 mm x 43 mm (5.43 inch x 4.62 inch x 1.69 inch )	
Weight	With heatsink	940 g (2.07 lbs.)	911 g (2.01 lbs.)
	Without heatsink	753g (1.66 lbs.)	725g (1.60 lbs.)
Color		Faceplate: Light Grey RAL7035 Chassis: Silver Pantone 877C	
Heatsink		1x Heatsink (aligned with thermal pads positioned on chassis hot spots) (H x D): 138 mm x 117.3 mm (5.43 inch x 4.62 inch)	



Mechanical	KSwitch D10 MMT 8G	KSwitch D10 MMT 6G-2GS
IP Protection	IP30	
Installation	DIN-Rail Wall mount (horizontal and vertical)	

**▲ CAUTION**

---

Horizontal mounting is only permitted with the heatsink facing upwards.

---

The switch variants share the same main dimensions and mechanical features, and differ only in faceplate design.

Figure 11: Mechanical Dimensions KSwitch D10 MMT 8G (mm)

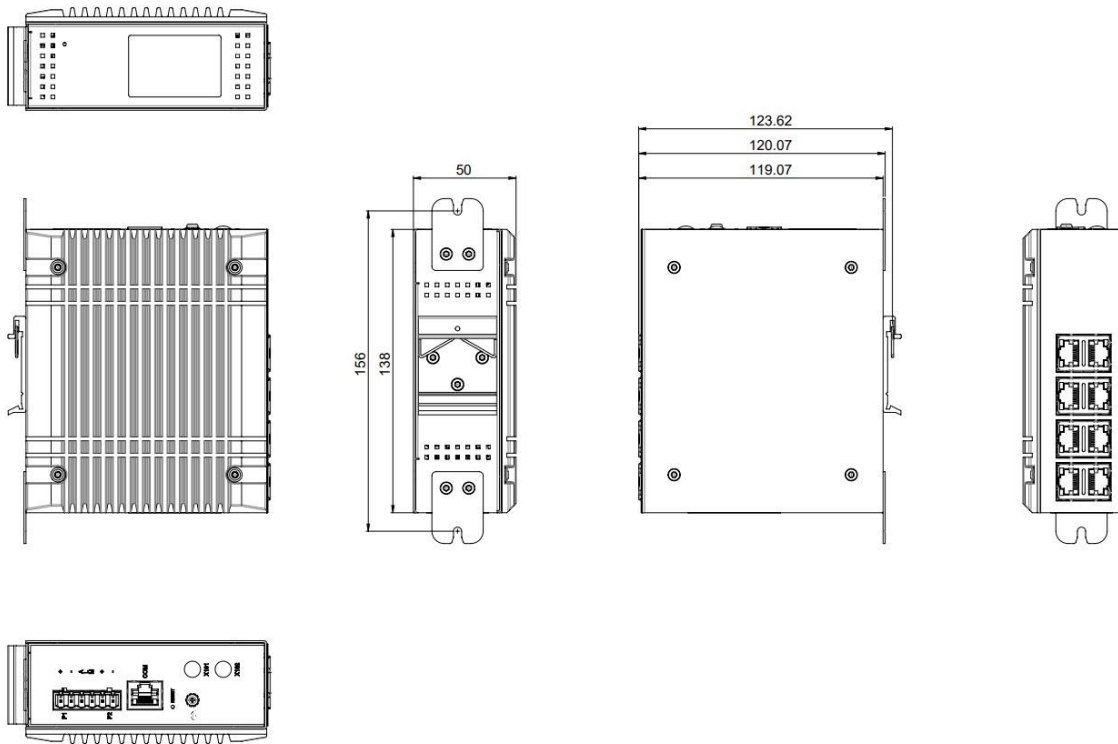
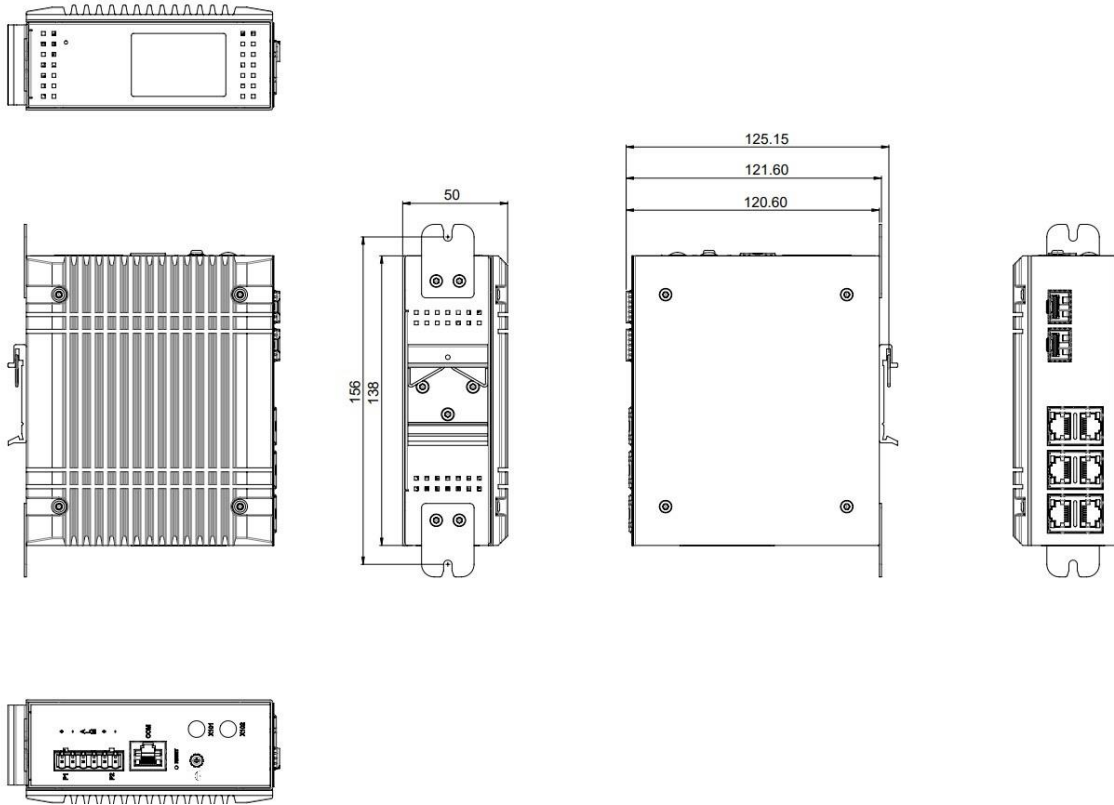


Figure 12: Mechanical Dimensions KSwitch D10 MMT 6G-2GS (mm)



## 7.4. Power Specification

The switch supports dual redundant 12 VDC to 58 VDC power inputs. The implemented external DC power supplies must fulfill the specified electrical ratings in this user guide and comply with the safety requirements of UL/IEC 62368-1.

Table 11: Electrical Specification

Power		KSwitch D10 MMT 8G	KSwitch D10 MMT 6G-2GS
Input	Power Terminal	Dual redundant power input on a removable 6-pin DC terminal block	
	Voltage Range	12 VDC to 58 VDC	
	Input Current	0.77 A @ 12V (typical)	0.63 A @ 12 V (typical)
Power Consumption		9.86 W (typical)	7.54 W (typical)
Protection		Reverse power protection	

### ⚠ CAUTION

Only connect the switch to an external power supply providing the voltage type (AC or DC) and the input power (max. current) specified on the Kontron Product Label and meeting the requirements of the Limited Power Source (LPS) and Power Source (PS2) of UL/IEC 62368-1 .

### ⚠ CAUTION

Before connecting to power connect the ground cable to the ground connector and ensure that the installation sites ground meets the grounding requirements specified in your local, national and international region.

### ⚠ CAUTION

The DC power supply must be connected to a well-fused power source. If access to power is restricted, guarantee disconnection using a separate cut-off device.

### NOTICE

After a brownout condition the used power supply must remain in the "off state" long enough to allow all internal voltages to discharge sufficiently. Failure to observe this required "off state" time may mean that parts of the switch or peripherals work incorrectly or suffer a reduction of MTBF. The minimum "off state" time, to allow internal voltages to discharge sufficiently, is dependent on the power supply and additional electrical factors. To determine the required "off state" time, each case must be considered individually. For more information, contact [Kontron Support](#).

### NOTICE

To protect the switch and any connected devices, a sufficient dimensioning of the power cable wires must be selected - according to the maximum electrical specifications on the product label - as stipulated by EN62368-1 .



When attaching power wires to P1+/- and P2+/- on the DC terminal block consider:

- DC terminal block pitch, 5.08 mm (0.2 inch)
- Wire strip length 7 mm (0.28 inch)

- Wire size range: Solid wire: 12 to 24 AWG and Stranded wire: 12 to 24 AWG
- Wire length 3 m (9.84 ft.) maximum



With dual power sources connected to the switch, the switch utilizes the power supply with the higher voltage or the most stable power supply.

## 7.5. Compliance

The KSwitch D10 MMT complies with the relevant requirements and the approximation of the laws relating to 'CE' and the standards that are constitutional parts of the declaration.

Table 12: CE Compliance

CE Mark (Europe)	
Directives	2014/30/EU: Electromagnetic Compatibility 2014/35/EU: Low Voltage 2011/65/EU: RoHS II 2001/95/EC: General Product Safety
EMC	EN 55032/CISPR 32 Electromagnetic Compatibility of multimedia equipment- Emission Requirements EN 61000-6-4 Electromagnetic compatibility (EMC) Part 6-4: Generic standards - Emission standard for industrial environments EN 55035 Electromagnetic Compatibility of multimedia equipment- Immunity Requirements EN 61000-6-2 Electromagnetic Compatibility (EMC) Part 6-2: Generic standards - Immunity for industrial environments
Safety	EN 62368-1 Audio/video, information and communication technology equipment - Part 1: Safety requirements

Table 13: International Compliance

USA/CANADA	
EMC	CFR 47 Part 15, Subpart B / ICES-003 Complies with part 15 FCC rules and regulations of title 47 of the CFR rules for class B products; under which an unintentional radiator may be operated, administrated and other conditions relating to the marketing of part 15 devices.
UKCA	
EMC	EN 55032/CISPR 32 Electromagnetic Compatibility of multimedia equipment- Emission Requirements EN 61000-6-4 Electromagnetic compatibility (EMC) Part 6-4: Generic standards - Emission standard for industrial environments EN 55035 Electromagnetic Compatibility of multimedia equipment- Immunity Requirements EN 61000-6-2

	Electromagnetic Compatibility (EMC) Part 6-2: Generic standards - Immunity for industrial environments
Safety	EN 62368-1 Audio/video, information and communication technology equipment - Part 1: Safety requirements
International Certifications	
Safety	IEC 62368-1 Audio/video, information and communication technology equipment - Part 1: Safety requirements




---

If the switch is modified, the prerequisites for specific approvals may no longer apply.

---




---

Kontron is not responsible for any radio television interference caused by unauthorized modifications of the delivered switch or the substitution or attachment of connecting cables and equipment other than those specified by Kontron. The correction of interference caused by unauthorized modification, substitution or attachment is the user's responsibility.

---

## 8/Software Interface

The switch's software includes the following parts:

- ▶ **Bootloader**  
The boot loader is responsible for booting.
- ▶ **NOS**  
The Network Operating System (NOS) provides Management interfaces to configure the Ethernet features available on the switch such as Port configuration, VLAN settings or Spanning Tree configurations. Access to the NOS is provided by either a Web Interface, Cisco like Command-line Interface (CLI) or SNMP.

### 8.1. Accessing the Switch

This chapter provides important information regarding how users access the switch and login.

#### 8.1.1. Accessing the IP address

User are require to know the IP address to be able to access the Switch NOS using the Web UI and Accessing the Switch NOS CLI using Telnet from a Remote Computer.

To access the switch IP Address, refer to Example 1 in Chapter 8.3.5: Configuration Examples using the CLI.

#### 8.1.2. Accessing the Switch NOS using the Web UI

Prerequisites:

- ▶ Switch IP address is known
- ▶ Remote computer has access to the switch network subnet




---

To access the switch IP Address, refer to Example 1 in Chapter 8.3.5: Configuration Examples using the CLI.

---

Further Prerequisites

Prerequisite	Description
HTML5	To connect to the Web UI, a Web browser supporting HTML5 is required.
HTTPS self-signed certificate	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. For further information about accepting HTTPS self-signed certificates, refer to your Web browser's documentation. NOTE: Factory default is HTTPS not enabled.
File download permission	File download from the site needs to be permitted. For further information about file download permission, refer to your Web browser's documentation.
Cookies	Cookies must be enabled in order to access the website. For further information about enabling cookies, refer to your Web browser's documentation.



---

Factory default is HTTPS not enabled.

---



---

The procedure may vary depending on the browser used. Examples provided use Firefox.

---

### 8.1.2.1. Access Procedure



---

The switch is shipped with default username 'admin' and with no password. It is strongly recommended to assign a strong password instead.

---



---

Username 'admin' cannot be removed or be changed, only its password.

---

To obtain the list of default user names and passwords:

1. From a remote computer that has access to the switch network, open a browser window and enter the IP address discovered for the switch.

### 8.1.3. Accessing the Switch NOS CLI using Telnet from a Remote Computer

Access is permitted using either an in-band Ethernet port (IP address) or the serial console port. For both options the default login and password is the same.

Default login account for NOS:

Login: admin

Prerequisites:

- ▶ Network switch IP address is known
- ▶ Remote computer has access to the switch network subnet
- ▶ Remote computer has an installed telnet client tool



---

To access the switch IP Address, refer to Example 1 in Chapter 8.3.5: Configuration Examples using the CLI.

---



---

PuTTY is recommended for Windows environments and telnet is recommended for Linux environments.

---



### 8.1.3.1. Setting up the Serial Console Port

The serial console port enables local management using a terminal emulator or a computer with terminal emulation software.



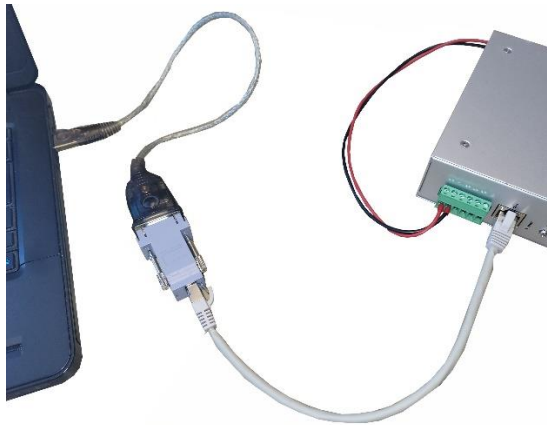
---

The serial console port is a serial port and requires only the serial baud rate 115200 and 8-N-1, to be set up. There is no flow control.

---

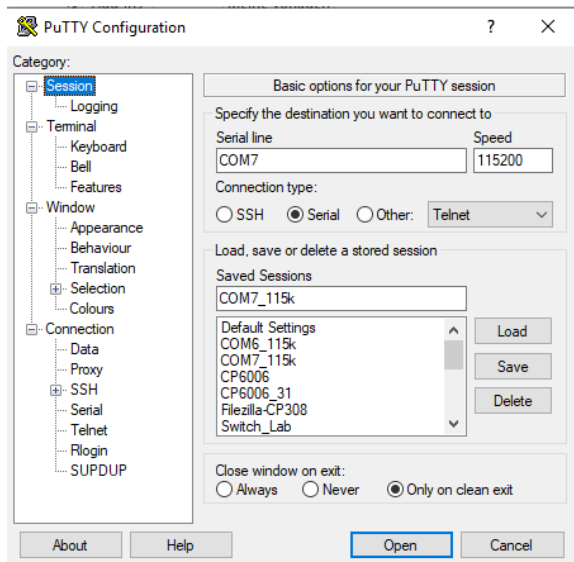
Use the serial adapter and a straight RJ45 cable to connect the switch serial console to a PC as shown in Figure 13 below:

Figure 13: Serial Console Port

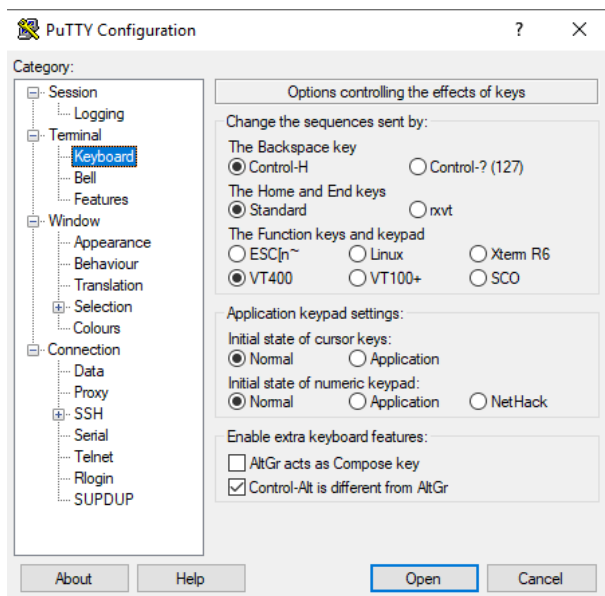


To use Putty to access the serial console port on the switch, perform the following:

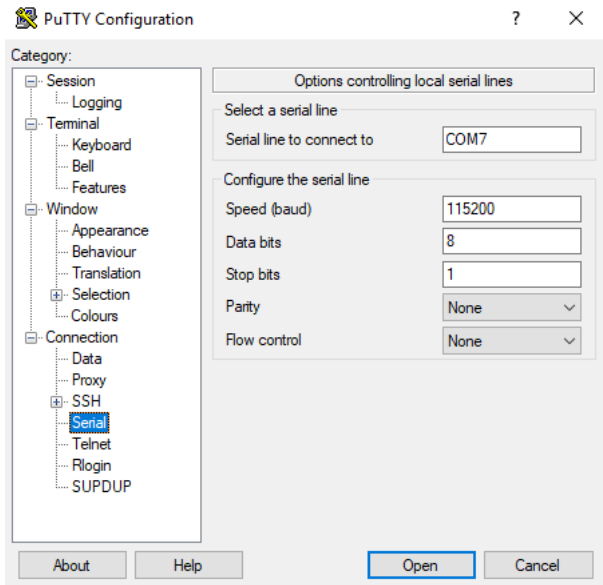
1. In the Category Window select choose <Session> and specify the <Serial Line>, <Speed> 115200 and then <Connection Type> Serial. Click on <Open>.



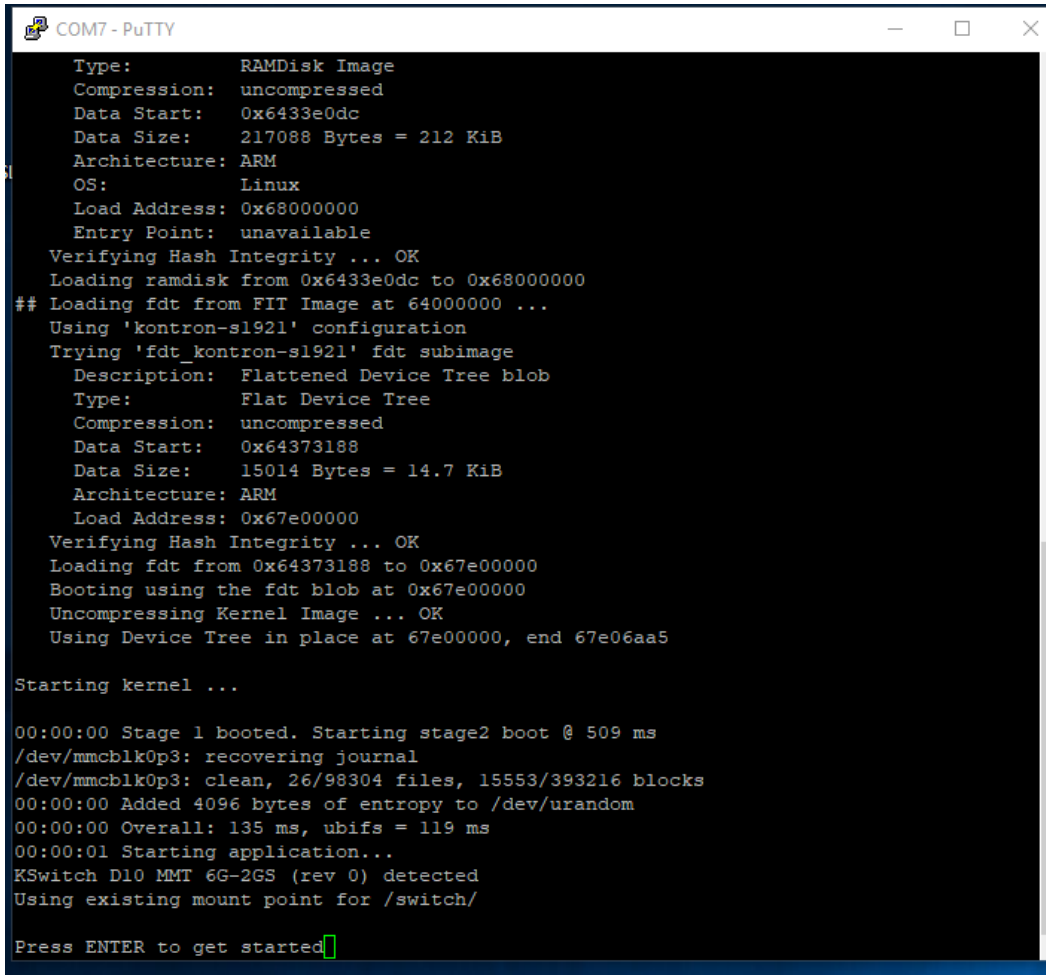
- In the Category Window select <Keyboard> and click on options as shown below. Click on <Open>.



- In the Category Window choose <Serial> and then choose the serial line to connect to, baud rate of 11520, select 8-N-1 (8-bit data -No parity-1-bit stop). Click on <Open>.



## 4. Terminal shows the serial console information.



```
COM7 - PuTTY
Type:          RAMDisk Image
Compression:  uncompressed
Data Start:   0x6433e0dc
Data Size:    217088 Bytes = 212 KiB
Architecture: ARM
OS:           Linux
Load Address: 0x68000000
Entry Point:  unavailable
Verifying Hash Integrity ... OK
Loading ramdisk from 0x6433e0dc to 0x68000000
## Loading fdt from FIT Image at 64000000 ...
Using 'kontron-s1921' configuration
Trying 'fdt kontron-s1921' fdt subimage
  Description: Flattened Device Tree blob
  Type:        Flat Device Tree
  Compression: uncompressed
  Data Start:  0x64373188
  Data Size:   15014 Bytes = 14.7 KiB
  Architecture: ARM
  Load Address: 0x67e00000
Verifying Hash Integrity ... OK
Loading fdt from 0x64373188 to 0x67e00000
Booting using the fdt blob at 0x67e00000
Uncompressing Kernel Image ... OK
Using Device Tree in place at 67e00000, end 67e06aa5

Starting kernel ...

00:00:00 Stage 1 booted. Starting stage2 boot @ 509 ms
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 26/98304 files, 15553/393216 blocks
00:00:00 Added 4096 bytes of entropy to /dev/urandom
00:00:00 Overall: 135 ms, ubifs = 119 ms
00:00:01 Starting application...
KSwitch D10 MMT 6G-2GS (rev 0) detected
Using existing mount point for /switch/

Press ENTER to get started
```

### 8.1.3.2. Access Procedure




---

The switch is shipped with default username 'admin' and with no password. It is strongly recommended to assign a strong password instead.

---




---

Username 'admin' cannot be removed or be changed, only its password.

---

To obtain the list of default user names and passwords:

1. From a remote computer, open a telnet client tool and connect with the NOS IP address, using the port 2031
2. Log in the switch NOS CLI using the appropriate credentials.

### 8.1.3.3. Deactivate Serial Timeout

```
# configure terminal
(config)# line console 0
(config-line)# exec-timeout 0
(config-line)# end
(config)# end
#
```

### 8.1.4. Accessing the Operating System

Access to the Linux shell is provided by the NOS application once debug features have been enabled by CLI command.

```
# platform debug allow
# debug system shell
#
```

### 8.1.5. Help Tools

#### 8.1.5.1. Switch Web User Interface Help

A comprehensive Web User Interface's Help Menu provides information about the overall set of functionalities and corresponding configuration options.

#### 8.1.5.2. Switch CLI Help

The switch CLI contains a context-sensitive help feature. Use the <?> symbol to display the next possible parameters or commands and their descriptions.

## 8.2. Managing the KSwitch D10 MMT Using the Web Interface

The KSwitch D10 MMT Web Management Interface provides a significant amount of information on how to configure and monitor the switch.



---

Kontron recommends using the Help feature to access more information.

---

### 8.3. Using the CLI

The Command-line interface (CLI) is used for configuring, monitoring, and maintaining the switch over CLI, Telnet, SSH. Use a baud rate of 115200 when using a USB serial interface.




---

It is strongly recommended to use the Web interface whenever possible to simplify user configuration and reduce configuration mismatch.

---




---

CLI interface may contain more configuration commands versus those affected as a result of user configuration changes over the web. This user guide covers only the commands affected whenever users change the switch configuration over the web interface.

---

All commands entered in CLI are followed by values, parameters or both. Parameters may be mandatory values, optional values, choices, or a combination. Values may be in a form of six hexadecimal numbers separated by colons (MAC address), for example 00:06:29:32:81:40, dotted-decimal notation (Area IDs), for example 0.0.0.1, slot/port number for example 1/1 or logical slot/port (applicable in case of a link-aggregation).

Command	Description
<parameter>	The < > angle brackets indicate that a mandatory parameter is to be entered in place of the brackets and text inside them.
[parameter]	The [ ] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.
choice1   choice2	The   indicates that only one of the parameters should be entered.
{ }	The curly braces indicate that a parameter must be chosen from the list of choices.

#### 8.3.1. Completing a Partial Command

Enter the first few letters of the command, and then press the Tab key. The command line parser will complete the command if the string entered is unique to the command. Another option will be to type the first few letters followed by <?>. This shows all the commands that start with the letters already typed.

#### 8.3.2. Command History

Use the <Up/Down> arrows keys to scroll between the commands you already typed. To display the entire history the #show history command can be used.

#### 8.3.3. Using the Backspace Key in NOS CLI

Other than expected, the backspace key deletes the character at the cursor location only. So it is required to move the cursor to this location before using the cursor to delete a character.

### 8.3.4. 'no' Commands

Almost all configuration commands have a corresponding 'no' form. The 'no' form is syntactically similar (but not necessarily identical) to the configuration command; however, it either resets the parameters to default values for the configurable item or disables the item altogether.

### 8.3.5. Configuration Examples using the CLI

The following chapters provide examples on how to setup dedicated features and configurations.

For more information on additional features and configuration options, see the CLI Help feature Chapter 8.1.5.2 Switch CLI Help.

#### 1. Query DHCP assigned IP address.

```
Starting kernel ...
00:00:00 Stage 1 booted. Starting stage2 boot @ 509 ms
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 26/98304 files, 15553/393216 blocks
00:00:00 Added 4096 bytes of entropy to /dev/urandom
00:00:00 Overall: 136 ms, ubifs = 120 ms
00:00:01 Starting application...
KSwitch D10 MMT 6G-2GS (rev 0) detected
Using existing mount point for /switch/
```

Press ENTER to get started <CR>

```
Username: admin
Password: <CR>
#show ip interface
Interface Address      Method Status
-----
VLAN 1  10.224.32.5/24  DHCP  UP
```

#### 2. How to set IP address (and hostname) manually via CLI and save it permanently.

This is required in case no DHCP server is present.

```
KSwitch D10 MMT 6G-2GS (rev 0) detected
Using existing mount point for /switch/
```

Press ENTER to get started <CR>

```
Username: admin
Password: <CR>
#configure terminal
(config)# hostname KSwitch-D10_1
KSwitch-D10-1(config)#interface vlan 1
KSwitch-D10-1(config-if-vlan)# ip addresss 192.168.170.60 255.255.255.0
KSwitch-D10-1(config-if-vlan)# do show ip interface
Interface Address      Method Status
-----
VLAN 1  192.168.170.60/24  Manual Up

KSwitch-D10-1(config-if-vlan)#
KSwitch-D10-1(config-if-vlan)# exit
```



```
KSwitch-D10-1(config)# exit
KSwitch-D10-1# copy running-config startup-config
Building configuration...
% Saving 1305 bytes to flash:startup-config
KSwitch-D10-1#
```

3. Check network port status

```
# show interface * status
Interface Mode Speed Aneg Media Type SFP Family Link Operational Warnings
-----
Gi 1/1 Enabled Auto Yes RJ45 N/A Down
Gi 1/2 Enabled Auto Yes RJ45 N/A Down
Gi 1/3 Enabled Auto Yes RJ45 N/A Down
Gi 1/4 Enabled Auto Yes RJ45 N/A Down
Gi 1/5 Enabled Auto Yes RJ45 N/A 1Gfdx
Gi 1/6 Enabled Auto Yes RJ45 N/A Down
2.5G 1/1 Enabled Auto Yes SFP None Down
2.5G 1/2 Enabled Auto Yes SFP 1G Optical Down
```

4. List currently active switch configuration.

```
# show running-config
```

5. Query system information

```
# show version
```

```
Serial Number : F220900011
MAC Address : 00-a0-a5-5c-6d-b8
Previous Restart : Cold

System Contact :
System Name :
System Location :
System Time : 2022-10-06T16:54:48+00:00
System Uptime : 00:14:19
```

Bootloader

```
-----
Image : u-boot
Version : HEAD-0.00-20220309231701
Date :
```

Primary Image

```
-----
Image : mmcblk0p2 (Active)
Version : GA-2.00-20221006151622
Date : 2022-10-06T16:40:30+00:00
Upload filename : istax_s1921.ext4.gz
```

Backup Image

```
-----
Image : mmcblk0p1
Version : ALPHA-1.01-20220404140901
Date : 2022-04-04T15:09:08+00:00
Upload filename : istax_s1921.ext4.gz
-----
```

SID : 1

-----

Chipset ID : LAN9668 Rev. A  
Board Type : Kontron KSwitch D10 (S1921)  
Flash Type : MMC-only  
Port Count : 8  
Product : Microchip IStax Switch  
Software Version : GA-2.00-20221006151622  
Build Date : 2022-10-06T16:40:30+00:00  
Code Revision : da9f565  
DPLL F/W Version : -

**6.** How to load factory defaults.

```
# reload defaults
% Reloading defaults. Please stand by.
# copy running-config startup-config
Building configuration...
% Saving 1218 bytes to flash:startup-config
```

For more information on additional features and configuration options, see the CLI Help feature chapter 8.1.5.2 Switch CLI Help.

## 8.4. General Maintenance Commands

### 8.4.1. Configure Terminal

Description - Start switch configuration. Terminal display will switch from # to (config)#.

Configure Terminal

	Parameter	Description
Parameter	-	N/A
Default	NA	
N.A	EXEC	
Mode	Enter configuration mode whenever starting switch configuration	
Example	# configure terminal. NOTE - You may also use the shortcut # conf t	

### 8.4.2. Interface

Description - Start interface (port) configuration. Terminal display will switch from (config)# to (config- if)#.



It is possible to configure same parameter for multiple interface by using syntax as 1/1-8 (configure same value for ports 1-8) as described in the command example.

Interface <port\_type> [ <port\_type\_list> ]

	Parameter	Description
Parameter	<port_type>	Port type Gigabit Ethernet, vlan
ALM	[ <port_type_list> ]	List of Port ID, ex. 1/1,3-5 1/1-8 1/1,2,4
Default	N.A	
Mode	Global Configuration	
Usage	Enter interface configuration mode to start configuring port parameters	
Example	Example#1 (enter configuration mode for ports 1, 3,4 and 5): (config)# interface GigabitEthernet 1/1,3-5 (config-if)#  Example#2 (enter configuration mode for ports 1 through 8) (config)# interface GigabitEthernet 1/1-8 (config-if)#	

### 8.4.3. Exit

Description - Go up one level in the configuration process. Logout from terminal/telnet/SSH session in case user was at top level.

Exit

	Parameter	Description
Parameter	-	N.A
Default	N.A	
Mode	Exit from current mode	
Usage	Whenever end in-depth configuration and need to go up one level, or to log out of the serial interface.	
Examples	Example#1: (config)# exit # Example#2: (config-if)# exit (config)#	

### 8.4.4. End

Description - End any in-depth configuration mode and go back to EXEC mode.

End

	Parameter	Description
Parameter	-	N.A
Default	N.A	
Mode	Go back to EXEC mode	
Usage	Whenever need to end in-depth configuration and go back to EXEC mode	
Examples	Example#1: (config-if)# end # Example#2: (config)# end #	

### 8.4.5. Show Running-Config

Description - View switch running configuration (the configuration being in use by the switch). User may change switch configuration without saving the changes, meaning that upon switch power down-up cycle it may operate completely different.

Show Running-Config

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to view the current configuration	
Examples	# show running-config	

#### 8.4.6. Show Running-Config All-Default

Description - View switch running configuration plus omitted default configuration.

Show Running-Config All-Default

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to view the current configuration including all default values	
Examples	# show running-config all-default	

#### 8.4.7. Dir

Description - Show all optional configuration files stored inside the switch.

Dir

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to view all configuration files stored in the flash.	
Examples	# dir	

#### 8.4.8. Copy Running-Config Startup-Config

Description- update (save) switch configuration to be used after reset or power-up.

Copy Running-Config Startup-Config

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to save switch configuration	
Examples	# copy running-config startup-config	

### 8.4.9. Copy Running-Config Flash:<file-name>

Description- copy running (or startup) configuration files to another file name or to TFTP server. Also vice versa from TFTP Server to switch local file.

**Copy** <Running Config | Startup-Config | Flash:file-name | tftp://server/filename>

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to copy switch configuration to another file or to TFTP Server or from TFTP Server to switch local file	
Examples	<p>Example#1 - save current configuration stored in switch flash to another file named "test" also inside switch FLASH.</p> <pre># copy running-config flash:test</pre> <p>Example#2 - save switch running configuration file to TFTP Server under name "test"</p> <pre># copy running-config tftp://192.168.0.40/test</pre>	

### 8.4.10. Del Flash:<file-name>

Description - delete configuration file stored in flash.

Del Flash:<file-name>

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to delete switch configuration stored in flash	
Examples	# del flash:test	

### 8.4.11. Reload Cold

Description - Switch performs software reset, turning Ethernet ports down and back up.

Reload Cold

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restart the switch	
Examples	# reload cold	

### 8.4.12. Reload Defaults

Description - restore to full factory default configuration.

#### Reload Defaults

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restore to factory default	
Examples	# reload defaults	

### 8.4.13. Reload Defaults Keep-IP

Description - Semi factory defaults, keeping IP and VLAN configuration unchanged.

#### Reload Defaults Keep-ip

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restore to factory default but keep IP address unchanged	
Examples	# reload defaults keep-ip	

### 8.4.14. Show Version

Description - Display switch software and hardware information.

#### Show Version

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to display switch information	
Examples	<pre># show version Software Version      : 1.13 (created on 2019-01-30T18:29:03+02:00) PoE Firmware         : 24034356.1056.003 MAC Address          : 00-05-5a-98-67-23 Serial Number        : 000038 Production Number    : 8301 System Date &amp; Time    : 1970-01-13T20:20:55+00:00 System Uptime        : 12d 20:20:55</pre>	

## 8.5. TSN Features

Time-Sensitive Networking (TSN) is a number of IEEE 802 standards that are defined by the IEEE TSN task group. These standards define mechanisms for deterministic real-time communication over Ethernet networks.

The following links gives an overview and status of the various TSN standards [https://en.wikipedia.org/wiki/Time-Sensitive\\_Networking](https://en.wikipedia.org/wiki/Time-Sensitive_Networking) and <http://www.ieee802.org/1/pages/tsn.html>.

This chapter covers:

- ▶ PTP (IEEE 802.1AS)
- ▶ Credit based shaper (IEEE 802.1Q-2014)
- ▶ Time aware shaper (IEEE 802.1Qbv)
- ▶ Frame preemption (IEEE 802.1Qbu)

FRER (Frame Replication and Elimination , 802.1CB-2017), Cut-through (IEEE 802.1Qcc) and Per-Stream Filtering and Policing (PSFP, IEEE 802.1Qci) are supported by the KSwitch-D10 as well. For more information, refer to Chapter 8.1.5: Help Tools. Switch CLI Help or the Web Interface,

### 8.5.1. IEEE 802.1AS Configuration

The following chapter provides useful commands to configure and monitor PTP behavior on the switch ports.

Please note, Software release GA-3.02 introduces a new recommended configuration pattern for the PTP 802.1as feature. This new pattern is mandatory at least if the Time Aware Scheduler feature is used.

Basic Configuration Snippet to enable 802.1AS on all ports

```
configure terminal
(config)#ptp ext output auto clk-domain 1
(config)#ptp 0 mode boundary profile 802.1as clock-domain 3
(config)#ptp 1 mode internal onestep ethernet twoway
(config)#ptp 1 internal src-clk-domain 3
interface *
(config-if)#ptp 0
```

Command to shown port PTP status information:

```
show ptp 0 port-state
```

More information about PTP configuration can be found in the documentation "AN1295 "PTP Configuration Guide" revision APPL2024.09", which can be provided on demand by Kontron FAE or support team.

### 8.5.2. Using TSN Functions with PTP Time Synchronisation

When using TAS and PSFP between network elements, it is required to have a common global time reference provided by PTP. When booting the KSwitch-D10, it will take some time for a configured PTP application to locked to the common time reference. It may cause malfunctioning of TAS and PSFP if a config-change is issued before the PTP time is in a 'Locked' or 'Locking' state. A function that can delay the issue of config-change until PTP is Locked/Locking or a configurable time has passed, can be configured with the CLI command: *tsn ptp-check*.

The full set of configuration options for PTP exceeds the scope for this document. Refer to the help function of the CLI or the Web Interface.

The syntax for the TSN delayed start function is:

Syntax Example:



```
tsn ptp-check procedure { none | ptp | wait }
tsn ptp-check ptp-port <0-3>
tsn ptp-check timeout <10-200>
no tsn ptp-check procedure
no tsn ptp-check ptp-port
no tsn ptp-check timeout
```

Where:

none	Procedure: Start TSN functions immediately without any delay
ptp	Procedure: Monitor the status of PTP time. Start if it is Locking or Locked.If Locking or Locked is not achieved within wait time, then start anyway
wait	Procedure: Wait timeout number of seconds before starting TSN functions
ptp-port	The PTP port to use for sensing PTP status
timeout	Set ptp-check-procedure timeout in seconds

Example:

```
(config)# tsn ptp-check procedure ptp
(config)# tsn ptp-check ptp-port 2
(config)# tsn ptp-check timeout 30
```

It is intended that after configuring *tsn ptp-check*, it should be saved to startup-config, and the delay function will only be executed once after a 'power on' or 'reload cold'.

### 8.5.3. Credit Based Shaper

Credit Based Shaper is defined in the IEEE 802.1Q-2014 standard and is the ability to control the traffic access bandwidth based on priorities. The highest priority queue can be assigned a higher access bandwidth relative to the available bandwidth, which in turn gives packets a higher chance to be transmitted in a busy network.

The mechanism is realized through increasing/decreasing credit value of the specific queues, i.e., the credit for high priority queues increases faster and therefore reaches the transmitting threshold more frequent than the low priority queues. The algorithm includes two parts, namely assigning priorities to traffic classes/queues and assigning relative access bandwidth (reflected in credits) to the queues.

#### 8.5.3.1. Configuration Examples

CLI commands example:

```
! Enable a 800 kbps credit based shaper on port 1, queue 6.
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# qos queue-shaper queue 6 800 kbps credit

! Disable the shaper on port 1, queue 6.
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# no qos queue-shaper queue 6

! Show configuration using 'show running-config'.
# show running-config
[...]
qos queue-shaper queue 6 800 kbps credit
```

#### 8.5.3.2. Status

CLI commands example:

```
!
```

Show status using 'show qos'.

```
# show qos
```

```
[...]
```

```
qos queue-shaper queue 0: disabled, rate 500 kbps, mode: line-rate, excess:
disabled, credit: disabled
qos queue-shaper queue 1: disabled, rate 500 kbps, mode: line-rate, excess:
disabled, credit: disabled
qos queue-shaper queue 2: disabled, rate 500 kbps, mode: line-rate, excess:
disabled, credit: disabled
qos queue-shaper queue 3: disabled, rate 500 kbps, mode: line-rate, excess:
disabled, credit: disabled
qos queue-shaper queue 4: disabled, rate 500 kbps, mode: line-rate, excess:
disabled, credit: disabled
qos queue-shaper queue 5: disabled, rate 500 kbps, mode: line-rate, excess:
disabled, credit: disabled
qos queue-shaper queue 6: enabled, rate 800 kbps, mode: line-rate, excess: disabled,
credit: enabled
qos queue-shaper queue 7: disabled, rate 500 kbps, mode: line-rate, excess:
disabled, credit: disabled
```

### 8.5.4. Time Aware Shaper (TAS)

Time Aware Shaper is defined in the IEEE 802.1Qbv standard and is the ability to allow transmission from each queue to be scheduled relative to a known global timescale.

The global time is maintained by using a specific version of Precision Time Protocol (PTP) as defined in IEEE 802.1AS-Rev.

#### 8.5.4.1. Configuration of Parameters

The syntax for TSN TAS interface level CLI configuration command is:

```
tsn tas always-guard-band
no tsn tas always-guard-band
```

Where:

```
always-guard-band:   Guard band is implemented for any queue to scheduled queues
                    transition.
no always-guard-band: Guard band is implemented for non-scheduled queues to scheduled
                    queues transition.
```

The syntax for TSN TAS interface level CLI configuration command is:

```
tsn tas base-time seconds <seconds> nanoseconds <nanoseconds>
tsn tas config-change
tsn tas control-list index <index> gate-state queue <queue> { open | closed }
time-interval <interval> [ operation { set | set-hold | set-release } ]
tsn tas control-list-length <length>
tsn tas cycle-time <time> { ms | us | ns }
tsn tas cycle-time-extension <extension>
tsn tas gate-enabled
tsn tas gate-states queue <queue> { open | closed }
tsn tas max-sdu queue <queue> <sdu>
```

The following parameters are defined in IEEE802.1Q: ieee802.1STMib

base-time	Admin Base Time.
config-change	Start a configuration change
control-list	Admin Control List
control-list-length	Admin Control List Length
cycle-time	Admin Cycle Time
cycle-time-extension	Admin Cycle Time Extension
gate-enabled	Enabled state of Time Aware Shaping
gate-states	Initial gate state for each queue
max-sdu	Queue Max SDU configuration
queue	Traffic class. 0-7.
Index	Index of Gate Control Entry
gate-state	Admin Gate State
time-interval	Time Interval in Nanoseconds
operation	set   set-hold   set-release

#### 8.5.4.2. Configuring Examples

CLI commands example:

```
! Create and start a Time Aware Shaper schedule on port 1.
! The schedule contains three gate control entries:
! 0: Open queue 7 and close all other queues for 20 milliseconds
! 1: Open queue 5-6 and close all other queues for 30 milliseconds
! 2: Open queue 0-4 and close all other queues for 50 milliseconds
! The schedule is repeated every 110 milliseconds
! TAS is scheduled to start at seconds 4300 nanoseconds 500
```

```

# configure terminal
! Disable always-guard-band
(config)# no tsn tas always-guard-band
(config)# interface 10GigabitEthernet 1/1
!
! Set max sdu size for queue 5 to 512 bytes
(config-if)# tsn tas max-sdu queue 5 512
!
! Enable Time Aware Shaper
(config-if)# tsn tas gate-enabled
!
! Set cycle-time to 110 milliseconds
(config-if)# tsn tas cycle-time 110 ms
!
! Set tsn tas cycle-time-extension 9000
(config-if)# tsn tas cycle-time-extension 9000
!
! Set gate state for queues 0-3 to closed
(config-if)# tsn tas gate-states queue 0-3 closed
!
! Set start time of schedule
(config-if)# tsn tas base-time seconds 4300 nanoseconds 500
(config-if)# !
!
! Configure gate control list
(config-if)# tsn tas control-list-length 3
(config-if)# tsn tas control-list index 0 gate-state queue 7 open time-interval
20000000 operation set-hold
(config-if)# tsn tas control-list index 1 gate-state queue 5-6 open time-interval
30000000 operation set-release
(config-if)# tsn tas control-list index 2 gate-state queue 0-4 open time-interval
50000000 operation set

! Start schedule
(config-if)# tsn tas config-change

! Show configuration using 'show running-config'.
# show running-config
no tsn tas always-guard-band
[...]
interface 10GigabitEthernet 1/1
tsn tas max-sdu queue 5 512
tsn tas gate-enabled
tsn tas gate-states queue 4-7 open
tsn tas cycle-time 110 ms
tsn tas cycle-time-extension 9000
tsn tas base-time seconds 4300 nanoseconds 500
tsn tas control-list-length 3
tsn tas control-list index 0 gate-state queue 7 open time-interval 20000000
operation set-hold
tsn tas control-list index 1 gate-state queue 5,6 open time-interval 30000000
operation set-release
tsn tas control-list index 2 gate-state queue 0-4 open time-interval 50000000
operation set
tsn tas config-change

```

### 8.5.4.3. Status

CLI commands example:

```

! Show status using 'show tsn tas status'.
# show tsn tas status interface 10GigabitEthernet 1/1
interface
GateEnabled :                TRUE

```

```

OperGateStates :          0x1f
OperCycleTime :          110 ms
OperCycleTimeExtension:  9000 nanoseconds
OperBaseTime :           4300 seconds, 500 nanoseconds
ConfigChangeTime :      4300 seconds, 500 nanoseconds
TickGranularity :       0 tenths of nanoseconds
CurrentTime :           4311 seconds, 827669856 nanoseconds
ConfigPending :         FALSE
ConfigChangeError :     0
SupportedListMax :      256
OperControlListLength : 3
GateControlEntry 0 :    GateStates 0x80, TimeInterval 20000000 nanoseconds, GateOperation
set-hold
GateControlEntry 1 :    GateStates 0x60, TimeInterval 30000000 nanoseconds, GateOperation
set-release
GateControlEntry 2 :    GateStates 0x1f, TimeInterval 50000000 nanoseconds, GateOperation
set

! Disable Time Aware Shaper on port 1.
# configure terminal
(config)# interface 10GigabitEthernet 1/1
(config-if)# no tsn tas gate-enabled

```

### 8.5.5. Configuration Considerations

The max-sdu parameter is only used to calculate the guard band time:  $gbt = \text{maxsdu} * 8 / \text{LINK\_SPEED}$ . Note, that on Fireant, frames larger than max-sdu are not rejected. The max-sdu is defined for each interface, queue and as a result, gbt's can be configured for each traffic class on an interface.

The required guard band time can be reduced if preemption is used. If the traffic class being closed consist of preemptible frames, and the class being opened consists of express frames, then a set-hold operation can be included as part of the gate operation. This causes any currently transmitting preemptible frame to be preempted, reducing the latency before the port is ready to transmit express frames.

When a gate operation closes an input in a scheduler element, that input is permanently blocked until another gate operation opens it again. Similarly, a set-hold on a port remains in effect until another gate operation does a set-release.

This needs to be kept in mind when stopping a TAS list. If the last gate operation in the TAS list leaves any scheduler element input closed, or leaves a set-hold in effect, they can be left indefinitely, possibly causing frames to be blocked in the switch.

If one of the gate operations in a TAS list opens everything, then the TAS list can be arranged so that this is the last operation in the TAS list. A TAS list always completes its cycle before stopping, thus this leaves everything open after the TAS list is stopped.

Alternatively, after stopping a TAS list that leaves inputs closed or set-hold in effect, it is necessary to configure a dummy TAS list with an "open all" gate operation and run it for one cycle.

#### 8.5.5.1. Configuration of Gate Control Entry

A GCE consists of 3 elements:

- ▶ gate-state: Specifies for each queue whether the gate shall be open or closed in this interval.
- ▶ time-interval: The time in nanoseconds where the gate has the open/close state as defined by the gate-state parameter.
- ▶ operation: The value may be set, set-hold, set-release.

The following options are as defined within Table 8-7 of IEEE 802.1Q-2018.

- ▶ **set:** The gates are immediately set to the states indicated in the gate-state parameter. After a time-interval has elapsed control passes to the next gate operation.
- ▶ **set-hold:** Performs all of the actions defined for the set operation. In addition, the start of this operation marks the point in the sequence of gate operations at which the MAC associated with the port is to have stopped transmitting preemptible frames. If frame preemption is not supported or not enabled, this operation behaves the same as set operation.
- ▶ **set-release:** Performs all of the actions defined for the set operation. In addition, the start of this operation marks the point in the sequence of gate operations at which the MAC associated with the port is permitted to resume transmitting preemptible frames; if an express frame is currently being transmitted by the MAC, the release takes effect at the end of that transmission. If frame preemption is not supported or not enabled this operation behaves the same as set operation.

The value of a time-interval should always be larger than the guard band time (as specified thru the values of max-sdu and LINK\_SPEED).

An open queue will always be opened for a small amount of time, even if the guard band time is larger than the configured time-interval.

**Restrictions:** For a GCE with set-hold, all queues opened must be Express queues. For a GCE with set-release all queues opened must be Preemptible queues. The same queue cannot be open in both a set-hold and a set-release operation.

#### 8.5.5.2. Configuration of Gate Control List

A Gate Control List (GCL) is a list of gate control entries (GCE). A GCL is configured by the control-list parameter. The number of GCEs in a control-list is defined by control-list-length parameter.

When defining a control-list, start with setting control-list-length. Then configure each GCE. The sum of all time-intervals in a control-list must be equal to or less than the cycle-time. Each queue must be open in at least one QCE.

#### 8.5.5.3. Configuration of Always-guard-band Option

The always-guard-band defines how the guard band values are calculated and has the following effect:

If a GCL does not contain set-hold and/or set-release operations the always-guard-band has no effect.

If a GCL does contain set-hold and set-release operations then:

- ▶ When always-guard-band = true a guard band is implemented on all queues, both Express and Preemptible queues.
- ▶ When always-guard-band = false a guard band is only implemented on Preemptible queues.

#### 8.5.5.4. Calculation of Guard Band Times

The Maximum SDU size parameter is used to calculate the guard band time:  $gbt = \text{max\_sdu[]} * 8 / \text{LINK\_SPEED}$

If frame preemption is enabled and a gate operation is set-hold, the guard band time in preemptible queues is automatically selected as the frame preemption min fragment size plus 64 bytes.



A queue is said to be preemptible, if frame preemption is enabled, and if this queue is not opened in a set-hold gate operation.

#### 8.5.5.5. Using Config-change and Base-time

The command "tsn tas config-change" signals the start of a configuration change. If the value of parameter base-time is in the future, the configuration change will be executed at base-time. If base-time is in the past, the configuration change will be executed as soon as possible. In practice it will be within approx 2 seconds, at a time which is an integral number of cycle-times ahead of the configured value of basetime. This way, the synchronisation between schedules in elements across a scheduled network can be maintained.

#### 8.5.5.6. Uncertainty Related to Last Frame in TAS Gate Open Interval

In the Fireant implementation of Time Aware Shaper function (IEEE 802.1Q-2018, Enhancements for Scheduled Traffic), frames that are buffered in the disassembler fifo on the egress port when the TAS gate closes are transmitted after the gate time  $T_s$ .

In a test, where frames of the same size are transmitted using TAS, the maximum number of frames transmitted 'N', is calculated as follows:

```
Ts:                gate open time interval
max_sdu_line:      configured value (including 8 bytes preamble + 12 bytes IFG)
speed:             link speed
guard_time:        max_sdu_line * 8 / speed
frame_size:        size of frames sent
frame_size_line:   size of frames sent including 8 bytes preamble + 12 bytes IFG
fifo_size:         size of fifo on the egress port. Depends on port speed
N = (Ts - guard_time) * speed/frame_size_line +
Max(fifo_size/frame_size, 1)
```

Example:

```
Ts = 100 us
speed = 1000,000,000 bit/sec
frame_size = 148 bytes
frame_size_line = 168 bytes
max_sdu_line = 276 bytes
guard_time = 276 * 8 / 1000,000,000 = 2.208 us
fifo_size: 1024 bytes (1G interface)
N = (100 us - 2.208 us) * 1000,000,000 / (168*8) + Max(1024/148, 1)
N = 72,76 + 6,9 = 79.68 frames
```

Frames can be prevented from transmission after  $T_s$  by increasing the guard time to accommodate for the amount of traffic queued up in the disassembler fifo as follows:

```
guard_time_safe * speed/frame_size_line = Max(fifo_size/frame_size, 1) <=>
guard_time_safe = Max(fifo_size/frame_size, 1) * frame_size_line/speed
```

Using the parameters from the Example:

```
guard_time_safe = 6,9 * 168 bytes * 8bits/byte / 1000,000,000 bit/sec = 9.3us
```

And thereby:

```
max_sdu_safe = guard_time_safe * speed / 8 bits/byte = 1162 bytes
max_sdu_line = 276 bytes + 1162 bytes = 1438 bytes.
```





## 8.5.6. Frame Preemption

Frame Preemption is defined in the IEEE 802.1Qbu and IEEE 802.3br standards.

Frame Preemption is the ability to suspend the transmission of a non time-critical frame, and allow for one or more time-critical frames to be transmitted. When the time-critical frames have been transmitted, the transmission of the non time-critical frame is resumed. A non time-critical frame could be preempted multiple times.

The use of Frame Preemption with Time Aware Shaping reduces the guard band needed from the size of the largest possible interfering frame to the size of the largest possible interfering fragment.

Frame Preemption must be enabled on both egress port level and on egress port/ queue level.

Frame Preemption is disabled by default on port level and disabled by default on port/queue level.

### 8.5.6.1. Configuration Examples

CLI commands example:

```

! Enable frame-preemption on port level for port 1.
# configure terminal
(config)# interface GigabitEthernet 1/1
! Enable frame-preemption on port (disabled by default)
(config-if)# tsn frame-preemption
! Enable frame-preemption on queue level for port 1, queue 0 and 1.
# configure terminal
(config)# interface GigabitEthernet 1/1
! Enable frame-preemption on queue 0 and 1
(config-if)# tsn frame-preemption queue 0-1
! Disable verification of preemption capability of link partner.
# configure terminal
(config)# interface GigabitEthernet 1/1
! Disable verification of preemption capability of link partner.
(config-if)# tsn frame-preemption verify-disable
! Do not wait to receive lldp message before enabling frame-preemption in transmit
direction.
# configure terminal
(config)# interface GigabitEthernet 1/1
! Do not wait to receive lldp message before enabling frame-preemption in transmit
direction.
(config-if)# tsn frame-preemption ignore-lldp
! Disable frame-preemption on port level for port 1
# configure terminal
(config)# interface GigabitEthernet 1/1
! Disable frame-preemption on port
(config-if)# no tsn frame-preemption
! Disable frame-preemption on on queue level for port 1, queue 0 and 1.
# configure terminal
(config)# interface GigabitEthernet 1/1
! Disable frame-preemption on queue 0 and 1
(config-if)# no tsn frame-preemption queue 0-1

! Show configuration using 'show running-config'.
! Note that frame-preemption on port level is disabled by default
! and not shown unless the 'all-defaults' option is used.
# show running-config
[...]
tsn frame-preemption queue 0
tsn frame-preemption queue 1

```

## 8.5.6.2. Status

CLI commands example:

```
! Show frame preemption port status using 'show tsn frame-preemption status'.
# show tsn frame-preemption status interface GigabitEthernet 1/1
interface GigabitEthernet 1/1
HoldAdvance : 1016 nanoseconds
ReleaseAdvance : 1016 nanoseconds
PreemptionActive : FALSE
HoldRequest : FALSE
StatusVerify : disabled
LocPreemptSupported : TRUE
LocPreemptEnabled : TRUE
LocPreemptActive : FALSE
LocAddFragSize : 0 (64 octets)
```

## 8.6. Network

### 8.6.1. Ethernet Ports - Configuration Commands

Configure Ethernet ports Link speed, max Ethernet packet size and flow control.

#### 8.6.1.1. Shutdown

Description- Enable/disable Ethernet port.

shutdown no

shutdown

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	Port List Interface configuration mode	
Usage	Use the command to disable the specified interface and use no form of this command to enable the interface	
Examples	<p>Example#1 (disable port 1)</p> <pre># configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# shutdown</pre> <p>Example#2 (disable ports 1 through 8)</p> <pre># configure terminal (config)# interface GigabitEthernet 1/1-8 (config-if)# shutdown</pre> <p>Example#3 (enable all ports)</p> <pre># configure terminal (config)# interface * (config-if)# no shutdown</pre>	

#### 8.6.1.2. Speed

Description- configure port speed.

**speed** { 1000 | 100 | 10 | auto }

	Parameter	Description
Parameter	10	10Mbps
	100	100Mbps
	1000	1000Mbps (1Gbps)
	auto	Auto negotiation
Default	All ports are set to Auto	
Mode	Port List Interface Mode	
Usage	Use to set the speed of the specified interface	
Examples	<p>Example#1 (set speed for port 1 to 100Mbps)</p> <pre># configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# speed 100</pre>	

	Parameter	Description
	Example#2 (set all ports to 1Gbps) # configure terminal (config)# interface * (config-if)# speed 1000	

### 8.6.1.3. Duplex

Description- configure interface duplex mode.

**duplex** { half | full | auto }

**no duplex**

	Parameter	Description
Parameter	half	Forced half duplex
	full	Forced full duplex
	auto	Auto negotiation of duplex mode.
Default	All ports are set to Auto	
Mode	Port List Interface Mode	
Usage	Use to set the duplex mode of the specified interface. Use the no form of the command	
Examples	Example#1 (set duplex for port 1 to half) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# duplex half	
	Example#2 (set all ports to 1Gbps) # configure terminal (config)# interface * (config-if)# speed 1000	

### 8.6.1.4. Flow Control

Description- configures flow control for the interface (slow temporarily packet transition upon request, or for packet reception, signal the remote transmitter to slow down temporarily its packet transition whenever switch reception buffer becomes to full).

**flowcontrol** { on | off }

**no flowcontrol**

	Parameter	Description
Parameter	on	Enable flow control
	off	Disable flow control
Default	All ports flow control receive and send is off	
Mode	Port List Interface Mode	
Usage	Use to set the flow control for the interface. Use the no form of the command to return to defaults.	
Examples	Example#1 (enable flow control for port 1)	

	Parameter	Description
	# configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# flowcontrol on	
	Example#2 (enable flow control for all ports) # configure terminal (config)# interface * (config-if)# flowcontrol on	

#### 8.6.1.5. MTU

Description- specify the Maximum Transmission Unit (MTU) Ethernet frame size for the interface.

**mtu** <max\_length>

**no mtu**

	Parameter	Description
Parameter	on	Enable flow control
	off	Disable flow control
Default	All ports flow control receive and send is off	
Mode	Port List Interface Mode	
Usage	Use to set the flow control for the interface. Use the no form of the command to return to defaults.	
Examples	Example#1 (set mtu for port 1 to 1518) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# mtu 1518  Example#2 ( set mtu for all ports to 1518) # configure terminal (config)# interface * (config-if)# mtu 1518	

## 8.6.2. Ethernet Port View Commands

View link status (up/down/speed), flow control, max frame size and mode.

### 8.6.2.1. Show Interface Status

Description- display status and configuration information for any port.

**show interface** <port\_type> [ <v\_port\_type\_list> ] **status**

	Parameter	Description
Parameter	<port_type>	Port type in GigabitEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5;2/2-4,6
Default	N.A	
Mode	EXEC mode	
Usage	Use to display current status of the specified interface	
Examples	Example#1 (show status and configuration for port#1) # show interface GigabitEthernet 1/1 status	
	Example#2 (show status and configuration for ports #1 through #5) # show interface GigabitEthernet 1/1-5 status	
	<pre> # show interface GigabitEthernet 1/1-5 status Interface          Mode      Speed &amp; Duplex  Flow Control  Max Frame  Excessive  Link ----- GigabitEthernet 1/1  enabled  Auto           disabled      9600       Discard    100fdx GigabitEthernet 1/2  enabled  Auto           disabled      9600       Discard    Down GigabitEthernet 1/3  enabled  Auto           disabled      9600       Discard    Down GigabitEthernet 1/4  enabled  Auto           disabled      9600       Discard    Down GigabitEthernet 1/5  enabled  Auto           disabled      9600       Discard    Down # </pre>	

### 8.6.3. IPv4, IPv6 - Configuration Commands

Configure static/dynamic IPv4, IPv6 address and mask, default gateway, DNS.

#### 8.6.3.1. IP Name-Server - DNS Server

Description- Set the DNS server for resolving domain names.

```
ip name-server [ <order> ] { <v_ipv4_ucast> | { <v_ipv6_ucast> [ interface vlan
<v_vlan_id_static> ] } | dhcp [ ipv4 | ipv6 ] [ interface vlan <v_vlan_id_dhcp> ] }
no ip name-server
```

	Parameter	Description
Parameter	<order>	Preference of DNS server (default selection is 0)
	<v_ipv4_ucast>	A valid IPv4 unicast address
	<v_ipv6_ucast>	A valid IPv6 unicast address
	dhcp	Dynamic Host Configuration Protocol
Default	No DNS server configured	
Mode	Global Configuration mode	
Usage	Set the DNS for resolving domain names. Use the no version of the command to return to default.	
Examples	<p>Example#1 ( DNS Server 0 setting is derived from any DHCPv4 VLANs-ID) (config)# ip name-server 0 dhcp</p> <p>Example#2 ( DNS Server 1 configured as a static IPv4 address) (config)# ip name-server 1 192.168.0.10</p> <p>Example#3 (DNS Server 1 setting is derived from DHCPv4 VLANs-ID 1) (config)# ip name-server 1 dhcp ipv4 interface vlan 1</p>	

#### 8.6.3.2. IP (ipv6) Address - IPv4, IPv6 Interface

Description- add IPv4, IPv6 interface.

```
ip address { { <address> <netmask> } | { dhcp [ fallback <fallback_address>
<fallback_netmask> [ timeout <fallback_timeout> ] ] [ client-id { <port_type>
<client_id_interface> | ascii <ascii_str> | hex<hex_str> } ] [ hostname <hostname> ] }
}
```

```
no ip address
```

```
ipv6 address <subnet>
```

```
no ipv6 address
```

	Parameter	Description
Parameter	<address>	IPv4 address
	<netmask>	IP netmask
	dhcp	Enable Dynamic Host Configuration Protocol
	fallback	DHCP fallback settings
	client-id	DHCP client identifier
	hostname	DHCP host name
	<subnet>	IPv6 prefix x:x::y/z
Default	N.A	

	Parameter	Description
Mode	VLAN Interface Configuration mode	
Usage	Add VLAN interface and set all IPv4, IPv6 parameters. Use the no version of the command to disable the selected VLAN interface. To remove it completely use no interface vlan <id> from Global configuration mode.	
Examples	<p>Example#1 ( Set VLAN2 static IP address to 192.168.1.50 mask length 24)</p> <pre>(config)#interface vlan 2 (config-if-vlan)# ip address 192.168.1.50 255.255.255.0</pre> <p>Example#2 ( Add VLAN 3 and set it to get IP address from DHCP using MAC of port 1 as Client ID with a hostname test)</p> <pre>(config)#interface vlan 3 (config-if-vlan)# ip address dhcp client-id GigabitEthernet 1/1 hostname test</pre>	

### 8.6.3.3. IP Routes (default gateway)

Description- Add new IP route.

```
ip route <ipv4_addr> <ipv4_netmask> <ipv4_gw> [ <distance> ]
```

```
no ip route <ipv4_addr> <ipv4_netmask> <ipv4_gw>
```

	Parameter	Description
Parameter	<ipv4_addr>	Network
	<ipv4_netmask>	Netmask
	<ipv4_gw>	Gateway
	<distance>	Distance value for this route
Default	N.A	
Mode	Global Configuration mode	
Usage	To route all unknown destination IP to default gateway use the following parameters: Network=0.0.0.0 Netmask=0.0.0.0 and Distance=1 To remove the route use no ip route command with all parameters for the selected route.	
Examples	<p>Example#1 (add IP route to gateway 192.168.1.1)</p> <pre>(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1 1</pre> <p>Example#2 ( remove IP route)</p> <pre>(config)#no ip route 0.0.0.0 0.0.0.0 192.168.1.1</pre>	



## 8.6.4. IPv4, IPv6 - View Commands

## 8.6.4.1. Show Interface VLAN

Description - View VLAN interface status and configuration.

show interface vlan [ <vlist> ]

	Parameter	Description
Parameter	<vlist>	VLAN list
Default	N.A	
Mode	EXEC mode	
Usage	Use to display current status and configuration of the specified interface	
Examples	<pre>Example#1 (show status and configuration for VLAN 1) # show interface vlan 1  # show interface vlan 1 VLAN1 LINK: 00-05-5a-98-67-23 Mtu:1500 &lt;UP BROADCAST MULTICAST&gt; IPv4: 192.168.0.50/24 192.168.0.255 IPv6: fe80::205:5aff:fe98:6723/64 &lt;&gt;</pre>	

### 8.6.5. NTP (Network Time Protocol) - Configuration Commands

Configure the switch NTP Servers IP. The NTP Server updates the switch with the correct GMT (Greenwich Mean Time).

#### 8.6.5.1. NTP Server - Configure NTP Server

Description- Enable or disable NTP server and specify the NTP server's parameters. Up to five NTP servers can be configured.

```
ntp no ntp
```

```
ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }
```

```
no ntp server <index_var>
```

	Parameter	Description
Parameter	<index_var>	NTP Server index (1-5)
	<ipv4_var>	IPv4 address of NTP server
	<ipv6_var>	IPv6 address of NTP server
	<name_var>	Domain name of NTP server
Default	N.A	
Mode	Global Configuration mode	
Usage	Enable NTP server by entering ntp command. Use a no version of the command to disable it. Specify the parameters of NTP server by entering ntp server command. Use a no version of the command to delete the specified NTP server.	
Examples	Example#1 (add NTP server 1 with IP address 192.168.1.2) (config)#ntp server 1 ip-address 192.168.1.2	
	Example#2 ( add NTP server 2 with domain <any-ntp-server>) (config)#ntp server 2 ip-address <any-ntp-server>	
	Example#3 (enable NTP server) (config)#ntp	

### 8.6.6. NTP (Network Time Protocol) - View Commands

#### 8.6.6.1. Show NTP Status - View NTP Status

Description - View NTP status and all configured NTP servers.

```
show ntp status
```

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC mode	
Usage	Use the command view status and configuration of NTP servers	
Examples	Example#1	
	#show ntp status	

## 8.6.7. Time Zone - Configuration Commands

Configure switch local time zone and daylight saving.

### 8.6.7.1. Clock Timezone - Time Zone Configuration

Description - configure time zone.

```
clock timezone <word16> <hour_var> [ <minute_var> [ <subtype_var> ] ]
```

```
no clock timezone
```

	Parameter	Description
Parameter	<word16>	Name of time zone up to 16 characters. Use `` for null input
	< hour_var >	Hours offset from UTC -23-23
	<minute_var>	Minutes offset from UTC 0-59
	<subtype_var>	Sub type of time zone 0-9
Default	(UTC) Coordinated Universal Time	
Mode	Global Configuration mode	
Usage	Specify the time zone and offsets from UTC. Use the no form of the command to return to default.	
Examples	Example#1 (Configure Eastern time zone with -05:00 from UTC) (config)#clock timezone Eastern -05 0	

### 8.6.8. Clock Summer-Time - Daylight Savings Time Configuration

Description - Configure daylight savings time.

```
clock summer-time <word16> date [ <start_month_var> <start_date_var>
<start_year_var>
<start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [
<offset_var> ] ]
clock summer-time <word16> recurring [ <start_week_var> <start_day_var>
<start_month_var>
<start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [
<offset_var>] ]
no clock summer-time
```

Parameter	Parameter	Description
Parameter	<word16>	Name of time zone in summer up to 16 characters. Use `` for null input
	<start_month_var>	Month to start (1-12)
	<start_date_var>	Date to start (1-31)
	<start_year_var>	Year to start (2000-2097)
	<start_hour_var>	Time to start (hh:mm)
	<end_month_var>	Month to end (1-12)
	<end_date_var>	Date to end (1-31)
	<end_year_var>	Year to end (2000-2097)
	<end_hour_var>	Time to end (hh:mm)
	<offset_var>	Offset to add in minutes (1-1439)
	<start_week_var>	Week number to start (1-5)
	<start_day_var>	Weekday to start (1-7)
	<end_week_var>	Week number to end (1-5)
	<end_day_var>	Weekday to end (1-7)
Default	Daylight savings time mode disabled	
Mode	Global Configuration mode	
Usage	Configure summer (daylight savings) time in absolute non-recurring mode (date) and recurring mode (recurring). Use the no form of the command to go back to default.	
Examples	Example#1 (Configure non-recurring Daylight Savings Time to start on March 10 2019 at 02:00AM and finish on November 3 2019 at 02:00AM) (config)#clock summer-time `` date 3 10 2019 02:00 11 3 2019 02:00	

## 8.6.9. Time Zone - View Commands

### 8.6.9.1. Show Clock Detail

Description - Display the detailed clock information.

show clock detail

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC mode	
Usage	Use to display clock information	
Examples	Example # show clock detail	

## 8.6.10. SysLog Report - Configuration Commands

Configure SysLog Server IP address. The switch sends SysLog messages during Power-Up and normal operation. The SysLog events are send by the switch over the Network to SysLog Server. The user has the option to filter some of the SysLog messages being send by the switch by configuring from what severity/importance SysLog messages the message should be send.

### 8.6.10.1. Logging - Enable and Configure SysLog

Description - System Log configuration commands.

logging on

```
logging host { <ipv4_addr> | <domain_name> }
```

```
logging level { informational | notice | warning | error }
```

no logging on

	Parameter	Description
Parameter	<ipv4_addr>	Name of time zone up to 16 characters. Use `` for null input
	<domain_name>	Hours offset from UTC -23-23
	informational	Severity 6: Informational messages
	notice	Severity 5: Normal but significant condition
	warning	Severity 4: Warning conditions
	error	Severity 3: Error conditions
Default	N.A	
Mode	Global Configuration mode	
Usage	Enable SysLog server, specify its address and what level of messages will be sent to it. Use the no logging on command to disable SysLog server.	
Examples	Example#1 (Enable SysLog server at 192.168.0.1 with Warning level messages) (config)#logging on (config)#logging host 192.168.0.1 (config)#logging level warning.  Example#2 (Disable SysLog server) (config)#no logging on	

## 8.6.11. SysLog Report - View Commands

### 8.6.11.1. Show Logging

Description - Show logging configuration and message summary.

```
show logging [ informational ] [ notice ] [ warning ] [
error ]
```

```
show logging <log_id> [ switch <switch_list> ]
```

	Parameter	Description
Parameter	informational	Severity 6: Informational messages
	notice	Severity 5: Normal but significant condition
	warning	Severity 4: Warning conditions
	error	Severity 3: Error conditions
	<log_id>	Message logging ID
	<switch_list>	List of switch ID (in a stacked system) ex, 1,3-5,7
Default	N.A	
Mode	EXEC mode	
Usage	Display SysLog server status and configuration and detailed logging messages.	
Examples	Example#1 (Show SysLog configuration on switch 1 and detailed log message 1) #show logging 1 switch 1  Example#2 ( Show SysLog configuration and detailed Error log messages) #show logging error	

## 8.6.12. MAC Table Learning - Configuration Commands

Provides various options regarding the way MAC address learning should be processed by the Ethernet Switch, and how to process a packet with unknown source MAC address, unknown destination MAC address, etc.

When a packet is received, it is classified by the packets's Source-MAC, Destination-MAC, VLAN-ID and Port number. As part of Ethernet Switch forwarding algorithm, the switch looks for Destination-MAC and VLAN inside the MAC learning table. If found, the packet will be forwarded to the specified port, otherwise the packet is flooded to all ports on same VLAN.

### 8.6.12.1. MAC Address-Table Aging-Time

Description- By default, dynamic entries are removed from the Mac table after 300 seconds. This process is called aging. Aging time can be configured to be in the range of 10 to 1000000 seconds or 0 to disable automatic aging.

```
mac address-table aging-time <v_0_10_to_1000000>
```

```
no mac address-table aging-time
```

	Parameter	Description
Parameter	<v_0_10_to_1000000>	Aging time in seconds, 0 disables aging
Default	Aging time is 300 seconds	
Mode	Global Configuration mode	
Usage	Set MAC address table aging time in seconds. Use the no version of the command to reset to default (300 seconds)	
Examples	Example#1 (Set aging time to 400 seconds) (config)# mac address-table aging-time 400  Example#2 ( Disable automatic aging) (config)# mac address-table aging-time 0	

### 8.6.12.2. MAC Address-Table Learning

Description - Each port can do learning in Auto mode (performed automatically as soon as the frame with unknown MAC is received) or Secured mode (only static MAC entries are learned and all other frames are dropped). MAC learning can also be disabled and no learning is performed. Specific VLANs can also be learning-disabled.

```
mac address-table learning [ secure ]
```

```
no mac address-table learning
```

```
mac address-table learning vlan <vlan_list>
```

```
no mac address-table learning vlan <vlan_list>
```

	Parameter	Description
Parameter	[ secure ]	Port Secure mode
Default	All ports are in Auto learning mode	
Mode	Port List Interface Mode (for specific port), Global Configuration Mode (for VLANs)	
Usage	Set MAC address table learning mode to Secure or back to Auto (command without [ secure ] parameter). Use the no version of the command to Disable learning.	



	Parameter	Description
Examples	Example#1 (Set MAC address learning to Secure on port 1) (config)# interface GigabitEthernet 1/1 (config-if)#mac address-table learning secure	
Examples	Example#2 ( Disable MAC address learning on ports 2-5) (config)# interface GigabitEthernet 1/2-5 (config-if)#no mac address-table learning  Example#3 (add VLAN2 to the list of learning disabled VLANs) (config)# no mac address-table learning vlan 2	

### 8.6.12.3. MAC Address-Table Static

Description - Assign a static mac address to the specific port or ports.

```
mac address-table static <v_mac_addr> vlan <v_vlan_id> { [ interface
<port_type> [ <v_port_type_list> ] ] }
```

```
no mac address-table static <v_mac_addr> vlan <v_vlan_id> { [
interface <port_type> [ <v_port_type_list> ] ] }
```

	Parameter	Description
Parameter	<v_mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
	<v_vlan_id>	VLAN IDs 1-4095
	<port_type>	GigabitEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
Default	N.A	
Mode	Global Configuration Mode	
Usage	Assigns a static MAC address to a port. Use the no version of the command to remove it.	
Examples	Example#1 (Assign static MAC address 00:11:22:33:44:55 to port 1 on VLAN 1) (config)#mac address-table static 00:11:22:33:44:55 vlan 1 interface Gi 1/1	

## 8.6.13. MAC Table Learning - View Commands

### 8.6.13.1. Show MAC Address-Table

Description - Display MAC address table entries.

```
show mac address-table [ conf | static | aging-time | { { learning | count } [
interface <port_type> [ <v_port_type_list> ] | vlan <v_vlan_id_2> ] } | { address
<v_mac_addr> [ vlan <v_vlan_id> ] } | vlan <v_vlan_id_1> | interface <port_type> [
<v_port_type_list_1> ] ]
```

	Parameter	Description
Parameter	conf	User added static MAC addresses
	static	All static MAC addresses
	aging-time	Display MAC address aging time
	learning	MAC address learning state (Learn/Secure/Disable)
	count	Total number of MAC addresses
Default	N.A	
Mode	EXEC Mode	
Usage	Show MAC address table entries in various views based on the specific parameter	
Examples	Example#1 (display all static MAC addresses) #show mac address-table static	
	Example#2 (display the MAC table entry for MAC address 00:11:22:33:44:55) #show mac address-table address 00:11:22:33:44:55	
	Example#3 (display the MAC table entry for port 2) #show mac address-table interface GigabitEthernet 1/2	
	Example#4 (display all MAC table entries) #show mac address-table # show mac address-table Type VID MAC Address Ports Static 1 00:00:00:00:00:11 GigabitEthernet 1/3-5 Dynamic 1 00:05:5a:03:99:b6 GigabitEthernet 1/9 Static 1 00:05:5a:98:67:23 CPU Dynamic 1 00:0a:cd:2d:b1:ed GigabitEthernet 1/10 Dynamic 1 18:68:cb:b5:85:03 GigabitEthernet 1/1 Static 1 33:33:00:00:00:01 GigabitEthernet 1/1-11 CPU Static 1 33:33:ff:98:67:23 GigabitEthernet 1/1-11 CPU Static 1 ff:ff:ff:ff:ff:ff GigabitEthernet 1/1-11 CPU	

## 8.6.14. Routing - View Commands

### 8.6.14.1. Show IP Route

Description- Display IPv4 route entry table with status information.

show ip route

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display routing information	
Examples	<pre>Example #show ip route # show ip route Codes: C - connected, S - static, O - OSPF,       * - selected route, D - DHCP installed route  C* 192.168.0.0/24 is directly connected, VLAN 1 #</pre>	

## 8.7. Access Control

Controls who can access the switch, from what type of Network interface, who will verify remote user username and password (by the switch locally, or by RADIUS/TACACS+ Authentication Server).

### 8.7.1. Local Users - Configuration Commands

Allows changing "admin" user password, adding or removing additional users and changing users' password.

#### 8.7.1.1. Username -Add Local User or Change Password

Description- Add, remove or change password of local users. Up to 20 users can be configured.

```
username { default-administrator | <input_username> } privilege <priv> password { unencrypted
```

```
<unencry_password> | encrypted <encry_password> | none }
```

```
no username <username>
```

	Parameter	Description
Parameter	<input_username>	User name allows letters, numbers and underscores
	<priv>	User privilege level 0-15. NOTE - Use only privilege level 15
	<unencry_password>	The UNENCRYPTED (Plain Text) user password. Any printable characters including space are accepted. Notice that you have no chance to get the Plain Text password after this command. The system will always display the ENCRYPTED password.
	<encry_password>	The ENCRYPTED (hidden) user password. Notice the ENCRYPTED password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Add a new user for the local switch access and add/change password	
Examples	Example#1 (add a user named usertest with unencrypted password of testuser) (config)# username usertest privilege 15 password unencrypted testuser	
	Example#2 (remove user named usertest) (config)# no username usertest	
	Example#3 (change the password of usertest to testuser123 ) (config)# username usertest privilege 15 password unencrypted testuser123	




---

The switch is shipped with default username 'admin' and with no password. It is strongly recommended to assign a strong password instead.

---



Username 'admin' cannot be removed or be changed, only its password.

## 8.7.2. Local Users - View Commands

### 8.7.2.1. Show User-Privilege

Description- Display all local users, privilege levels and passwords

show user-privilege

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display information about all local user accounts	
Examples	Example <pre># show user-privilege  # show user-privilege username admin privilege 15 password encrypted 64d0dfc93d6b24b6ad00! 0dc81cb0e9865f737d4d7d1fb8e83be6cb687dd5fce85a26d9d21a754b753d1a1 "</pre>	

### 8.7.2.2. Show Users ←New Command, Need to Update TOC

Description- Display information on how remote users are connected at the moment to the switch. Serial is represented as "con", Telnet is represented as "vty".

show users

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display information on how remote users are connected	
Examples	Example <pre># show users  # show users Line is con 0. * You are at this line now. Connection is from Console. User name is admin. Privilege is 15. Elapsed time is 0 day 0 hour 12 min 48 sec. Idle time is 0 day 0 hour 0 min 0 sec.  Line is vty 0. Connection is from 192.168.0.40:63043 by Telnet. User name is admin. Privilege is 15. Elapsed time is 0 day 0 hour 5 min 29 sec. Idle time is 0 day 0 hour 5 min 29 sec.</pre>	

### 8.7.3. Web Server - Configuration Commands

Controls whether switch embedded Web Server should operate in HTTP or HTTPS mode. HTTPS use TLS v1.2 encryption to encrypt all Web Network traffic between the user web browser and the switch Web Server.

#### 8.7.3.1. IP HTTP Secure-Server

Description- Configure Web Server to use only HTTPS (secure and encrypted operation mode) or HTTP (unsecure operation mode) as well.

```
ip http secure-server
no ip http secure-server
```

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure Web Server to use HTTPS. Use the no version of the command to use HTTP	
Examples	Example (config)# ip http secure-server (config)# no ip http secure-server	

#### 8.7.3.2. IP HTTP Secure-Certificate

Description- Manage Web Server certificate. Use this command to delete the current certificate, generate a new self-signed RSA certificate or upload a PEM certificate using URL over http, tftp or ftp.

```
ip http secure-certificate { upload <url_file> [ pass-phrase <pass_phrase> ] | delete
| generate }
```

	Parameter	Description
Parameter	<url_file>	Uniform Resource Locator. It is a specific character string that constitutes a reference to a resource. Syntax: <protocol>://[<username>[:<password>]@]<host>[:<port>][/ <path>]/<file_name> If the following special characters: space !\"#\$%&'()*+/,/:;=>?@[\\]^_`{ }~ need to be contained in the input URL string, they should be percent-encoded. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
	<pass_phrase>	Privacy key pass phrase string if uploading certificate protected by a specific passphrase.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Manage the HTTPS certificate (PEM format)	
Examples	Example#1 (upload the HTTPS certificate from TFTP server)	

	Parameter	Description
	(config)# ip http secure-certificate upload tftp://10.9.52.103/test_ca.pem	
	Example#2 (delete current certificate) (config)# ip http secure-certificate delete	

## 8.7.4. Web Server - View Commands

### 8.7.4.1. Show IP HTTP

Description- Use this command to show status information about the secure HTTP web server.

show ip http

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display the secure HTTP web server status	
Examples	<pre>Example # show ip http  # show ip http Switch secure HTTP web server is enabled Switch secure HTTP web redirection is enabled Switch secure HTTP certificate is presented</pre>	

## 8.7.5. Telnet/SSH/Web - Configuration Commands

**Authentication Method Configuration** - Configures Which Network interface as telnet, SSH, Web or local console should be enabled or disable, and how remote user username + password will be authenticated. Should it be done locally by the switch or by remote RADIUS/TACACS+ Authentication Server.

**Accounting Method Configuration** - Configures if the switch should send Accounting messages to remote TACACS+ Accounting server whenever remote user login/logout, and report any CLI command typed by the user over Console, Telnet or SSH.

### 8.7.5.1. aaa Authentication Login

Description- Configures how a user is authenticated when logging into the switch via one of the management client interfaces - console, telnet, ssh or web. Each one of the interfaces may have up to three authentication servers. In case the first authentication server is down, then second authentication server will be accessed instead. The same procedure applies to the third authentication server in case both the first and second authentication servers are down.




---

Rejection of remote user by any of the authentication servers will reject the remote user. The three remote authentication servers are used only as a backup in case one of the authentication services is down.

---



Disabling authentication by all three authentication services will disable management interface (console, Telnet, SSH, Web).

Local- use the switch local user database.

Radius- use remote RADIUS server

Tacacs- use remote TACACS+ server.

```
aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [ { local | radius | tacacs } [ { local | radius | tacacs } ] ] }
```

```
no aaa authentication login { console | telnet | ssh | http }
```

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure user authentication method for a specific management interface. Use the no version of the command to disable the interface.	
Examples	<p>Example#1 (configure SSH to be authenticated 1st by RADIUS Server. In case it is down, then by TACACS Server, and in case it is also down, then be authenticated locally)</p> <pre>(config)#aaa authentication login ssh radius tacacs localconfig)# aaa authentication login ssh radius tacacs local</pre> <p>Example#2 (disable Telnet remote access)</p> <pre>(config)# no aaa authentication login telnet</pre>	

### 8.7.5.2. aaa Accounting

Description - Configure what type of activity over a specific interface (console, telnet or ssh) is reported to the TACACS+ accounting server. Possible options are "CLI Commands", and Exec=Login/Logout.

CLI Commands - every CLI command entered by the user will be mirrored to the accounting server. Exe (Login/Logout) - every login/logout of remote user will be reported to the accounting server.

```
aaa accounting { console | telnet | ssh } tacacs { [ commands <priv_lvl> ] [ exec ] }
```

```
no aaa accounting { console | telnet | ssh }
```

	Parameter	Description
Parameter	[commands <priv_lvl> ]	All CLI commands equal and above the privilege level are accounted
	[ exec ]	Only remote user login/logout is reported
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure accounting method and reporting. Use the no version of the command to disable accounting.	
Examples	<p>Example#1 (configure accounting for ssh to report all CLI activity and any login/logout )</p> <pre>(config)# aaa accounting ssh tacacs commands 15 exec</pre>	



	Parameter	Description
	Example#2 (disable accounting for Telnet)	(config)# no aaa accounting telnet

## 8.7.6. Telnet/SSH/Web - View Commands

### 8.7.6.1. Show aaa

Description - Display the current authentication, authorization and accounting statuses and methods for all interfaces.

show aaa

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	EXEC Mode	
Usage	Display the current status of authentication, authorization and accounting.	
Examples	<pre> Example # show aaa  # show aaa Authentication :   console : local   telnet  : disable   ssh    : radius tacacs local   web    : local Authorization :   console : no, commands disabled   telnet  : no, commands disabled   ssh    : no, commands disabled Accounting :   console : no, commands disabled, exec disabled   telnet  : no, commands disabled, exec disabled   ssh    : tacacs, commands 15 enabled, exec enabled           </pre>	

## 8.7.7. Access Management - Configuration Commands

Access Management - configures from what remote IP address remote user will be able to access the Switch management interface over Web, SNMP, Telnet/SSH.

### 8.7.7.1. Access Management

Description - Enable/disable access management mode and configure up to 16 entries.

access management

no access management

```
access management <access_id> <access_vid> <start_addr> [ to <end_addr> ] { [ web ] [ snmp ] [ telnet ] | all }
```

```
no access management <access_id_list>
```

	Parameter	Description
Parameter	<access_id>	ID of access management entry (1-16)
	<access_vid>	VLAN ID for the access management entry (1-4095)
	<start_addr>	Start IPv4 or IPv6 unicast address
	<end_addr>	End IPv4 or IPv6 unicast address
Default	N.A	
Mode	Global Configuration Mode	

	Parameter	Description
Usage		Enable access management mode and configure up to 16 entries. Use the no version of the command to disable access management globally or a specific entry.
Examples		<p>Example#1 (configure access management entry 1 on VLAN4 for IPv4 address 192.168.0.40 - 192.168.0.70 on all interfaces)</p> <pre>(config)# access management 1 4 192.168.0.40 to 192.168.0.70 all</pre> <p>Example#2 (disable access management entry 1)</p> <pre>(config)# no access management 1</pre>

## 8.7.8. Access Management - View Commands

### 8.7.8.1. Show Access Management

show access management [ statistics | <access\_id\_list> ]

	Parameter	Description														
Parameter	<access_id_list>	ID of access management entry (1~16)														
Default	N.A															
Mode	EXEC Mode															
Usage		Display access management status and all entries or statistics or a specific entry.														
Examples		<p>Example#1 (show access management configuration)</p> <pre># show access management</pre> <pre># show access management Switch access management mode is disabled W: WEB/HTTPS S: SNMP T: TELNET/SSH</pre> <table border="1"> <thead> <tr> <th>Idx</th> <th>VID</th> <th>Start IP Address</th> <th>End IP Address</th> <th>W</th> <th>S</th> <th>T</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>4</td> <td>192.168.0.40</td> <td>192.168.0.70</td> <td>Y</td> <td>Y</td> <td>Y</td> </tr> </tbody> </table> <p>Example#2 (show access management statistics)</p> <pre>#show access management statistics</pre> <pre># show access management statistics Access Management Statistics: ----- HTTP   Receive:    0  Allow:      0  Discard:    0 HTTPS  Receive:    0  Allow:      0  Discard:    0 SNMP   Receive:    0  Allow:      0  Discard:    0 TELNET Receive:    0  Allow:      0  Discard:    0 SSH    Receive:    0  Allow:      0  Discard:    0</pre>	Idx	VID	Start IP Address	End IP Address	W	S	T	1	4	192.168.0.40	192.168.0.70	Y	Y	Y
Idx	VID	Start IP Address	End IP Address	W	S	T										
1	4	192.168.0.40	192.168.0.70	Y	Y	Y										

## 8.8. VLAN

### 8.8.1. VLAN Configuration Commands and Port Types

#### VLAN Access

VLAN is a mean to split switch ports into sub port groups while each group is totally isolated from the other as if we are using two or more independent switches. Such splitting is done by assigning different VLAN-IDs to various groups of ports, each group is assigned a different VLAN-ID and the ports for each group are configured as Access ports meaning that VLAN tagging and port splitting is done internally by the switch. The packets transmitted over Access ports are the normal Ethernet ports with no VLAN tagging.

#### VLAN Trunk

VLAN Trunk port configuration allow multiple VLAN-IDs to travel over the same Ethernet cable or local LAN Network with absolute isolation between the VLANs traveling over the same infrastructure.

#### VLAN Port Types:

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

#### VLAN Port Type - Unaware:

On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

#### VLAN Port Type - C-Port:

On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

#### VLAN Port Type - S-Port:

On egress, if frames must be tagged, they will be tagged with an S-tag.

On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag.

Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.




---

If the S-port is configured to accept Tagged and Untagged frames (see Ingress Acceptance in the following text), frames with a C-tag are treated like frames with an S-tag.

---

If the S-port is configured to accept Untagged Only frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.

#### VLAN Port Type - S-Custom-Port:

On egress, if frames must be tagged, they will be tagged with the custom S-tag.

On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.




---

If the S-port is configured to accept Tagged and Untagged frames (see Ingress Acceptance in the following text), frames with a C-tag are treated like frames with an S-tag.

---

If the Custom S-port is configured to accept Untagged Only frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.

#### 8.8.1.1. VLAN - Create VLAN

Description- Create one or more VLANs in **Access mode**. By default, only single VLAN #1 is enabled with all ports assigned to this VLAN in Access mode.

```
vlan <vlist>
```

```
no vlan <vlist>
```

	Parameter	Description
Parameter	<vlist>	ISL VLAN IDs. Individual elements are separated by commas
Default	None	
Mode	Global Configuration mode	
Usage	Create allowed Access VLANs. Use the no version of the command to delete VLANs.	
Examples	Example#1 (Create Access VLANs 10,11,12,200 and 300) (config)# vlan 10-12,200,300  Example#2 ( Delete VLAN 12) (config)# no vlan 12	

#### 8.8.2. VLAN Ethertype S-Custom-Port

Description- Specifies the Ethertype/TPID (specified in hexadecimal) used for Custom S-Ports. The setting is in force for all ports set to S-Custom port type.




---

S-Custom VLAN port type is used whenever double VLAN tagging (Q-in-Q, 802.1ad) is in use.

---

```
vlan ethertype s-custom-port <etype>
```

	Parameter	Description
Parameter	<etype>	EtherType (Range: 0x0600-0xffff)
Default	TPID is set to 0x88A8	
Mode	Global Configuration mode	
Usage	Specifies the ethertype/TPID for Custom S-Ports	
Examples	Example#1 (Set TPID=8888) (config)# vlan ethertype s-custom-port 0x8888	

	Parameter	Description
	Example#2 ( Set TPID back to default 88A8)	(config)# no vlan ethertype s-custom-port

### 8.8.3. Switchport Mode

Description- Defines the port mode as access (default), trunk or hybrid unconditionally.

```
switchport mode { access | trunk | hybrid }
```

	Parameter	Description
Parameter	access	Configure a switch port mode is access
	trunk	Configure a switch port mode is trunk
	hybrid	Configure a switch port mode is hybrid
Default	The switch port default mode is access	
Mode	Port List Interface Mode	
Usage	Set port mode	
Examples	Example#1 (configure the port 3 mode as trunk) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk	

#### 8.8.3.1. Switchport Access VLAN

Description - Configure VLAN ID to the selected Switchport.

```
switchport access vlan <pvid>
```

```
no switchport access vlan
```

	Parameter	Description
Parameter	<pvid>	VLAN ID of the VLAN
Default	Default VLAN is VLAN1	
Mode	Port List Interface Mode	
Usage	Configure a port VLAN ID for a port. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 with PVID 4) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode access (not needed, access mode is default) (config-if)# switchport access vlan 4	

### 8.8.3.2. Switchport Trunk Native VLAN

Description - Configure VLAN ID to be added internally by the Switch whenever native VLAN packet (packet with no VLAN header) is received.

```
switchport trunk native vlan <pvid>
```

```
no switchport trunk native vlan
```

	Parameter	Description
Parameter	<pvid>	VLAN ID of the native VLAN when this port is in trunk mode
Default	Trunk native default VLAN is VLAN1	
Mode	Port List Interface Mode	
Usage	Configure a port VLAN ID for a trunk port. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as trunk with PVID 4) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 4	

### 8.8.3.3. Switchport Trunk VLAN Tag Native

Description- Port in Trunk mode may control the tagging of frames on egress. Options are default Untag Port VLAN (frames classified to the Port VLAN are transmitted untagged and all other frames are transmitted with the relevant tag) and Tag all (all frames transmitted with a tag).

```
switchport trunk vlan tag native
```

```
no switchport trunk vlan tag native
```

	Parameter	Description
Parameter	N.A	N.A
Default	Frames classified to the Port VLAN (Native VLAN) do not get tagged on egress.	
Mode	Port List Interface Mode	
Usage	Set the trunk port egress tagging to all. Use the no version of the command to revert to default (untag native VLAN)	
Examples	Example#1 (configure port 3 as trunk with PVID 4 and set egress tagging to tag all) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 4 (config-if)# switchport trunk vlan tag native	



### 8.8.3.4. Switchport Trunk Allowed VLAN

Description- Ports in Trunk mode may control which VLANs they are allowed to become members of. By default, Trunk port will become a member of all VLANs (1-4095):

```
switchport trunk allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
no switchport trunk allowed vlan
```

	Parameter	Description
Parameter	all	All VLANs are allowed (1-4095)
	none	Port will not become member of any VLAN
	add	Add VLANs to the current list
	remove	Remove VLANs from the current list
	except	All VLANs except the following (VLAN ID or list)
	<vlan_list>	VLAN IDs of the allowed VLANs. Individual elements are separated by commas and ranges are specified with a dash.
Default	All VLANs are allowed (1-4095)	
Mode	Port List Interface Mode	
Usage	Configure allowed VLANs for a trunk port. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as trunk and exclude VLAN 10 and 30,31,32 from allowed VLANs) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan except 10,30-32	

### 8.8.3.5. Switchport Forbidden VLAN

Description- Configure the port to never become a member of one or more VLANs.

```
switchport forbidden vlan { add | remove } <vlan_list>
no switchport forbidden vlan
```

	Parameter	Description
Parameter	add	Add forbidden VLANs to the current list of forbidden VLANs
	remove	Remove forbidden VLANs from the current list of forbidden VLANs
Default	Trunk Port may become a member of all possible VLANs	
Mode	Port List Interface Mode	
Usage	Configure VLANs that a trunk port may not become a member. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as trunk and add VLAN 4 to the list of forbidden VLANs) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport forbidden vlan add 4	

### 8.8.3.6. Switchport Hybrid Native VLAN

Description - Configure VLAN ID (PVID) for the hybrid port (Native VLAN).

```
switchport hybrid native vlan <pvid>
```

```
no switchport hybrid native vlan
```

	Parameter	Description
Parameter	<pvid>	VLAN ID of the native VLAN when this port is in hybrid mode
Default	Hybrid native default VLAN is VLAN1	
Mode	Port List Interface Mode	
Usage	Configure a port VLAN ID for a hybrid port. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 4 as hybrid with PVID 5) # configure terminal (config)# interface GigabitEthernet 1/4 (config-if)# switchport mode hybrid (config-if)# switchport hybrid native vlan 5	

### 8.8.3.7. Switchport Hybrid Port-Type

Description- Specifies the port type in hybrid mode.

```
switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
```

```
no switchport hybrid port-type
```

	Parameter	Description
Parameter	unaware	Port is not aware of VLAN tags. No matter the received frame is tagged or untagged, port adds a tag (based on PVID) to the frame and then forward it.
	c-port	Customer port. If the received frame is untagged, C-port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be forwarded without adding a tag.
	s-port	Provider port. Port only accepts untagged frames. If the received frame is untagged, S-port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be discarded.
	s-custom-port	Custom provider port. When Ethertype is set to 0x8100, S-custom ports do the same as C-ports: If the received frame is untagged, S-custom port adds a tag (based on PVID) to the frame and then forward it; If the frame is already tagged, it will be forwarded without adding a tag.
Default	Hybrid Port type is C-port	
Mode	Port List Interface Mode	
Usage	Configure hybrid port type. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as hybrid Unaware type) # configure terminal	

	Parameter	Description
	(config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid port-type unaware	

### 8.8.3.8. Switchport Hybrid Ingress-Filtering

Description- enable/disable ingress filtering.

```
switchport hybrid ingress-filtering
```

```
no switchport hybrid ingress-filtering
```

	Parameter	Description
Parameter	N.A	N.A
Default	Ingress filtering disabled	
Mode	Port List Interface Mode	
Usage	Enable ingress filtering. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as hybrid and enable ingress filtering) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid ingress-filtering	

### 8.8.3.9. Switchport Hybrid Acceptable-Frame-Type

Description- Set Ingress acceptance criteria.

```
switchport hybrid acceptable-frame-type { all | tagged | untagged }
```

```
no switchport hybrid acceptable-frame-type
```

	Parameter	Description
Parameter	all	Both tagged and untagged frames are accepted
	tagged	Only frames tagged with the corresponding port type tag are accepted.
	untagged	Only untagged frames are accepted.
Default	Hybrid Port is set to accept all frames (tagged and untagged)	
Mode	Port List Interface Mode	
Usage	Configure type of frames accepted on ingress. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as hybrid and accept tagged frames only on ingress) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid acceptable-frame-type tagged	

### 8.8.3.10. Switchport Hybrid Egress-Tag

Description- Configure Egress tagging.

```
switchport hybrid egress-tag { none | all [ except-native ] }
```

```
no switchport hybrid egress-tag
```

	Parameter	Description
Parameter	none	No Egress tagging. All frames transmitted without a tag.
	all	Tag all frames. All frames transmitted with a tag.
	except-native	Tag all frames except frames classified to native VLAN.
Default	Hybrid Port is set to tag all frames except frames classified to native VLAN	
Mode	Port List Interface Mode VLAN.	
Usage	Configure egress tagging. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as hybrid and set egress tagging to all) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid egress-tag all	

### 8.8.3.11. Switchport Hybrid Allowed VLAN

Description- Ports in Hybrid mode may control which VLANs they are allowed to become members of. By default Hybrid port will become a member of all VLANs (1-4095).

```
switchport hybrid allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
```

```
no switchport hybrid allowed vlan
```

	Parameter	Description
Parameter	all	All VLANs are allowed (1-4095)
	none	Port will not become member of any VLAN
	add	Add VLANs to the current list
	remove	Remove VLANs from the current list
	except	All VLANs except the following (VLAN ID or list)
	<vlan_list>	VLAN IDs of the allowed VLANs. Individual elements are separated by commas and ranges are specified with a dash.
Default	All VLANs are allowed (1-4095)	
Mode	Port List Interface Mode	
Usage	Configure allowed VLANs for a hybrid port. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as hybrid and exclude VLAN 10 and 30,31,32 from allowed VLANs) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid allowed vlan except 10,30-3	

## 8.8.4. View VLAN Members

### 8.8.4.1. Show VLAN

Description- provides overview of membership status of VLAN users and VLANs configured for each interface.

```
show vlan [ id <vlan_list> | name <name> | brief ] [ all ]
```

	Parameter	Description
Parameter	id <vlan_list>	VLAN status by VLAN ID
	name <name>	VLAN status by VLAN name
	brief	VLAN summary information
	all	Show all VLANs (if left out only access VLANs are shown)
Default	N.A	
Mode	EXEC mode	
Usage	Display VLAN membership status overview	
Examples	Example#1 (Show VLAN summary information for all vlans) #show vlan brief all  Example#2 ( Show VLAN information for port 1 configured by Admin) #show vlan status interface GigabitEthernet 1/1 admin	

## 8.8.5. View VLAN Ports

### 8.8.5.1. Show VLAN Status

Description- Shows VLAN status for a specific interface (port) configured by a specific user.

```
show vlan status [ interface <port_type> [ <plist> ] ] [ admin | all | combined | conflicts | mstp | nas | rmirror ]
```

	Parameter	Description
Parameter	interface <port_type>	Show the VLANs configured for a specific interfaces and port type (GigabitEthernet)
	<plist>	List of Port ID, ex, 1/1,3-5
	admin	Show the VLANs configured by administrator
	all	Show VLANs configured VLANs for all VLAN users
	combined	Show the combined set of configured VLANs
	mstp	Show the VLANs configured by MSTP
	Nas	Show the VLANs configured by NAS
	mirror	Show the VLANs configured by Remote mirroring
Default	N.A	
Mode	EXEC mode	
Usage	Display VLAN membership status overview.	
Examples	Example#1 ( Show VLAN information for port 1 configured by Admin) #show vlan status interface GigabitEthernet 1/1 admin	

## 8.9. Spanning Tree

### 8.9.1. STP Bridge Configuration Commands

Spanning Tree Protocol (STP), and its variations as RSTP and MSTP, is used to prevent possible Network loops that without STP will cause broadcast storming. It also offers redundancy path from Switch to Switch or Path to Path over multiple switches by supporting Network loops under the control of STP. STP algorithm will make sure that at any given time only one path out of multiple possible loops will be active, those allowing the switch to use multiple backup paths in case main connection path go down.

#### 8.9.1.1. Spanning-Tree Mode

Description- Configure STP protocol version.

```
spanning-tree mode { stp | rstp | mstp }
```

```
no spanning-tree mode
```

	Parameter	Description
Parameter	stp	Spanning Tree protocol 802.1D
	rstp	Rapid Spanning Tree protocol 802.1w
	mstp	Multiple Spanning Tree protocol 802.1s
Default	Default protocol is MSTP	
Mode	Global Configuration Mode	
Usage	Set STP protocol version. Use the no version of the command to revert to default.	
Examples	Example#1 (set STP to RSTP) # configure terminal (config)# spanning-tree mode rstp	

### 8.9.1.2. Spanning-Tree System Settings

Description- Configure STP system settings used by all STP Bridge instances in the switch.

Basic STP global setting commands:

```
spanning-tree mst <instance=0> priority <prio>
spanning-tree mst hello-time <hellotime>
spanning-tree mst forward-time <fwdtime>
spanning-tree mst max-age <maxage> [ forward-time <fwdtime> ]
spanning-tree mst max-hops <maxhops>
spanning-tree transmit hold-count <holdcount>
```

Advanced STP global setting commands:

```
spanning-tree edge bpdu-filter
spanning-tree edge bpdu-guard
spanning-tree recovery interval <interval>
```

	Parameter	Description
Parameter	<instance>	STP bridge instance. Must be 0 (zero)
	priority <prio>	Bridge Priority Supported values are 0-61440. Only values divisible by 4096 are allowed. For example, 4096, 8192, etc. Default value is 32768.
	<hellotime>	Interval between sending STP BPDUs. Valid values are 1-10 seconds. Default is 2 seconds.
	<fwdtime>	Forward delay used by STP Bridges to transit Root and Designated Ports to Forwarding. Valid values are 4-30 seconds. Default is 15..
	<maxage>	Maximum age of the information transmitted by the Bridge when it is a Root Bridge. Valid values are 6-40 seconds. Default is 20..
	<maxhops>	Defines how many bridges a root bridge can distribute its BPDUs. Valid values are 6-40 hops. Default is 20
	<holdcount>	Number of BPDUs a bridge port can send per second. Valid range 1-10 BPDUs per second. Default is 6.
	<interval>	Time to pass before a port in error-disabled state can be enabled. Values are 30-86400 seconds (24 hours). Default is port error recovery disabled.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure STP system settings. Use the no version of the command to revert to default.	
Examples	<pre>Example (Configure STP settings) # configure terminal (config)# spanning-tree mode mstp (config)# spanning-tree mst 0 priority 36864 (config)# spanning-tree mst hello-time 3 (config)# spanning-tree mst max-age 25 forward-time 16 (config)# spanning-tree mst max-hops 25</pre>	

	Parameter	Description
	(config)# spanning-tree transmit hold-count 7 (config)# spanning-tree edge bpdu-filter (config)# spanning-tree edge bpdu-guard (config)# spanning-tree recovery interval 120	



### 8.9.1.3. Spanning-Tree Port Settings

Description- Configure STP CIST settings for the specific physical and aggregated ports.

```
spanning-tree Enable STP on the port
no spanning-tree Disable STP on the port
spanning-tree mst <instance=0> cost { <cost> | auto }
spanning-tree mst <instance=0> port-priority <prio>
spanning-tree edge
spanning-tree auto-edge
spanning-tree restricted-role
spanning-tree restricted-tcn
spanning-tree bpdu-guard
spanning-tree link-type { point-to-point | shared | auto }
```

	Parameter	Description
Parameter	<instance>	STP bridge instance. Must be 0 (zero)
	cost { <cost>   auto }	Controls the path cost incurred by the port. Auto setting will set the cost as appropriate by link speed using 802.1D recommended values. User defined value can also be entered and the valid range is 1-200000000. Default is auto.
	port-priority <prio>	Represents the port priority. Must be divisible by 16, supported values are 0-240. For example, 16, 32, etc. Default value is 128
	link-type { point-to-point   shared   auto }	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. Default is auto.
	edge	Defines whether the port is connecting directly to edge devices. Default is non-edge.
	auto-edge	Enables auto edge detection on the port.
	restricted-role	If enabled causes the port not to be selected as Root port.
	restricted-tcn	If enabled causes the port not to propagate received topology change notifications to other ports.
	Bpdu-guard	If enabled causes the port to disable itself upon receiving valid BPDUs.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Configure STP CIST settings for the specific physical and aggregated ports. Use the no version of the command to revert to default.	
Examples	<pre>Example (Configure STP CIST settings for port 1) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# spanning-tree (config-if)# spanning-tree mst 0 cost auto (config-if)# spanning-tree mst 0 port-priority 16 (config-if)# spanning-tree edge (config-if)# spanning-tree restricted-role</pre>	

	Parameter	Description
	(config-if)# spanning-tree bpdu-guard	
	(config-if)# spanning-tree link-type point-to-point	

## 8.9.2. STP Bridges View Commands

### 8.9.2.1. Show Spanning-Tree

Description- Provides a detailed status information on a STP bridge instance, along with port state for all active ports associated.

```
show spanning-tree [ summary | active | { interface <port_type> [ <v_port_type_list> ] }
| { detailed [ interface <port_type> [ <v_port_type_list_1> ] ] } | { mst [
configuration | { <instance> [ interface<port_type> [<v_port_type_list_2> ] ] } ] } ]
```

	Parameter	Description
Parameter	summary	STP summary
	active	STP active interfaces
	interface <port_type>	Choose port and type in Gigabit Ethernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
	detailed	STP statistics
	mst	Multiple STP
	configuration	Show MSTI to VLAN mapping
	<instance>	STP bridge instance (CIST=0, MSTI1=1...)
Default	N.A	
Mode	EXEC Mode	
Usage	Display information on STP	
Examples	Example (Display CIST port state for port 8) # show spanning-tree interface GigabitEthernet 1/8  Example (Display STP detailed Bridge status) #show spanning-tree mst 0	

## 8.10. Port Mirroring

### 8.10.1. Port Mirroring Configuration

Port Mirroring allows the user to mirror (duplicate) Rx/Tx/Both traffic from one or more ports to another dedicated debug port where a network analyzer can be attached to analyze the network traffic.

#### 8.10.1.1. Monitor Session

Description - Enable Port Mirroring.

```
monitor session <session_number = 1>
```

```
no monitor session <session_number = 1>
```

	Parameter	Description
Parameter	<session_number= 1>	Mirror session number must be set as 1
Default	N.A	
Mode	Global Configuration Mode	
Usage	Enable traffic mirroring from one or more ports to a dedicated mirroring port. Use the no version of the command to disable.	
Examples	Example (Enable port mirroring) # configure terminal (config)# monitor session 1	

#### 8.10.1.2. Port Configuration

Description - Configure port mirroring parameters.

```
monitor session <session_number> [ destination { interface <port_type> [ <di_list> ]
} | source
{ interface <port_type> [ <si_list> ] [ both | rx | tx ] | cpu [ both | rx | tx ] } ]
```

	Parameter	Description
Parameter	<session_number = 1>	Mirror session number must be set as 1
	destination	Mirror destination port
	<port_type>	Port type in GigaEthernet
	<di_list>	Port ID, ex, 1/1
	source	Mirror source ports
	<si_list>	List of Port ID, ex, 1/1,3-5
	both	Received and transmitted frames are mirrored on the destination port.
	rx	Only received frames are mirrored to the destination
	tx	Only transmitted frames are mirrored to the destination port
cpu	Mirror source CPU	
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure which Switch ports to mirror, and to which port to mirror it to. Disable MAC address learning for the destination port.	

	Parameter	Description
Examples		Example (Set port 11 as a destination port to mirror received frames only on ports 1-5 )
Examples		# configure terminal (config)# monitor session 1 destination interface GigabitEthernet 1/11 (config)# monitor session 1 source interface GigabitEthernet 1/1-5 rx (config)# monitor session 1




---

Disable MAC address learning to the port used to mirror the traffic of the monitored ports. To disable select the port to be configured, and type the command: no mac address-table learning.

---

## 8.11. System Information

There are numerous "show" commands, that can be used to get information about system or interface status.

### 8.11.1. Read LAN9668 Temperature

```
Show green-ethernet fan
```

### 8.11.2. Read Phy Temperature

```
Show thermal-protect
```

### 8.11.3. Interface Status

```
# show interface * status
```

Interface	Mode	Speed	Aneg	Link	Operational Warnings
Gi 1/1	Enabled	Auto	Yes	1Gfdx	
Gi 1/2	Enabled	Auto	Yes	Down	
Gi 1/3	Enabled	Auto	Yes	Down	
Gi 1/4	Enabled	Auto	Yes	Down	
Gi 1/5	Enabled	Auto	Yes	Down	
Gi 1/6	Enabled	Auto	Yes	Down	
Gi 1/7	Enabled	Auto	Yes	Down	
Gi 1/8	Enabled	Auto	Yes	Down	

### 8.11.4. Interface Capabilities

```
# show interface GigabitEthernet 1/1 capabilities
```

```
GigabitEthernet 1/1 Capabilities:
SFP Family:          None
SFP Vendor Name:     None
SFP Vendor P/N:      None
SFP Vendor S/N:      None
SFP Vendor Revision: None
SFP Date Code:       None
SFP Transceiver:     None
Dual Media Port:     Yes
Speed cap:           10,100,1000,auto
Duplex cap:          half,full,auto
Flowcontrol:         Yes
Trunk encap. type:   802.1Q
Trunk mode:          access,hybrid,trunk
Channel:             Yes
Broadcast suppression: 0-0 kbps/1-1024000 fps
```

### 8.11.5. Interface Statistics

```
# show interface GigabitEthernet 1/1 statistics
```

```
GigabitEthernet 1/1 Statistics:
Rx Packets:          1707   Tx Packets:          45122
Rx Octets:           734539 Tx Octets:           5945994
Rx Unicast:           19    Tx Unicast:           6
Rx Multicast:        1684   Tx Multicast:        45109
```

```

Rx Broadcast:                4    Tx Broadcast:                7
Rx Pause:                    0    Tx Pause:                    0

Rx 64:                        13   Tx 64:                        8
Rx 65-127:                   174  Tx 65-127:                   42293
Rx 128-255:                   0    Tx 128-255:                   0
Rx 256-511:                   1520 Tx 256-511:                   2821
Rx 512-1023:                  0    Tx 512-1023:                  0
Rx 1024-1526:                 0    Tx 1024-1526:                 0
Rx 1527-      :               0    Tx 1527-      :               0

Rx Priority 0:                 1707 Tx Priority 0:                 40
Rx Priority 1:                  0    Tx Priority 1:                  0
Rx Priority 2:                  0    Tx Priority 2:                  0
Rx Priority 3:                  0    Tx Priority 3:                  0
Rx Priority 4:                  0    Tx Priority 4:                  0
Rx Priority 5:                  0    Tx Priority 5:                  0
Rx Priority 6:                  0    Tx Priority 6:                  0
Rx Priority 7:                  0    Tx Priority 7:                 45082

Rx Drops:                     0    Tx Drops:                     0
Rx CRC/Alignment:             0    Tx Late/Exc. Coll.:           0
Rx Undersize:                  0
Rx Oversize:                   0
Rx Fragments:                  0
Rx Jabbers:                    0
Rx Filtered:                   1688
    
```

# show interface \* statistics packets up

Interface	Rx Packets	Tx Packets
GigabitEthernet 1/1	3332	943810378
GigabitEthernet 1/2	0	943813871
GigabitEthernet 1/3	0	87864701
GigabitEthernet 1/4	0	87864765
GigabitEthernet 1/5	5199	20
2.5GigabitEthernet 1/1	2333504117	2336115589
2.5GigabitEthernet 1/2	2336113810	2333509227

## 8.12. Managing the Switch Using SNMP

The Managed Information Base (MIB) is a collection of information organized hierarchically and used to manage network devices (such as router and switches) in a communication network. MIB is most often associated and managed using the SNMP.

The switch's NOS provides a set of MIBs that are used to configure the switch using SNMP by any SNMP browser.

For information on the switch's supported MIBs, visit Kontron's [Customer Section](#).



## 9/Maintenance

### 9.1. Hardware Maintenance

The switch contains no user serviceable parts. Maintenance or repair on the switch may only be carried out by qualified personnel authorized by Kontron.

Return the switch to Kontron for maintenance and repair, see Chapter 10.1: Returning Defective Merchandise.




---

The switch contains no user serviceable parts. For maintenance and repair, return the switch to Kontron, see Chapter 10.1: Returning Defective Merchandise.

---

### 9.2. Software Maintenance

Prerequisites:

- ▶ A server configured for the desired protocol is available and accessible from the switch NOS.
- ▶ The .gz upgrade file provided by Kontron was downloaded on the server.

#### 9.2.1. Reset and Restore Switch

##### 9.2.1.1. Reload Cold

Description - Command switch to perform software reset, turning Ethernet ports down and back up.

```
reload cold
```

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restart the switch	
Examples	# reload cold	

##### 9.2.1.2. Reload Defaults Keep-IP

Description - Command switch to restore its configuration to semi factory default (only running configuration), keeping switch IP and VLAN configuration unchanged, in order to maintain remote Network connectivity.




---

New semi factory default configuration is not automatically saved. You must issue a command as "copy running-config startup-config" in order to make the new configuration change permanent.

---

```
reload defaults keep-ip
```

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restore to factory default but keep IP address unchanged	
Examples	# reload defaults keep-ip	

### 9.2.1.3. Reload Defaults

Description - restore switch to full factory default configuration (only running configuration)



New factory default configuration is not automatically saved. You must issue a command as "copy running-config startup-config" in order to make the new configuration change permanent.



Connection to the device may be lost unless remote user is connected on the same LAN or has direct access to the device over serial (USB virtual COMM).

reload defaults

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to restore to factory default	
Examples	# reload defaults	

## 9.2.2. Switch Configuration

### 9.2.2.1. Download Switch Configuration to TFTP-Server

Description- copy switch running-config, startup-config or another configuration file stored inside the switch to remote TFTP-Server.

**copy** <running-config | startup-config | flash:configuration-file-name> tftp://<TFTP-Server IP>/<filename>

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to copy one of the switch configurations to TFTP Server	
Examples	Example #1 - copy running configuration to TFTP Server under name test Example #2 - save switch running configuration file to TFTP Server under name "test" # copy running-config tftp://192.168.0.40/test	

	Parameter	Description
		Example #2 - copy switch local configuration file named test1 to TFTP-Server under name "switch-test-config-file". #copy flash:test1 tftp://192.168.0.40/switch-test-config-file

#### 9.2.2.2. Upload Configuration File from TFTP-Server to Switch

Description - Upload configuration file from TFTP Server to any configuration file stored inside the switch internal FLASH memory except default-configuration (which is read-only).

```
copy <tftp://server-IP/filename> running-config | startup-config | flash:<file-name>
```

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to upload switch configuration from TFTP Server to switch local file	
Examples	<p>Example - Upload from TFTP-Server configuration file named test1 to switch running-configuration</p> <pre>copy tftp://192.168.0.40/test1 running-config copy copy tftp://192.168.0.40/test flash:test1</pre> <p>Example #2 - upload configuration file "test" to running configuration</p> <pre># copy tftp://192.168.0.40/test running-config</pre>	

#### 9.2.2.3. Activate One of the Already Stored Configuration Files

Description - Select which configuration file already stored inside the switch FLASH to activate, replacing the running configuration. To view the list of possible configuration files, use the command "dir".




---

The activated configuration file will not be saved to startup-config automatically. Use copy running-config startup-config command to save it.

---

```
copy flash:<file-name> running-config
```

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to activate one of the switch other locally stored configuration files	
Examples	<p>Example #1 - activate configuration file "test"</p> <pre># copy flash:test running-config</pre>	

#### 9.2.2.4. Delete Configuration

Description - Delete configuration file from flash. To check the files stored in flash use "dir" command.

```
delete <flash:filename>
```

### 9.2.3. Software Update

#### 9.2.3.1. Upload New Version

Description - Upload a new software version to the switch.

firmware upgrade <url\_file>

	Parameter	Description
Parameter	<url_file>	Specific character string that constitutes a reference to a resource. Syntax:<protocol>://[<username>[:<password>]@]<host>[:<port>][/< path>]/<file_name> If the following special characters: space !\"#\$%&'()*+/,/:;<=>?@[\\]^`{ }~ need to be contained in the input URL string, they should be percent-encoded.
Default	N.A	
Mode	EXEC	
Usage	Use this command to upgrade switch software version.	
Examples	Example - download switch new software version from TFTP Server # firmware upgrade tftp://192.168.0.40/new_image.mfi	

#### 9.2.3.2. Select Active Image

Description - Swap the active and alternative image.




---

Backup software version is the one used before latest software update was performed.  
Note that using this command again will swap to the new software version that was just uploaded.

---

firmware swap

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to activate alternative (backup) image	
Examples	Example - swap the active and alternative images # firmware swap	

## 10/ Technical Support

For technical support contact our Support Department:

- ▶ E-mail: support@kontron.com
- ▶ Phone: +49-821-4086-888

Make sure you have the following information available when you call:

- ▶ Product ID Number (PN),
- ▶ Serial Number (SN)



---

The serial number can be found on the switch's Type Label.

---

Be ready to explain the nature of your problem to the service technician.

### 10.1. Returning Defective Merchandise

All equipment returned to Kontron must have a Return of Material Authorization (RMA) number assigned exclusively by Kontron. Kontron cannot be held responsible for any loss or damage caused to the equipment received without an RMA number. The buyer accepts responsibility for all freight charges for the return of goods to Kontron's designated facility. Kontron will pay the return freight charges back to the buyer's location in the event that the equipment is repaired or replaced within the stipulated warranty period. Follow these steps before returning any product to Kontron.

1. Visit the RMA Information website:

<http://www.kontron.com/support-and-services/support/rma-information>

Download the RMA Request sheet for Kontron Europe GmbH and fill out the form. Take care to include a short detailed description of the observed problem or failure and to include the product identification information (Name of product, Product number and Serial number). If a delivery includes more than one product, fill out the above information in the RMA Request form for each product.

2. Send the completed RMA-Request form to the fax or email address given below at Kontron Europe GmbH. Kontron will provide an RMA-Number.

Kontron Europe GmbH  
RMA Support  
Phone: +49 (0) 821 4086-0  
Fax: +49 (0) 821 4086 111  
Email: service@kontron.com

3. The goods for repair must be packed properly for shipping, considering shock and ESD protection.



---

Goods returned to Kontron Europe GmbH in non-proper packaging will be considered as customer caused faults and cannot be accepted as warranty repairs.

---

4. Include the RMA-Number with the shipping paperwork and send the product to the delivery address provided in the RMA form or received from Kontron RMA Support.



## 11/ Warranty

Kontron defines product warranty in accordance with regional warranty definitions. Claims are at Kontron's discretion and limited to the defect being of a material nature. To find out more about the warranty conditions and the defined warranty period for your region, following the steps below:

1. Visit Kontron's Term and Conditions webpage.

<http://www.kontron.com/terms-and-conditions>

2. Click on your region's General Terms and Conditions of Sale.

### 11.1. Limitation/Exemption from Warranty Obligation

In general, Kontron shall not be required to honor the warranty, even during the warranty period, and shall be exempted from the statutory accident liability obligations in the event of damage caused to the product due to failure to observe the following:

- ▶ General safety instructions for IT equipment within this user guide
- ▶ Warning labels on the product and warning symbols within this user guide
- ▶ Information and hints within this user guide

Additionally, alterations or modifications to the product that are not explicitly approved by Kontron, described in this user guide, or received from Kontron Support as a special handling instruction will void your warranty.

Within the warranty period, the product should only be opened by Kontron. Removing the protection label and opening the product within the warranty period exempts the product from the statutory warranty obligation.

Due to their limited service life, parts which by their nature are subject to a particularly high degree of wear (wearing parts) are excluded from the warranty beyond that provided by law.



## List of Acronyms

Table 14: List of Acronyms

AAA	Authentication, Authorization and Accounting	MMF	Multi-Mode Fiber
AC	Alternating Current	MSTI	Multiple Spanning Tree Instance
AVB	Audio Video Bridge	MTU	Maximum Transmission Unit
ACL	Access Control List	MSTP	Multiple Spanning Tree Protocol
BiDi	Bidirectional	NOS	Network Operation Software
BPDU	Bridge Protocol Data Unit	NTP	Network Time Protocol
CFR	Code of Federal Regulations	OS	Operating System
CLI	Command Line Interface	PD	Powered Device
CPU	Central Processing Unit	PN	Part Number
DC	Direct Current	PS2	Power Source 2
DHCP	Dynamic Host Configuration Protocol	PSB	Power Source Backbone
DNS	Domain Name Server	PSE	Power Sourcing Equipment
DPLL	Digital Phase Lock Loop	PTC	Packet Time Clock
DSCP	Differential Service Point Code	PTP	Precision Time protocol
DWRR	Deficit-weighted Round Robin Queuing	QoS	Quality of Service
ECT	Embedded Computing Technology	REACH	Registration, Evaluation, Authorization and Restriction of Chemicals
EEC	Ethernet Equipment Clock	RGMII	Reduced Gigabit Medium Independent Interface
EMC	Electro Magnetic Compliance	Rohs	Restriction of Hazardous Substances
ESD	Electrostatic Discharge	RMA	Return of Material Authorization
FCC	Federal Communications Commission	RSPT	Rapid Spanning Tree Protocol
gbt	Gate Band Time	RTC	Real Time Clock
GCE	Gate Control Entry	RX	Receive
GCL	Gate Control List	SC	Standard Connector
GMT	Greenwich Mean Time	SDU	Session Date Unit
GPIO	General Purpose Input Output	SFP	Small Form-factor Pluggable
GVRP	GARP VLAN Registration Protocol	SM	Single Mode
IETF	Internet Engineering Task force	SMF	Single Mode Fiber
IGMP	Internet Group Management Protocol	SN	Serial Number
ICMP	Internet Control Message Protocol	SNMP	Simple Network Management Protocol
IoT	Internet of Things	SPQ	Strict Priority Queuing
IP	Internet Protocol	STP	Shielded Twisted Pair
IPS	Internet Protocol Suite	STP	Spanning Tree Protocol
L/A	Link/Activity	TAS	Time Aware Shaper
LACP	Link Aggregation Control Protocol	TCP	Transmission Control protocol
LAN	Local Area Network	TSN	Time Sensitive Networking
LC	Lucent Connector	TX	Transmit
LED	Light Emitting Diode	UTC	(UTC) Coordinated Universal Time
LPS	Limited Power Source	UDP	User datagram protocol
MAC	Media Access Control	UTP	Unshielded twisted Pair
MDI	Medium Dependent Interface	VDC	Volts Direct Current
MDIX	Medium Dependent Interface- cross over	VLAN	Virtual Local Area Network
MIB	Management Information Base	WEEE	Waste Electrical and Electronic Equipment
MLD	Multicast Listener Discovery		
MM	Multi Mode		




## About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). As a part of technology group S&T, Kontron, together with its sister company S&T Technologies, offers a combined portfolio of secure hardware, middleware and services for Internet of Things (IoT) and Industry 4.0 applications. With its standard products and tailor-made solutions based on highly reliable state-of-the-art embedded technologies, Kontron provides secure and innovative applications for a variety of industries. As a result, customers benefit from accelerated time-to-market, reduced total cost of ownership, product longevity and the best fully integrated applications overall.

For more information, please visit: [www.kontron.com](http://www.kontron.com)

---



### Global Headquarters

Kontron Europe GmbH

Gutenbergstraße 2  
85737 Ismaning,  
Germany  
Tel.: +49 821 4086-0  
Fax: +49 821 4086-  
111  
[info@kontron.com](mailto:info@kontron.com)