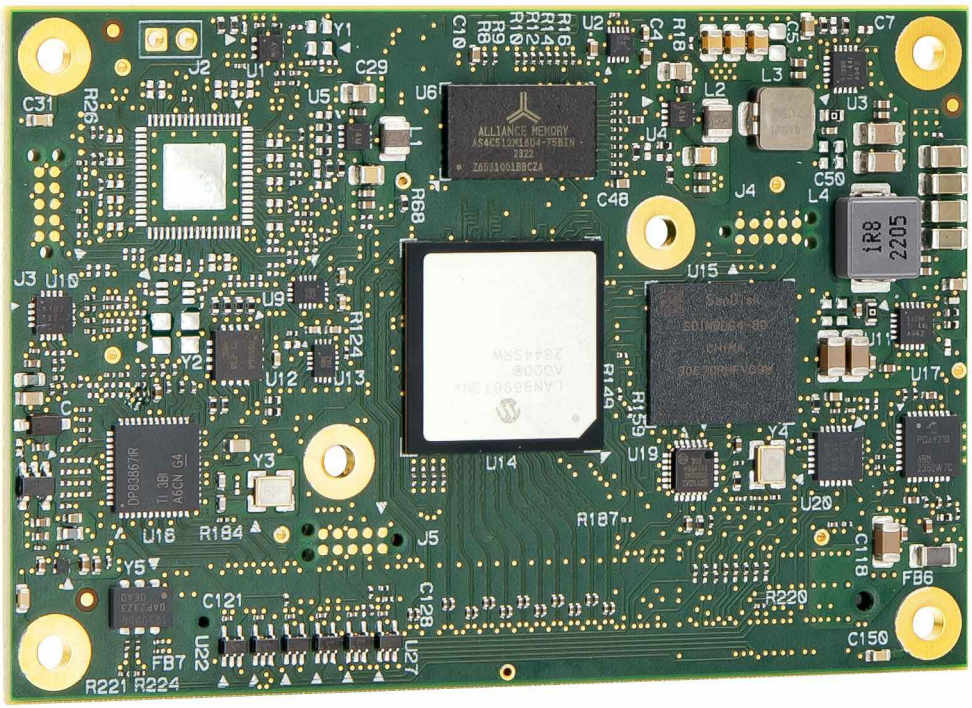


KSwitch M20 Embedded Ethernet Switch Module

User Guide Rev. 1.0

Doc. ID 1080-1661

kontron
The Power of IoT

This page has been intentionally left blank

KSwitch M20 – 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.

Kontron Europe GmbH
Gutenbergstraße 2
85737 Ismaning
Germany
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.

NOTICE This product is not intended for use or suited for storage or operation in corrosive environments, in particular under exposure to sulfur and chlorine and their compounds. For information on how to harden electronics and mechanics against these stress conditions, contact Kontron Support.

Revision History

Revision	Brief Description of Changes	Date of Issue	Author
1.0	Initial version	03-Aug-2026	CW

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

⚠DANGER	**DANGER** indicates a hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	**WARNING** indicates a hazardous situation which, if not avoided, could result in death or serious injury.
NOTICE	**NOTICE** indicates a property damage message.
⚠CAUTION	**CAUTION** indicates a hazardous situation which, if not avoided, may result in minor or moderate injury
	**Electric Shock!** This symbol and title warn of hazards due to electrical shocks (> 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.
	**ESD Sensitive Device!** This symbol and title inform 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.
	**Caution: HOT Surface!** Do NOT touch! Allow to cool before servicing.
	**Caution: Laser!** This symbol inform 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.
	**Caution: High Sound Pressure!** This symbol and title indicate that high sound pressure is possible with headphones. There is a risk of hearing damage. Do not listen at high volume levels for long periods of time.

Security

This symbol and title indicate general information and guidelines regarding the product's cyber security to ensure secure installation, operation, maintenance and disposal of the product within the user's end environment.

This symbol indicates general information about the product and the user guide.

This symbol precedes helpful hints and tips for daily use.

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.

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" 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 lithium battery.

⚠CAUTION	**Risk of Explosion** Rick of explosion if the lithium Battery is replaced by an incorrect Type. Dispose of used lithium batteries according to the 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 visit Quality | Kontron and Material Compliance | Kontron.

Table of Contents

List of Tables

List of Figures

1/Introduction

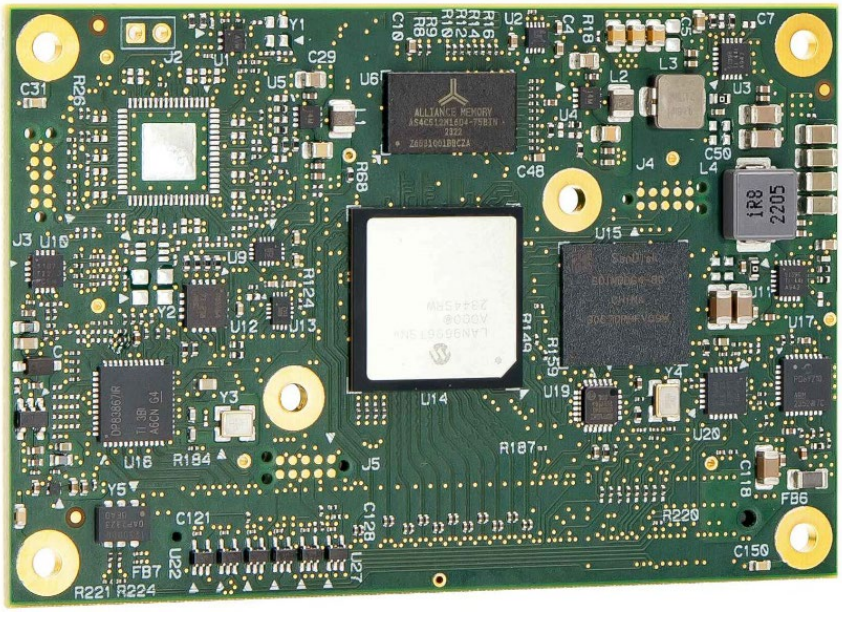
This user guide describes the KSwitch M20 embedded Ethernet switch module, also known as KSwitch M20 module or product within this user guide. This user guide focuses on describing the KSwitch M20 module's special features and how to set up, install, operate, maintain and dispose of the KSwitch M20 module properly. New users are recommended to study the instructions within this user guide before connecting the KSwitch M20 module to power.

The Kontron KSwitch M20 module is a modular non-blocking fully managed 1/2.5/5/10 Gigabit Ethernet switch supporting flexible port configuration via 10x 10G SerDes, up to 28 ports. The Kontron KSwitch M20 module with Precision Time Protocol (PTP) and Time Sensitive Network (TSN) provides a rich and versatile feature set to integrate Ethernet switching functions on custom carrier board designs. The IEEE 1588v2 features enable precise timing synchronization and packet time stamping for time sensitive applications. It also supports intelligent Power Over Ethernet devices by built in firmware. The KSwitch M20 module is designed for future oriented applications that require out-standing bandwidth and communication safety.

The KSwitch M20 module is based on the PICMG COM Express® Rev 3.0 mini standard and can be integrated on compliant COM Express® mini custom carrier boards.

The KSwitch M20 module is designed for use within railway and rolling stock equipment according to EN 50155 and operation in industrial grade temperatures. Whatever you need to integrate, the KSwitch M20 module is the ideal fit for all kinds of high performance Ethernet switching, either in military, avionic or industrial applications.

Figure 1: KSwitch M20 Embedded Ethernet Switch Module



General KSwitch M20 module features are:

- Managed Time Sensitive Networking (TSN) Ethernet switch based on the LAN969xTSN family
  - Non-blocking fully managed, 1/2.5/5/10 Gigabit Ethernet Switch
  - 44 GBps tp 100 Gbps scalable bandwidth
  - Flexible Ethernet port configuration via 10x 10G SerDes, up to 28 ports
  - 10/100/1000BASE-T MDI IF (optional)
  - MIIM Interfaces for CL22 and CL45 devices
  - Precision Time Protocol (PTP), and Reference and Synchronization clock distribution interfaces

- Ethernet Physical interface
  - Switch Auto-Configuration USB 2.0 Physical interface
- POE
  - IEEE 1588v2 and PoE PSE support
- Status LEDs
  - Smart serial LED bus distribution
- Clock distribution
  - Real Time Clock (RTC) supported with Supercap or battery on the custom carrier board
- Compliance
  - According to EN 50155:2021 Railway and Rolling stock
  - CE
- Environmental
  - Industrial grade, and highly reliable and shock and vibration resistant
  - Extended Temperature Range
- Form-factor
  - PICMG COM Express® Rev 3.0 mini module:
  - Size (84 mm x 55 mm)
- Single 220-pin carrier interface connector
  - 5 mm and 8 mm stack height options (module bottom to carrier board top)
  - Reduced Z component height
- Power
  - Input power supply 12 VDC (wide range)
  - Via single 220-pin carrier interface connector

1.1. Carrier Board

A carrier board is not included in the KSwitch M20 module's delivery. Kontron provides a Carrier Board Design Guide, to aid the development of a KSwitch M20 custom carrier board designed for the user's application. The carrier board design guide for the KSwitch M20 module is available in Kontron's Customer Section.

For the Carrier Board Design Guide in the Customer Section click on Switches > TSN Network > KSwitch M20 > KSwitch M20 Design Information > Design Guide KSwitch M20-xxxT.

For more information on the carrier board design, contact Kontron Support.

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 workplace that is access controlled.
- CAUTION: Risk of explosion if the lithium battery is replaced incorrectly (short-circuited, reverse-poled, wrong lithium battery type). Dispose of used lithium 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 functional earth 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.

For the General Safety Instruction in English, French and German, visit the KSwitch M20 product web page and scroll down to Downloads and click on > Manuals> General Safety Instructions.

2.1. 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:

ESD Sensitive Device!
Keep electrostatic sensitive parts in their containers until they arrive at the ESD-safe workplace. Always be properly grounded when touching a sensitive board, component, or assembly.

For more Information, see the Special Handling and Unpacking Instruction within this user guide and Chapter 2.2: Grounding Methods.

2.2. Grounding Methods

The following measures help to avoid electrostatic damage to the device:

1. Cover workstations with approved antistatic material. Always wear a wrist strap connected to the workplace, as well as properly grounded tools and equipment.
2. Use antistatic mats, heel straps, or air ionizers for more protection.
3. Always handle electrostatically 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 the work area free of non-conductive materials such as ordinary plastic assembly aids and styrofoam.
7. Use field service tools such as cutters, screwdrivers, and vacuum cleaners that are conductive.
8. Always place drives and boards with the PCB-assembly-side down on the foam.

3/Shipment and Packaging

3.1. Packaging

The KSwitch M20 embedded Ethernet switch module is packaged together with all parts, in a specific cardboard package designed to provide adequate protection and absorb shock.

3.2. Unpacking

To unpack the KSwitch M20 module 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 product.
5. Check the product for visible shipping damage.

If you notice shipping damage or inconsistencies between the contents and the original order, contact your dealer.

3.3. Switch Variants

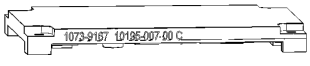
This scope of delivery describes the parts included in your delivery. Check that the delivery is complete and contains the items listed. If damaged or missing items are discovered, contact your dealer.

Table 1: KSwitch M20 Module Variants

Part	Quantity	Part Number	Part Description
KSwitch M20 M100T	1	1074-2710	KSwitch M20 module, 100 Gbps, TSN Support
KSwitch M20 M64T	1	1074-2711	KSwitch M20 module, 64 Gbps, TSN Support

3.4. Accessories

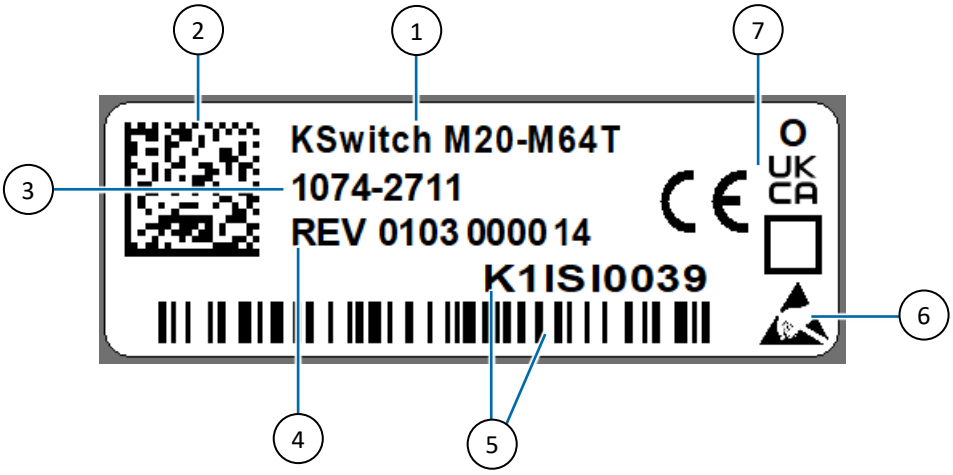
Table 2: List of Accessories

Part	Part Name	Part Number	Description
	Heatspreader Plate	1073-9167	COMe form-factor Heatspreader Plate (HSP)

3.5. Type Label and Product Identification

The type label contains specific KSwitch M20 module identification information and technical information.

Figure 2: Type Label Example



1. Part Number
2. QR Code
3. Order number
4. Revision number
5. Serial Number and bar code
6. ESD Warning
7. Compliance

4/Switch Interfaces

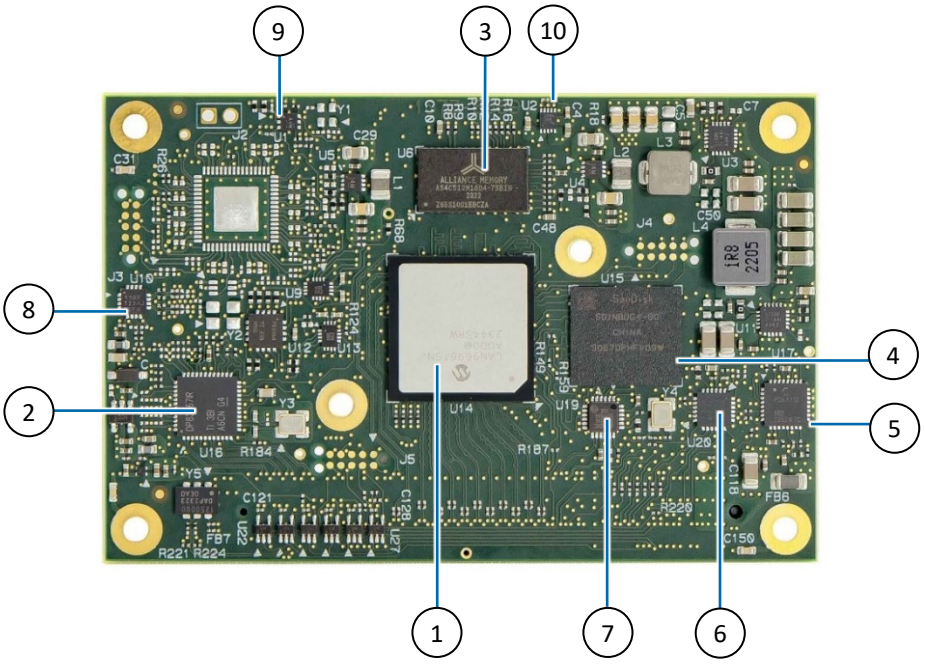
Before implementing the KSwitch M20 embedded Ethernet switch module, Kontron recommends new users to take a few minutes to learn about the KSwitch M20 module features.

The KSwitch M20 module is installed on a custom carrier board provided by the user. For information regarding carrier board design requirements, Kontron provides a Carrier Board Design Guide. The design guide is available on Kontron's Customer Section and describes how to design a custom specific carrier board for the KSwitch M20 managed Ethernet switch module.

For the Carrier Board Design Guide in the Customer Section click on Switches > TSN Network > KSwitch M20 > KSwitch M20 Design Information > Design Guide KSwitch M20-xxxT.

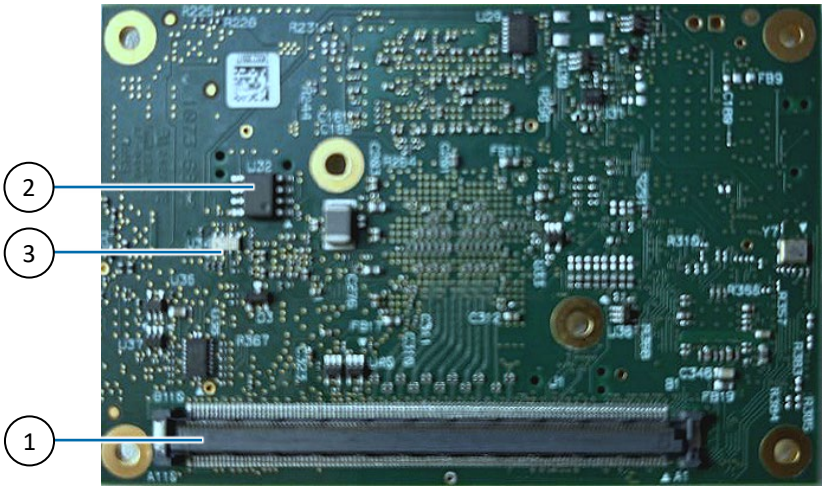
4.1. KSwitch M20 Module Views

Figure 3: Top Side View



1. Microchip LAN969x SOC (U14)
2. Ethernet Physical Layer transceiver (U16)
3. System memory DDR4 memory down (U6)
4. eMMC storage (U15)
5. PoE+ controller (U17)
6. Micro Controller Unit (MCU) (U20)
7. USB 2.0 Physical Layer (U19)
8. Clock (U10)
9. Reset (U1)
10. Reset 2nd stage (U2)

Figure 4: Bottom Side View



1. Mini 220-pin carrier interface connector
2. SPI Nor Flash (U32)
3. RTC device (U34)

4.2. System on a Chip

The KSwitch M20 module implements the Microchip LAN969xTSN Switch SOC featuring the following:

- 10x 10Gbps SerDes for various physical interfaces configurations.
- Flexible port configuration via 10x 10G SerDes, up to 28 ports with default port configuration is:
  - 6x QSGMII (24x 10/100/1000BASE-T) and
  - 4x 10G-USXGMII (4x 1/2.5/5G/10GBASE-T)
  - Up to 28 x 1Gb/s ports or 10x10GBASE-T can be supported (on-request only)
- Managed Time Sensitive Networking (TSN) and Precision Time Protocol (PTP)
- 44 Gbps to 102 Gbps scalable bandwidth
- Ethernet MDI
- 10/100/1000BASE-T MDI IF (option)
- MIIM Interfaces for CL22 and CL45 devices

Table 3: Ethernet Port and SOC Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
B2/B3	PHY_MDI0+/-	Ethernet PHY MDI 0+/-	In/Out	MDI lanes, Physical Layer signals
B5/B6	PHY_MDI1+/-	Ethernet PHY MDI 1+/-	In/Out	
B8/B9	PHY_MDI2+/-	Ethernet PHY MDI 2+/-	In/Out	
B12/B13	PHY_MDI3+/-	Ethernet PHY MDI 3+/-	In/Out	
B39/B40	SW_ETH_S0_RX-/+	Differential receive lanes [0]	In	Microchip LAN969xTSN Ethernet SerDes receiver lanes.
B43/B44	SW_ETH_S1_RX-/+	Differential receive lanes [1]	In	
B46/B47	SW_ETH_S2_RX-/+	Differential receive lanes [2]	In	

Pin	Signal	Description	Type	Comment
B40/B50	SW_ETH_S3_RX-/+	Differential receive lanes [3]	In	AC coupled on module.
B52/B53	SW_ETH_S5_RX-/+	Differential receive lanes [4]	In	
B55/B56	SW_ETH_S5_RX-/+	Differential receive lanes [5]	In	
B58/B59	SW_ETH_S6_RX-/+	Differential receive lanes [6]	In	
B61/B62	SW_ETH_S7_RX-/+	Differential receive lanes [7]	In	
B64/B65	SW_ETH_S8_RX-/+	Differential receive lanes [8]	In	
B67/B68	SW_ETH_S9_RX-/+	Differential receive lanes [9]	In	
A39/A40	SW_ETH_S0_TX-/+	Differential transmit lanes [0]	Out	Microchip LAN969xTSN Ethernet SerDes transmit lanes. AC coupled on module.
A43/A44	SW_ETH_S1_TX-/+	Differential transmit lanes [1]	Out	
A46/A47	SW_ETH_S2_TX-/+	Differential transmit lanes [2]	Out	
A49/A50	SW_ETH_S3_TX-/+	Differential transmit lanes [3]	Out	
A52/A53	SW_ETH_S4_TX-/+	Differential transmit lanes [4]	Out	
A55/A56	SW_ETH_S5_TX-/+	Differential transmit lanes [5]	Out	
A58/A59	SW_ETH_S6_TX-/+	Differential transmit lanes [6]	Out	
A61/A62	SW_ETH_S7_TX-/+	Differential transmit lanes [7]	Out	
A64/A65	SW_ETH_S8_TX-/+	Differential transmit lanes [8]	Out	
A67/A68	SW_ETH_S9_TX-/+	Differential transmit lanes [9]	Out	
B20	SW_MDC0_1V8	MIIM data clock	Out	Microchip LAN969xTSN MIIM controller [0/1] Media Dependent Clock
B22	SW_MDC1_1V8	MIIM data clock	Out	
A20	SW_MDIO0_1V8	Switch MIIM data input/output	In/Out	Microchip LAN969xTSN MIIM controller [0/1] Media Dependent Data Input Output
A22	SW_MDIO1_1V8	Switch MIIM data input/output	In/Out	
B15	SW_IRQ2_MIIM_1V8#	Interrupt pin	In	Microchip LAN969xTSN Interrupt. Signal is active low.

4.3. PoE/PoE+ Controller

The KSwitch M20 module supports enhanced mode PoE capabilities, as specified in IEEE 802.3af, IEEE 802.3at, IEEE 802.3bt, and PoE standards, on all external Ethernet ports.

PoE/PoE+ power distribution is achieved using the Microchip PD69210 PoE/PoE+ PSE controller and external PSE device(s) such as Microchip PD69208T4, PD69204T4, or PD69208M PoE manager. The PoE/PoE+ PSE controller uses the ESPI interface with 3.3 VIO signals to communicate with one or more PoE PSE managers. The PoE/PoE+ PSE controller supports 28 KSwitch M20 module 4-pair or 2-pair logical ports.

Note: To support PoE the custom carrier board must support a PoE subsystem and must handle the PoE PSE module interface as defined in the KSwitch M20 Carrier Board Design Guide.

The PSE controller provides a “System OK signal that can be used to drive an external healthy LED signal.

For the Carrier Board Design Guide in the Customer Section click on Switches > TSN Network > KSwitch M20 > KSwitch M20 Design Information > Design Guide KSwitch M20-xxxT.

Table 4: PoE PSE Controller Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
A78	POE_CON_ESPI_MISO_3V3	eSPI Master In, Slave Out	In	Microchip PD69210 eSPI Master In, Slave Out for external PoE PSE manager.
B76	POE_CON_ESPI_SCK_3V3	eSPI Chip Select	Out	Microchip PD69210 eSPI Serial Clock for external PoE PSE manager.
B77	POE_CON_ESPI_CS_3V3#	eSPI Chip Select	Out	Microchip PD69210 eSPI Chip select for external PoE PSE manager. Signal is active low.
B78	POE_CON_ESPI_MOSI_3V3	eSPI Master Out Slave In	Out	Microchip PD69210 eSPI Master Out Slave In for external PoE PSE manager.
B83	POE_DIS_PORTS_3V3#	Disable all PoE ports	In	Microchip PD69210 input signal disable all PoE ports. Signal is active low.
B84	POE_SYS_OK_3V3	System OK for PoE ports	Out	Microchip PD69210 PoE system okay signal. Used to drive Healthy led.

4.4. System Memory

The KSwitch M20 module supports 1 GByte DDR4 system memory on the KSwitch M20 module (memory down). The DDR4 memory is accessed via SOC's 16-bit DDR4 interface using in-band ECC.

The DDR4 memory device is soldered down on the KSwitch M20 module and cannot be exchanged.

4.5. eMMC Storage

The KSwitch M20 module supports 4 GByte pseudoSLC embedded Multimedia Card (eMMC) memory. The eMMC memory stores application firmware and configuration data. The eMMC memory is accessed for programming via the SOC's Secure Digital Multimedia Card Controller (SDMMC) bus. The SOC's SDMMC0 and SDMMC1 signals support the eMMC Specification V5.01, the SDIO V3.0 Specification and the SD memory card specification V3.0. With eMMC Boot mode the SDMMC0 controller connects to the eMMC memory.

4.6. NOR Flash Memory

The KSwitch M20 module supports up to 2 MByte NOR Flash memory. The NOR Flash memory is accessed for reading and programing via the SOC Quad SPI (QSPI) bus.

The used cases of the NOR Flash Memory are:

- To provide failsafe boot firmware (U-Boot) for disaster recovery of the application firmware.
- To provide FRU information data.

4.7. Clock Distribution

The KSwitch M20 module complies with the IEEE 802.1 Time Sensitive Networking (TSN) standard and IEEE 1588v2 Precision Time Protocol (PTP) standard for precise time and frequency synchronization that reduce inaccuracy between devices over a network. The PTP pins are used to synchronize the Ethernet PHY TimeOfDay, and to synchronize the implemented carrier board via the Carrier interface connector.

The KSwitch M20 module's clock distribution supports 125 MHZ for Gb PHYs such as Microchip's LAN8814 as well as 156.25 MHz for 10 Gb PHYs such as Broadcom's BCM84891LM.

Table 5: PTP and Clock Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
A27	CAR_1PPS_IN_1V8	Clock input signal.	In	For external PHY time synchronization, on the carrier board.
B27	CAR_1PPS_OUT_1V8	Single ended pulse per second output	Out	For external PHY time synchronization, on the carrier board.
A28	CAR_1PPS_FB_COMP_1V8	Clock pulse per second signal	In	For external PHY time synchronization, on the carrier board.
A36	REFCLK_125M00-	125 MHz Reference clock-	Out	Differential 125 MHz Reference clock for external PHYs
A37	REFCLK_125M00+	125 MHz Reference clock+	Out	
B24	REFCLK_156M25-	156.25 MHz Reference clock-	Out	Differential 156.25 MHz Reference clock for external PHYs
B25	REFCLK_156M25+	156.25 MHz Reference clock+	Out	

4.8. Interrupt (IRQ)

The KSwitch M20 module supports an interrupt signal from the carrier board. The carrier board's PHYs interrupt signal is multiplexed via an I2C expander to the KSwitch M20 module's Pin-B15.

Table 6: Interrupt Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
B15	SW_IRQ2_MIIM_1V8#	Interrupt	In	Microchip LAN969xTSN interrupt signal is active low.
B16	CAR_I2C_INT_1V8#	I2C/SMB interrupt/SMB Alert	In	Microchip LAN969xTSN I2C/SMB interrupt /SMB Alert signal.

4.9. I2C Bus

The KSwitch M20 module's embedded I2C controller connects to the Carrier interface connector and transfers I2C serial data at the set I2C clock frequency (standard mode 100 kHz, fast mode 400 kHz and fast mode plus 1 MHz) between the KSwitch M20 module and the carrier board.

The two-wire interface (TWI) I2C bus uses bi-directional 1.8 V signaling and can be used by any I2C compatible devices

The SOC's FLEXCOM interface 3 is configured to use the I2C interface.

Table 7: I2C Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
A30	CAR_I2C_SDA	I2C/SMB Serial Data	In/ Out	Microchip LAN969xTSN I2C/SMB serial data. Add 10K pull-up resistor, Kontron recommends a pull-up voltage between 1.8 V and 3.3 V.
B16	CAR_I2C_INT_1V8#	I2C/SMB Interrupt /SMB Alert	In	Microchip LAN969xTSN I2C/SMB interrupt /SMB Alert signal.
B30	CAR_I2C_SCL	I2C/SMB Serial Data	Out	Microchip LAN969xTSN I2C/SMB serial clock. Add 10K pull-up resistor, Kontron recommends a pull-up voltage between 1.8 V and 3.3 V.
B79	SW_I2C_RST_3V3#	I2C/SMB Reset Output	Out	Active low signal

4.10. PCIe

The KSwitch M20 module supports a PCIe 3.0 x1 interface accessible via the external PCIe Host. The PCIe reference clock frequency is 100 MHz.

Table 8: PCIe Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
A33	PCIE-TX+	PCIE Transmit Data+	Out	PCIE differential transmit data positive, to external Root Complex, AC-Coupled on module. Reserved, leave pin open.
A34	PCIE-TX-	PCIE Transmit Data-	Out	
B33	PCIE-RX+	PCIE Receive data+	In	PCIE differential receive data positive, to external Root Complex, AC-Coupled on module. Reserved, leave pin open.
B34	PCIE-RX-	PCIE Receive data-	In	
B36	PCIE-CLK+	PCIe clock +	In	PCIE 100 MHz differential reference clock +

Pin	Signal	Description	Type	Comment
B37	PCIE-CLK-	PCIe clock -	In	PCIE 100 MHz differential reference clock -
A19	SW_FSD0_PCIE_PERST_1V8#	PCIE fundamental Reset	In	Reset from external host to LAN9696TSN Reserved, leave pin open. (1K pull-up to 1.8 V on module)

4.11. Real Time Clock (RTC)

The KSwitch M20 module supports a Real Time Clock (RTC) device (RV-8803-C7) including an integrated CMOS circuit with a XTAL to keep track of the current time accurately. If the primary power source is switched off or unavailable, the RTC's low power consumption enables the RTC to continue to keep time using a lower secondary power source to be supported on the carrier board.

Kontron recommends supplying enough power to the RTC device to retain the time accurately using a Supercap buffer with a 72 hour lifetime or a 3 V Lithium battery on the implemented carrier board.

Table 9: RTC Signal on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
A-101	V_3V0_VBAT	Power In	PWR-In	Power in from the RTC battery (Lithium battery or Supercap)

Kontron recommends user to supply the RTC using one of the following on the carrier board:

- Supercap buffer with a 72-hour lifetime
- 3 V Lithium battery

4.12. Reset

The KSwitch M20 module does not include a reset. If a reset is required, Kontron recommends implementing the SOC's reset signal on the carrier board.

Table 10: Reset Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
A16	SW_PUSHB_RST_IN_1V8#	Reset button	In	Push-Button Reset input from carrier board, active low. A high to low transition leads to a warm reset of the module. If held reset is released and the reset button state can be read by switch.
A19	SW_FSD0_PCIE_PERST_1V8#	PCIE fundamental Reset	In	Reset from external host to LAN9696TSN Reserved, leave pin open. (1K pull-up to 1.8 V on module)
B79	SW_I2C_RST_3V3#	I2C/SMB reset output	Out	Active low signal
B82	SW_PHY_RST_1V8#	Reset	Out	Reset signal to local and external PHYs

4.13. Smart LEDs

The KSwitch M20 module includes a Smart LED bus micro controller (IT MSPM0L1304T) that merges the SOC and PSE controller as well as the input power states information to a single programmable LED bit stream. The Ethernet port, PoE/PoE+ port and power states signals are distributed to the carrier board using the SMART LED signals.

Table 11: Smart LED Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
B89	SMART_LED_DO_1V8	Smart LED	Out	SMART LED for the serial data stream
B84	POE_SYS_OK_3V3#	PoE System OK	Out	Microchip PD69210 PoE system OK signal. Used to drive healthy LED.
B91	CAR_STATUS_L2_1V8	Carrier board status L2 inputs signal.	In	MCU carrier board status L2 input signal The status can be integrated into the SMART LED data stream. Add 10K pull down to carrier board if not used
B92	CAR_STATUS_L3_1V8	Carrier board status L3 input signal.	In	MCU carrier board status L3 input signal. The status can be integrated into the SMART LED data stream. Add 10K pull down to carrier board if not used

4.14. UART0/1

The KSwitch M20 module supports serial communications with serial RX/TX ports supplied by the SOC, with the option for a second UART port, on the carrier board.

The KSwitch M20 module's UART0 (FLEXCOM0) interface delivers the boot trace or TF-A monitor and offers management via the UART0 115200 baud/8/N serial interface.

TF-A (Trusted Firmware A) and boot trace UART modes are configured for 115200 baud/8/N.

Table 12: UART Interface Signals on the Carrier Interface Connector

Pin	Signal	Description	Type	Comment
A17	SW_FC0_UART_TXD_5V0	UART Transmit interface	In	LAN969xTSN FLEXCOM0 UART interface
B17	SW_FC0_UART_RXD_5V0	UART Receive interface	Out	LAN969xTSN FLEXCOM0 UART interface
A74	SW_GPIO66_FLEX2_TXD_1V8	FLEX2 Transmit	In/Out	LAN969xTSN, usable as FLEXCOM2 UART interface. Reserved without DPLL, leave pin open.
A75	SW_GPIO65_FLEX2_RXD_1V8	FLEX2 Receive	In/Out	LAN969xTSN, usable as FLEXCOM2 UART interface. Reserved without DPLL, leave pin open.
A76	SW_GPIO64_FLEX2_SCK_1V8	FLEX2 SCK/DPLL SCK	In/Out	LAN969xTSN, usable as FLEXCOM2 UART interface. Reserved without DPLL, leave pin open.

Pin	Signal	Description	Type	Comment
A77	SW_GPIO63_1V8	SPARE IRQ5/DPLL_CS#	In/Out	LAN969xTSN, usable as FLEXCOM2 UART interface. Reserved without DPLL, leave pin open.

4.15. USB 2.0 Host

The KSwitch M20 module supports a USB 2.0 Host acting as a physical layer (PHY) and supports configuration of the host using USB 2.0 signaling. The USB 2.0 host uses the SOC's UTMI+ low-pin interface (ULPI) interface at 1.8 V.

The USB 2.0 host supports standard USB compliant functions such as VBUS sense, fault detection and power enable.

Note: In case the custom carrier board does not support USB. The carrier board must handle the USB module interface as defined in the Carrier Board Design Guide for the KSwitch M20.

Table 13: USB 2.0 Host on the Carrier Interface Connector Signals

Pin	Signal	Description	Type	Comment
A71	SW_USB_PWR_OC_DET_1V8#	USB overcurrent/fault detection	In	
B71	USB_UD+	USB 2.0	In/Out	USB 2.0 data signals
B72	USB_UD-	USB 2.0	In/Out	USB 2.0 data signals
B73	V_5V_USB_VBUS	USB 5.0 V power distribution	Power In	For external device
B74	SW_USB_PWR_EN_1V8	USB power enable	Out	For external device

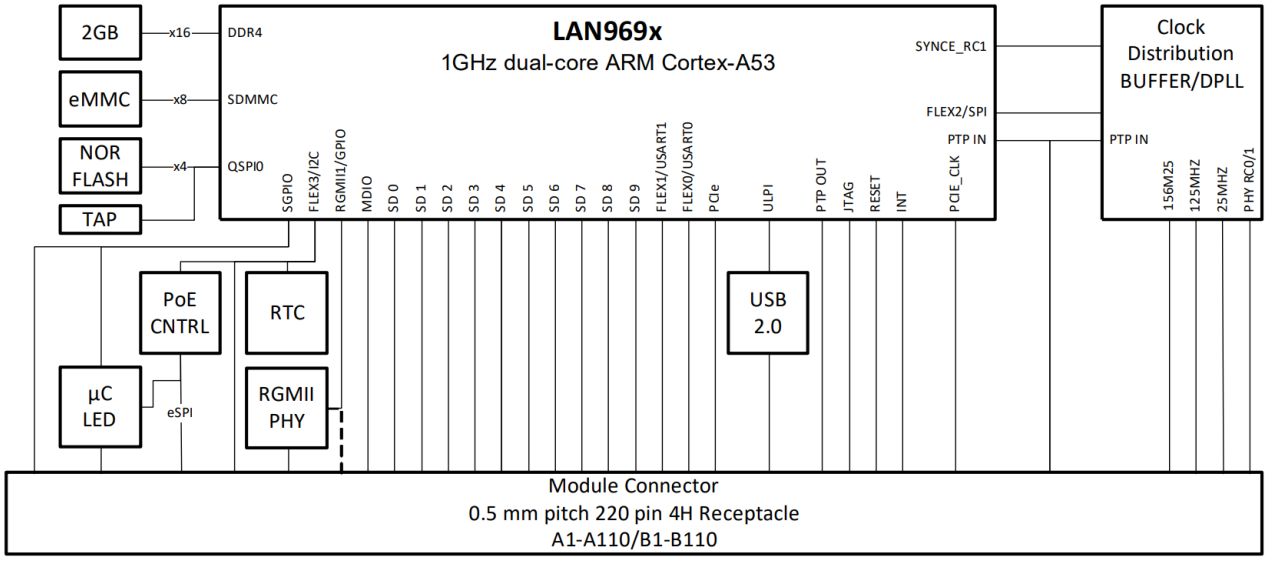
5/Switch Specification

Before implementing the KSwitch M20 embedded Ethernet switch module, Kontron recommends new users to take a few minutes to learn about the KSwitch M20 module's technical specification requirements.

5.1. Functional Block Diagram

The following diagram provides additional information concerning board functionality and component layout.

Figure 5: KSwitch M20 Module Block Diagram



5.2. Hardware Specification

Table 14: Hardware Specification

Network	
Device	Microchip LAN969x TSN Switch Family with 1GHz dual core ARM Cortex-A53
OS	Microchip iStaX
Operating Mode	Store and forward, full wire-speed, Non-blocking switch core. Low latency cut-through forwarding mode
Memory	
System	Up to 2 GB DDR4 memory down (1 GB/2 GB options)
Storage	8 GB eMMC for Failsafe boot firmware
U-Boot Flash	2 MB NOR QSPI Flash QSPI interface Tag connector footprint allows initial programming of the QSPI NOR Flash.
Controllers	
Poe PSE Controller	Microchip PD69210 PoE PSE controller IC Supporting up to 30 W per port Complies with IEEE 802.3af/at Controls and monitors external PoE manager devices (such as PD69204T4) via the SPI bus.
LED Controller	TI MSPM0L1304TRGER LED controller Supports LED options for the user designed carrier board: › Link/Activity LED: Indicates Ethernet port activity and link › PoE Power LED: Indicates if power is supplied or delivered › Speed LED: Indicates the Ethernet port's speed
USB PHY Transceiver	Microchip USB3343-CP enhanced single supply Hi-Speed USB 2.0 ULPI transceiver Provides a physical layer (PHY) USB Link Power Management support
Ethernet (RGMII) PHY Transceiver	TI DP83867ISRGZT I Interface to the MAC: RGMII, SGMII Speed: 10Base-Te/100BaseTX/1000Base-T
Interfaces	
Ethernet SerDes	Flexible port configuration via 10x 10Gpbs SerDes: - 10GBASE-KR - 10GBASE-R - 10G-USXGMII - 5GBASE-KR - 5GBASE-R - 5G-USXGMII - QSGMII - 2.5GBASE-KX - 2.5GBASE-X - 2.5G SGMII - 1000BASE-KX - 1000BASE-X - SGMII - 100BASE-FX
	Initial Port Mapping : 6x QSGMII (24x 10/100/1000BASE-T) & 4x 10G-USXGMII (4x 10GBASE-T) Other port maps on request

Interfaces	
Ethernet MDI	10/100/1000BASE-T MDI (Optional) / Shared with GPIO/RGMII
PCIe Endpoint	External PCIe Host can access the LAN969xTSN via PCIe 3.0 x1 interface (option). Note: LAN9696TSN Endpoint requires an external PCIe 100MHz clock.
USB Host	USB 2.0 with VBUS sense, fault detection and power enable
I2C	Two Wire Bus Bi-directional with one data (Bi-directional) and one clock line
GPIO	General Purpose IO, 1.8 VIO
POE ESPI	PoE Controller ESPI interface, 3.3 VIO
UART	1x UART 1.8V onboard connector, X1, X1b Note: A second UART may be offered for debugging on the carrier board.
LEDS	
Power	Power Good
Ethernet	Link/Act/Speed
PoE/PoE+	Off/On/Fail
Timer	
RTC	Micro Christal RTC RV8803 holds time of day information over a reset. KSwitch M20 module does not include an RTC buffer or battey. Carrier board must provide RTC hold up Supercap Buffer with a 72-hour (approx.) lifetime or a battery.
Thermal	
Temperature Sensors	Internal Microchip LAN9696TSN temperature sensors External sensors may be offered for temperature control on the carrier board.
Heatspreader plate	Mounted on KSwitch M20 module
Miscellaneous	
Watchdog timer	Internal Microchip LAN9696 TSN Watchdog
Tag Connect	Tag connector provides programming interfcase for the DPLL. Initial programming of the QSPI Flash.
Option	
SyncE & IEEE 1588 DPLL	Microchip ZL30732

Table 15: Ethernet Specification

Bridge, VLAN, Protocols	
Switching	IPv4/IPv6 unicast and multicast L2 switching
Routing	IPv4/IPv6 unicast and multicast L3 forwarding with RPF
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	IGMPv1, IGMPv2, IGMPv3, MLDv1 MLDv2
	Up to 255 multicast groups
	IGMP snooping, querying

Bridge, VLAN, Protocols	
Network Discovery	IEEE 802.1ab LLDP
Traffic Management & QoS	Traffic Management & QoS
Priority	IEEE 802.1p QoS
No. of Queues per port	8
Scheduling schemes	Strict Priority Queuing (SPQ) Deficit-Weighted Round Robin Queuing (DWRR)
Time Sensitive Networking	
Shaping & Fillter	IEEE 802.1Qbv-2015 Time Aware Shaping IEEE 802.1Qbu/802.3br – Frame Preemption IEEE 802.1Qav AVB traffic shaping IEEE 802.1Qci-2017 per Stream Filtering and Policing
Redundancy/ Reliability	Redundancy with IEEE 802.1CB Frame Replication and Elimination for Reliability (FRE), Protection switching (line or ring)
Forwarding Scheme	Cut-through option per TSN Stream and Store and Forward
Timing and Synchronization	IEEE 802.1AS-2020 1-step and 2-step IEEE 1588v2 1-step and 2-step for Ordinary Clock Boundary Clock and Transparent Clock
Network Redundancy	
Spanning Tree Protocol	IEEE 802.1D/1w/1S, STP/RSTP/MSTP
Port Trunk / LACP	Static trunk or LACP (Link Aggregation Control Protocol) G.8032, MRP IEC-62439-2 2016
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 and Command Line Interface (CLI)
Interfaces	SNMP v1/v2c, Trap, Telnet (5 sessions) RFC 3411 SNMP Management Frameworks RFC 3414 User-based Security Model for SNMPv3 RFC 3415 View-based access Control Model for SNMP RFC 2613 SMON - PortCopy
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 and ICMP Ping
DHCP	Client Mode, Server Mode, Relay Mode, Snooping

Management	
Network Time Synchronozation	NTP client
System Status	Device info/status Ethernet port status
Green Ethernet	Port power savings

5.3. Power Specification

The KSwitch M20 module receives power from a customized carrier board via the Carrier interface connector and must be connected to a carrier board to power on. The Carrier interface connector limits the amount of power received by the KSwitch M20 module. The KSwitch M20 module must be supplied with enough power to guarantee stable functionality. It is recommended to provide KSwitch M20 module with more power than required from a stable power source.

⚠CAUTION

Carrier Board Switched Off

Before connecting the KSwitch M20 module to a carrier board using the Carrier interface connector, ensure that the carrier board is switched off and disconnected from the main power supply. Failure to disconnect the main power supply could result in personal injury and damage to the KSwitch M20 module and/or carrier board.

⚠CAUTION

Handle Carefully

Handling and operation of the KSwitch M20 module is permitted only for skilled personnel within an ESD-safe workplace with access control.

ESD Sensitive Device!

Keep electrostatic sensitive parts in their containers until they arrive at the ESD-safe workplace. Always be properly grounded when touching a sensitive board, component, or assembly.

The KSwitch M20 module supports a 12 VDC +/- 20% single-supply voltage and supplies two output voltages (3.3 VDC & 1.8 VDC) on the Carrier interface connector.

Table 16: Electrical Specification

Electrical	Description	Note
Input Voltage	12 VDC +/- 20% Wide range (4.75 VDC up to 20 VDC)	Carrier board power to M20 module.
Output Voltage	3.3 VDC +/- 3% @1A 1.8 VDC +/- 3% @0.5A	VIO power distribution to the carrier board.
Power Consumption	5 W	KSwitch M20 Module

⚠CAUTION

Power Supply

Only connect to an external power supply delivering the specified input rating and complying with the requirements of Safety Extra Low Voltage (SELV) and Limited Power Source (LPS) or (PS2) of UL/IEC 62368-1.

NOTICE

Wire Cross-section

To protect external power lines of peripheral devices, make sure that the wires have the right diameter to withstand the maximum available current and the enclosure of the peripheral device fulfils the fire-protection requirements of IEC/EN 62368-1.

NOTICE

Hold Up Time

If any of the supply voltages drop below the allowed operating level longer than the specified hold-up time, all the supply voltages should be shut down and left OFF for a time long enough to allow the internal board voltages to discharge sufficiently.

If the OFF time is not observed, parts of the board or attached peripherals may work incorrectly or even suffer a reduction of MTBF. The minimum OFF time depends on the implemented PSU model and other electrical factors and must be measured individually for each case.

5.3.1. Protective Earth Digital Ground

The KSwitch M20 module supports a digital ground that acts as a reference point for a single ground connection to reduce noise and other unintended interference. This digital ground must be connected to the carrier board's ground plane!

The KSwitch M20 module's digital ground must be connected to the carrier board's ground plane!

5.4. Environmental Specification

Table 17: Environmental Specification

Environment	Description
Temperature (operating) According to: EN 50155:2021, class OT4, ST1	-40°C to +85°C (-40°F to 158°F)
Temperature (non-operating) According to: EN 50155:2021 & EN 60068-2-2	-40°C to +85°C (-40°F to 158°F)
Humidity According to: EN 50125-1	+25°C/+55°C, 100 % Relative Humidity (max.)
Humidity According to: EN 60068-2-78	93% RH at 40°C, non-condensing
Shock (non-operating) According to: EN 61373:2010/AC:2017-09	Category: 1, class B Severity: 50 m/s^2 Duration: 30 ms
Vibration (non-operating) According to: EN 61373:2010/AC:2017-09:	Category: 1, Class B Severity: 11.44 m/s^2 (long-life) Duration: 5 hr.

Environment	Description
Vibration (operating) According to: EN 61373 :2010/AC:2017-09	Category: 1, Class B Severity: 2.02 m/s^2 (functional) Duration: 10 min.
Altitude	+3,000 m max.
MTBF	1395631.30 hours @ 40°C Ground Benign (GB) For variants: KSwitch M20-M100T & KSwitch M20-M64T

5.5. Thermal Specification

The KSwitch M20 module supports an extended temperature range. For thermal management a heatspreader plate is available and a thermal sensor. The operating temperature with the heatspreader plate is the maximum measurable temperature on any part on the heatspreader's surface and without the heatspreader plate the maximum measurable temperature on any spot on the KSwitch M20 module's surface.

Table 18: Thermal Specification

Thermal	Description
Heatspreader	standard PICMG COM.0 COM Express® Revision 3.0 mini heatspreader plate
Temperature Sensors	One on module temperature sensor provided by the Microchip LAN969xTSN device. Note: Additional temperature sensors must be implemented on a custom carrier board.

5.5.1. Heatspreader Plate (HSP)

The KSwitch M20 module supports a standard PICMG COM.0 COM Express® Revision 3.0 mini Heatspreader Plate (HSP) that shares the same dimensions as the KSwitch M20 module. All KSwitch M20 module critical components are located on the top side and connect to the heatspreader plate's thermal pads (Figure 6. Pos. 3.), designed to aid heat dissipation away from the critical thermal components. The heatspreader plate attaches to the KSwitch M20 module using two screws with 4.5 mm threaded M2.5 or clear 2.7 mm (Figure 6. Pos. 2.).

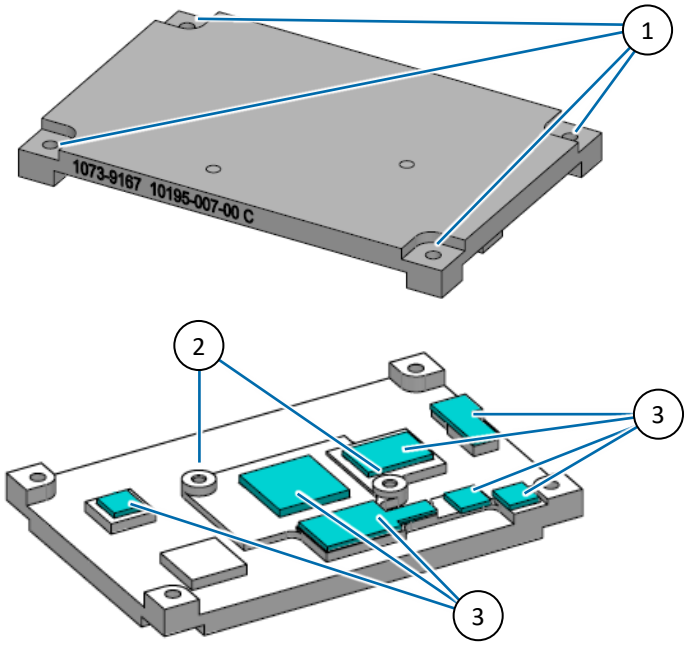
The heatspreader plate is NOT a heatsink. Kontron recommends using the heatspreader plate in conjunction with an external cooling device such as a heatsink that meets the application and environmental conditions and maintains the heatspreader plate at the specified operating temperatures on any spot of the heatspreader's surface.

Hot Surface

Heatspreader plate and additional cooling solution can get very hot. To avoid burns and personal injury when handling the KSwitch M20 module:

- Do not touch when in operation
- Allow to cool before handling
- Wear protective gloves

Figure 6: Heatspreader Plate (top and bottom sides)



1. 4x Mounting opening for standoffs (HSP, module to carrier board)
2. 2x Mounting holes for standoffs (module to HSP)
3. Thermal pads

5.6. Mechanical Specification

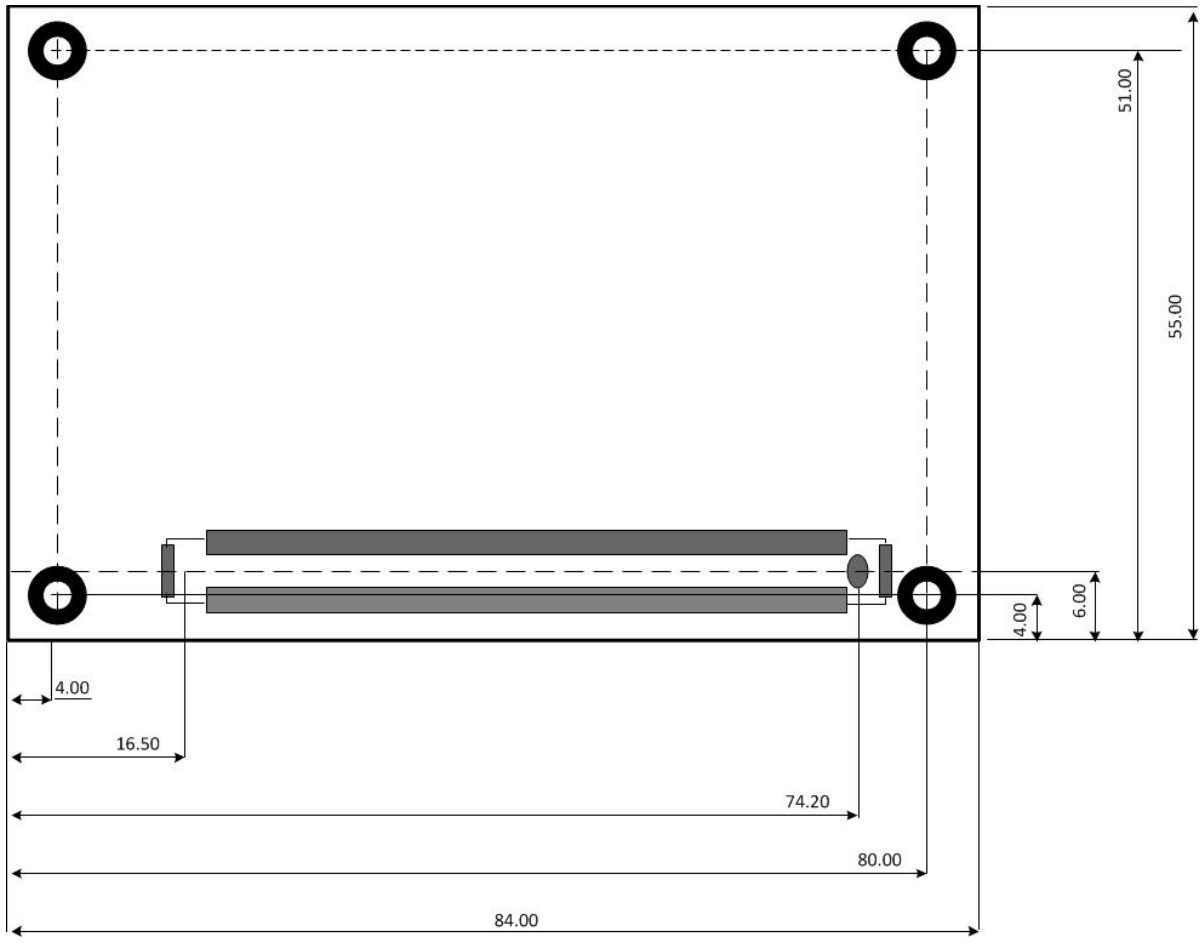
The KSwitch M20 module is based on the PICMG COM.0 COM Express Rev 3.0 mini module form-factor.

Table 19: Mechanical Specification

Mechanical	Description
Dimension	84 mm x 55 mm (3.3 inch x 2.17 inch)
Form-factor	COM Express mini module
Height	13 mm (0.51 inch), module bottom to HSP top 18 mm (0.71 inch), carrier board bottom to HSP top with 5 mm stack height 21 mm (0.83 inch), carrier board bottom to HSP top with 8 mm stack height
Weight	50 g (0.11 lbs) approx.
Installation	4 x Mounting openings, HSP, module to carrier board 2 x Mounting openings, module to HSP

5.6.1. Dimensions

Figure 7: Dimensions (mm)



In the above diagram the Carrier interface connector is shown as if seen through the KSwitch M20 module on the rear side.

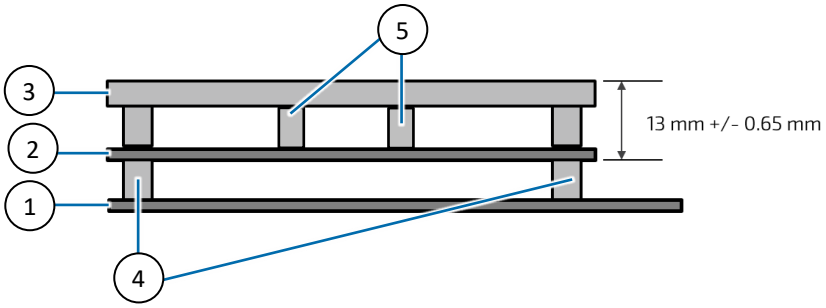
5.6.2. Module Height

The COM Express® specification defines a module height of approximately 13 mm, when measured from the bottom of the KSwitch M20 module's PCB board to the top of the heatspreader plate.

The overall height depends on additional factors:

- Height of the user defined external cooling solution
- Height of the required standoff:
  - 5 mm standoff = total assembly height 18 mm
  - 8 mm standoffs = total assembly height 21 mm

Figure 8: Height with Heatspreader Plate (side view)



1. Carrier board
2. KSwitch M20 module
3. Heatspreader plate (HSP)
4. 4x Standoffs carrier to module (5 mm to 8 mm)
5. 2x Standoffs HSP to module

The heatspread plate's standoffs are four 4.5 mm threaded M2.5 or clear 2.7 mm.

5.7. Compliance

The KSwitch M20 module plans to comply with the requirements and the approximation of the laws relating to compliance for Railway, CE, and international standards (or later thereof) that are constitutional parts of the declaration.

Table 20: CE Compliance

Europe- CE Mark and UKCA	
Directives	**2014/30/EU** Electromagnetic Compatibility **2014/35/EU** Low Voltage **2011/65/EU** RoHS II
EMC	**EN 55032** Electromagnetic compatibility of multimedia equipment (MME)- Emission Requirements **EN 55035** Electromagnetic compatibility of multimedia equipment (MME- Immunity requirements **EN 61000-6-4** Electromagnetic compatibility (EMC) – Part 6-4: Generic standards - Emission for industrial environments **EN 61000-6-2** Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity standard for industrial environments **EN 63000** Technical documentation for the assessment of electrical and electronic products with respect to the restriction of hazardous substances
Safety (CB Scheme)	**EN 62368-1** Audio/video, information and communication technology equipment - Part 1: Safety requirements

For the Document of Conformity (DOC), visit Kontron's Customer Section and click on Switches > TSN Network > KSwitch M20 > KSwitch M20 Application Notes and Documentation.

If the KSwitch M20 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 KSwitch M20 module. The user is responsible for the correction of interference.

The transmission and reception of data cannot be guaranteed, and corruption may occur or data may be lost. The KSwitch M20 module should not be used in environments where the failure to send data could result in personal injury or damage. Kontron is not responsible for personal injuries or damage caused by delays, errors or failures to transmit or receive data using the KSwitch M20 module.

5.7.1. Compliance for Railway/Rolling Stock Applications

The KSwitch M20 module was only tested for EN 50155:2021 compliance while installed in Kontron's KSwitch R20 and KSwitch R16 series of managed L2/L3 Ethernet switch systems. The system integrator is responsible for conducting EN 50155:2021 compliance testing within the system integrator's system enclosure.

For EN 50155:2021 compliance information, visit the KSwitch R20 and KSwitch R16 product websites and scroll down to Download>Manuals to download the KSwitch R20 and KSwitch R16 user guide.

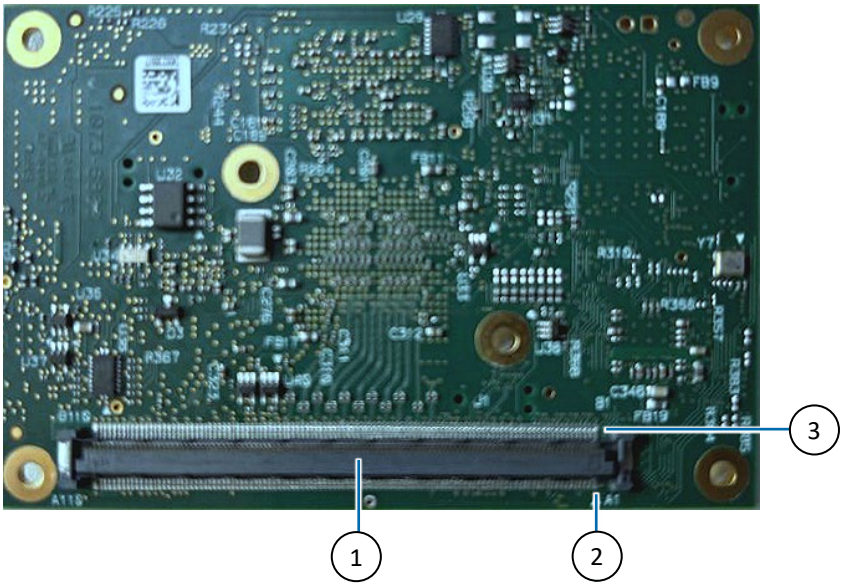
The KSwitch M20 module was tested for EN 50155:2021 compliance while installed in the KSwitch R20 /KSwitch R16 systems. The system integrator is responsible for conducting EN 50155:2021 compliance testing within the system integrator's system enclosure.

6/Carrier Interface Connector

The carrier interface connector is located on the rear side of the KSwitch M20 module. The carrier interface connector contains 220-pins with two rows (row A and row B). Row A contains pins A1 to A110, and row B contains B1 to B110. The carrier interface connector inserts into a corresponding interface connector on the custom carrier board. The carrier board supplies the KSwitch M20 module with power and interface signals via the carrier interface connector.

The carrier board's corresponding interface connector must comply with the KSwitch M20 module's (0.5 mm pitch free height 220 pin 4H) carrier interface connector, with a stack height of 5 mm min.

Figure 9: Carrier Interface Connector



1. 220-pin Carrier interface connector
2. Pin-A1
3. Pin B1

6.1. Carrier Interface Connector Pin Assignments

The terms used in the carrier interface connector pin assignment tables and a description of the signal are described in the table below.

Table 21: General Signal Description

Type	Description	Type	Description
NC	Not Connected (on this product)	**Out**	Output
I/O	Input/Output (Bi-directional)	**PWR**	Power Connection
In	Input	**PWR-In**	Power Input
+ and -	Differential Pair Differentiator	**PWR-Out**	Power Output
GND	Power Ground Connection	**GND**	Power Ground Connection
SW	Indicates a KSwitch M20 signal	**CAR**	Indicates a carrier board signal

The carrier interface connector contains two rows Row A contains pins A1 to A110, and row B contains B1 to B110. The following table lists the pin assignment of the KSwitch M20 module's interface connector pins A (1-110).

Table 22: Carrier Interface Connector Row A (1 to 110) Pin Assignment

Pin	Signal	Description	Type	Comment
A1	GND	Ground	GND	Ground
A2	SW_GPIO42_1V8		In/Out	Reserved w/o RGMII PHY
A3	SW_GPIO43_1V8		In/Out	Reserved w/o RGMII PHY
A4	SW_GPIO44_1V8		In/Out	Reserved w/o RGMII PHY
A5	SW_GPIO45_1V8		In/Out	Reserved w/o RGMII PHY
A6	SW_GPIO46_1V8		In/Out	Reserved w/o RGMII PHY
A7	SW_GPIO47_1V8		In/Out	Reserved w/o RGMII PHY
A8	GND	Ground	GND	Ground
A9	SW_GPIO48_1V8		In/Out	Reserved w/o RGMII PHY
A10	SW_GPIO49_1V8		In/Out	Reserved w/o RGMII PHY
A11	GND	Ground	GND	Ground
A12	SW_GPIO50_1V8		In/Out	Reserved w/o RGMII PHY
A13	SW_GPIO51_1V8		In/Out	Reserved w/o RGMII PHY
A14	SW_GPIO52_1V8		In/Out	Reserved w/o RGMII PHY
A15	SW_GPIO53_1V8		In/Out	Reserved w/o RGMII PHY
A16	SW_PUSHB_RST_IN_1V8#	Reset button	In	Push-Button Reset input from carrier, low active. A high to low transition leads to a warm reset of the module. If held reset is released and the reset button state can be read by switch.
A17	SW_FC0_UART_RXD_1V8	Serial UART Receiver input	In	LAN969xTSN FLEXCOM0 UART interface
A18	NC	-	-	Not Connected
A19	SW_FSD0_PCIE_PERST_1V8#	PCIE fundamental Reset	In	Reset from external host to LAN9696TSN Reserved, leave pin open. (1K pull-up to 1.8 V on module)
A20	SW_MDIO0_1V8	MIIM data input/output 0	In/Out	Microchip LAN969xTSN MIIM controller 0 Media Dependent Data Input Output.
A21	GND	Ground	GND	
A22	SW_MDIO1_1V8	MIIM data input/output 1	In/Out	Microchip LAN969xTSN MIIM controller 1

Pin	Signal	Description	Type	Comment
				Media Dependent Data Input Output.
A23	GND	Ground	GND	Ground
A24	DPLL_RCLK_PHY0_1V8	DPLL reference clock PHY0	In	SyncE & IEEE 1588 DPLL clock channel. Reserved, leave pin open.
A25	DPLL_RCLK_PHY1_1V8	DPLL reference clock PHY1	In	SyncE & IEEE 1588 DPLL clock channel 1 Reserved, leave pin open.
A26	GND	Ground	GND	Ground
A27	CAR_1PPS_IN_1V8	Clock input signal	In	For external PHY time synchronization, on the carrier.
A28	CAR_1PPS_FB_COMP_1V8	Clock pulse per second signal	In	For external PHY time synchronization, on the carrier.
A29	GND	Ground	GND	Ground
A30	CAR_I2C_SDA	I2C/SMB serial data	In/Out	Microchip LAN969xTSN I2C/SMB serial data. Add 10K pull-up resistor, Kontron recommends a pull-up voltage between 1.8V and 3.3V.
A31	GND	Ground	GND	Ground
A32	GND	Ground	GND	Ground
A33	PCIE_TX+	PCIE Transmit Data+	Out	PCIE differential transmits data to external Root Complex, AC-Coupled on KSwitch M20 module. Reserved, leave pin open.
A34	PCIE_TX-	PCIE Transmit Data-	Out	
A35	GND	Ground	GND	Ground
A36	REF_CLK_125M00-	Differential Ethernet Reference clock 125 MHZ	Out	Differential 125 MHz Reference clock for external PHYs.
A37	REF_CLK_125M00+	Differential Ethernet Reference clock 125 MHZ	Out	
A38	GND	Ground	GND	Ground
A39	SW_ETH_S0_TX-	Differential Transmit Lane [0]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A40	SW_ETH_S0_TX+	Differential Transmit Lane [0]+	Out	
A41	GND	Ground	GND	Ground
A42	GND	Ground	GND	Ground

Pin	Signal	Description	Type	Comment
A43	SW_ETH_S1_TX-	Differential Transmit Lane [1]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A44	SW_ETH_S1_TX+	Differential Transmit Lane [1]+	Out	
A45	GND	Ground	GND	Ground
A46	SW_ETH_S2_TX-	Differential Transmit Lane [2]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A47	SW_ETH_S2_TX+	Differential Transmit Lane [2]+	Out	
A48	GND	Ground	GND	Ground
A49	SW_ETH_S3_TX-	Differential Transmitr Lane [3]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A50	SW_ETH_S3_TX+	Differential Transmitr Lane [3]+	Out	
A51	GND	Ground	GND	Ground
A52	SW_ETH_S4_TX-	Differential Transmit Lane [4]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A53	SW_ETH_S4_TX+	Differential Transmit Lane [4+]	Out	
A54	GND	Ground	GND	Ground
A55	SW_ETH_S5_TX-	Differential Transmit Lane [5]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A56	SW_ETH_S5_TX+	Differential Transmit Lane [5]+	Out	
A57	GND	Ground	GND	Ground
A58	SW_ETH_S6_TX-	Differential Transmit Lane [6]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A59	SW_ETH_S6_TX+	Differential Transmit Lane [6]+	Out	
A60	GND	Ground	GND	Ground
A61	SW_ETH_S7_TX-	Differential Transmit Lane [7]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A62	SW_ETH_S7_TX+	Differential Transmit Lane [7]+	Out	
A63	GND	Ground	GND	Ground
A64	SW_ETH_S8_TX-	Differential Transmit Lane [8]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A65	SW_ETH_S8_TX+	Differential Transmit Lane [8]+	Out	
A66	GND	Ground	GND	Ground

Pin	Signal	Description	Type	Comment
A67	SW_ETH_S9_TX-	Differential Transmit Lane [9]-	Out	Microchip LAN969xTSN Ethernet SerDes lane. AC coupled on module.
A68	SW_ETH_S9_TX+	Differential Transmit Lane [9]+	Out	
A69	GND	Ground	GND	Ground
A70	GND	Ground	GND	Ground
A71	SW_USB_PWR_OC_DET_1V8#	USB overcurrent/fault detection	In	USB overcurrent/fault detect input, low active.
A72	SW_GPIO25_PWM_CON_1V8	MCU signal	In/Out	Reserved w/o MCU. Reserved leave pin open
A73	SW_GPIO26_TACH_CON_1V8	MCU signal	In/Out	
A74	SW_GPIO66_FLEX2_TXD_1V8	FLEX2_Transmit	In/Out	LAN969xTSN is usable as FLEXCOM2 UART interface. Reserved without DPLL, leave pin open.
A75	SW_GPIO65_FLEX2_RXD_1V8	FLEX2_Receive	In/Out	
A76	SW_GPIO64_FLEX2_SCK_1V8	FLEX2_SCK/DPLL_SCK	In/Out	
A77	SW_GPIO63_1V8	SPARE_IRQ5/DPLL_CS#	In/Out	
A78	POE_CON_ESPI_MISO_3V3	eSPI Master In Slave Out for external PoE PSE manager.	In	If the carrier does not support a PoE subsystem. Leave unconnected, pull-up on switch module.
A79	NC	-	-	Not Connected
A80	GND	Ground	GND	Ground
A81	MCU_UART_RXD_CON_1V8	UART Receive	In	Debug only, leave unconnected
A82	SW_VCORE3_1V8	Reserved Debug	In	
A83	SW_VCORE2_1V8	Reserved Debug	In	
A84	SW_VCORE1_1V8	Reserved Debug	In	
A85	SW_VCORE0_1V8	Reserved Debug	In	
A86	SW_SGPIO_DI_CON_1V8	MCU signal	In	Reserved without MCU. Reserved, leave pin open.
A87	SW_SGPIO_LD_CON_1V8	MCU signal	Out	
A88	SW_SGPIO_DO_CON_1V8	MCU signal	Out	
A89	SW_SGPIO_CK_CON_1V8	MCU signal	Out	
A90	GND	Ground	GND	Ground
A91	JTAG_TCK_1V8	JTAG Test Clock, 1.8V	In	Production debugging only
A92	JTAG_TMS_1V8	JTAG Test Mode Select, 1.8V	In	
A93	JTAG_TDI_1V8	JTAG Test Data Input	In	
A94	JTAG_TRST_1V8	JTAG Test Reset,	In	
A95	JTAG_EN_1V8	JTAG chain enable	In	
A96	GND	Ground	GND	Ground
A97	V_1V8	Power Out (1.8 V)	PWR-Out	Power Out
A98	V_1V8	Power Out (1.8 V)	PWR-Out	Power Out
A99	V_1V8	Power Out (1.8 V)	PWR-Out	Power Out
A100	GND	Ground	GND	Ground

Pin	Signal	Description	Type	Comment
A101	V_3V0_VBAT	Power IN	PWR-In	Power IN from carrier to the RTC device on module.
A102	V_3V3	Power Out (3.3 V)	PWR-Out	Power Out
A103	V_3V3	Power Out (3.3 V)	PWR-Out	Power Out
A104	GND	Ground	GND	Ground
A105	VCC_12V	Power IN (12 V)	PWR-In	Power IN from carrier board
A106	VCC_12V	Power IN (12 V)	PWR-In	Power IN from carrier board
A107	VCC_12V	Power IN (12 V)	PWR-In	Power IN from carrier board
A108	VCC_12V	Power IN (12 V)	PWR-In	Power IN from carrier board
A109	VCC_12V	Power IN (12 V)	PWR-In	Power IN from carrier board
A110	GND	Ground	GND	Ground

The following table lists the pin assignment of the KSwitch M20 module's interface connector pins Row B (1-110)

Table 23: Carrier Interface Connector Row B (1 to 110) Pin Assignment

Pin	Signal	Description	Type	Comment
B1	GND	Ground	GND	Ground
B2	PHY_MDI0+	Ethernet PHY MDI0+	In/Out	Ethernet PHY MDI differencial pair 0
B3	PHY_MDI0-	Ethernet PHY MDI0-	In/Out	
B4	GND	Ground	GND	Ground
B5	PHY_MDI1+	Ethernet PHY MDI1+	In/Out	Ethernet PHY MDI differencial pair 1
B6	PHY_MDI1-	Ethernet PHY MDI1-	In/Out	
B7	GND	Ground	GND	Ground
B8	PHY_MDI2+	Ethernet PHY MDI2+	In/Out	Ethernet PHY MDI differencial pair 2
B9	PHY_MDI2-	Ethernet PHY MDI 2-	In/Out	
B10	GND	Ground	GND	Ground
B11	GND	Ground	GND	Ground
B12	PHY_MDI3+	Ethernet PHY MDI3+	In/Out	Ethernet PHY MDI differencial pair 2
B13	PHY_MDI3-	Ethernet PHY MDI3-	In/Out	
B14	GND	Ground	GND	Ground
B15	SW_IRQ2_MIIM_1V8#	Interrupt	In	Microchip LAN969xTSN interrupt signal is active low.
B16	CAR_I2C_INT_1V8#	I2C/SMB interrupt/SMB Alert	In	Microchip LAN969xTSN I2C/SMB interrupt /SMB Alert signal.
B17	SW_FC0_UART_TXD_1V8	FLEXCOM0 UART interface	Out	Serial UART transmitter output.
B18	NC	-	-	Not Connected
B19	GND	Ground	GND	Ground
B20	SW_MDC0_CON_1V8	Switch MIIM 0 data clock	Out	Microchip LAN969xTSN MIIM controller 0 Media Dependent Clock.
B21	GND	Ground	GND	Ground
B22	SW_MDC1_1V8	Switch MIIM 1 data clock	Out	Microchip LAN969xTSN MIIM controller 1 Media Dependent Clock.
B23	GND	Ground	GND	Ground
B24	REFCLK_156M25-	Reference clock 156.25 MHZ	Out	Differential 156.25 MHz Reference clock for external PHYs.
B25	REFCLK_156M25+	Reference clock 156.25 MHZ	Out	
B26	GND	Ground	GND	Ground

Pin	Signal	Description	Type	Comment
B27	CAR_1PPS_OUT_1V8	Single ended 1 pulse per second output	Out	For external PHY time synchronization, on the carrier.
B28	DPLL0_10MHZ_OUT_1V8	DPLL0 output signal 10 MHz	Out	Reserved DPLL, leave pin open.
B29	GND	Ground	GND	Ground
B30	CAR_I2C_SCL	I2C/SMB serial data	Out	Microchip LAN969xTSN I2C/SMB serial clock. Add 10K pull-up resistor, Kontron recommends a pull-up voltage between 1.8 V and 3.3 V.
B31	GND	Ground	GND	Ground
B32	GND	Ground	GND	Ground
B33	PCIE_RX+	PCIE differential receive data	In	Reserved, leave pin open.
B34	PCIE_RX-	PCIE differential receive data	In	Reserved, leave pin open.
B35	GND	Ground	GND	Ground
B36	PCIE_CLK+	PCIe clock positive	In	Reserved, leave pin open.
B37	PCIE_CLK-	PCIe clock negative	In	Reserved, leave pin open.
B38	GND	Ground	GND	Ground
B39	SW_ETH_S0_RX-	Differential Receive Lane [0]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B40	SW_ETH_S0_RX+	Differential Receive Lane [0]+	In	
B41	GND	Ground	GND	Ground
B42	GND	Ground	GND	Ground
B43	SW_ETH_S1_RX-	Differential Receive Lane [1]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B44	SW_ETH_S1_RX+	Differential Receive Lane [1]+	In	
B45	GND	Ground	GND	Ground
B46	SW_ETH_S2_RX-	Differential Receive Lane [2]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B47	SW_ETH_S2_RX+	Differential Receive Lane [2]+	In	
B48	GND	Ground	GND	Ground
B49	SW_ETH_S3_RX-	Differential Receive Lane [3]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B50	SW_ETH_S3_RX+	Differential Receive Lane [3]+	In	
B51	GND	Ground	GND	Ground

Pin	Signal	Description	Type	Comment
B52	SW_ETH_S4_RX-	Differential Receive Lane [4]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B53	SW_ETH_S4_RX+	Differential Receive Lane [4]+	In	
B54	GND	Ground	GND	Ground
B55	SW_ETH_S5_RX-	Differential Receive Lane [5]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module..
B56	SW_ETH_S5_RX+	Differential Receive Lane [5]+	In	
B57	GND	Ground	GND	Ground
B58	SW_ETH_S6_RX-	Differential Receive Lane [6]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B59	SW_ETH_S6_RX+	Differential Receive Lane [6]+	In	
B60	GND	Ground	GND	Ground
B61	SW_ETH_S7_RX-	Differential Receive Lane [7]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B62	SW_ETH_S7_RX+	Differential Receive Lane [7]+	In	
B63	GND	Ground	GND	Ground
B64	SW_ETH_S8_RX-	Differential Receive Lane [8]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B65	SW_ETH_S8_RX+	Differential Receive Lane [8]+	In	
B66	GND	Ground	GND	Ground
B67	SW_ETH_S9_RX-	Differential Receive Lane [9]-	In	Microchip LAN969xTSN Ethernet SerDes receiver lane. AC coupled on module.
B68	SW_ETH_S9_RX+	Differential Receive Lane [9]+	In	
B69	GND	Ground	GND	Ground
B70	GND	Ground	GND	Ground
B71	USB_UD+	USB 2.0+	In/Out	USB 2.0 positive Data signals, bidirectional
B72	USB_UD-	USB 2.0-	In/Out	USB 2.0 negative Data signals, bidirectional
B73	V_5V_USB_VBUS	USB 5.0 V power distribution	Power-In	USB VBUS voltage sense input.
B74	SW_USB_PWR_EN_1V8	USB power enable	Out	USB Power enable for external devices. Active high.
B75	NC	-	-	Not Connected

Pin	Signal	Description	Type	Comment
B76	POE_CON_ESPI_SCK_3V3	eSPI Serial Clock	Out	Microchip PD69210 eSPI Serial Clock for external PoE PSE manager.
B77	POE_CON_ESPI_CS_3V3#	eSPI Chip Select	Out	Microchip PD69210 eSPI Chip select for external PoE PSE manager. Signal is active low.
B78	POE_CON_ESPI_MOSI_3V3	eSPI Master Out Slave In	Out	Microchip PD69210 eSPI Master Out Slave In for external PoE PSE manager.
B79	SW_I2C_RST_3V3#	I2C/SMB reset output	Out	Active low signal
B80	GND	Ground	GND	Ground
B81	MCU_UART_TXD_CON_1V8		Out	Reserved for debugging. Leave unconneted.
B82	SW_PHY_RST_1V8#	PHY Reset	Out	Microchip LAN969XTSN reset to external LAN PHYs, low active.
B83	POE_DIS_PORTS_3V3#	Disable all PoE ports	In	Microchip PD69210 input signal disable all PoE ports. Signal is active low.
B84	POE_SYS_OK_3V3#	PoE System OK	Out	Microchip PD69210 PoE system okay signal. Used to drive Healthy LED.
B85	MCU_DEBUG_CON_PA19_1V8	MCU Debug	In/Out	Reserved for debugging. Leave unconneted.
B86	MCU_CON_PA21_1V8	MCU Debug	In/Out	Reserved for debugging. Leave unconneted.
B87	MCU_CON_PA20_SWCLK_1V8	MCU Debug	In	Reserved for debugging. Leave unconneted.
B88	MCU_CON_PA19_SWDIO_1V8	MCU Debug	In/Out	Reserved for debugging. Leave unconneted.
B89	SMART_LED_DO_1V8	SMART LED	Out	Smart LED for the Serial data stream output. The module distributes a Smart LED bitstream.
B90	GND	Ground	GND	Ground
B91	CAR_STATUS_L2_1V8	Carrier status L2 inputs signal.	In	MCU carrier status L2 input signal. The status can be integrated into the SMART LED datastream. Add 10K pull down to carrier if not used.

Pin	Signal	Description	Type	Comment
B92	CAR_STATUS_L3_1V8	Carrier status L3 input signal.	In	MCU carrier status L3 input signal. The status can be integrated into the SMART LED datastream. Add 10K pull down to carrier if not used.
B93	JTAG_TDO_1V8	JTAG Test Data Output	Out	Reserves for debugging.
B94	SW_JTAG_CPU_RST	JTAG CPU Reset#	In	Reserved for debugging. Leave unconnected. Pull-up on module.
B95	SW_JTAG_SEL	JTAG select, selects between CPU and Test Tap controller	In	Reserved for debugging. Leave unconnected. Pull-up on module.
B96	GND	Ground	GND	Ground
B97	V_1V8	Power Out (1.8 V)	PWR-Out	Power Out
B98	V_1V8	Power Out (1.8 V)	PWR-Out	Power Out
B99	V_1V8	Power Out (1.8 V)	PWR-Out	Power Out
B100	GND	Ground	GND	Ground
B101	V_3V3	Power Out (3.3 V)	PWR-Out	Power Out
B102	V_3V3	Power Out (3.3 V)	PWR-Out	Power Out
B103	V_3V3	Power Out (3.3 V)	PWR-Out	Power Out
B104	GND	Ground	GND	Ground
B105	VCC_12V	Power In (12 V)	PWR-In	Power IN from carrier board
B106	VCC_12V	Power In (12 V)	PWR-In	Power IN from carrier board
B107	VCC_12V	Power In (12 V)	PWR-In	Power IN from carrier board
B108	VCC_12V	Power In (12 V)	PWR-In	Power IN from carrier board
B109	VCC_12V	Power In (12 V)	PWR-In	Power IN from carrier board
B110	GND	Ground	GND	Ground
MTG1	MTG1	Ground	GND	Ground
MTG2	MTG2	Ground	GND	Ground

7/Installation

The KSwitch M20 module inserts into a compatible PICMG 3.1 COMexpress (COMe) mini standard single 220-pin carrier interface connector on a custom carrier board and is secured using four screws with standoffs.

7.1. Before Installing

Before installing the KSwitch M20 module on a custom carrier board ensure that the carrier board is switched off and disconnected from the main power source. Failure to disconnect the carrier board from the main power source could result in personal injury and/or damage to the KSwitch M20 module and carrier board.

Take the clearance of the KSwitch M20 module into consideration by observing:

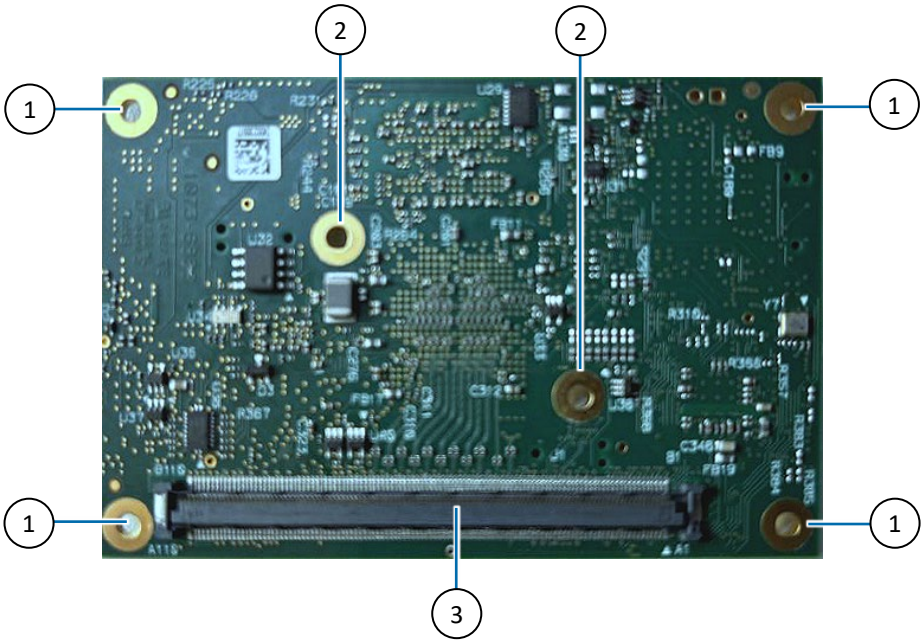
- The clearance height of carrier board's top side components and KSwitch M20 module's bottom side components must be restricted in application with vibration.
- Carrier board's interface connector height determines the stack option height (5 mm or 8 mm) and defines the clearance between the carrier board's top side and the KSwitch M20 module's bottom side surface.

Observe the following safety precautions when installing or operating the KSwitch M20 module. Kontron assumes no responsibility for any damage resulting from failure to comply with these requirements.

⚠CAUTION	**Carrier Board Switched Off** Ensure that the carrier board is switched off and disconnected from the main power supply. Failure to disconnect the carrier board's main power supply could result in personal injury and damage to the KSwitch M20 module and/or carrier board.
⚠CAUTION	**Securely Fasten** Securely fasten the KSwitch M20 module to a carrier board using appropriate retaining screws and stand-offs to ensure proper grounding and avoid loosening caused by vibration or shock.
⚠CAUTION	**Handle Carefully** Handling and operation of the KSwitch M20 module is permitted only for skilled personnel within an ESD-safe workplace with access controlled.
	**ESD Sensitive Device!** Keep electrostatic sensitive parts in their containers until they arrive at the ESD-safe workplace. Always be properly grounded when touching a sensitive board, component, or assembly.
	The KSwitch M20 module is installed on a custom carrier board. The clearance distance between the carrier board and the KSwitch M20 module cannot be specified by Kontron.
	The carrier board's interface connector must be a COM0 0.5 mm pitch free height 220-pin, 4H plug, with a stack height of 5 mm or 8 mm.

7.2. Installation and Removal Procedure

Figure 10: Mounting Features



1. 4x Mounting openings for carrier board standoffs
2. 2x Mounting openings for Heatspreader plate
3. Carrier Interface connector (module).

To install the KSwitch M20 module on a carrier board, perform the following:

1. Ensure that the carrier board is switched off properly and disconnected from the main power source.
2. Install the heatspreader plate to the top side of the KSwitch M20 module (Figure 10, pos.2) using the two screws provided with the heatspreader.
3. Insert the KSwitch M20 module's Carrier interface connector (Figure 10, pos. 3) carefully into the carrier board's corresponding interface connector and carefully press the connectors together to engage.
4. Fasten the KSwitch M20 module with heatspreader plate to the carrier board using the four mounting openings (Figure 10, pos. 1), and four screws (4x M2.5) and threaded standoffs (M2.5) with the correct height for the carrier board's connector (5 mm or 8 mm). This ensures proper grounding and avoids loosening caused by vibration or shock.
5. Remove the KSwitch M20 module from the carrier board by performing the previous steps in the reverse order.

For the Carrier Board Design Guide, visit Kontron's Customer Section .
In the Customer Section click on Switches > TSN Network > KSwitch M20 > KSwitch M20 Design Information > Design Guide KSwitch M20-xxxT.

8/Starting up

The KSwitch M20 module receives power from the 220-pin carrier interface connector. The carrier interface connector inserts into the custom carrier board's compatible 220-pin interface connector to power up.

The KSwitch M20 module must be connected to a corresponding interface connector on the custom carrier board to power up.

8.1. Before Starting Up

Before connecting the KSwitch M20 module to a carrier board, ensure that the carrier board is switched off and disconnected from the main power supply at the time of connection. Failure to disconnect the main power supply from the carrier board could result in personal injury and damage to the KSwitch M20 module and/or carrier board.

The following safety precautions must be observed when starting up or operating the KSwitch M20 module. Kontron assumes no responsibility for any damage resulting from failure to comply with these requirements.

⚠CAUTION

Carrier Board Switched Off

Ensure that the carrier board is switched off and disconnected from the main power supply. Failure to disconnect the carrier board's main power supply could result in personal injury and damage to the KSwitch M20 module and/or carrier board.

⚠CAUTION

Handle Carefully

Handling and operation of the KSwitch M20 module is permitted only for skilled personnel within an ESD-safe workplace with access control.

ESD Sensitive Device!

Keep electrostatic sensitive parts in their containers until they arrive at the ESD-safe workplace. Always be properly grounded when touching a sensitive board, component, or assembly.

8.2. Starting Up Procedure

To start the KSwitch M20 module, perform the following:

1. Install the KSwitch M20 module on the carrier board as described in Chapter 7/ Installation.
2. Connect the carrier board to the main power supply.
3. The KSwitch M20 module starts automatically when the carrier board is powered on.

9/Software Interface

The KSwitch M20 module provides direct access to the Microchip LAN969xTSN Switch with Microchip iStaX OS via a 1.8 V UART interface to manage the KSwitch M20. The UART interface is the only active management interface when the KSwitch M20 module is delivered and vital for the KSwitch M20 module's initial setup.

Kontron strongly recommends that the UART interface be made accessible on the custom carrier board as a Service Management Port, to support initial configuration and debugging.

For the Carrier Board Design Guide, visit Kontron's Customer Section .Switches > TSN Network>KSwitch M20>KSwitch M20 Design Information>Design Guide KSwitch M20-xxxT.

Kontron strongly recommends making the UART interface accessible for service usage as a Service Management Port on the custom carrier board, for first time configuration and debugging.

All software installed by the user is at the user's own risk. Kontron is not responsible for any malfunction, data loss, outage and other problems caused by software installed by the user.

Kontron is not responsible for the loss of stored, transmitted and received data. It is the user's responsibility to consider access control and protection measures required to prevent unwanted access.

9.1. Setting up the Service Management Port (COM)

UART interface configuration requires the KSwitch M20 module to be connected to and powered on via the custom carrier board, with user access to the Service Management Port (COM) serial port with the following connection:

- Serial baud rate 115200
- 8-N-1
- No flow control

To set up the KSwitch M20 module initially via the Service Management Port (COM), connect the Service Management Port to a remote computer and use software to access the Service Management Port in the category window:

1. Select <Session> and specify the <Serial Line>, <Speed> 115200 and then <Connection Type> Serial. Click on <Open>.
2. Select <Keyboard> and click on <Options>. Click on <Open>.
3. Select <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. The terminal displays the Service Management Port information.

ESD Sensitive Device!

A sudden discharge of electrostatic electricity can destroy static-sensitive devices. Keep electrostatic sensitive parts in their containers until they arrive at the ESD-safe workplace. Always be properly grounded when touching a sensitive board, component, or assembly.

Kontron recommends using PuTTY for Windows and telnet for Linux environments.

On delivery the default username is ‘admin’ and there is no password.
Username ‘admin’ cannot be removed or be changed, only it’s password.
Kontron strongly recommends assigning a strong password.

9.2. Help Tools

9.2.1. Web User Interface (UI) Help

The Web user interface (UI) supports a comprehensive help menu providing information about functions and corresponding configuration options.

9.2.2. Command Line Interface (CLI) Help

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

9.3. Configuration Examples using the CLI

The following information explains how to setup dedicated CLI features and configurations.

For more information on CLI features and configuration options, refer to the CLI Help feature. For more information, see Chapter 9.2.2: Command Line Interface (CLI) Help, above.

9.3.1. To Query DHCP assigned IP Address

The DHCP server provides the assigned IP address.

```
Starting kernel ...

00:00:00 Stage 1 booted. Starting stage2 boot @ 876 ms
/dev/mmcblk0p7: recovering journal
/dev/mmcblk0p7 primary superblock features different from backup, check forced.
/dev/mmcblk0p7: Feature orphan_present is set but orphan file is clean.
CLEARED.
/dev/mmcblk0p7: 30/90288 files (3.3% non-contiguous), 15030/360448 blocks
00:00:01 Starting application...
Using existing mount point for /switch/

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

9.3.2. Set IP Address manually via CLI and Save

In case no DHCP server is present. Set the IP address manually via CLI and save both permanently.

```
Press ENTER to get started

Username: admin
Password: <CR>

#configure terminal
```

```
EthernetSwitch(config)# interface vlan 1
EthernetSwitch(config-if-vlan)# ip address 192.168.170.60 255.255.255.0
EthernetSwitch(config-if-vlan)# end

EthernetSwitch# show ip interface
Interface Address            Method Status
--------- ------------------ ------ ------
VLAN 1    192.168.170.60/24  Manual UP

EthernetSwitch# copy running-config startup-config
```

9.4. Firmware Update

Firmware updates can be implemented using Web UI or CLI. For both methods, network access must be configured.

For the Carrier Board Design Guide, visit Kontron's Customer Section .Switches > TSN Network>KSwitch M20>KSwitch M20 Design Information>Design Guide KSwitch M20-xxxT.

To update the firmware to the KSwitch M20 module on the custom carrier board using the Web-Interface, ensure that the firmware upgrade file *.gz from the firmware package is accessible on the system running the web browser.

To update the firmware, perform the following:

1. Access the Web Interface to discover the current firmware version.
   `Monitor -> System -> Information Page.`
2. Download the firmware upgrade file ***.gz**.
3. Execute the firmware update.
   `Maintenance -> Software -> Upload page.`
4. After installing the new firmware, the KSwitch M20 reboots.
5. Previous firmware is stored as '**Alternate Image**' and the new firmware is stored as '**Active Image**'.

9.5. General Maintenance Commands

The general maintenance commands described how to show, change, delete and reload a configuration and move between levels.

The commands in this chapter are general examples and may not reflect the port configuration of your specific KSwitch M20 module, also known as Switch in this chapter.

9.5.1. Configure Terminal Command

Configure Terminal command description – Start switch configuration. Terminal display switches from **#** to (config)#.

Configure Terminal

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

9.5.2. Interface

Interface command description – Start interface (port) configuration. Terminal display switches from (config)# to (config- if)#.

To configure the same parameter for multiple interfaces use the syntax 1/1-8, this configures the same value for ports 1-8.

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)#	

9.5.3. Exit

Exit command description - Goes 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	To end in-depth configuration and go up one level, or to log out of the serial interface.	
Examples	Example#1: (config)# exit # Example#2: (config-if)# exit (config)#	

9.5.4. End

End command 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	To end in-depth configuration and go back to EXEC mode	
Examples	Example#1: (config-if)# end # Example#2: (config)# end #	

9.5.5. Show Running-Config

Show Running –Config command description - View switch running configuration. The user may change switch configuration without saving the changes. Upon switch power down-up cycle the switch may operate differently.

Show Running-Config

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	To view the current configuration	
Examples	# show running-config	

9.5.6. Show Running-Config All-Default

Show Running.Config All-Default command description - View switch running configuration plus omitted default configuration.

Show Running-Config All-Default

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

9.5.7. Dir

Dir command description - Show all optional configuration files stored inside the switch.

Dir

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

9.5.8. Copy Running-Config Startup-Config

Copy Running-Config Startup-Config command description– Updates and saves the switch configuration to be used after reset or power-up.

Copy Running-Config Startup-Config

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	To save switch configuration.	
Examples	# copy running-config startup-config	

9.5.9. Copy Running-Config Flash:<file-name>

Copy Running-Config Flash:<file-name> command 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	To copy switch configuration to another file or TFTP Server, or from TFTP Server to a switch local file.	
Examples	Example#1 - save current configuration stored in switch flash to another file named “test” also inside switch FLASH. # copy running-config flash:test Example#2 - save switch running configuration file to TFTP Server named “test”. # copy running-config tftp://192.168.0.40/test	

9.5.10. Del Flash:<file-name>

Del Flash:<file-name> command description - deletes configuration file stored in flash.

Del Flash:<file-name>

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

9.5.11. Reload Cold

Reload Cold command description – Switch performs software reset, turning Ethernet ports down and back up.

Reload Cold

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	To restart the switch	
Examples	# reload cold	

9.5.12. Reload Defaults

Reload Defaults command description – restore to full factory default configuration.

Reload Defaults

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

9.5.13. Reload Defaults Keep-IP

Reload Defaults Keep-IP command description - Semi factory defaults, keeping IP and VLAN configuration unchanged.

Reload Defaults Keep-ip

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

9.5.14. Show Version

Show Version command description – Display switch software and hardware information.

Show Version

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	To display switch information	

Examples	# show version
	
	`# show version`
	`KSwitch M20 (config-if)# do show version`
	
	`Serial Number : 0000000000`
	`MAC Address : 00-a0-a5-79-26-74`
	`Previous Restart : Cold`
	
	`System Contact :`
	`System Name : KSwitch M20`
	`System Location :`
	`System Time : xxxx-xx-xxTxx:xx:xx+xx:xx`
	`System Uptime : 5d 00:12:23`	

	Parameter	Description
	Bootloader Image :u.boot Version :HEAD-0.00-20241013221501 Date : Primary Image Image version : mmcblk0p5 (Active) Date : HEAD-0.00-20241016100112 Backup Image Image : mmcblk0p6 Version : HEAD-0.00-20241016100112 Date ----------	
	SID : 1 ----------	
	Chip ID : LAN9667 Rev. A Board type : Kontron KSWitch M20 Flash type : MMC only Port Count : 8 Product : Microchip ISTAX Switch Software Version : HEAD-0.00-20241013221501 Build Date : xxxx-xx-xxTxx:xx:xx+xx:xx Code Revision : 456ebb41 POE Version : HW Ver. :0, poemcu type:26, sw ver:3.55, param:0, build=14, internal sw#=1200, Asic Patch#=2004	

Date information is shown in the following format:

year-month-day

Time (T) hours: minutes: seconds

Example: 2026-01-30T15:30:45+00:00

9.6. TSN and PTP Management Commands

The Time-Sensitive Networking (TSN) Mangement commands are a set of IEEE 802 standards defining mechanisms for deterministic real-time communication over Ethernet networks, based on PTP timing synchronization.

9.7. Network Management Commands

The Network Management commands configure Ethernet ports Link speed, max Ethernet packet size and flow control.

The commands in this chapter are general examples and may not reflect the port configuration of your specific KSwitch M20 variant t, also known as Switch in this chapter.

9.7.1. Ethernet Ports - Configuration Commands

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

9.7.1.1. Shutdown

Description- Enable/Disable Ethernet port.

shutdown
no shutdown

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

9.7.1.2. Speed

Description- configure port speed.

speed { 1000 | 100 | 10 | auto }

	Parameter	Description
Parameter	10	10Mbps
	100	100Mbps
	1000	1000Mbps (1Gbps)

	Parameter	Description
	auto	Auto negotiation
Default	All ports are set to Auto	
Mode	Port List Interface Mode	
Usage	To set the speed of the specified interface	
Examples	Example#1 (set speed for port 1 to 100Mbps) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# speed 100 Example#2 (set all ports to 1Gbps) # configure terminal (config)# interface * (config-if)# speed 1000	

9.7.1.3. 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	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	

9.7.1.4. Flow Control

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

flowcontrol { on | off }
no flowcontrol

	Parameter	Description
Parameter	on	Enable flow control
	off	Disable flow control

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

9.7.1.5. MTU

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

mtu <max_length>

no mtu

	Parameter	Description
Parameter	<max_length>	Maximum frame size in bytes (1518-9600 bytes)
Default	Alle Ports mtu 9600 bytes	
Mode	Port List Interface Mode	
Usage	To specify the MTU frame size.	
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	

9.7.2. Ethernet Port View Commands

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

9.7.2.1. 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	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`
	
	`Interface Mode Speed&Duplex Flow Control Max Frame Excessive Link`
	`GigabitEthernet 1/1 enable Auto disable 9600 Discard 100fdx`
	`GigabitEthernet 1/2 enable Auto disable 9600 Discard Down`
	`GigabitEthernet 1/3 enable Auto disable 9600 Discard Down`
	`GigabitEthernet 1/4 enable Auto disable 9600 Discard Down`
	`GigabitEthernet 1/5 enable Auto disable 9600 Discard Down`	

9.7.3. IPv4, IPv6 – Configuration Commands

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

9.7.3.1. 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	To set the DNS for resolving domain names. Use the no version of the command to return to default.	
Examples	Example#1 (DNS Server 0 setting is derived from any DHCPv4 VLANs-ID) (config)# ip name-server 0 dhcp Example#2 (DNS Server 1 configured as a static IPv4 address) (config)# ip name-server 1 192.168.0.10 Example#3 (DNS Server 1 setting is derived from DHCPv4 VLANs-ID 1) (config)#ip name-server 1 dhcp ipv4 interface vlan 1	

9.7.3.2. 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	To add VLAN interface and set all IPv4, IPv6 parameters. Use the no version to disable the selected VLAN interface. To remove the VLAN interface completely use no interface vlan <id> from Global configuration mode.	
Examples	Example#1 (Set VLAN2 static IP address to 192.168.1.50 mask length 24) (config)#interface vlan 2 (config-if-vlan)# ip address 192.168.1.50 255.255.255.0 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) (config)#interface vlan 3 (config-if-vlan)# ip address dhcp client-id GigabitEthernet 1/1 hostname test Example#3 (Set up a fallback IP that the switch assigns itself if no DHCP is available or the DHCP is not reachable. Optionally, a custom timeout in seconds can be specified (default: 60 seconds). (config#)interface vlan 1 (config-if-vlan)#ip address dhcp fallback 192.168.1.100 255.255.0.0 timeout 120	

9.7.3.3. 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	Example#1 (add IP route to gateway 192.168.1.1) (config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1 1 Example#2 (remove IP route) (config)#no ip route 0.0.0.0 0.0.0.0 192.168.1.1	

9.7.4. IPv4, IPv6 – View Commands

9.7.4.1. 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	To display current status and configuration of the specified interface.	
Examples	Example#1 (show status and configuration for VLAN 1) # show interface vlan 1 VLAN1 Link: 00-05-5a-98-67-23 Mtu:1500 <UP BROADCAST MULTICAST> IPV4: 192.168.0.50/24 192.168.0.255 IPV6: fe80::205:5aff:fe98:6723/64	

9.7.5. NTP (Network Time Protocol) – Configuration Commands

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

9.7.5.1. 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	To enable NTP server by entering ntp command. Use a no version of the command to disable the NTP server. 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	

9.7.6. NTP (Network Time Protocol) – View Commands

9.7.6.1. 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	To view status and configuration of the NTP servers	
Examples	Example#1 #show ntp status	

9.7.7. Time Zone – Configuration Commands

Configure switch local time zone and daylight saving.

9.7.7.1. 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	To 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	

9.7.8. 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	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	To 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	

9.7.9. Time Zone – 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	To display clock information	
Examples	Example # show clock detail	

9.7.10. 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 can filter some of the SysLog messages sent by the switch, by configuring the severity/importance SysLog.

9.7.10.1. 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	To enable the SysLog server, specify its address and the level of messages to 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	

9.7.11. SysLog Report – View Commands

9.7.11.1. 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	To 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	

9.7.12. MAC Table Learning – Configuration Commands

Provides options regarding the way MAC address learning is processed by the Ethernet Switch, and how to process a packet with unknown source MAC address, unknown destination MAC address, etc. When received, a packet is classified by the packet's Source-MAC, Destination-MAC, VLAN-ID and Port number. As part of the 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 the same VLAN.

9.7.12.1. 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 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	To set MAC address table aging time in seconds. Use the no version 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	

9.7.12.2. MAC Address-Table Learning

Description - Each port can perform 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	To 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.	
Examples	Example#1 (Set MAC address learning to Secure on port 1) (config)# interface GigabitEthernet 1/1 (config-if)#mac address-table learning secure	

	Parameter	Description
	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	

9.7.13. MAC Address-Table Static

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	To assign a static MAC address to a port. Use the no version of the command to remove the MAC address.	
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	

9.7.14. MAC Table Learning – View Commands

9.7.14.1. 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	To 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 ½ Example#4 (display all MAC table entries) #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
```

9.7.15. Routing – View Commands

9.7.15.1. 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	To display routing information	

Examples	Example
	`#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`
	`#`	

9.8. Access Control/Security Management Commands

The access control and security management commands define access to the switch, the type of network interface and who will verify remote user username and password (switch locally, or Authentication Server).

The commands in this chapter are general examples and may not reflect the port configuration of your specific KSwitch M20 variant, also known as Switch in this chapter.

9.8.1. Local Users - Configuration Commands

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

9.8.1.1. 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	To 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 Kswitch M20 is delivered with default username 'admin' and with no password.
It is strongly recommended to assign a strong password.
Username 'admin' cannot be removed or be changed, only its password

9.8.2. Local Users - View Commands

9.8.2.1. 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	To display information about all local user accounts	

Examples	Example
	`# show user-privilege`
	`Username admin privilege 15 Password encrypted 64d0dfc93d6b24b6ad00 0dc81cb0e9865f737d4d7d1fb8e83be6cb687dd5fce85a26d9d21a754b753d1a1`	

9.8.2.2. Show Users

Description- Display information on how remote users is 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	To display information on how remote users are connected	

Examples	Example
	`# show users`
	`Line is con 0`
	`  You are at this line now.`
	`  Connection is from consol`
	`  User name is admin`
	`  Privillage is 15`
	`  Elapsed time os 0 day 0 hour 5 min 5 sec`
	`  Idel 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`
	`  Privillage is 15`
	`  Elapsed time os 0 day 0 hour 5 min 5 sec`
	`  Idel time is 0 day 0 hour 0 min 0 sec`	

9.8.3. Web Server - Configuration Commands

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

9.8.3.1. 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	To 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	

9.8.3.2. 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 are contained in the input URL string, they should be percent-encoded: space!\"#$%&'()*+,/:;<=>?@[\\]^`{|}~ A valid file name is a text string from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The max. length is 63 and hyphen must not be first character. A file name containing only '.' 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	To manage the HTTPS certificate (PEM format)	
Examples	Example#1 (upload the HTTPS certificate from TFTP server) (config)# ip http secure-certificate upload tftp://10.9.52.103/test_ca.pem	

	Parameter	Description
	Example#2 (delete current certificate) (config)# ip http secure-certificate delete	

9.8.4. Web Server - View Commands

9.8.4.1. 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	To display the secure HTTP web server status	

Examples	Example
	`# show ip http`
	`Switch secure HTTP web server is enabled`
	`Switch secure HTTP web redirection is enabled`
	`Switch secure HTTP certificate is presented`	

9.8.5. 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 entered by the user over the console, Telnet or SSH.

9.8.5.1. 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 the remote user by any of the three authentication servers rejects 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 disables the 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	To configure the user authentication method for a specific management interface. Use the no version of the command to disable the interface.	
Examples	Example#1 (configure SSH to be authenticated 1st by RADIUS Server. In case the RADIUS Server is down, then by the TACACS Server, and in case the TACACS Server is also down, then to be authenticated locally). (config)#aaa authentication login ssh radius tacacs localconfig)# aaa authentication login ssh radius tacacs local Example#2 (disable Telnet remote access) (config)# no aaa authentication login telnet	

9.8.5.2. 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	To configure accounting method and reporting. Use the no version of the command to disable accounting.	
Examples	Example#1 (configure accounting for ssh to report all CLI activity and any login/logout) (config)# aaa accounting ssh tacacs commands 15 exec Example#2 (disable accounting for Telnet) (config)# no aaa accounting telnet	

9.8.6. Telnet/SSH/Web - View Commands

9.8.6.1. 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	To display the current status of authentication, authorization and accounting.	

Examples	Example
	`# show aaa`
	`Authentication :`
	`  Console : Local`
	`  telnet  : disable`
	`  ssh  : radius tacacs local`
	`  web  : local`
	`Authentication :`
	`  Console : no, commands disabled`
	`  telnet  : no, commands disabled`
	`  ssh  : no, commands disabled`
	`Authentication :`
	`  Console : no, commands disabled, exec disabled`
	`  telnet  : no, commands disabled, exec disabled`
	`  ssh  : tacacs, commands 15 enabled, exec enabled`	

9.8.7. Access Control List - Configuration Commands

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

9.8.7.1. Access Management

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

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	
Usage	To 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	Example#1 (configure access management entry 1 on VLAN4 for IPv4 address 192.168.0.40 – 192.168.0.70 on all interfaces) (config)# access management 1 4 192.168.0.40 to 192.168.0.70 all Example#2 (disable access management entry 1) (config)# no access management 1	

9.8.8. Access Control List - View Commands

9.8.8.1. 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	To display access management status and all entries or statistics or a specific entry.	
Examples	Example#1 (show access management configuration)	

```
# show access management
Switch access management mode is disabled
W: WEB/HTTP
S: SNMP
T: Telnet/SSH
Idx  VID  Start IP Adress   End IP Address     W S T
---  ---  ----------------  ---------------    - - -
1    4    192.168.0.40      192.168.0.70       Y Y Y
```

	Parameter	Description
	Example#2 (show access management statistics) #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	

9.9. VLAN Management Commands

The VLAN access port is a means to split switch ports into sub port groups while each group is totally isolated from the other as if using two or more independent switches. The splitting is achieved 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 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 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

VLAN Port Type	Description
Unaware	On ingress, all frames, whether carrying a VLAN tag or not, are classified to the Port VLAN, and possible tags are not removed on egress.
Type-C	On ingress, frames with a VLAN tag with TPID = 0x8100 are classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame is classified to the Port VLAN. If frames must be tagged on egress, they are tagged with a C-tag.
Type-S	On ingress, if frames must be tagged, they will be tagged with an S-tag. On ingress, frames with a VLAN tag with TPID = 0x88A8 are 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, frames without this TPID are dropped. If the S-port is configured to accept Untagged Only frames, S-tagged frames are 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 are classified to the VLAN embedded in the tag instead of the port VLAN ID.
Type-S-Custom-Port	On egress, if frames must be tagged, they are 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 are 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, frames without this TPID are dropped. If the Custom S-port is configured to accept Untagged Only frames, custom S-tagged frames are 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 are classified to the VLAN embedded in the tag instead of the port VLAN ID.

If the S-port is configured to accept Tagged and Untagged frames, frames with a C-tag are treated like frames with an S-tag.

The commands in this chapter are general examples and may not reflect the port configuration of your specific KSwitch M20 variant, also known as Switch in this chapter.

9.9.1. 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	To 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	

9.9.2. 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	To specify the ethertype/TPID for Custom S-Ports	
Examples	Example#1 (Set TPID=8888) (config)# vlan ethertype s-custom-port 0x8888 Example#2 (Set TPID back to default 88A8) (config)# no vlan ethertype s-custom-port	

9.9.2.1. 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 as access
	trunk	Configure a switch port mode as trunk
	hybrid	Configure a switch port mode as hybrid
Default	The switch port default mode is access	
Mode	Port List Interface Mode	
Usage	To 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	

9.9.2.2. 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	

9.9.2.3. 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	

	Parameter	Description
Usage	To 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	

9.9.2.4. 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	To 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	

9.9.2.5. 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.

	Parameter	Description
Default	All VLANs are allowed (1-4095)	
Mode	Port List Interface Mode	
Usage	To 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	

9.9.2.6. 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	To 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	

9.9.2.7. 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	To 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	

	Parameter	Description
	(config)# interface GigabitEthernet 1/4 (config-if)# switchport mode hybrid (config-if)# switchport hybrid native vlan 5	

9.9.2.8. 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, independent of a tagged or untagged received frame, port adds a tag (based on PVID) to the frame and then forwards 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	To 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 (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid port-type unaware	

9.9.2.9. 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	To 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	

	Parameter	Description
	(config-if)# switchport hybrid ingress-filtering	

9.9.2.10. 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	To 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	

9.9.2.11. 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	To 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	

9.9.2.12. Switchport Hybrid Allowed VLAN

Description- Ports in Hybrid mode may control which VLANs they are allowed to become members of. By default the Hybrid port becomes 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	To 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	

9.9.3. View VLAN Members

9.9.3.1. 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	To 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	

9.9.4. View VLAN Ports

9.9.4.1. 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	To 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	

9.10. Spanning Tree

The Spanning Tree Protocol (STP), and variations [Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP)], prevents possible Network loops that without STP causes broadcast storming. STP 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 make sure that at any given time only one path out of multiple possible loops is active, thus allowing the switch to use multiple backup paths in case main connection path go down.

The commands in this chapter are general examples and may not reflect the port configuration of your specific KSwitch M20 variant, also known as Switch in this chapter.

9.10.1. STP Bridge Configuration Commands

9.10.1.1. 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	To 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	

9.10.1.2. 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 BPDU information. 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	To configure STP system settings. Use the no version of the command to revert to default.	
Examples	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	

	Parameter	Description
	(config)# spanning-tree mst max-age 25 forward-time 16 (config)# spanning-tree mst max-hops 25 (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	

9.10.1.3. 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	To configure STP CIST settings for the specific physical and aggregated ports. Use the no version of the command to revert to default.	

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

9.10.2. STP Bridges View Commands

9.10.2.1. Show Spanning-Tree

Description- Provides 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	To 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	

9.11. Port Mirroring

The commands in this chapter are general examples and may not reflect the port configuration of your specific KSwitch M20 variant, also known as Switch in this chapter.

9.11.1. Port Mirroring Configuration

The port mirroring management commands allow 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.

9.11.1.1. 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	To 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	

9.11.1.2. 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	

	Parameter	Description
Mode	Global Configuration Mode	
Usage	To configure which Switch ports to mirror, and to which port to mirror it to. Disable MAC address learning for the destination port.	
Examples	Example (Set port 11 as a destination port to mirror received frames only on ports 1-5) # 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	

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

9.12. System Information Management Commands

The system information commands such as the numerous “# show” commands, can be used to extract information regarding the system or interface status. numerous “show” commands, can be used to extract information about system or interface status.

The commands in this chapter are general examples and may not reflect the port configuration of your specific KSwitch M20 variant, also known as Switch in this chapter.

9.12.1. Read Phy Temperature

```
Show thermal-protect
```

9.12.2. Interface Status

The Interface status depends on the switch’s Ethernet port configuration. The following examples are for different port interface outputs.

Example 1.

```
# show interface * status

EthernetSwitch# show interface * status
Interface  Mode     Speed   Aneg       Link    Operational Warnings
---------- -------- ------- ---------- ------- --------------------
Fa 1/1     Enabled  Auto    Yes        100fdx
Fa 1/2     Enabled  Auto    Yes        Down
Fa 1/3     Enabled  Auto    Yes        Down
Fa 1/4     Enabled  Auto    Yes        Down
Fa 1/5     Enabled  Auto    Yes        Down
Fa 1/6     Enabled  Auto    Yes        Down
Fa 1/7     Enabled  Auto    Yes        Down
Fa 1/8     Enabled  Auto    Yes        Down
Fa 1/9     Enabled  Auto    Yes        Down
Fa 1/10    Enabled  Auto    Yes        Down
Fa 1/11    Enabled  Auto    Yes        Down
Fa 1/12    Enabled  Auto    Yes        Down
Fa 1/13    Enabled  Auto    Yes        Down
Fa 1/14    Enabled  Auto    Yes        Down
Fa 1/15    Enabled  Auto    Yes        Down
Fa 1/16    Enabled  Auto    Yes        Down
Fa 1/17    Enabled  Auto    Yes        Down
Fa 1/18    Enabled  Auto    Yes        Down
Fa 1/19    Enabled  Auto    Yes        Down
Fa 1/20    Enabled  Auto    Yes        Down
Gi 1/1     Enabled  Auto    Yes        Down
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
```

Example 2.

```
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
```

9.12.3. 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
```

9.12.4. 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
```

9.13. SNMP and MIB Management Commands

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.

A 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 supported MIBs for the KSwitch M20, visit Kontron's Customer Section.

9.14. Autoinstall Switch Configuration features using USB Dongle

When the KSwitch M20 module is installed on a carried board within a switch system it is possible to autoinstall the switch configuration using a USB dongle if a USB port is provided.

The commands in this chapter are general examples and may not reflect the port configuration of your specific KSwitch M20 variant, also known as Switch in this chapter.

9.14.1. Autoinstall Introduction

The autoinstall feature supports automated transfer of switch configuration from USB stick to system.
The main use-case is easy switch configuration during possible field replacements by storing configuration information on external media.

For this purpose, a USB stick is always attached to the switch. In case of field replacement, a USB stick is connected to the new unit. Switch configuration is transferred to new unit without manual operator input.
Foer protection against unauthorized modifications an optional password protection is implemented.
In detail, switch configuration files can be stored as password protected zip files on the USB stick.
This password protected zip files are handled by routines from libzip library and are therefore compatible with most zip tools.

With enabled autoinstall features, the switch checks if file on stick is different to current startup-config and if different, copies file from stick as new startup-config to system and performs reboots

9.14.2. LED L1 Autoinstall Status

The status of the autoinstall feature can be observed without logging into the system if the KSwitch M20 LED status signals have been implemented on the carrier board. The indication LED may report switch application information, including the autoinstall status.

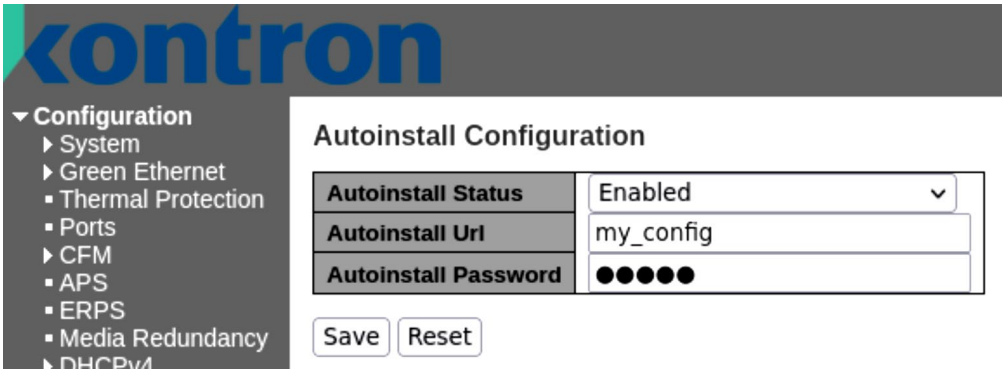
After boot, the status LED reports for two mins the autoinstall status of switch and USB stick.

9.14.3. Enable Autoinstall Feature

```
EthernetSwitch(config)# autoinstall startup-config <url> [password <password> encrypted|
unencrypted]

E.g. EthernetSwitch(config)# autoinstall startup-config usb:my_config password 1234
unencrypted
```

Figure 11: Autoinstall Configuration Screen



Encrypted/Unencrypted Parameter:

autoinstall startup-config <url> [password <password> encrypted| unencrypted]

copy startup-config <url> autoinstall [password <password> encrypted| unencrypted]

9.14.4. Disable Autoinstall Feature

```
EthernetSwitch(config)# no autoinstall startup-config
```

9.14.5. Prepare USB Storage

Run one time CLI command to format and partition (ext4) USB device.

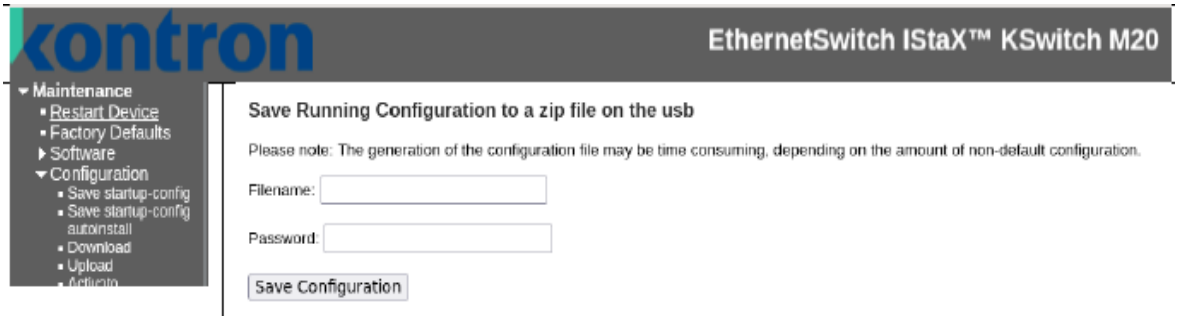
```
EthernetSwitch# format usb
```

Note: *format usb* deletes all data on USB stick without further question)

9.14.6. Generate and Store Autoinstall File on USB Storage

```
EthernetSwitch# copy startup-config <url> autoinstall [password <password> encrypted|
unencrypted]
E.g. EthernetSwitch# copy startup-config usb:my_config autoinstall password 1234
unencrypted
```

Figure 12: Store Autoinstall File Screen



9.14.7. Query Autoinstall Status

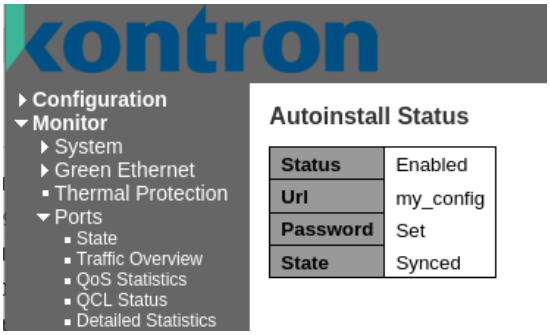
```
EthernetSwitch# show autoinstall startup-config

Autoinstall : Enabled
URL : usb:my_config
Password : Set
State : Synced
```

States:

- Not Available = not yet determined, e.g. feature just enabled, reboot not yet done
- Failed = Password does not match or file on stick is not password protected.
- Synced = Switch config on system and stick are identical.

Figure 13: Autoinstall Status Screen




```
EthernetSwitch# dir usb

Directory of USB storage device:
rw 2025-02-05 15:44:24 3325 my_config
rw 2025-02-05 15:33:31 16384 lost+found
2 files, 19709 bytes total.

USB size: 1415286784 bytes (1349.7 MiB)
USB free: 1389641728 bytes (1325.3 MiB)
USB total free: 1414807552 bytes (1349.3 MiB) (incl. reserved space)
```

9.14.8. Example 1: Prepare Autoinstall Setup Locally on Switch

For set up locally on a switch, enable the config file on switch.

e.g.:

```
EthernetSwitch(config)# autoinstall startup-config usb:my_config password 1234 unencrypted
EthernetSwitch(config)# exit
EthernetSwitch# copy running-config startup-config
EthernetSwitch# copy startup-config usb:my_config autoinstall password 1234 unencrypted
EthernetSwitch# reload cold
```

9.14.9. Example 2: Generate Password Protected Autoinstall File External, File Transfer via USB Stick

9.14.9.1. Copy running-config to USB Device

```
EthernetSwitch# copy startup-config usb:my_config_unprot
```

Disconnect USB stick from KSwitch-M20 carrier board assembly and mount it on external Linux system with adapter cable. If changed switch settings are required, edit autoinstall file.

9.14.9.2. Generate Password Protected Autoinstall File

```
[user@FC35]# cat my_config_unprot | zip -e > my_config
Enter password: 1234
Verify password: 1234
adding: my_config_unprot (deflated 77%)

[user@FC35]# ls
my_config_unprot my_config
```

9.14.9.3. Check Password Protected Autoinstall File

```
[user@FC35]# unzip -t my_config
Archive: my_config
[my_config] my_config password: 1234
testing: my_config OK
No errors detected in compressed data of my_config.
```

Remove the USB stick from external Linux system, connect it to KSwitch-M20 carrier board assembly.
The system's auto-mounter detects the USB stick automatically.

9.14.9.4. Enable Autoinstall Feature

```
EthernetSwitch(config)# autoinstall startup-config usb:my_config password 1234 unencrypted
```

9.14.9.5. Extract Password Protected Autoinstall File on External Linux System

For testing purposes, it might be helpful to extract the contents of a password-protected file on external box.

```
[user@FC35]# unzip -p my_config > my_config_unprot
[my_config] my_config password: 1234
```

9.14.10. Example 3: Copy Autoinstall Files between KSwitch M20 Module and External Linux System via Network

The switch CLI provides the possibility to copy files via network.
For environments where autoinstall files are generated on external Linux systems, it is not necessarily required to mount an USB stick on the external system.

9.14.10.1. Copy running-config to External Linux System with scp

```
EthernetSwitch# copy running-config scp://<user>:<pwd>@<host>[:port]//<path>/<file> save-
host-key
E.g. EthernetSwitch# copy running-config
scp://mst:<pwd>@192.168.170.66//opt/M20/my_config_unprot save-host-key
```

Note: for scp protocol:

```
<ip>//<path> specifies absolute path
<ip>/<path> specifies path relative to scp user home dir.
```

Other possible protocols are tftp or http.

9.14.10.2. Generate Password Protected Autoinstall File on External Box

```
[user@FC35]# cat my_config_unprot | zip –e > my_config
Enter password: 1234
Verify password: 1234
adding: my_config_unprot (deflated 77%)
```

9.14.10.3. Copy pwd Protected Autoinstall File to USB Stick on KSwitch-M20 Carrier Board

```
EthernetSwitch# copy scp://<user>:<pwd>@<host>[:port]//<path>/<file> usb:<file> save-host-
key
E.g. EthernetSwitch# copy scp://mst:<pwd>@192.168.170.66//opt/M20/my_config usb:my_config
save-host-key
```

9.14.10.4. Enable Autoinstall Feature

```
EthernetSwitch(config)# autoinstall startup-config usb:my_config password 1234 unencrypted
```

10/ Maintenance

The KSwitch M20 module contains no user serviceable hardware parts. Return the KSwitch M20 module to Kontron for maintenance and repair, see Chapter 11.1: Returning Defective Merchandise.

The KSwitch M20 module's heatspreader plate and any possible additional cooling solution may become hot to touch. To avoid burn or personal injury Kontron recommends allowing the KSwitch M20 module to cool before handling the KSwitch M20 module.

Handling and Operation

⚠CAUTION

Handling and operation of the KSwitch M20 module is permitted only for skilled personnel aware of the associated dangers, within an ESD-safe workplace with access control.

ESD Sensitive Device!

Keep electrostatic sensitive parts in their containers until they arrive at the ESD-safe workplace. Always be properly grounded when touching a sensitive board, component, or assembly.

Hot Surface

Heatspreader plate and additional cooling solution can get very hot. To avoid burns and personal injury when handling the KSwitch M20 module:

- Do not touch when in operation
- Allow to cool before handling
- Wear protective gloves

For the Carrier Board Design Guide, visit Kontron's Customer Section .

In the Customer Section click on Switches > TSN Network > KSwitch M20 > KSwitch M20 Design Information > Design Guide KSwitch M20-xxxT.

10.1. Hardware Reset

The KSwitch M20 module does not include a hardware reset function. This feature is only available if the SOC's reset signal is implemented on a custom carrier board.

To reset the KSwitch M20 module, switch off by disconnecting the power properly. Then wait approximately 10 seconds before reconnecting the KSwitch M20 module to power.

11/ 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 Type Label, located on the KSwitch M20 module's rear panel.

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

11.1. 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 Kontron Support Webpage. Scroll down to the RMA (Return of Material Authorization) Procedures.
2. 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.
3. 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

4. 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 a customer caused faults and cannot be accepted as warranty repairs

5. 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.

12/ Storage and Transportation

12.1. Storage

If the KSwitch M20 module is not in use for an extended period time, disconnect the KSwitch M20 module from the power supply. If it is necessary to store the KSwitch M20 module, re-pack the KSwitch M20 module as originally delivered to avoid damage. The storage facility must meet the KSwitch M20 module's environmental storage (non-operating) requirements as stated within this user guide. Kontron recommends keeping the original packaging material for future storage or warranty shipments.

12.2. Transportation

To ship the KSwitch M20 module use the original packaging, designed to withstand impact and adequately protect the KSwitch M20 module.

When packing or unpacking the KSwitch M20 module, always take shock and ESD protection into consideration and use an ESD-safe working area.

13/ Warranty

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

14/ Disposal

14.1. Disposal

Dispose of the product in accordance with country, state, or local regulations and requirements as part of your disposal and decommissioning policies or recycle the product or parts of the product for re-use after performing data sanitization to erase sensitive data stored on the product's memory devices.

When disposing of the product

- Remove any product labels from the product that could indicate ownership and provide a clue to the type of data stored on the memory device.
- Comply with your company's environmental requirements and the requirements of Waste Electrical and Electronic Equipment (WEEE) directive.
- Use data sanitization guidelines to ensure that data sensitive to your business and/or confidential or proprietary data and software is removed from the product using a data sanitization method that stops the data from being retrieved or reconstructed.

14.2. 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 becomes 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.

14.3. Data Sanitization

Data sanitization is the process of permanently erasing or destroying sensitive data on the product's memory devices to prevent unauthorized access to data sensitive to your business and/or confidential/proprietary data stored on the memory devices.

When designing a system, the user must plan for data sanitization and design in memory devices that are easier to sanitize, memory devices from manufactures that provide an effective data erasure tool or a return to factory default command.

When performing data sanitization, the user must consider if the product's memory devices contain sensitive data and develop a data sanitization plan to erase all sensitive data in accordance with country, state, or local data sanitization regulations and requirements or as part of your disposal and decommissioning policies.

Data Sanitization

Users are responsible for erasing sensitive data on memory devices in accordance with country, state, or local data sanitization regulations and requirements, or as part of your disposal and decommissioning policies.

Kontron recommends performing data sanitization when reusing the product in a different user environment, sending the product in for repair, disposing of the product or decommissioning the product.

General guidelines when performing data sanitization on memory devices containing data sensitive to your business and/or confidential/proprietary data:

- Before powering down, consider if power is required to perform data sanitization on the product's memory devices.
- When disconnected from the power source, dismantle all removable memory devices from the product and erase sensitive data.
- Volatile memory devices only store data temporarily. Data on volatile memory can be erased easily by disconnecting the power/removing the battery for approximately 24 hours.
- Non-volatile memory devices store data permanently and retain information when disconnected from power. Data on von-volatile memory must be actively erased using one of the following methods:
  - Use an accredited third-party software tool that provides an audit trail, capable of performing a complete data clean including areas such as hidden data and bad blocks not accessed by general service-based utilities.
  - Use the physical destruction methods on memory devices that cannot be securely software erased. The aim of the destruction is to break the silicon die within the chips package into two or more parts to prevent reading data from the die. Fragments should be no longer than 6 mm. If this service is performed by a third party obtain destruction certificates for confirmation.
  - Use the manufacture's data erasure tool for sanitization or return to factory default command (if provided by the manufacturer). The manufactures tools and commands have been designed to fulfil the data sanitization requirement of the manufacture's specific memory device(s).
- Always verify that all sensitive data has been effectively sanitized.

Dismantle Removable Memory

Dismantle all removable memory devices and erase sensitive data for reuse by using:

- An accredited third-party software tool.
- Manufacture's data erasure tool' or 'return to factory default command'. (if provided)
- If the removable memory is not for reuse, physically destruct the memory according to data sanitization guidelines.

Erase Data

To ensure that forensic tools cannot be used to recover sensitive data:

- Use an accredited third-party software tool, with an audit trail, capable of performing a complete data clean, including areas such as hidden data and bad blocks not accessed by general service-based utilities.
- Use the manufacture's data erasure tool or return to factor default command designed to fulfil the data sanitization requirement of the manufacture's specific memory device(s).

Physical Destruction

When physically destructing the memory:

- Follow proper safety protocols.
- Break the chip packaged silicon die into two or more parts, fragments <= 6 mm.
- Check both sides as memory devices may be positioned on the rear side.
- Use a third-party destruction company providing certificates for confirmation.

14.4. Statement of Memory Volatility

The KSwitch M20 module statement of memory volatility provides the user with a detailed list of the product's memory devices and their volatility, to enable the user to develop a suitable data sanitization plan.

For the memory location on the KSwitch M20 module, see Figure 3: Top Side View.

In some cases, special tools and/or software are necessary to access the memory

The Statement of Memory Volatility is a list of the known possible memory devices and due to configuration options may differ from your delivered product.

Users are responsible for all memory devices located on the custom carrier board.

Table 24: Statement of Memory Volatility

Memory	Ref. Design Location	Memory Size[2]	Volatile	Alterable in Field[1]	Battery Backed Up	Data Type	Write Protection	Emergency Erase	Process to Clear
NOR/ FLASH	U32	2 MB	No	Yes	No	User data	No	No	No
eMMC	U15	Up to 2 GB	No	Yes	No	User data	No	No	No
DDR4	U6	Up to 2 GB	Yes	Yes	No	User data	No	No	Disconnect from power

[1] In some cases special tools and/or software are necessary to access the memory.

[2] Memory size may vary, as over time devices reach EOL or newer higher-density memory devices are introduced.

15/ Cyber Security

Cyber security is an important aspect to consider when installing, operating, maintaining and disposing of the KSwitch M20 module. This chapter provides cyber security guidelines for the user.

Security White Paper

For cyber security guidelines to protect your Kontron product from potential cyber security threats, refer to Kontron's Security White paper.

Security Measures

Kontron is not aware of the final target end user environment in which the product operates. It is not possible for Kontron to provide precise instructions for your cyber security measures. Kontron strives to provide hints for considerations for your threat analysis and to point out particular security mechanisms implemented in Kontron products.

15.1. Security Defense Strategy

When developing your security defense strategy consider implementing the following guidelines to help you effectively secure the KSwitch M20 module:

- Policies and procedures developed in association with the product's/end environment's security.
- Instructions and recommendations for periodic security maintenance activities and reporting product security incidents.
- Security network controls/setting such as firewall rules.
- Third party software tools that further protect the product.
- Authentication to access the product, limit user privileges and managing user accounts.
- Data encryption.
- Reduced number of potential security entry points.
- BIOS/OS and security updates that do not compromise the product's operation or defense in depth strategy.
- User accounts with length and complexity requirements.
- Supplied default passwords are changed.
- Limited network access (IP address range).
- Installation of anti-virus and malware software.
- Network access requirements such as VPN.

Appendix: List of Acronyms

AC	Alternating Current
AVB	Audio Video Bridge
bps	bits per second
CE	Conformitè Europëenne
COM	Communication (serial port)
COMe	Computer-on-Module Express
DC	Direct Current
DDR	Double Data rate
DHCP	Dynamic Host Configuration Protocol
DPLL	Digital Phase Locked loop
DWRR	Deficit-Weighted Round Robin
eMMC	embedded MultiMediaCard
EMC	ElectroMagnetic compatibility
ESD	ElectroStatic Discharge
FCC	Federal Communications Commission
FRE	Frame Replication and Elimination
FRU	Field Replaceable Units
GbE	Giga Bit Ethernet
GPIO	General Purpose Input Output
HSP	Heatspreader Plate
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IOT	Internet of Things
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LED	Light Emitting Diode
LLC	Logical Link Control
LPC	Limited Power Source
MAC	Medium Access Control
MCU	Micro Controller Unit
MDI	Media Dependent Interface
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Before Failure
NEBS	Network Equipment Building Systems
OSI	Open Systems Interconnection
PSU	Power Supply Unit
PXE	Preboot Execution Environment
RAM	Random Access memory
RDIMM	Registered DIMM
REACH	Registration, Evaluation, Authorization and restriction of Chemicals
RMA	Return of Material Authorization
RTC	Real Time Clock
SBC	Single Board Computer
SEL	System Event Log
ShMC	Shelf Management Controller
SMBus	System Management Bus
SMWI	System Monitor Web Interface
SOL	Serial Over LAN
SRAM	Synchronous Dynamic Random Access Memory
SSD	Solid State Drive
SSH	Secure Shell
TPM	Trusted Platform Module
UDIMM	Unregisterd DIMM
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
WEEE	Waste Electrical and Electronic Equipment
WoL	Wake on LAN

About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT) and offers individual solutions in the areas of Internet of Things (IoT) and Industry 4.0 through a combined portfolio of hardware, software and services. With its standard and customized products based on highly reliable state-of-the-art technologies, Kontron provides secure and innovative applications for a wide variety of industries. As a result, customers benefit from accelerated time-to-market, lower total cost of ownership, extended product lifecycles and the best fully integrated applications.

For more information, please visit: https://www.kontron.com

Global Headquarters

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: +49 8214 4086-0
info@kontron.com

www.kontron.de

The Power of IoT