User Guide

KSwitch R20 and KSwitch R16 Managed L2/L3 Ethernet Switch

User Guide Rev. 1.8

Doc. ID 1074-2763 -English

This page has been intentionally left blank

KSwitch R20 and KSwitch R16 – 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	21-Mar-2025	CW
1.1	Input Voltage (P1) connector updated due to pin-2 & pin-4 usage. Updates for Chapter 9.7.1.5 and a new dimension diagram.	30-Jul-2025	CW
1.2	Changes in Chapters 4.3.1 and 7.2 with Pin-2 standard and Pin-4 option	11-Aug-2025	CW
1.3	Changes in Chapters 4.3.1 and 7.2 with Pin-2 standard and Pin-4 option. Updated Table 9 LED L1 Red functions.	01-Oct-2025	CW
1.4	Updated Table 9 LED color of P1 and P2.	05-Dec-2025	CW
1.5	Updated Table 3 Pin-2 and Pin-3 for 100/10Base-T signal	10-Dec-2025	CW
1.6	In Chapter 9.7.3.2, added Example#3 Set up a fallback IP that the switch assigns itself.	08-Jan-2026	CW
1.7	In Chapter 9.1.1, added IP auto assignment address.	13-Jan-2026	CW
1.8	New Chapter 9.11.3 Mirror Data Traffic and Tag with VLAN	02-Feb-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.
⚠CAUTION	**CAUTION** indicates a hazardous situation which, if not avoided, may result in minor or moderate injury **ATTENTION** indique une situation dangereuse qui, si elle n'est pas évitée, peut entraîner des blessures mineures ou modérées.
NOTICE	**NOTICE** indicates a property damage message.
⚠	**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 and title 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.
⚠	**High sound pressure!** This symbol and title inform of the risk of high sound pressure 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.

i	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 Kontron product is equipped with a lithium battery, take the following precautions when replacing the lithium battery.

⚠CAUTION	Risk of Explosion if the lithium Battery is replaced by an incorrect Type. Dispose of used lithium batteries according to the instructions. Risque d'explosion si la pile au lithium est remplacée par une pile de type incorrect. Éliminez les piles au lithium usagées conformément aux 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 www.kontron.com/about-kontron/corporate-responsibility/quality-management.

Table of Contents

List of Tables

List of Figures

1/Introduction

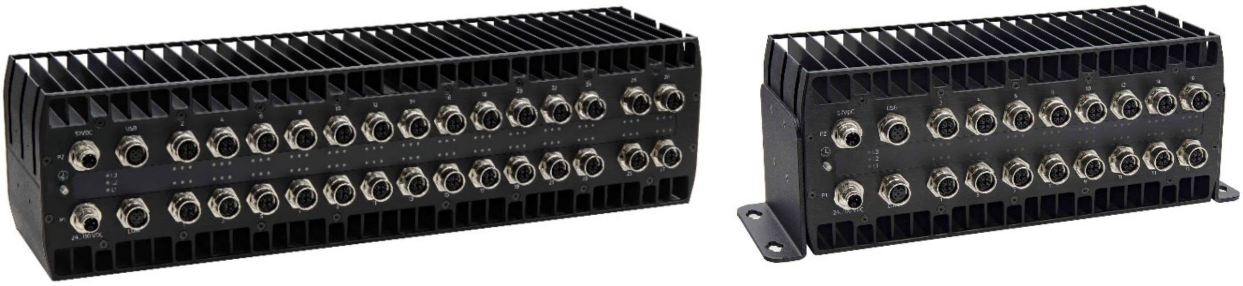
This user guide describes the KSwitch R20 and KSwitch R16 series of managed L2/L3 Ethernet switches featuring Power over Ethernet (PoE) transmission and Time sensitive Network (TSN), known as switch within this user guide. This user guide focuses on describing the switch's special features and how to set up, install, operate and maintain the switch properly. Kontron recommends new users to study the instructions within this user guide before switching on the switch.

The KSwitch R20 supports up to 28-ports and the KSwitch 16 supports up to 16-ports with Power over Ethernet (PoE/PoE+) transmission circuitry on all Ethernet ports and automatic Powered Device (PD) requirement detection. The switch's flexible port configuration supports fast Ethernet (10/100BASE-T), Gigabit Ethernet (10/100/1000BASE-T) and 10 GbE Ethernet (1000/2500/5000/10GBASE-T) ports.

The switch is designed for use within railway and rolling stock equipment according EN50155 and for operation in rugged environments requiring industrial grade temperature and IP54; where the switch can be easily and flexibly installation using two side brackets or wall mount or for 19" rack mount.

The switch offers a range of configuration options such as variable power connections (PoE 90 W or 600 W power) and real time capabilities (PTP/TSN).

Figure 1: KSwitch R20 and KSwitch R16



The KSwitch R20 and KSwitch R16 general features are:

- Based on Kontron's family of KSwitch M20 managed L2/L3 Ethernet Switch COMe modules
- Up to 28-Ethernet Ports (KSwitch R20)
- Up to 16 –Ethernet Ports (KSwitch R16)
- Ethernet port options: Fast Ethernet (10/100BASE-T), Gigabit Ethernet (10/100/1000BASE-T), 10Gigabit Ethernet (1000/2500/5000/10GBASE-T)
- PTP/TSN Time Synchronization IEEE standards including: IEEE 1588v2 & IEEE 802.1 AS-2020 for Precision timing
- Status LEDS for Ethernet ports (Activity/ Speed/ PoE)
- Serial Management Port
- Railway compliant EN50155
- Protection class IP54
- Rugged housing (448 mm x 118 mm x 106 mm)
- Industrial grade temperature range 40°C to +70°C (10 min. @ +85°C)
- Rugged -highly shock and vibration resistant
- Accepted in NEBS and ETSI installations
- Wall mountable
- Input Voltage (P1):
  - 24 VDC to 110 VDC (Wide Input Range)
  - PoE power budget of 90 W, with 30 W max. per port
- Auxiliary PoE Input Voltage (P2):
  - 50 VDC to 57 VDC
  - PoE power budget of 600 W max., with 30 W max. per port

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 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 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.
- 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 PS2 (UL/IEC 62368-1)
  - no cables or parts without insulation in electrical circuits with dangerous voltage or power should be touched directly or indirectly
  - a reliable protective 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 disconnect able
  - 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 full General Safety Instruction in English, German and French, visit Kontron's Kswitch R20 or KSwitch R16 product web pages in Downloads> Manuals> General Safety Instructions.

2.1. Instructions générales de sécurité

Veuillez lire attentivement ce passage et prendre bonne note des instructions, qui ont été compilées pour votre sécurité et pour assurer une application conforme aux réglementations prévues. Le non-respect des consignes de sécurité générales suivantes peut entraîner des blessures pour l'utilisateur et/ou des dommages pour le produit. En cas de non-respect des consignes, Kontron Europe est exonéré de la responsabilité en cas d'accident, ceci s'applique également pendant la période de garantie.

Le produit a été construit et testé conformément aux exigences de sécurité de base pour les applications basse tension (DBT) et a quitté le fabricant dans un état impeccable en matière de sécurité. Pour maintenir cet état et pour garantir également un fonctionnement sûr, l'opérateur doit non seulement respecter les conditions d'utilisation correctes du produit, mais aussi les consignes de sécurité générales suivantes :

- Le produit doit être utilisé conformément à la documentation du produit, dans laquelle sont décrites les instructions de sécurité pour le produit et pour l'opérateur. Celles-ci contiennent des directives pour la mise en place, l'installation et le montage, la maintenance, le transport ou le stockage.
- L'installation électrique sur place doit répondre aux exigences des réglementations locales spécifiques du pays.
- Si un câble d'alimentation est fourni avec le produit, seul ce câble doit être utilisé. N'utilisez pas de rallonge pour connecter le produit.
- Afin de garantir une circulation d'air suffisante pour refroidir le produit, veuillez vous assurer que les ouvertures de ventilation ne sont pas couvertes ou obstruées. Si un élément filtrant est fourni, celui-ci doit être nettoyé régulièrement. Ne placez pas le produit à proximité de sources de chaleur ou d'endroits humides. Veillez à ce que le produit soit bien ventilé.
- Ne connecter le produit qu'à une alimentation externe fournissant le type de tension (AC ou DC) et la puissance d'entrée (courant max.) spécifiés sur l'étiquette du produit Kontron et répondant aux exigences de la source d'alimentation (PS2) de UL/IEC 62368-1.
- Seuls les produits ou les pièces qui répondent aux exigences de la source d'alimentation (PS1) de la norme UL/IEC 62368-1 peuvent être connectés aux interfaces (E/S) disponibles du produit.
- Avant d'ouvrir le produit, assurez-vous qu'il est bien débranché du secteur.
- Le fait d'éteindre le produit par son bouton de mise en marche ne le déconnecte pas du secteur. Une déconnexion complète n'est possible que si le câble d'alimentation est retiré de la prise murale ou du produit. Veillez à ce que l'accès soit libre et facile pour permettre la déconnexion.
- Le produit ne peut être ouvert que pour l'insertion ou le retrait de cartes supplémentaires (selon la configuration du produit). Cette opération ne peut être effectuée que par des opérateurs qualifiés.
- Si des extensions sont effectuées, les points suivants doivent être respectés :
  - toutes les réglementations légales en vigueur et toutes les données techniques sont respectées
  - la consommation électrique d'une carte supplémentaire ne dépasse pas les limites spécifiées
  - la consommation actuelle du produit ne dépasse pas la valeur indiquée sur l'étiquette du produit.
- Seuls les accessoires d'origine approuvés par Kontron Europe peuvent être utilisés.
- Veuillez noter que la sécurité des opérations n'est plus possible lorsque l'une des conditions suivantes s'applique.
  - le produit présente des dommages visibles ou
  - le produit ne fonctionne plus. Dans ce cas, le produit doit être éteint et il faut s'assurer que le produit ne puisse plus être utilisé.

- La manipulation et le fonctionnement du produit ne sont autorisés que pour le personnel formé dans un lieu de travail dont l'accès est contrôlé.
- ATTENTION: Risque d'explosion en cas de remplacement incorrect de la pile au lithium (court-circuit, inversion de polarité, mauvais type de pile au lithium). Éliminez les piles au lithium usagées conformément aux instructions du fabricant.
- Ce produit n'est pas adapté à une utilisation dans des endroits où des enfants sont susceptibles d'être présents
- Instructions de sécurité supplémentaires pour les circuits d'alimentation en courant continu
- Pour garantir un fonctionnement sûr, veuillez observer ce qui suit:
  - l'alimentation électrique externe en courant continu doit répondre aux critères des PS2 (UL/IEC 62368-1)
  - aucun câble ou pièce non isolée dans les circuits électriques ayant une tension ou une puissance dangereuse ne doit être touché directement ou indirectement
  - une connexion à la terre fonctionnelle fiable est fournie
  - un dispositif de déconnexion approprié et facilement accessible est utilisé dans l'application (par exemple, un dispositif de protection contre les surintensités), si le produit lui-même n'est pas en mesure d'être déconnecté.
  - un dispositif de déconnexion, s'il est prévu dans le produit ou s'il en fait partie, doit déconnecter les deux pôles simultanément
  - l'interconnexion des circuits électriques de différents produits ne présente aucun risque électrique
- Un dimensionnement suffisant des fils du câble d'alimentation doit être choisi - en fonction des spécifications électriques maximales figurant sur l'étiquette du produit - comme stipulé par les réglementations EN62368-1 ou VDE0100 ou EN60204 ou UL61010-1.

2.2. Electrostatic Discharge (ESD)

A sudden discharge of electrostatic electricity can destroy static-sensitive devices or micro-circuitry. Therefore, proper packaging and grounding techniques are necessary precautions to prevent damage.
Always take the following precautions:

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 2.3: Grounding Methods.

2.3. Grounding Methods

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

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.

2.4. Thermal Conditions

The switch is passively cooled using a heatsink. There is a risk of burns or injury when touching the heatsink.

Hot Surface

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

- Do not touch the cooling fins when the switch is in operation
- Allow the switch to cool before handling
- Wear protective gloves

Surface chaude

Les ailettes de refroidissement peuvent devenir très chaudes. Pour éviter les brûlures et les blessures :

- Ne pas toucher les ailettes de refroidissement lorsque l'interrupteur est en fonctionnement
- Laisser refroidir l'interrupteur avant de le manipuler
- Porter des gants de protection

Heiße Oberfläche

Die Kühlrippen können sehr heiß werden. Um Verbrennungen und Verletzungen zu vermeiden:

- Berühren Sie die Kühlrippen nicht, wenn der Schalter in Betrieb ist.
- Lassen Sie den Schalter vor der Handhabung abkühlen
- Tragen Sie Schutzhandschuhe

3/Shipment and Packaging

3.1. Packaging

The KSwitch R20 and KSwitch R16 switch series are packaged together with all parts, in a switch specific cardboard package designed to provide adequate protection and absorb shock.

3.2. Unpacking

To unpack the switch, perform the following:

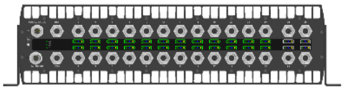
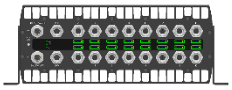
1. Remove packaging.
2. Do not discard the original packaging. Keep the original packaging for future transportation or storage.
3. Check the delivery for completeness by comparing the delivery with the original order.
4. Keep the associated paperwork. It contains important information for handling the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

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

3.3. Scope of Delivery

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: Scope of Delivery

Part	Part Number	Part Description
	1073-5327	KSwitch R20 with 24x 1GbE and 4x10GbE Ethernet 2x Side brackets 1x M12 5-pin female Coding K-power connector
	1074-7783	KSwitch R16 with 16x 1 GbE ports 2x Side brackets 1x M12 5-pin female Coding K-power connector

3.4. Accessories

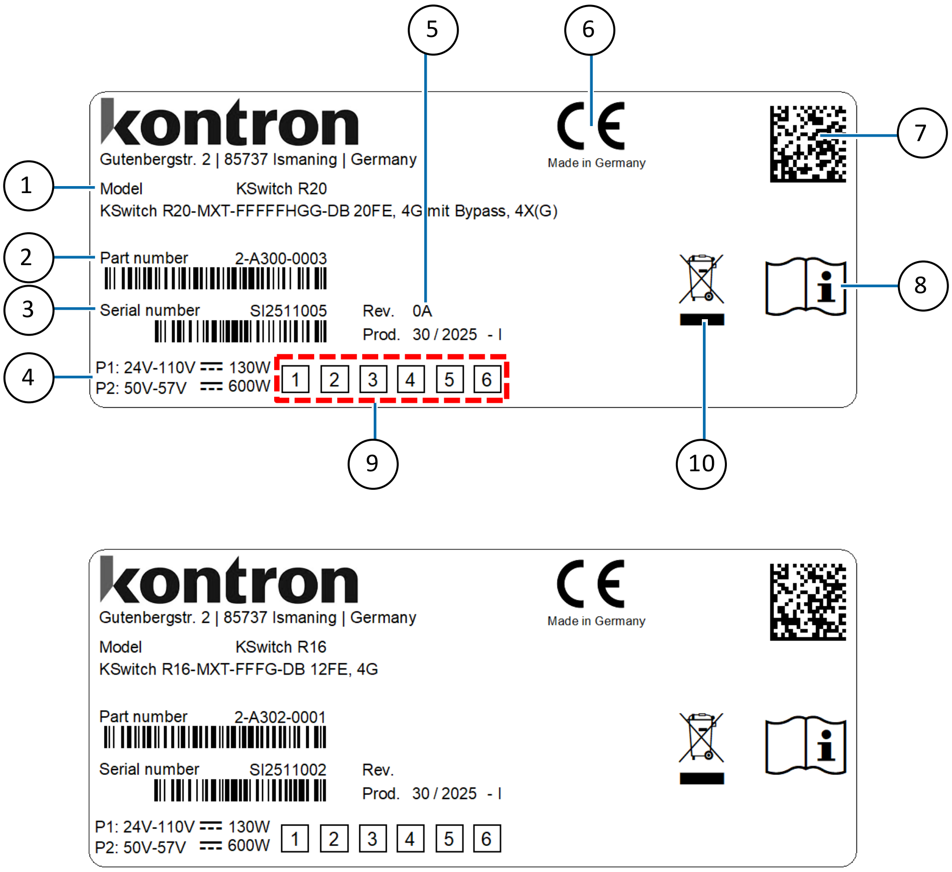
Table 2: List of Accessories

Part	Part Number	Description
	Manufacturer: Phoenix Contact Article number: 1074-7511	Product Name: M12 Connector, 4+PE poles, shielded, Push › M12 5-pin, Coding K (female) › Cable outer diameter 8 mm to 13 mm › Wire cross section of 1.5 mm^2 (max.) with ferrules or 2.5 mm^2 (max.) without ferrules › AWG 16 with ferrules or AWG 14 without ferrules
	Manufacturer: TERZ Article number: KALIBER-XS1-1100-911100	Product Name: Service Port Dongle – USB › M12. A-Coded 4-pin (male) › USB 2.0 memory stick › 8Gbit, Single-level Cell (SLC) NAND Flash › IP65/IP67 › Stainless steel housing › Length 53 mm, diameter 21.4 mm › Green Status LED (ON active, OFF no activity and Blinking data transfer)

3.5. Product Label and Product Identification

The product label contains specific KSwitch R20 or KSwitch R16 switch series technical information. The product label is located on the switch’s rear side.

Figure 2: Product Label Example



1. Product variant
   (KSwitch R20 or KSwitch R16)
2. Part Number with bar code
3. Serial Number with bar code
4. Electrical Specification
5. Revision and Production date
6. Compliance
7. QR Code
8. Read product information
9. Internal production markings
10. Dispose of properly

4/Switch Features

Before implementing the KSwitch R20 or KSwitch R16 switch series, Kontron recommends new users to take a few minutes to learn about the switch's various features.

4.1. Faceplate Features

The faceplate features the Ethernet ports each with three indication LEDs with a border. The Ethernet ports support Fast Ethernet (10/100BASE-T), Gigabit Ethernet (10/100/1000BASE-T) and 10 Gigabit Ethernet (100/1000/2500/ 5000/ 10GBASE-T) ports. The two power connectors (P1 & P2) support three Indication LEDs (L1, L2, L3) to display power and application status. The USB port and COM port provide user service management.

NOTICE

M12 Connector are IP54 compliant

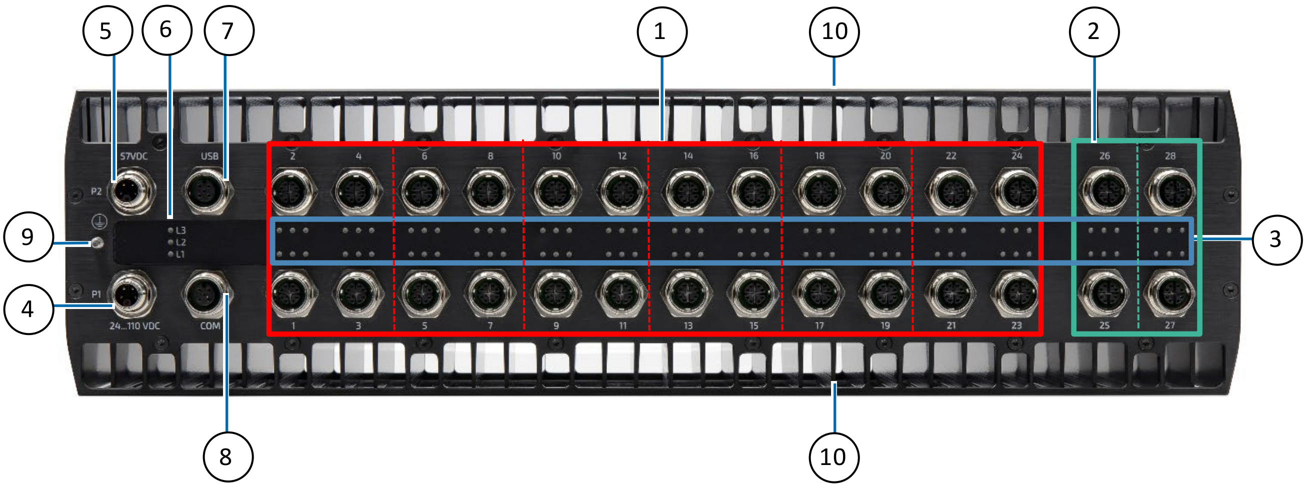
All faceplate connectors are M12 connectors and IP54 compliant.

NOTICE

M12 Mating Connector

For railway rolling stock installation, the implemented mating connector must be lockable.

Figure 3: Faceplate [1-28] Port Example



1. Ports [1-24] Fast Ethernet (10/100BASE-T), with M12-D connector(s) **or** Gigabit Ethernet (10/100/1000BASE-T), with M12-X connector(s)
2. Ports [25-28] 10Gigabit (100/1000/2500/5000/10GBASE-T) with M12-X connector(s)
3. 3x LED indicators per port with encompassing border
4. 1x Input Voltage (P1) 24 VDC to 110 VDC, (PoE Budget 90 W) with M12-K connector
5. 1x Auxiliary PoE Input Voltage (P2) 50 VDC to 57 VDC, (PoE Budget 600 W) with M12-L connector
6. 3x Indicator LED (L1, L2, L3)
7. 1x USB port M12 lockable connector
8. 1x Serial Management port (COM RS232) M12-A connector
9. 1x Protective earth stud (M4)
10. Cooling fins

Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) are not interchangeable and connect to differently rated external DC power supplies. Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) have different connector types to prevent incorrect power cable connection.

4.2. Ethernet Ports

The Ethernet ports each support three LEDs with a border encompassing the LEDs that illuminate to specify the Ethernet port type, and PoE/PoE+ transmission circuitry. The Ethernet ports options are Fast Ethernet (10/100BASE-T), Gigabit Ethernet (10/100/1000BASE-T) and 10 Gigabit Ethernet (100/1000/2500/5000/10GBASE-T).

Kontron recommends the use of cabling using supported cabling standard or better cable.

Fast Ethernet uses 4-pin M12-D connectors and Gigabit Ethernet uses 8-pin M12-X connectors. The Ethernet LEDs border indicates the port's Ethernet type.

Supported Ethernet cable for Ethernet networks connections up to 100 m/328 ft. are:

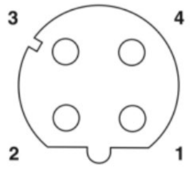
- Fast Ethernet (10/100BASE-T) CAT5e cables
- Gigabit Ethernet (10/100/1000BASE-T) CAT6a cables
- 10 Gigabit Ethernet (1000/2500/5000/10GBASE-T) CAT6a cable

4.2.1. Fast Ethernet

The fast Ethernet connectors are M12 D-Coded, female, 4-pin connectors with inner push-pull, locking thread and IP54 protection.

Connect to the fast Ethernet connectors using CAT5e cable or better.

Table 3: Fast Ethernet (10/100BASE-T) Ports Pin Assignment

M12 D-Coded Female, 4-pin	Pin	100/10BASE-T Signal	PoE/PoE+
	1	Tx+	Positive post
	3	Tx-	
	2	Rx+	Negative post
	4	Rx-	
Mating Connector	M12 D-Coded, male, 4-pin with push-pull or locking thread.		

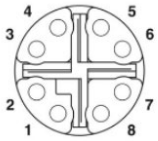
Signal	Direction/Type	Description
Tx+/-	Out	Transmit +/- 10/100BASE-T MDI differential transmit signal pair
Rx+/-	In	Receive +/- 10/100BASE-T MDI differential receive signal pair
V-52V	Power	Positive post of the PoE power supply rail
RTN	Return	Negative post (Return) of the PoE power supply rail

4.2.2. Gigabit Ethernet

The Gigabit Ethernet connectors are M12 X-Coded, female, 8-pin connectors with inner push-pull, locking thread and IP54 protection.

Connect to the Gigabit Ethernet connectors using CAT6A cabling or better.

Table 4: Gigabit Ethernet 10/100/1000BASE-T Ports Pin Assignment

M12 X-Coded Female, 8-pin	Pin	1000BASE-T Signal	10/100BASE-T Signal	PoE/PoE+
	1	BI-DA+	Tx+	Positive Post
	2	BI-DA-	Tx-	
	3	BI-DB+	Rx+	Negative post
	4	BI-DB-	Rx-	
	5	BI-DC+		
	6	BI-DC-		
	7	BI-DD+		
	8	BI-DD-		
Mating Connector	M12 X-Coded, male, 8-pin with push-pull or locking thread.			

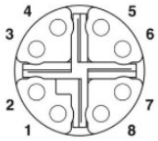
Signal	Direction/Type	Description
BI-Dx+/-	In/Out	Bi-directional pair x +/- 1000BASE-T MDI differential signal pair
Tx+/-	Out	Transmit +/- 10/100BASE-T MDI differential transmit signal pair
Rx+/-	In	Receive +/- 10/100BASE-T MDI differential receive signal pair
V-52V	Power	Positive post of the PoE power supply rail
RTN	Return	Negative post (Return) of the PoE power supply rail

4.2.3. 10 Gigabit Ethernet

The 10 Gigabit Ethernet connectors are M12 X-Coded, female, 8-pin connectors with inner push-pull, locking thread and IP54 protection.

Connect to the Gigabit Ethernet connectors using CAT6A cabling or better.

Table 5: 10 Gigabit Ethernet 1000/2500/5000/10GBASE-T Ports Pin Assignment

M12 X-coded Female, 8-pin	Pin	10G/5000/2500/1000BASE-T Signal	PoE/PoE+
	1	BI-DA+	Positive Post
	2	BI-DA-	
	3	BI-DB+	Negative post
	4	BI-DB-	
	5	BI-DC+	
	6	BI-DC-	
	7	BI-DD+	
	8	BI-DD-	
Mating Connector	M12 X-Coded, male, 8-pin with push-pull or locking thread.		

Signal	Direction/Type	Description
BI-Dx+/-	In/Out	Bi-directional pair x +/- 100/1000/2500/5000/10GBASE-T MDI differential signal pair
V-52V	Power	Positive post of the PoE power supply rail
RTN	Return	Negative post (Return) of the PoE power supply rail

4.2.4. Ethernet LED Indicators

The three Ethernet port LEDs indicate the normal operation of the switch and in case of failure may be used for faultfinding. The three LEDs are located at each Ethernet port and indicate (from left to right) the link/activity, PoE speed and connection speed.

Table 6: Ethernet Port LED Indicators

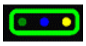
LEFT LED		Middle LED		Right LED	
Link/Act	**Description**	**PoE**	**Description**	**Speed**	**Description**
Off	Link down & no activity	Off	No Power to PD[1]	Off	No Link
On Green	Link up & no activity	On Blue	Power to PD in 2P Mode, PoE/PoE+[1]	On Yellow	10 Mbps
Flashing Green	Link up & activity	On Amber	Power to PD in 4P Mode[1]	On Amber	Link speed 100Mbps
		Flashing Amber	Power failure, see “show poe“ command for specific information	On Green	Link speed 1000Mbps, 2500Mbps, 5000Mbps
				On White	10000Mbps

[1] Powered device (PD) is a device powered by the switch functioning as a Power Source Equipment (PSE).

4.2.5. Ethernet LED Indicators Border

Each Ethernet port includes three LEDs with a border encompassing the LEDs. This board illuminates in three different colors to indicate if the port is operating as a Fast Ethernet, Gigabit Ethernet or 10 Gigabit Ethernet port.

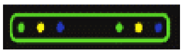
Fast Ethernet port (10/100BASE-T)



Gigabit Ethernet port (10/100/1000BASE-T)

10 Gigabit Ethernet port (100/1000/2500/5000/10GBASE-T)

If two ports are joined together, these ports support the bypass function, that is available on request.



Bypass ports

For more information, see to Chapter 0:
Bypass (on request).

4.2.6. PoE/PoE+

The PoE/PoE+ transmission circuitry is included on all Ethernet ports with a maximum of 30 W per port and automatic detection of the connected PD’s PoE type and supply class, to power the PD accordingly.

When the Input Voltage (P1) connector is connected to power the internal PoE power budget is 90 W and when the Auxiliary PoE Input Voltage Connector (P2) is connected to power the internal PoE power budget is 600 W.
When connecting PDs do not exceed the switch’s respective maximum power budget of 90 W or 600 W.

Each port provides full IEEE 802.3af/at functionality, for PoE supply classes [1 to 4]:

› Class 0 IEEE 802.3af	12.95 W at PD
› Class 1 IEEE 802.3af	3.84 W at PD
› Class 2 IEEE 802.3af	6.49 W at PD
› Class 3 IEEE 802.3af	12.95 W at PD
› Class 4 IEEE 802.3at PoE+	25.5 W at PD

Kontron recommends the use of a nominal voltage of 57 VDC to avoid possible malfunction due to undervoltage.

4.2.7. Time Sensitive Network (TSN)

The switch supports Time Sensitive Networking (TSN) for precision timing and synchronization. TSN is a number of IEEE 802 standards defining mechanisms for deterministic real-time communication over Ethernet networks.

The switch supports the following TSN standards:

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

Additional supported TSN standards not discussed in this user guide are:

- FRER (Frame Replication and Elimination (IEEE 802.1CB-2017)
- Cut-through (IEEE 802.1Qcc)
- Per-Stream Filtering and Policing (PSFP, IEEE 802.1Qci)

For more information, refer to Chapter 9.1.4: Help Tools.

4.2.8. Bypass (on request)

The switch can be equipped with a bypass function on request. In the event of a power failure, the bypass Ethernet port pairs are connected internally to ensure data communication between connected devices. The bypass Ethernet port supports a maximum network cable length of 30 m.

The bypass Ethernet ports do not support PoE/PoE+

The bypass feature is only available on request.

4.3. Power Connectors (P1 & P2)

Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) are not interchangeable and connect to differently rated external DC power supplies. Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) have different connector types to prevent incorrect power cable connection.

4.3.1. Input Voltage (P1)

The Input Voltage (P1) is the main power connection that powers the switch when connected to an external 24 VDC to 110 VDC DC power supply and supports an internal PoE power budget of 90 W. Only connect Input Voltage (P1) connector an external 24 VDC to 110 VDC DC power supply that meets the requirements specified on the switch's product label and in the electrical specification within this user guide, see Table 14: KSwitch R20 and KSwitch R16 Electrical Supply Specification.

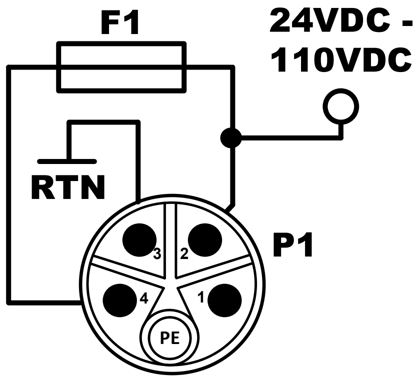
The Input Voltage (P1) is mandatory and must always be connected to an external 24 VDC to 110 VDC power supply!

The Input Voltage (P1) connector includes two VIN+ pins (Pin-2, Pin-4). Power must be supplied by connecting to only one of the Input Voltage (P1) connector's VIN+ pins. The unused VIN+ Pin must be protected against user direct and indirect contact. This is to eliminate the risk of an electrical shock as the two VIN+ Pins (Pin-2 or Pin-4) are internally connected and hazardous voltages passing through them

Kontron recommends connecting power to VIN+ Pin-2. This connection requires the use of a mandatory external fuse (Fuse Type: 10 A, 250 VDC, slow blow). If blown this fuse can be replaced by a skilled employee.

The alternative option of connecting power to VIN+ Pin-4 uses the switch's internal fuse (F1). If the internal fuse (F1) is blown, the fuse can only be replaced by returning the product to Kontron.

Figure 4: Input Voltage (P1) and Internal Fuse (F1)



DANGER

Hazardous Voltages – Input Voltage (P1) Connector

Hazardous voltages are passed through the switch between Pin-2 and Pin-4 and there is a risk of electrical shock if the user touches the unused pin contact or a connected cable. Protect the unused VIN pin against indirect or direct contact.

WARNING

Input Voltage (P1) Connector VIN+ Pins

Power must be supplied by connecting to only one of the Input Voltage (P1) connector's VIN+ pins (Pin-2, Pin-4)

WARNING

External Fuse Mandatory!

Kontron recommends connecting power to VIN+ Pin-2. In this case, a mandatory external fuse (Fuse Type: 10 A, 250 VDC, slow blow) must be used.

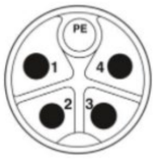
⚠WARNING

Power Source Requirements

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

The Input Voltage (P1) connector is a M12 K-coded male 5-pin connector with outer push-pull, locking thread and IP54 protection. The mating Input Voltage (P1) connector is available as a spare part, see Table 2: List of Accessories. Before wiring the mating Input Voltage (P1) connector observe the corresponding safety instructions and information included in this chapter and refer to Chapter 7.2: Wiring the Mating Input Voltage (P1) Connector.

Table 7: Input Voltage (P1) M12-K-Coded Connector Pin Assignment

M12-K Coded Male 4P+PE-Pin	Pin	Signal	Direction	Description
	1	-	-	NC
	2	VIN+	In	24 VDC to 110 VDC (Mandatory external fuse: 10 A, 250 VDC, slow blow). Kontron recommended VIN+ connection
	3	GND	Out	Ground
	4	VIN+	In	24 VDC to 110 VDC (Internal fuse (F1). Alternative VIN+ connection)
	5	PE	-	Protective Earth
Mating Connector	M12 K-Coded, female, 5-pin (4-pin + PE) with push-pull or locking thread.			

4.3.2. Auxiliary PoE Input Voltage (P2)

The Auxiliary PoE Input Voltage (P2) is optional and does not power the switch and must always be used in conjunction with the Input Voltage (P1) connector. The Auxiliary PoE Input Voltage connector (P2) increases the PoE power budget to 600 W max. when connected an external PoE power supply (50 VDC to 57 VDC, 600 W).

The Auxiliary PoE Input Voltage (P2) power connection to the switch VIN+ (POE 50 VDC – 57 VDC) always requires a mandatory external fuse (Fuse Type: 12 A, > 63 VDC, slow blow).

Due to cable resistance, power dissipation will occur, and the full PoE power budget is not delivered to the PD device. The cable resistance depends on the Ethernet cable(s) length and cannot be determined by Kontron.
The P2 power cable must not exceed the recommended maximum length of 3 m (9.84 ft.).

⚠WARNING

External Fuse Mandatory

An external fuse (Fuse Type: 12 A, > 63 VDC, slow blow) is mandatory and always required when connecting POE (50 VDC to 57 VDC) power to the Auxiliary PoE Input Voltage (P2) connector.

The P2 power cable must not exceed the recommended maximum length of 3 m (9.84 ft.).

The external PoE power supply must meet the requirements specified on the switch's product label and in the electrical specification within this user guide, see Table 14: KSwitch R20 and KSwitch R16 Electrical Supply Specification.

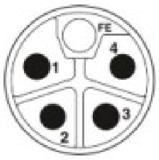
⚠WARNING

Power Source Requirements (P2)

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

The Auxiliary PoE Input Voltage connector is an M12-L code connector with IP54 protection and outer push-pull with a locking thread suitable for industrial applications and environments.

Table 8: PoE Port M12 L-Coded Connector Pin Assignment

M12 L-Coded Male 4P+FE Pin	Pin	Signal	Direction	Description
	1	VIN+	In	50 VDC to 57 VDC (external fuse) Positive post of PoE 600 W power supply
	2	GND	Out	Ground PoE Negative post of PoE 600 W power supply
	3	GND	Out	Ground PoE Negative post of PoE 600 W power supply
	4	VIN+	In	50 VDC to 57 VDC (external fuse) Positive post of PoE 600 W power supply
	5	FE		Functional Earth
Mating Connector	M12 L-Coded, female, 5-pin (4-pin + FE) with push-pull or locking thread.			

4.3.3. Indication LEDs

The three indication LEDs L1, L2 and L3 indicate the power state of the Input Voltage (P1), Auxiliary PoE Input Voltage (P2) connection and L1 indicates switch application information.

Table 9: Indication LED (L1, L2, L3)

LED Name	LED Color	LED Description
L3 (PoE P2 Status)	Off	No valid power to P2
	Blue	Valid power to P2
L2 (PoE P1 Status)	Off	No valid power to P1
	Blue	Valid power to P1
L1	Off	Switch application not running
	Green	Switch application running
	Red	Switch application critical/fatal occurred (system will restart)
	Blinking Red	Switch application error occurred (see log)
	Blinking Green	Firmware upgrade in progress
	Blinking Yellow	Auto-install feature enabled
	Blinking Green/Yellow	Auto-install status synced
	Blinking Red/Yellow (for 2 minutes)	Auto-install status failed

4.4. Protective Earth Stud

The protective earth M4 stud connects to a ground cable with an M4 ground ring of the right thickness to enable a nut with washers to secure the ground ring to the protective earth stud. The user is responsibility for supplying a ground cable of adequate length, and with a suitable M4 ground ring that complies with all applicable local, national and international grounding requirements.

⚠CAUTION

Use Proper Cabling Procedures

- Connect the ground cable to the protective earth M4 stud.
- Connect all Ethernet cables.
- Connect the power cable to the Input Voltage (P1).

⚠CAUTION

Ground Properly

The applied ground must meet the ground requirements specified in this user guide and in your local, national and international region.

Ground Cable

Ground cable requirements:

- The ground cable must be long enough to connect the switch to the electrical installation's ground connection.
- The ground cable's M4 ground ring must be the right thickness to enable a nut with washers to secure the ground ring on to the switch's protective earth stud.

4.5. Service Management Port (COM)

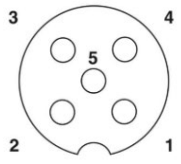
The serial service management port (COM) enables local management of the switch and provides an easy way to configure the switch using the Command Line Interface (CLI).

The COM port features are:

- RS232 (Tx and Rx signals only) without hardware flow control
- Up to 115 KBaud (default 115 kBaud)

The COM port connector is M12-A coded female 5-pin connector with inner push-pull.

Table 10: COM RS232 Port M12-A Coded 5-pin Pin Assignment

M12-A-Coded Female 5-pin	Pin	RS232 Signal	Direction	Description
	1	TXD#	Out	RS232 Transmit signal
	2	DSR	In	RS232 Data Set Ready signal (Reserved debugging only)
	3	GND	-	Filtered digital Ground, non–isolated
	4	CTS	In	RS232 Clear To Send signal (Reserved debugging only)
	5	RXD#	In	RS232 Receive signal
Mating Connector	M12 A-Coded, male, 5-pin with push-pull or locking thread.			

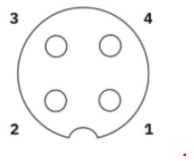
4.6. USB Port

The USB 2.0 port enables an external configuration/software update dongle to be easily attached. The dongle pairs with the switch, to enable a secure exchange of communication between the switch and dongle via an encrypted protocol.

The dongle needs no additional power supply when connected to the switch. The dongle automatically loads the stored configuration when the switch is booted and/or switched on and remains in the USB port during operation. For more information, see Table 2: List of Accessories.

The USB Port is a M12- A coded female 4-pin connector with inner push-pull.

Table 11: USB Port M12-A Coded 4-pin Pin Assignment

M12-A-Coded Female 4-pin	Pin	Signal	Direction	Description
	1	VBus	Out	+5V VBUS non-isolated
	2	D-	In/Out	USB 2.0 data signals
	3	D+	In/Out	USB 2.0 data signals
	4	GND	In	Filtered digital ground, none-isolated
Mating Connector	M12 A-Coded, male, 4-pin with push-pull or locking thread.			

4.7. Cooling Fins

The switch is passively cooled and designed to optimize heat dissipation from internal critical components to the in-built cooling fins to promote heat dissipation into the ambient environment.

To aid heat dissipation observe that airflow over the cooling fins is not obstructed as this can cause heat to build-up.

⚠CAUTION

Hot Surface

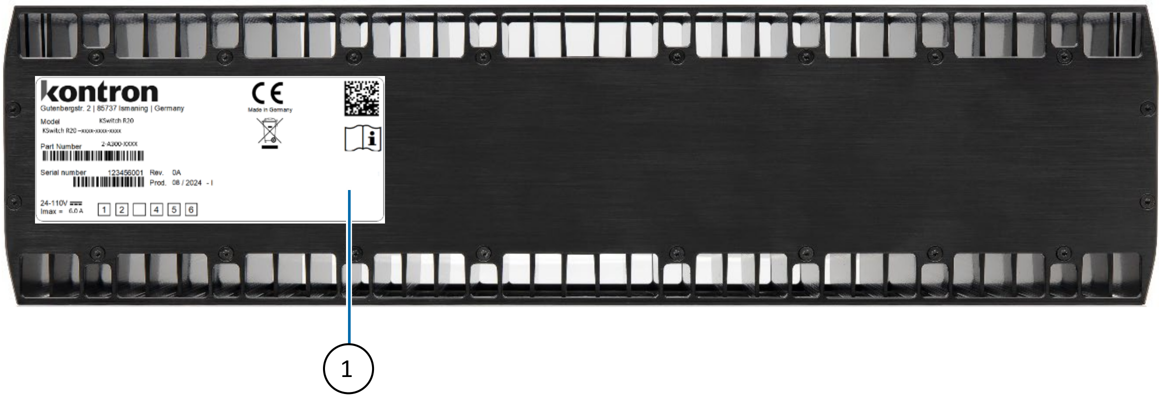
Cooling fins can get very hot. To avoid burns and personal injury:

- Do not touch the cooling fins when the switch is in operation
- Allow the switch to cool before handling
- Wear protective gloves

4.8. Rear Side Features

The rear side includes no functional features. The switch's product label is located on the rear side.

Figure 5: Rear Side



1. Kontron Product label

4.9. Internal Features

4.9.1. RTC Supercap Buffer

The Real Time Clock (RTC) is powered by a Supercap buffer that charges during operation and tracks the time and saves the CMOS settings when the switch is disconnected from the power supply or switched off. The length of time the RTC Supercap buffer holds the time information may vary, as the Supercap buffer time depends on the ambient temperature in the operating environment and the duration of the connection time to the power supply.

The supercap buffer bridges a power failure of up to 72 hours if it is connected to a power supply for 1 hour and fully charged.

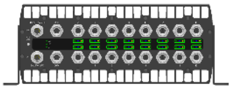
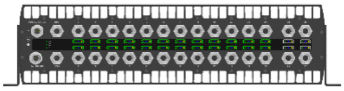
To achieve the maximum RTC Supercap buffer time:

- The Supercap must be fully loaded, this depends on how long the switch has been connected to the power supply.
- The ambient temperature must remain within the temperature limits specified in this user guide.

5/Switch Configuration Variants

The KSwitch R20 and KSwitch R16 series variants support the following standard port combinations.

Table 12: KSwitch R20 and KSwitch R16 Series Variants

KSwitch Series	Fast Ethernet (10/100BASE-T)	Gigabit Ethernet (10/100/1000BASE-T)	10 GBit Ethernet (1000/2500/5000/10GBASE-T)
KSwitch R16			
 KSwitch R16 MXT-GGGG		16-ports	
KSwitch R20			
 KSwitch R20 MXT-GGGGGGXX		24-ports[1]	4 ports

[1] On request: bypass on power fail on ports-18 and 20 or ports-22 to 24

The Ethernet ports support modular configuration enabling different KSwitch R20 and KSwitch R16 Switch Ethernet port type combinations on request.

The bypass feature providing fail-safe network access between two of the Gigabit Ethernet ports in the case of power fail, is also available on request

For more information, contact your local Kontron sales representative or Kontron Inside Sales.

6/Installing

6.1. Before Installing

Before installing the Kswitch R20 and KSwich R16 switch series, observe the standard precautions within this user guide and ensure that the installation site meets the switch's requirements as stated within this user guide. The switch is easily installed using either wall mount or 19" rack mount brackets. When installing the switch consider the orientation of the switch and take care not to obstruct the airflow over the cooling fins, as this can stop sufficient heat dissipating into the ambient environment and cause heat to build up.

⚠CAUTION

Installation Orientation

The switch may be wall mounted in four possible directions, to suit the installation site's requirements.

⚠CAUTION

Weight

When installing the switch, consider the switch's weight, a second installer may be required depending on the ease of access to the installation location:

- Always install the switch using both brackets
- Always use the specified number of screws

⚠CAUTION

Airflow and Clearance

If airflow and clearance are not considered the switch may overheat and can cause a fire or malfunction. The avoid overheating:

- Operate in a well-ventilated environment to enable heat dissipation.
- Ensure that the switch's cooling fins do not obstruct the airflow over the switch.
- Leave the specified clearance distance to prevent the switch from overheating.

⚠CAUTION

Damage due to Heat and Damp

The switch is sealed with an internal IP54 seal, to avoid damaging the switch:

- Store in a dry place.
- Do not subject the switch to direct heat
- Prevent condensation damage by avoiding large temperature variations

NOTICE

Faceplate Connectors

All faceplate connectors are IP54 compliant. Only use IP54 compliant mating connectors of the type listed in this user guide. Other connectors might cause damage to the switch.

Leave sufficient space on the switch's faceplate to access the power connector(s) and ports.

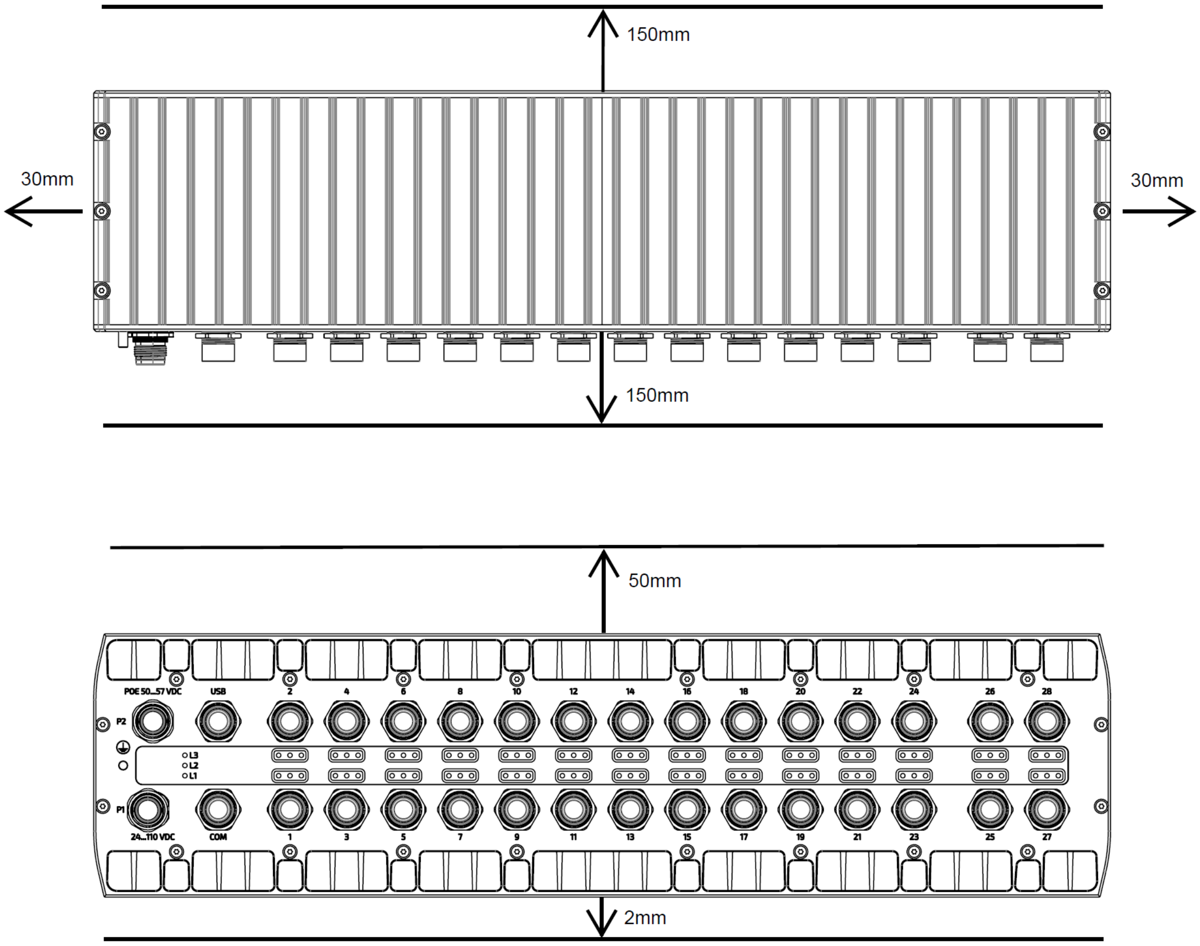
6.2. Minimum Clearance

To provide a maximum thermal airflow away from the switch, observe the minimum clearance distances to surrounding parts when installing the switch.

The faceplate clearance may be more than the minimum thermal clearance distance, due to the length of the installed faceplate connectors. The user is responsible for providing the M12 faceplate connectors, therefore Kontron cannot specify this distance within this user guide. The user is responsible for considering this requirement.

ℹ The clearance required on the faceplate may be more than the required thermal clearance due to the length of the installed faceplate connectors.

Figure 6: Minimum Clearance



6.3. Installation Procedure – Wall Mount

The two L-shaped side brackets attach to the left and right sides of the switch using two screws. Four additional screws (provided by the user) are required to install the switch on the mount surface.

⚠CAUTION

Installation Orientation

The switch may be wall mounted in four possible orientations to suit the installation site's requirements.

⚠CAUTION

Installation Mount-surface

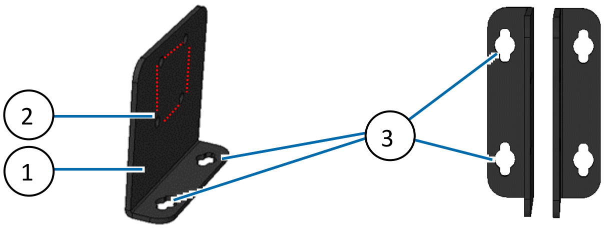
Kontron recommends installing the switch on a clean, smooth and flat mount-surface, capable of bearing the weight of the switch.

i

The four screws required to attach the switch to the mount-surface are not provided.

The user is responsible for providing screws with the required head size and length for the thickness and type of the mount-surface material

Figure 7: Side Brackets

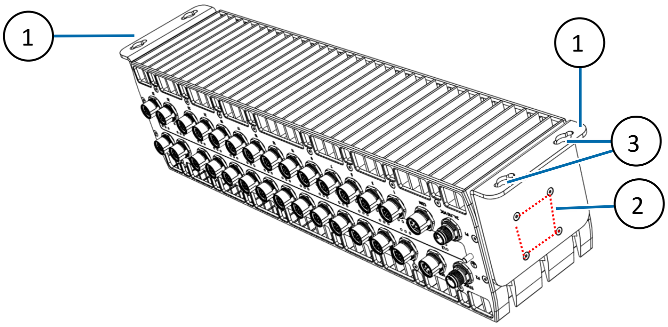


1. Side bracket(s)
2. Four symmetrical screws openings
3. Two keyhole slot openings

To install the switch to the mount-surface at the installation site using the two side brackets, perform the following:

1. Prepare the mount surface and ensure the installation site meets the switch's requirements.
2. Attach the two side brackets firmly to the switch's left and right sides, using the eight retaining screws provided with the brackets. Secure the screws with a thread locking compound to prevent loosening.
3. Measure and mark the mount-surface screw holes to match the position of the keyhole slot openings.
4. Drill the holes and secure the four screws. Leave an approx. 5 mm gap behind the screw head.
5. Slot the switch with installed side brackets over the four screws and slide the switch downwards to the narrow part of the keyhole slot. Fasten the screws and secure using a thread locking compound to prevent loosening.

Figure 8: Mounting with Two Side Brackets (bottom side facing upwards)



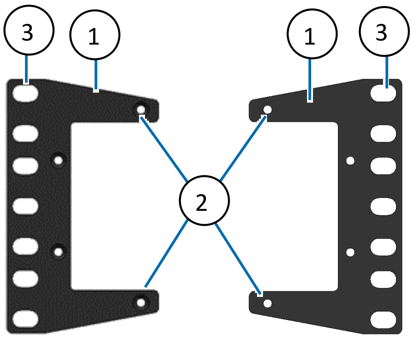
1. Two Side brackets
2. Four retaining screws
3. Two keyhole slot openings

6.4. Installation Procedure 19” Industrial Rack Cabinet

The two 19” rack brackets attach to the left and right sides of the switch with two screws. Four additional screws and cage nuts (provided by the user) are required to install the switch within a 19” industrial rack cabinet. Kontron recommends using a well-ventilated 19” industrial rack cabinet that enables air to flow over the cooling fins.

Leave the minimum clearance distance as specified within this user guide when mounting the switch on top of or below other system within the 19” industrial rack cabinet, see Chapter 6.2: Minimum Clearance.

Figure 9: 19” Rack Brackets



1. 19” Rack bracket(s)
2. Two retaining screws
3. Openings for screws and cage nuts

⚠CAUTION

Ensure Sufficient Airflow.

Ensure that the 19” industrial rack cabinet is well ventilated and supports heat dissipation and transfer away from the switch without obstructions.

⚠CAUTION

Stable 19” Industrial Rack Cabinet

Mount only in a stable 19" industrial rack cabinet and use proper installation procedures:

- Mount systems from the bottom up
- Place heavy systems lower down
- Bolt the cabinet to the floor or anchor the cabinet to the wall

⚠CAUTION

Verify Secure Mounting

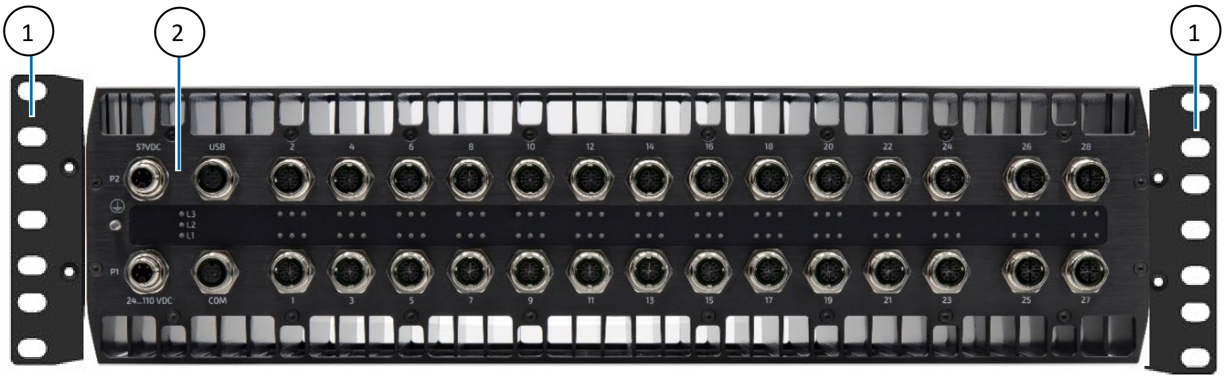
Fasten both 19” rack mount brackets to the front side posts of the 19” industrial rack cabinet using all four screws and cage nuts (to be provided by the user) to provide full support for the switch’s weight.

The four screws and cage nuts required to attach the switch to the 19” rack cabinet’s front side posts are not provided. The user is responsible for providing screws with the required head size and length.

To install the switch using the 19” rack brackets, perform the following:

1. Attach the 19” rack brackets firmly to the left and right sides of the switch using the four retaining screws provided with the brackets. Secure the screws with a thread locking compound to prevent loosening.
2. Mount the switch on both front side posts of the 19" industrial rack cabinet with secure the switch with four cage nuts and screws (2 screws per post) to be provided by user. Always use all four screws to provide full support of the switch’s weight.

Figure 10: 19” Rack Brackets Installed



1. 19” rack brackets with openings for front side post cage nuts
2. Faceplate with access to connectors

6.5. De-installing the switch

When de-installing the switch, take into consideration that the switch may be hot. Always switch off the switch properly as described in this user guide and allow the switch to cool before de-installing.

⚠CAUTION

Hot Surface

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

› Do not touch the cooling fins when the switch is in operation.
› Allow the switch to cool before handling.
› Wear protective gloves.

To de-install the switch from a wall or 19” industrial rack cabinet, perform the following:

1. Disconnect the switch from the power source properly, as described in Chapter 7.4 Switching Off.
2. Allow the switch to cool adequately.
3. Remove the Ethernet port cable(s).
4. Remove the COM port cable and the USB dongle.
5. Disconnect the ground cable from the protective earth stud.
6. De-install the switch by removing the four screws fastening the switch’s side brackets to a wall mount-surface or a 19” industrial rack cabinet.
7. When decommissioning the switch, read and adhere to the information within Chapter 14/: Disposal including the data sanitation information.

7/Starting Up

7.1. Before Starting Up

Before starting up the KSwitch R20 and KSwitch R16 series switch read the instructions in this user guide and observe the safety instructions in Chapter 2/General Safety Instructions. If connected incorrectly the switch may malfunction or short circuit damaging the switch or causing serious injury. When attaching cables check the labelling to avoid mixing up electrically incompatible connectors and ports, as this may cause unwanted behavior and damage.

The Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) power connectors connects to separate external DC power supplies that meets the requirements specified in this user guide see Chapter 8.3: Power Specification.

⚠WARNING

Power Source Requirements

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

⚠CAUTION

Switch Off and Disconnect

The switch is only properly switched off when disconnected from the external DC power supply, by removing the power cable from the Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) connectors or the external DC power supply(s).

⚠CAUTION

Access to Power Cables

The power cable connecting to Input Voltage (P1) must be easily accessible. If the operational environment restricts access to power cables, disconnection must be guaranteed using a separate cut-off fixture.

⚠CAUTION

Use Proper Cabling Procedures

1. Connect the ground cable to the protective earth M4 stud.
2. Connect all Ethernet cables.
3. Connect the power cable to the Input Voltage (P1).

⚠CAUTION

Damage

Before connecting the power cable(s), ensure that the power and ground cables and connectors show no signs of visible damage or breakage.

ℹ The Input Voltage (P1) is mandatory and must be connected to an 24 VDC to 110 VDC external DC power supply!

ℹ The P2 power cable must not exceed the recommended max. length of 3 m (9.84 ft.).

7.2. Wiring the Mating Input Voltage (P1) Connector

When wiring the mating Input Voltage (P1) connector users must only connect power to one of the Input Voltage (P1) connector VIN+ pins (Pin-2 or Pin-4). The unused VIN+ Pin must be protected against user direct and indirect contact. This is to eliminate the risk of an electrical shock as the two VIN+ Pins (Pin-2 or Pin-4) are internally connected and hazardous voltages passing through them

Kontron recommends connecting to VIN+ Pin-2. This connection requires the use of a mandatory external fuse (Fuse Type: 10 A, 250 VDC, slow blow). The alternative option is connecting to Pin-4. This connection used the switch's internal fuse (F1). For more information, see Chapter 4.3.1: Input Voltage (P1).

⚠DANGER

Hazardous Voltages – Input Voltage (P1) Connector

Hazardous voltages are passed through the switch between Pin-2 and Pin-4 and there is a risk of electrical shock if the user touches the unused pin contact or a connected cable. Protect the unused VIN pin against indirect or direct contact.

⚠WARNING

Input Voltage (P1) Connector VIN+ Pins

Power must be supplied by connecting to only one of the Input Voltage (P1) connector's VIN+ pins (Pin-2, Pin-4)

⚠WARNING

External Fuse Mandatory!

Kontron recommends connecting power to VIN+ Pin-2. In this case a mandatory external fuse (Fuse Type: 10 A, 250 VDC, slow blow) must be used.

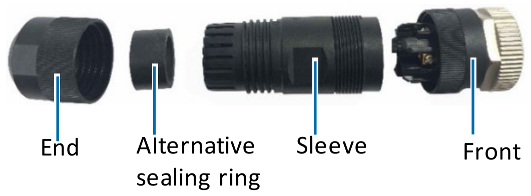
The user is responsible for wiring the Input Voltage (P1) mating connector with a suitable power cable and marking the wires clearly (+/-/Protective Earth) to ensure a proper connection from the external DC power supply. The mating Input Voltage connector (M12 K-Code) is available as a spare part, see Table 2: List of Accessories.

i

The power cable must meet the power connector's requirements of an outer cable diameter of 8 mm to 13 mm.

To wire the supplied M12 K-Code connector, perform the following:

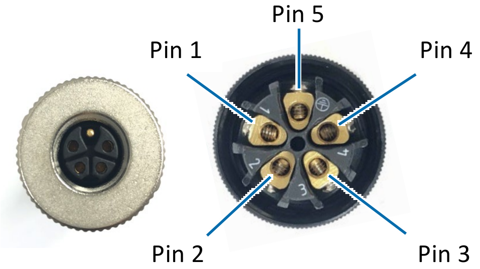
1. Open the M12 K-Code connector packaging and locate the four items included in the delivery.



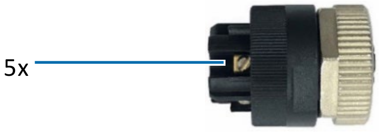
2. If required, change the pre-installed sealing ring to the alternative sealing ring. The alternative sealing ring is for cables with a diameter greater than 10.5 mm.

3. Before wiring the connector pins, insert the power cable through the M12 K-Code connector's end and sleeve.
4. Prepare the wires by removing approximately 30 mm of the power cable coating.
5. Strip each wire end by approximately 8 mm and twist the striped wire-ends.
6. Loosen the pin screws far enough to insert the end of the stripped wires.

7. Insert the corresponding stripped wire into the M12 K-Code connector pin:
   - Pin 1: NC
   - Pin 2: VIN+ (24 VDC to 110 VDC) (external fuse)
   - Pin 3: Gound
   - Pin 4: VIN+ 24 VDC- to 110 VDC (internal fuse)
   - Pin 5: Protective Earth



8. Fasten the five screws for each pin to secure the wires.



9. Close the M12 K-Code connector by screwing the front, sleeve and end securely together.

7.3. Starting up

The switch starts automatically when the Input Voltage (P1) is connected to an external DC power supply.

To start the switch, perform the following:

1. Mount the ground cables ring on the protective earth's M4 stud by inserting the ground ring followed by a washer, spring washer and M4 nut. Secure the nut.
2. Connect Ethernet cables to the Ethernet ports.
3. Prepare the M12 K-Code mating power connector with suitable wiring as described in Chapter 7.2: Wiring the Mating Input Voltage (P1) Connector.
4. Connect the power cable to the Input Voltage (P1) connector on the faceplate.
5. Connect the other end of the power cable to the external DC power source, with the required rating for the switch.
6. The switch starts automatically when connected to power and the power LED(s) illuminates as described in Table 9: Indication LED (L1, L2, L3).

7.4. Switching Off

Always switch off the switch properly as described in this user guide. When initially switched off the switch may still be hot, and users must allow the switch to cool before handling.

⚠CAUTION

Switch Off and Disconnect

The switch is only properly switched off when disconnected from the external DC power supply, by removing the power cable from the Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) connectors or the external DC power supply(s).

To switch off the switch, perform the following:

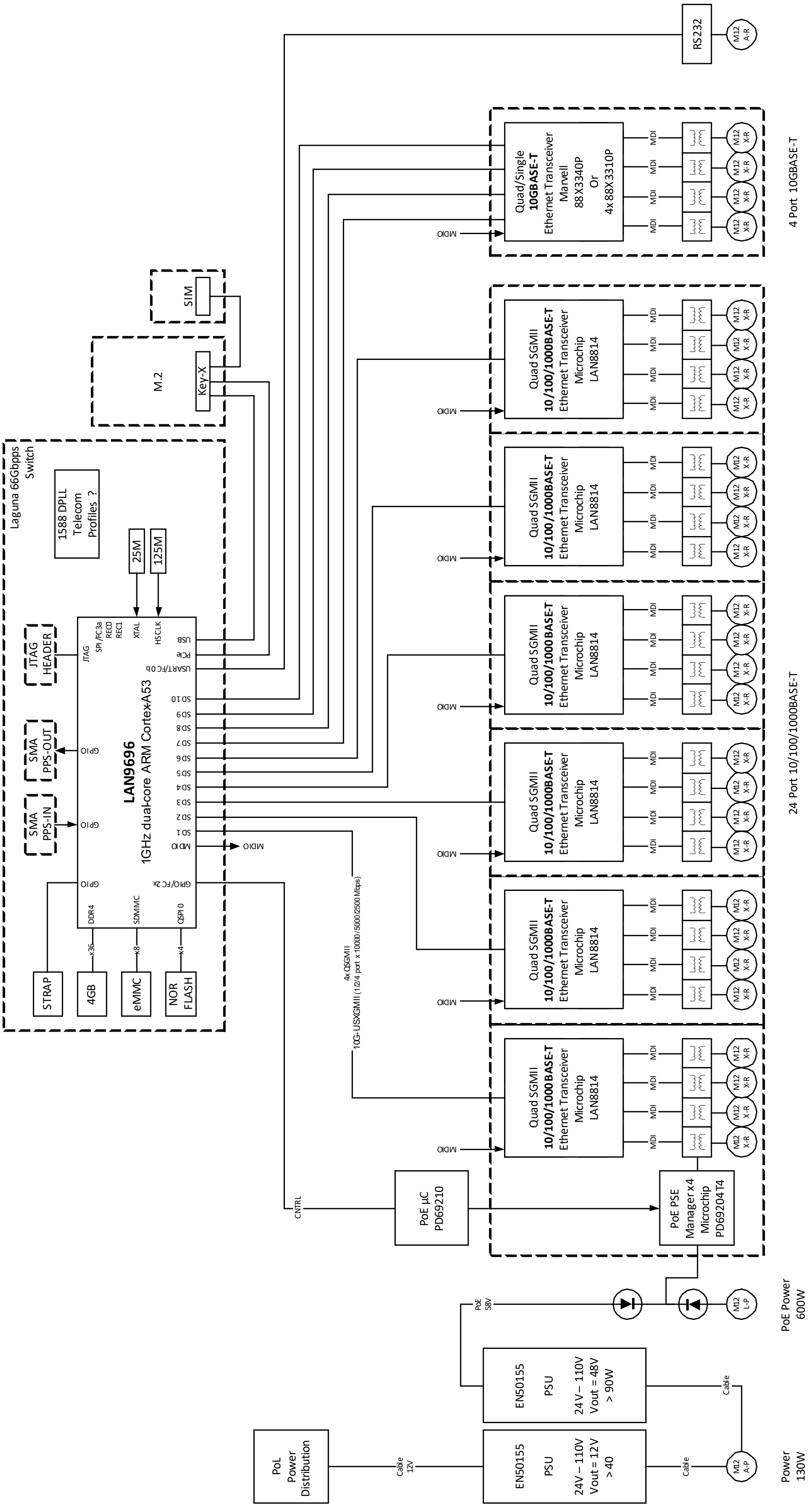
1. Disconnect the power cable from the Input Voltage (P1) connector on the faceplate or the external DC power supply.
2. Disconnect the power cable from the optional Auxiliary PoE Input voltage (P2) connector (if installed) on the faceplate or the external DC power supply.

8/Technical Specification

8.1. Functional Block Diagram

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

Figure 11: KSwitch R20 28-port Functional Block Diagram


RS232
M12 A-R
Quad/Single 10GBASE-T Ethernet Transceiver Marvell 88X3340P Or 4x 88X3310P
MDI
MDIO
M12 X-R
4 Port 10GBASE-T
SIM
M.2
Key-X
Laguna 66Gbpps Switch
1588 DPLL Telecom Profiles ?
25M
125M
JTAG HEADER
SMA PPS-OUT
SMA PPS-IN
STRAP
4GB
eMMC
NOR FLASH
LAN9696
1GHz dual-core ARM Cortex-A53
JTAG
SPI/FC3a
REC0
REC1
XTAL
HSCLK
USB
PCIe
USART/FC 0b
SD10
SD9
SD8
SD7
SD6
SD5
SD4
SD3
SD2
SD1
MDIO
GPIO
GPIO/FC 2x
DDR4
SDMMC
QSPI 0
x36
x8
x4
4x QSGMII
10G-USXGMII (1/2/4 port x 10000/5000/2500 Mbps)
Quad SGMII 10/100/1000BASE-T Ethernet Transceiver Microchip LAN8814
24 Port 10/100/1000BASE-T
CNTRL
PoE µC PD69210
PoE PSE Manager x 4 Microchip PD69204T4
PoE 58V
M12 L-P
PoE Power 600W
EN50155 PSU 24V – 110V Vout = 48V > 90W
Cable
EN50155 PSU 24V – 110V Vout = 12V > 40
Cable 12V
PoL Power Distribution
M12 A-P
Power 130W

8.2. Hardware Specification

Table 13: KSwitch R20 and KSwitch R16 Managed L2/L3 Ethernet Switch Hardware Specification

Network	Description
Device	Microchip LAN969x TSN Switch Family
OS	Microchip iStaX
Operation Mode	Store and forward, full wire-speed, non-blocking switch core Low latency cut-through forwarding mode
Port Mapping	Flexible port configuration: › 24x 1000BASE-T, 4x 10G BASE-T › 16x 1000BASE-T Basic Ethernet Port modular group: › 10/100BASE-T ports and supported multiples thereof › 10/100/1000BASE-T ports and supported multiples thereof › 1000/2500/5000/10GBASE-T ports and supported multiples thereof All with M12-D or M12-X coded push pull connectors and PoE (PSE) capability. Other port maps on request.
Ethernet Copper Ports	**Description**
Speed	Fast Ethernet (10/100BASE-T) Gigabit Ethernet (10/100/1000BASE-T) 10 Gigabit Ethernet (10GBASE-T)
MDI/MDIX Auto-crossover	Support straight or cross wired cables
Auto negotiation / Duplex	10/100/1000/2500/5000/10GBASE-T speed auto-negotiation; full & half duplex
LEDs	LEFT: **Link/Activity**: Indicated the Ethernet port's activity and link MIDDLE: **PoE Power**: Indicates if power is supplied or delivered at the port RIGHT: **Speed**: Indicated the Ethernet port's speed
Connector Type	M12 D-Code (10/100BASE-T) M12-X-Code (10/100/1000BASE-T and 100/1000/2500/5000/10GBase-T)
Cable Requirements	Cat 5e or better with 10/100BASE-T Cat 6a or better with 10/100/1000BASE-T Cat 6a or better with 100/1000/2500/5000/10GBase-T (For Ethernet networks connections up to 100 m/328 ft.)
Time Sensitive Networking (TSN)	**Description**
Shaping & Fillter	IEEE 802.1Qbv-2015 -Time Aware Shaping IEEE 802.1Qbu/802.3br -Frame Pre-emption 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 (FRER) Protection switching (line or ring)
Forwarding Scheme	Cut-through option per TSN Stream and Store and Forward
Timing & Synchronization	IEEE 802.1AS-2020 1-step and 2-step IEEE 1588v2 1-step and 2-step for ordinary, boundary and transparent clocks

Network Redundancy	Description
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
Bridge, VLAN, Protocols	**Description**
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
Network Discovery	IEEE 802.1ab LLDP
Traffic Management & QoS	**Description**
Priority	IEEE 802.1p QoS
No. of queues per port	8
Scheduling schemes	Strict Priority Queuing (SPQ) Deficit-Weighted Round Robin Queuing (DWRR)
Security	**Description**
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	**Description**
User Management	Web-based management, 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
Diagnostic	Syslog, Level Info / Warning / Error
	Port Mirror, Per VLAN mirroring, CPU Load Monitor
	Traffic Counter
	ICMP Ping
DHCP	Client Mode, Server Mode, Relay Mode, Snooping
Network Time	NTP Client
System Status	Device info/status; Ethernet port status
Green Ethernet	Port power savings

8.3. Power Specification

The Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) connectors connect to separate differently rated external DC power supplies and are not interchangeable. The external DC power supplies must fulfill the switch's specified electrical ratings as stated within this user guide and comply with the safety requirements of UL/IEC 62368-1 and the power supply requirements of EN 50155.

For Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) connector information, see Chapter 4.3: Power Connectors (P1 & P2) and the subsequent sub-chapters.

Table 14: KSwitch R20 and KSwitch R16 Electrical Supply Specification

Power Source		Description
Input Voltage (P1)	Input Voltage	24 VDC to 110 VDC
	Input Current	5.4 A max. @24 VDC
	Holdup Time	10 ms
Auxiliray PoE Input Voltage (P2)	Input Voltage	57 VDC (Range 50 VDC to 57 VDC)[1]
PoE Ports	PoE Power Budget (P1 connected)	Internal PoE Budget 90 W (30 W max. per port) With full IEEE 802.3af/at functionality
	PoE Power Budget (P1 & P2 connected)	External PoE Budget of max. 600 W (30 W max. per port) With full IEEE 802.3af/at functionality

[1] Kontron recommends the use of a nominal voltage of 57 VDC to avoid possible malfunction due to undervoltage.

⚠DANGER

Hazardous Voltages – Input Voltage (P1) Connector

Hazardous voltages are passed through the switch between Pin-2 and Pin-4 and there is a risk of electrical shock if the user touches the unused pin contact or a connected cable. Protect the unused VIN pin against indirect or direct contact.

⚠WARNING

Power Source Requirements

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

⚠CAUTION

Switch Off and Disconnect

The switch is only properly switched off when disconnected from the external DC power supply, by removing the power cable from the Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) connectors or the external DC power supply(s).

⚠CAUTION

Access to Power Cables

The power cable connecting to Input Voltage (P1) must be easily accessible. If the operational environment restricts access to power cables, disconnection must be guaranteed using a separate cut-off fixture.

⚠CAUTION

Ground Properly

Before connecting to power, connect the ground cable to the protective earth stud and ensure that the installation site's ground meets the grounding requirements specified in your local, national and international region.

NOTICE

Power Cable Dimensioning

To protect the switch and any connected devices, ensure that the power cables are sufficiently dimensioned according to the switch's maximum electrical specifications and as stipulated by EN 62368-1.

NOTICE

Hold Up Time

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

Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) are not interchangeable and connect to differently rated external DC power supplies.

Input Voltage (P1) and Auxiliary PoE Input Voltage (P2) have different connector types to prevent incorrect power cable connection.

The P2 cable must not exceed the recommended max. length of 3 m (9.84 ft.).

Due to cable resistance power dissipation occurs and the full PoE power is not delivered to the PD device. The cable resistance depends on the Ethernet cable(s) length and cannot be determined by Kontron.

8.3.1. Power Supply Protection

The external DC power supply must incorporate protection such as over current protection, inrush current protection, over voltage protection, and under voltage (brownout) protection against fluctuations and interruptions in the delivered DC power supply and the power supply requirements of EN 50155 for railway application.

8.4. Environmental Specification

The KSwitch R20 and KSwitch R16 switch series complies with the following environmental requirements.

Table 15: KSwitch R20 and KSwitch R16 Environmental Specification

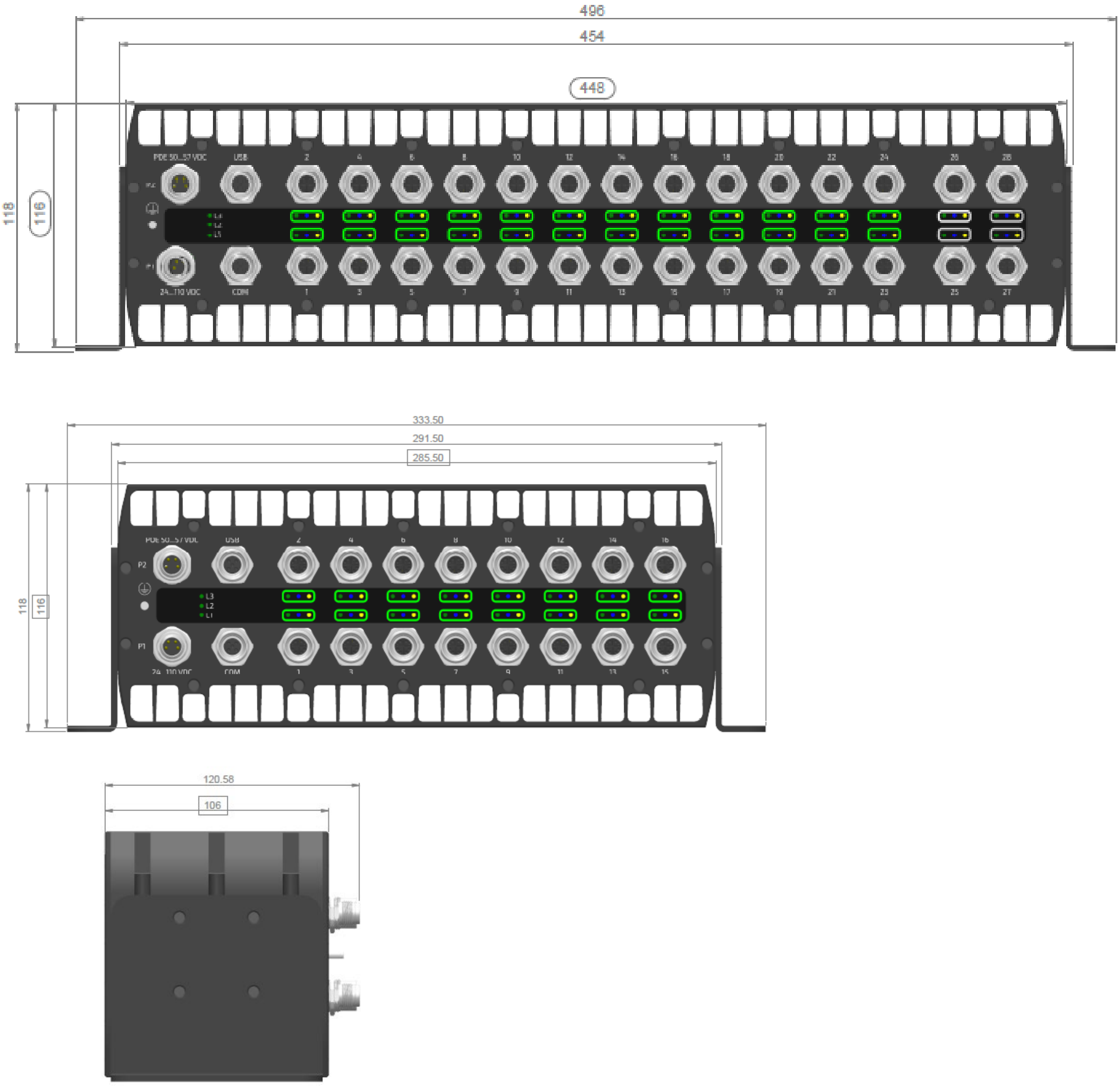
Environmental	Description
Temperature (operating)	Temp. Class OT4: -40°C to +70°C (-40°F to 158°F) Temp. Class ST1: OT4 +15°C (duration: 10 min.) Temp. Class TX: -40°C to +85°C According to: EN 50155: Railway Applications- Rolling stock- electronic equipment, IEC 60068-2-1: Cold, IEC 60068-2-2: Dry heat
Temperature (non-operating)	-40°C to +85°C According to: EN 50155: Railway Applications- Rolling stock- electronic equipment, IEC 60068-2-1: Cold and IEC 60068-2-2: Dry heat
Humidity	+25 / +55 °C, 100 % r.h According to: EN 50125-1: Railway applications - Environmental conditions for equipment - Part 1: Rolling stock and on-board equipment and EN 60068-2-78: Damp heat, steady state
	+40 °C, 93 % r.h. non-condensing According to: EN 60068-2-78: Damp heat, steady state
Shock (non-operating)	Category: 1, class B Severity: 50 m/s^2 Duration: 30 ms According to: EN 61373: Railway applications- Rolling stock equipment- Shock and vibration tests
Vibration (operating)	Waveform: random Category: 1, Class B Severity: 11.44 m/s^2 Duration: 15 hr. (3 directions with 5 hr. per direction According to: EN 61373: Railway applications- Rolling stock equipment- Shock and vibration tests
Vibration (non-operating)	Waveform: random Category: 1, Class B Severity: 2.02 m/s^2 Duration: 30 min. (3 directions with 10 min. per direction According to: EN 61373: Railway applications- Rolling stock equipment- Shock and vibration tests
Salt Mist	48 hr.
Altitude	3000 m
IP Protection	IP54
MTBF	290,000 hr. according Telecordia 40°C GB (Values are product specific & available on request)

8.5. Mechanical Specification

Table 16: KSwitch R20 and KSwitch R16 Mechanical Specification

Mechanical	Description
Dimension (W x H x D)	**KSwitch R20**: 448 mm x 116 mm x 106 mm (17.64” x 4.57” x 4.17”) (without side brackets) 496 mm x 118 mm x 106 mm (19.53“ x 4.65“ x 4.17“) (with side brackets) **KSwitch R16**: 285.50 mm x 116 mm x 106 mm (11.24“ x 4.57“ x 4.17“)(without side brackets) 333.50 mm x 118 mm x 106 mm (13.1“ x 4.65“ x 4.17“) (with side brackets)
Chassis	Aluminum, Black anodized Front cover silk screen
Cooling	Cooling fins (passive)
Weights	KSwitch R20: 4.5 kg approx. KSwitch R16: 3.4 kg approx.
Installation	Wall mount Rack mount

Figure 12: KSwitch R20 and KSwitch R16 Dimension Diagrams (mm)



8.6. Thermal Specification

The switch is passively cooled and fanless with no ventilation openings. Cooling fins encompasses the maximum area on the switch's top and bottom sides, to aid heat dissipation into the surrounding ambient environment. When installing the switch consider the orientation of the switch and take care not to obstruct the airflow over the cooling fins, as this can stop sufficient heat dissipating into the ambient environment and cause a build-up of heat.

⚠CAUTION

Airflow and Clearance

If airflow and clearance are not considered the switch may overheat and can cause a fire or malfunction. The avoid overheating:

- Operate in a well-ventilated environment to enable heat dissipation.
- Ensure that the switch's cooling fins do not obstruct the airflow over the switch.
- Leave the specified clearance distance to prevent the switch from overheating.

⚠CAUTION

Hot Surface

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

- Do not touch the cooling fins when the switch is in operation.
- Allow the switch to cool before handling.
- Wear protective gloves

8.6.1. Clearance

To provide a maximum airflow away from the switch, observe the minimum distances to surrounding parts, known as clearance within this user guide.

Kontron recommends user to observe the following specified clearance distances of 150 mm/5.91 inch (faceplate and rear side), 50 mm/ 1,97 inch (top side), 2 mm/ 0.08 inch (bottom side), 30 mm/ 1.18 inch (left and right sides), see Figure 6: Minimum Clearance.

⚠CAUTION

Minimum Clearance Distance

Leave sufficient clearance (keep out area) to prevent the switch from overheating! Observe the specified clearance distances of 150 mm/5.91 inch (faceplate and rear side), 50 mm/ 1,97 inch (top side), 2 mm/ 0.08 inch (bottom side), 30 mm/ 1.18 inch (left and right sides).

8.7. Compliance

The KSwitch R20 and KSwitch R16 switch series 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 17: KSwitch R20 and KSwitch R16 Compliance Railway

	Railway
General	**EN 50155** Railway Applications- Rolling stock- electronic equipment Class K1: Sockets for integrated circuits and/or edge connectors are permitted
EMC	**EN 50121-3-2** Railway applications - Electromagnetic compatibility – Part 3-2: Rolling stock – Apparatus
Safety (CB Scheme)	**EN 50153** Railway applications - Rolling stock - Protective provisions relating to electrical hazards **EN 50124-1** Railway applications - Insulation coordination – Part 1: Basic requirements - Clearances and creepage distances for all electrical and electronic equipment **EN ISO 13732-1** Ergonomics of the thermal environment - Methods for the assessment of human responses to contact with surfaces – Part 1: Hot surfaces (ISO 13732-1:2006) **EN 45545-1** Railway applications - Fire protection on railway vehicles - Part 1: General

Table 18: KSwitch R20 and KSwitch R16 Compliance CE

CE Mark	
Directives	**2014/30/EU** Electromagnetic Compatibility **2014/35/EU** Low Voltage **2011/65/EU** RoHS II
EMV	**EN 55032** Electromagnetic compatibility of multimedia equipment- Emission Requirements **EN 55035** Electromagnetic compatibility of multimedia equipment - Immunity requirements **EN 61000-6-2** Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environment EN 61000-6-4 Electromagnetic compatibility (EMC) – Part 6-4: Generic standards - Emission Standard for industrial environment
Safety (CB Scheme)	**EN 62368-1** Audio/video, information and communication technology equipment Part 1: Safety Requirement

Table 19: KSwitch R20 and KSwitch R16 Compliance International

International Mark	
EMV	**IEC 55032** Electromagnetic compatibility of multimedia equipment- Emission Requirements **IEC 55035** Electromagnetic compatibility of multimedia equipment - Immunity requirements **IEC 61000-6-2** Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environment **IEC 61000-6-4** Electromagnetic compatibility (EMC) – Part 6-4: Generic standards - Emission Standard for industrial environment
Safety (CB Scheme)	**IEC 62368-1** Audio/video, information and communication technology equipment Part 1: Safety Requirement

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

ℹ The switch 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 switch.

ℹ Routing cables away from EMI sources that may cause interference and packet loss and use shielded/screen cables to prevent any electromagnetic noise from interfering with cable transmission.

9/Software Interface

The KSwitch R20 and KSwitch R16 switch series is pre-installed with software and firmware and a Network Operating System (NOS) with management interfaces to configure the Ethernet features available on the switch such as port configuration, VLAN settings or Spanning Tree configurations.

Examples of commands provided within this chapter use the KSwitch R20 switch as the example switch but are applicable to all KSwitch R20 and KSwitch R16 switch variants.

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. Accessing the Switch

Access to the NOS is provided by a Web User Interface (UI), Command-line Interface (CLI) or Simple Network Management Protocol (SNMP). To access the switch's NOS the switch's IP address is required and the remote computer must have access to the switch's network subnet.

9.1.1. Accessing the IP Address

To access the switch's IP Address, perform the following:

Query DHCP assigned IP address, Example:

```
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
```

If the switch does not receive a DHCP IP address within 120 seconds, the switch will automatically assign IP address 192.0.2.1/24 to VLAN 1.

9.1.2. Accessing the NOS using the Web User Interface (UI)

When accessing the NOS using the Web UI, the procedure may vary depending on the browser used and the user must consider the following prerequisites.

Table 20: NOS Web UI Prerequisite

Prerequisite	Description
IP address	Switch's IP address known.
Remote access	Remote computer has access to the switch's network subnet.
HTML5	Web browser supports HTML5.
HTTPS self-signed certificate[1]	Upon connection to the Web UI, it is mandatory to accept the HTTPS self-signed certificate. NOTE: Factory default is HTTPS not enabled!

Prerequisite	Description
File download permission[1]	File download from the site needs to be permitted.
Cookies[1]	Cookies must be enabled in order to access the website.

[1] For further information about file download permission, refer to the Web Browser Documentation.

On delivery the switch's default username is 'admin' and no password is set.

The username 'admin' cannot be removed or changed, only the password can be changed.

Kontron strongly recommended assigning a strong password.

To access the switch IP Address, see Chapter 9.1.1: Accessing the IP Address.

To obtain the list of default user names and passwords:

1. Open a browser window (on a remote computer with access to the switch network) and enter the switch's IP address, http://[SWITCH_IP].

9.1.3. Accessing the NOS using the Command Line Interface (CLI)

To access the switch's CLI use the Ethernet port (IP address) or the service management port (COM). When accessing the NOS using the CLI, users must consider the following prerequisites.

Table 21: NOS CLI Prerequisites

Prerequisite	Description
IP address	Switch's IP address known.
Remote access	Remote computer has access to the switch's network subnet.
Client tool	Remote computer has an installed client tool e.g. telnet.

To access the switch IP Address, see Chapter 9.1.1: Accessing the IP Address.

For the Ethernet port (IP address) and the service management port (COM), the default login and password are the same.

To obtain the list of default user names and passwords:

1. From a remote computer, open a telnet client tool and connect with the IP address, using the predefined port
2. Login to the switch's NOS CLI using the appropriate login and password.

   Default login account for NOS:

   ```
   Login: admin
   ```

9.1.3.1. Setting up the Service Management Port (COM)

The service management port (COM) is a serial port. The serial connection requirements for the service management port (COM) are:

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

To set up the service management port (COM), connect the switch's (COM) to a remote computer and use as shown in this example Putty software to access the switch's service management port (COM) 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.

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

On delivery the switch's default username is 'admin' and there is no password.

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

Kontron strongly recommends assigning a strong password.

9.1.3.2. Deactivate Serial Timeout

The serial timeout is deactivated once enabled by the CLI command.

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

9.1.3.3. Accessing the Operating System

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

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

9.1.4. Help Tools

9.1.4.1. Switch Web User Interface (UI) Help

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

9.1.4.2. Switch Command Line Interface (CLI) Help

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

9.2. Managing the Switch using the Web User Interface (UI)

The Web User Interface (UI) provides a significant amount of information on how to configure, monitor and maintain the switch.

Kontron recommends using the Web UI's help feature to access more information.

Kontron recommends using the Web UI whenever possible to simplify user configuration and reduce configuration mismatch.

9.3. Managing the Switch using the Command Line Interface (CLI)

The Command Line Interface (CLI) can be used to configure, monitor, and maintain the switch via Telnet, SSH. Use a baud rate of 115200 when using a USB serial interface.

The CLI contains more configuration commands versus those affected as a result of user configuration changes over the Web UI. This user guide only covers the commands affected when users change the switch configuration via the Web UI.

Kontron recommends using the Web UI whenever possible to simplify user configuration and reduce configuration mismatch.

All commands entered in CLI are followed by values, parameters or both. Parameters may be mandatory values, optional values, choices, or a combination.

Values may be in a form of:

- Six hexadecimal numbers separated by colons (MAC address), for example 00:06:29:32:81:40
- Dotted-decimal notation (Area IDs), for example 0.0.0.1
- Slot/port number for example: 1/1
- Logical slot/port (applicable in case of a link-aggregation)

Table 22: CLI Parameter Command

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

9.3.1. Completing a Partial Command

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

Or enter the **<?>** key for a list of the next possible commands.

9.3.2. Command History

Use the **<Up/Down>** arrows keys to scroll between the commands you already typed. To display the entire history use the show history command.

```
#show history
```

9.3.3. Using the Backspace Key in NOS CLI

The **<Backspace>** key deletes the character at the cursor location only. Users are required to move the cursor to this location before using the **<Backspace>** key to delete the character at the curser.

9.3.4. ‘no' Commands

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

```
# no
```

9.3.5. Configuration Examples using the CLI

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

For more information on additional features and configuration options, see the CLI Help feature Chapter 9.1.4.2 Switch Command Line Interface (CLI) Help.

9.3.5.1. To Query DHCP 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
```

9.3.5.2. To Set IP address (and hostname) manually via CLI and Save

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

```
Press ENTER to get started <CR>

Username: admin
Password: <CR>
#configure terminal
(config)# hostname KSwitch-R20-1
KSwitch-R20-1(config)#interface vlan 1
KSwitch-R20-1(config-if-vlan)# ip address 19exit
2.168.170.60 255.255.255.0
KSwitch-R20-1(config-if-vlan)# do show ip interface
Interface Address            Method Status
--------- ------------------ ------ ------
VLAN 1    192.168.170.60/24  Manual Up

KSwitch-R20-1(config-if-vlan)#
KSwitch-R20-1(config-if-vlan)# exit
KSwitch-R20-1(config)# exit
KSwitch-R20-1# copy running-config startup-config
Building configuration...
% Saving 1305 bytes to flash:startup-config
KSwitch-R20-1#
```

9.3.5.3. To Check Network Port Status

The port status depends on the Ethernet port configuration. The following shows examples of different port status outputs.

Example 1.

```
# show interface * status
Interface    Mode     Speed   Aneg    Media Type  SFP Family  Link        Operational Warnings
--------- -----  ------ ----  ----- ---- ----------  ----    --------------------

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
```

Example2.

```
KSwitch-R20-1# show interface * status
Interface  Mode     Speed   Aneg       Link    Operational Warnings
---------- -------- ------- ---------- ------- --------------------
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
Gi 1/9     Enabled  Auto    Yes        Down
Gi 1/10    Enabled  Auto    Yes        Down
Gi 1/11    Enabled  Auto    Yes        Down
Gi 1/12    Enabled  Auto    Yes        Down
Gi 1/13    Enabled  Auto    Yes        Down
Gi 1/14    Enabled  Auto    Yes        Down
Gi 1/15    Enabled  Auto    Yes        Down
Gi 1/16    Enabled  Auto    Yes        Down
Gi 1/17    Enabled  Auto    Yes        Down
Gi 1/18    Enabled  Auto    Yes        Down
Gi 1/19    Enabled  Auto    Yes        Down
Gi 1/20    Enabled  Auto    Yes        Down
Gi 1/21    Enabled  Auto    Yes        Down
Gi 1/22    Enabled  Auto    Yes        Down
Gi 1/23    Enabled  Auto    Yes        Down
Gi 1/24    Enabled  Auto    Yes        Down
Gi 1/25    Enabled  Auto    Yes        Down
10G 1/1    Enabled  Auto    Yes        Down
10G 1/2    Enabled  Auto    Yes        Down
10G 1/3    Enabled  Auto    Yes        Down
10G 1/4    Enabled  Auto    Yes        Down
```

9.3.5.4. To List Currently Active Switch Configuration

```
KSwitch-R20-1# show running-config
Building configuration...
hostname KSwitch-R20-1
username admin privilege 15 password encrypted
7710abc4a6c4ee12a96ee9e4ff68700097707ec2acb58640cf9c1924a5c27bc24767008b3747e803fa2dbf3e789f0a51ea3
10351bd0712b9b3f8cc1c419969a9
!
vlan 1
!
!
!
!
spanning-tree mst name 02-00-c1-07-30-7b revision 0
poe power-supply-limit 90
!
!
voice vlan oui 00-01-E3 description Siemens AG phones
voice vlan oui 00-03-6B description Cisco phones
voice vlan oui 00-0F-E2 description H3C phones
voice vlan oui 00-60-B9 description Philips and NEC AG phones
voice vlan oui 00-D0-1E description Pingtel phones
voice vlan oui 00-E0-75 description Polycom phones
voice vlan oui 00-E0-BB description 3Com phones
!
--------
```

Example 1.

```
interface FastEthernet 1/2
!
interface FastEthernet 1/3
!
interface FastEthernet 1/4
!
interface FastEthernet 1/5
!
interface FastEthernet 1/6
!
interface FastEthernet 1/7
!
interface FastEthernet 1/8
!
interface FastEthernet 1/9
!
interface FastEthernet 1/10
!
interface FastEthernet 1/11
!
interface FastEthernet 1/12
!
interface FastEthernet 1/13
!
interface FastEthernet 1/14
!
interface FastEthernet 1/15
!
interface FastEthernet 1/16
!
interface FastEthernet 1/17
!
interface FastEthernet 1/18
!
interface FastEthernet 1/19
!
interface FastEthernet 1/20
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet ½
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
!
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
```

Example 2.

```
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
interface GigabitEthernet 1/4
!
interface GigabitEthernet 1/5
!
interface GigabitEthernet 1/6
!
interface GigabitEthernet 1/7
!
interface GigabitEthernet 1/8
!
interface GigabitEthernet 1/9
!
interface GigabitEthernet 1/10
!
interface GigabitEthernet 1/11
!
interface GigabitEthernet 1/12
!
interface GigabitEthernet 1/13
!
interface GigabitEthernet 1/14
!
interface GigabitEthernet 1/15
!
interface GigabitEthernet 1/16
!
interface GigabitEthernet 1/17
!
interface GigabitEthernet 1/18
!
interface GigabitEthernet 1/19
!
interface GigabitEthernet 1/20
!
interface GigabitEthernet 1/21
!
interface GigabitEthernet 1/22
!
interface GigabitEthernet 1/23
!
interface GigabitEthernet 1/24
!
interface GigabitEthernet 1/25
!
interface 10GigabitEthernet 1/1
!
interface 10GigabitEthernet 1/2
!
interface 10GigabitEthernet 1/3
!
interface 10GigabitEthernet 1/4
!
```

```
---------

interface vlan 1
 ip address 192.168.170.60 255.255.255.0
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
line vty 2
!
line vty 3
!
```

```
line vty 4
!
line vty 5
!
line vty 6
!
line vty 7
!
line vty 8
!
line vty 9
!
line vty 10
!
line vty 11
!
line vty 12
!
line vty 13
!
line vty 14
!
line vty 15
!
!
End
```

9.3.5.5. To Query System Information

```
KSwitch-R20-1# show version

Serial Number     : 0000000000
MAC Address       : 00-a0-a5-79-26-74
Previous Restart : Cold

System Contact    :
System Name       : KSwitch-R20-1
System Location   :
System Time       : 2024-10-21T10:46:28+00:00
System Uptime     : 4d 23:50:12


Bootloader
----------
Image             : u-boot
Version           : HEAD-0.00-20241013221501
Date              :

Primary Image
-------------
Image             : mmcblk0p5 (Active)
Version           : HEAD-0.00-20241016100112
Date              : 2024-10-16T10:56:18+00:00

Backup Image
------------
Image             : mmcblk0p6
Version           : HEAD-0.00-20241016100112
Date              : 2024-10-16T10:56:18+00:00

------------------
SID : 1
------------------
Chipset ID        : LAN9697 Rev. A
Board Type        : Kontron KSwitch M20
Flash Type        : MMC-only
Port Count        : 29
Product           : Microchip IStaX Switch
Software Version : HEAD-0.00-20241016100112
Build Date        : 2024-10-16T10:56:18+00:00
Code Revision     : 456ebb41
PoE Version       : HW Ver.:0, poe mcu type:26, sw ver:3.55, param:0, build=14, internal sw#=1200,
Asic Patch#=20046
```

9.3.5.6. To Load Factory Defaults

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

9.4. Firmware Update

For the switch's firmware updates, visit Kontron's Customer Section and click on TSN Network KSwitch R20/R16 > Firmware and Software.

Firmware updates can be implemented using Web UI or CLI. For both methods, network access must be configured. For more information, refer to the relevant sections chapter within this user guide.

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 switch 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.

9.5.1. Configure Terminal Command

Configure Terminal command description – Start switch configuration. Terminal display will switch 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 will switch from (config)# to (config- if)#.

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

Interface <port_type> [<port_type_list>]

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

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	Whenever end in-depth configuration and need to go up one level, or to log out of the serial interface.	

	Parameter	Description
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	Whenever need 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, meaning that upon switch power down-up cycle the switch may operate completely different.

Show Running-Config

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

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	Use this command 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	Use this command 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– Update (save) switch configuration to be used after reset or power-up.

Copy Running-Config Startup-Config

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

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	Use this command to copy switch configuration to another file or to TFTP Server or from TFTP Server to 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 under name “test” # copy running-config tftp://192.168.0.40/test	

9.5.10. Del Flash:<file-name>

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

Del Flash:<file-name>

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

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	Use this command 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	Use this command to restore to factory default	
Examples	# reload defaults	

9.5.13. Reload Defaults Keep-IP

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

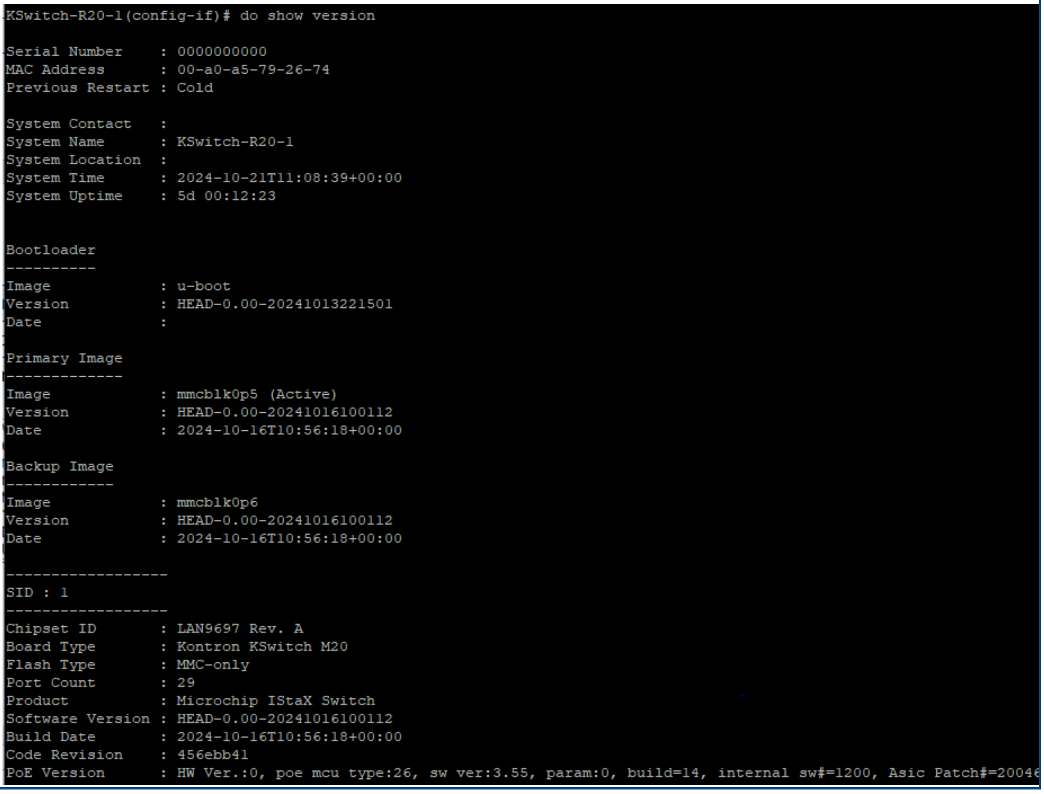
Reload Defaults Keep-ip

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command 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	Use this command to display switch information	
Examples	# show version 	

```
KSwitch-R20-1(config-if)# do show version

Serial Number     : 0000000000
MAC Address       : 00-a0-a5-79-26-74
Previous Restart  : Cold

System Contact    :
System Name       : KSwitch-R20-1
System Location   :
System Time       : 2024-10-21T11:08:39+00:00
System Uptime     : 5d 00:12:23


Bootloader
----------
Image             : u-boot
Version           : HEAD-0.00-20241013221501
Date              :

Primary Image
-------------
Image             : mmcblk0p5 (Active)
Version           : HEAD-0.00-20241016100112
Date              : 2024-10-16T10:56:18+00:00

Backup Image
------------
Image             : mmcblk0p6
Version           : HEAD-0.00-20241016100112
Date              : 2024-10-16T10:56:18+00:00

------------------
SID : 1
------------------
Chipset ID        : LAN9697 Rev. A
Board Type        : Kontron KSwitch M20
Flash Type        : MMC-only
Port Count        : 29
Product           : Microchip IStaX Switch
Software Version  : HEAD-0.00-20241016100112
Build Date        : 2024-10-16T10:56:18+00:00
Code Revision     : 456ebb41
PoE Version       : HW Ver.:0, poe mcu type:26, sw ver:3.55, param:0, build=14, internal sw#=1200, Asic Patch#=20046
```

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.

For configuration information, refer to the dedicated separate PTN and TSN Configuration Guides:

- Kontron_AN-PTP_Configuration Guide.pdf
- Kontron_AN-TSN_Configuration Guide.pdf

Further information may also be available by referring to Chapter 9.1.4: Help Tools for further information.

For the PTN and TSN Configuration Guides, visit Kontron’s Customer Section.

9.7. Network Management Commands

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

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	Use the command 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)
	auto	Auto negotiation
Default	All ports are set to Auto	
Mode	Port List Interface Mode	
Usage	Use to set the speed of the specified interface	
Examples	Example#1 (set speed for port 1 to 100Mbps) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# speed 100	

	Parameter	Description
	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	Use to set the duplex mode of the specified interface. Use the no form of the command	
Examples	Example#1 (set duplex for port 1 to half) # configure terminal (config)# interface GigabitEthernet 1/1 (config-if)# duplex half	

9.7.1.4. Flow Control

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

flowcontrol { on | off }
no flowcontrol

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

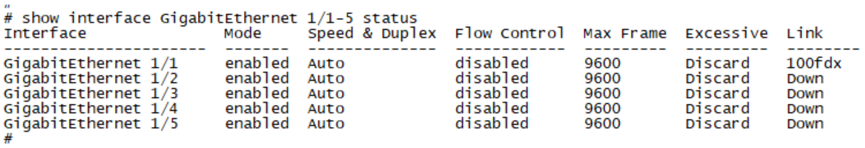
9.7.2. Ethernet Port View Commands

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	Use to display current status of the specified interface	
Examples	Example#1 (show status and configuration for port#1) # show interface GigabitEthernet 1/1 status Example#2 (show status and configuration for ports #1 through #5) # show interface GigabitEthernet 1/1-5 status 	

```
#
# show interface GigabitEthernet 1/1-5 status
Interface               Mode     Speed & Duplex  Flow Control  Max Frame  Excessive  Link
----------------------  -------  --------------  ------------  ---------  ---------  --------
GigabitEthernet 1/1     enabled  Auto            disabled      9600       Discard    100fdx
GigabitEthernet 1/2     enabled  Auto            disabled      9600       Discard    Down
GigabitEthernet 1/3     enabled  Auto            disabled      9600       Discard    Down
GigabitEthernet 1/4     enabled  Auto            disabled      9600       Discard    Down
GigabitEthernet 1/5     enabled  Auto            disabled      9600       Discard    Down
#
```

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	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	
Mode	VLAN Interface Configuration mode	
Usage	Add VLAN interface and set all IPv4, IPv6 parameters. Use the no version of the command to disable the selected VLAN interface. To remove it completely use no interface vlan <id> from Global configuration mode.	

	Parameter	Description
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>

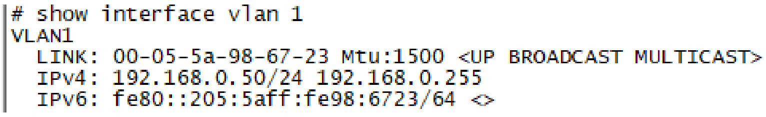
	Parameter	Description
Parameter	<ipv4_addr>	Network
	<ipv4_netmask>	Netmask
	<ipv4_gw>	Gateway
	<distance>	Distance value for this route
Default	N.A	
Mode	Global Configuration mode	
Usage	To route all unknown destination IP to default gateway use the following parameters: Network=0.0.0.0 Netmask=0.0.0.0 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	Use to display current status and configuration of the specified interface	
Examples	Example#1 (show status and configuration for VLAN 1) # show interface vlan 1 	

```
# show interface vlan 1
VLAN1
   LINK: 00-05-5a-98-67-23 Mtu:1500 <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 NTP Servers IP. The NTP Server updates the switch with the correct GMT (Greenwich Mean Time).

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	Enable NTP server by entering ntp command. Use a no version of the command to disable it. Specify the parameters of NTP server by entering ntp server command. Use a no version of the command to delete the specified NTP server.	
Examples	Example#1 (add NTP server 1 with IP address 192.168.1.2) (config)#ntp server 1 ip-address 192.168.1.2 Example#2 (add NTP server 2 with domain <any-ntp-server>) (config)#ntp server 2 ip-address <any-ntp-server> Example#3 (enable NTP server) (config)#ntp	

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	Use the command view status and configuration of 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	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	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 - View Commands

9.7.9.1. Show Clock Detail

Description - Display the detailed clock information.

show clock detail

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

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 has the option to filter some of the SysLog messages being send by the switch by configuring from what severity/importance SysLog messages the message should be send.

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	Enable SysLog server, specify its address and what level of messages will be sent to it. Use the no logging on command to disable SysLog server.	
Examples	Example#1 (Enable SysLog server at 192.168.0.1 with Warning level messages) (config)#logging on (config)#logging host 192.168.0.1 (config)#logging level warning Example#2 (Disable SysLog server) (config)#no logging on	

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	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 Ethernet Switch forwarding algorithm, the switch looks for Destination-MAC and VLAN inside the MAC learning table. If found, the packet will be forwarded to the specified port, otherwise the packet is flooded to all ports on same VLAN.

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	Set MAC address table aging time in seconds. Use the no version of the command to reset to default (300 seconds)	
Examples	Example#1 (Set aging time to 400 seconds) (config)# mac address-table aging-time 400 Example#2 (Disable automatic aging) (config)# mac address-table aging-time 0	

9.7.12.2. MAC Address-Table Learning

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

mac address-table learning [secure]
no mac address-table learning
mac address-table learning vlan <vlan_list>
no mac address-table learning vlan <vlan_list>

	Parameter	Description
Parameter	[secure]	Port Secure mode
Default	All ports are in Auto learning mode	
Mode	Port List Interface Mode (for specific port), Global Configuration Mode (for VLANs)	
Usage	Set MAC address table learning mode to Secure or back to Auto (command without [secure] parameter). Use the no version of the command to Disable learning.	
Examples	Example#1 (Set MAC address learning to Secure on port 1) (config)# interface GigabitEthernet 1/1 (config-if)#mac address-table learning secure 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>]]}

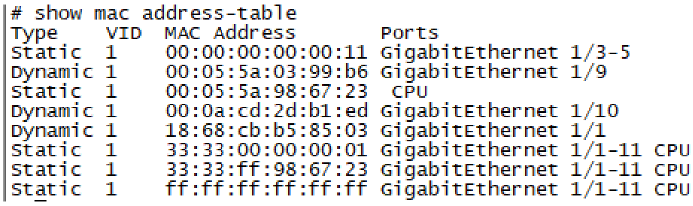
	Parameter	Description
Parameter	<v_mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
	<v_vlan_id>	VLAN IDs 1-4095
	<port_type>	GigabitEthernet
	<v_port_type_list>	List of Port ID, ex, 1/1,3-5
Default	N.A	
Mode	Global Configuration Mode	
Usage	Assigns a static MAC address to a port. Use the no version of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

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>]]

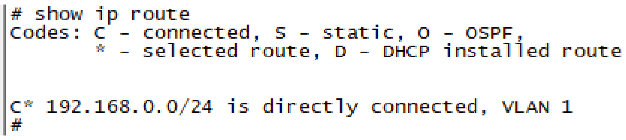
	Parameter	Description
Parameter	conf	User added static MAC addresses
	static	All static MAC addresses
	aging-time	Display MAC address aging time
	learning	MAC address learning state (Learn/Secure/Disable)
	count	Total number of MAC addresses
Default	N.A	
Mode	EXEC Mode	
Usage	Show MAC address table entries 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  # 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	Display routing information	
Examples	Example #show ip route 	

```
# show ip route
Codes: C - connected, S - static, O - OSPF,
       * - selected route, D - DHCP installed route


C* 192.168.0.0/24 is directly connected, VLAN 1
#
```

9.8. Access Control/Security Management Commands

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

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	Add a new user for the local switch access and add/change password	
Examples	Example#1 (add a user named usertest with unencrypted password of testuser) (config)# username usertest privilege 15 password unencrypted testuser Example#2 (remove user named usertest) (config)# no username usertest Example#3 (change the password of usertest to testuser123) (config)# username usertest privilege 15 password unencrypted testuser123	

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

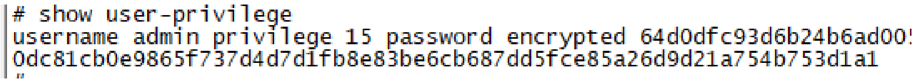
Username 'admin' cannot be removed or be changed, only its password.

9.8.2. Local Users - View Commands

9.8.2.1. Show User-Privilege

Description- Display all local users, privilege levels and passwords

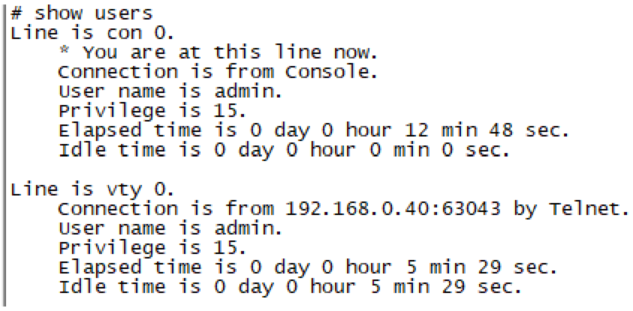
show user-privilege

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

9.8.3. Web Server - Configuration Commands

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

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	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 }

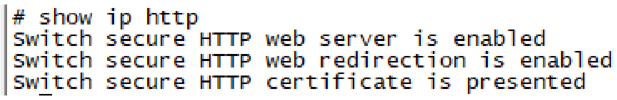
	Parameter	Description
Parameter	<url_file>	Uniform Resource Locator. It is a specific character string that constitutes a reference to a resource. Syntax: <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name> If the following special characters: space !\"#$%&'()*+,/:;<=>?@[\\]^`{|}~ need to be contained in the input URL string, they should be percent-encoded. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.
	<pass_phrase>	Privacy key pass phrase string if uploading certificate protected by a specific passphrase.
Default	N.A	
Mode	Global Configuration Mode	
Usage	Manage the HTTPS certificate (PEM format)	
Examples	Example#1 (upload the HTTPS certificate from TFTP server) (config)# ip http secure-certificate upload tftp://10.9.52.103/test_ca.pem Example#2 (delete current certificate) (config)# ip http secure-certificate delete	

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

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

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

Local- use the switch local user database.
Radius- use remote RADIUS server
Tacacs- use remote TACACS+ server.

aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }
no aaa authentication login { console | telnet | ssh | http }

	Parameter	Description
Parameter	N.A	N.A
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure user authentication method for a specific management interface. Use the no version of the command to disable the interface.	
Examples	Example#1 (configure SSH to be authenticated 1st by RADIUS Server. In case it is down, then by TACACS Server, and in case it is also down, then be authenticated locally) (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 }

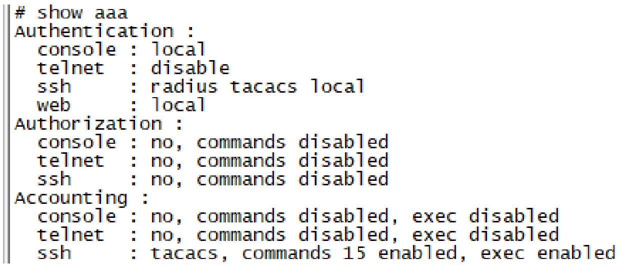
	Parameter	Description
Parameter	[commands <priv_lvl>]	All CLI commands equal and above the privilege level are accounted
	[exec]	Only remote user login/logout is reported
Default	N.A	
Mode	Global Configuration Mode	
Usage	Configure accounting method and reporting. Use the no version of the command to 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	Display the current status of authentication, authorization and accounting.	
Examples	Example # show aaa 	

```
# show aaa
Authentication :
  console : local
  telnet  : disable
  ssh     : radius tacacs local
  web     : local
Authorization :
  console : no, commands disabled
  telnet  : no, commands disabled
  ssh     : no, commands disabled
Accounting :
  console : no, commands disabled, exec disabled
  telnet  : no, commands disabled, exec disabled
  ssh     : tacacs, commands 15 enabled, exec enabled
```

9.8.7. Access Control List - Configuration Commands

Access Control List - configures from what remote IP address 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	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

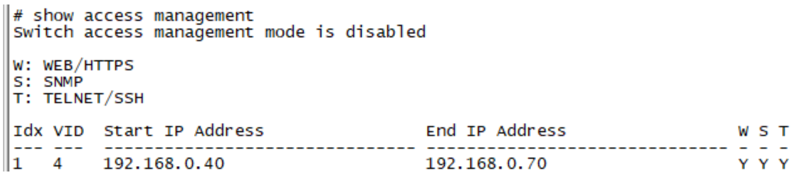
9.8.8.1. Show Access Management

show access management [statistics | <access_id_list>]

<table>
<tr><th></th><th>Parameter</th><th>Description</th></tr>
<tr><td><b>Parameter</b></td><td><access_id_list></td><td>ID of access management entry (1~16)</td></tr>
<tr><td><b>Default</b></td><td colspan="2">N.A</td></tr>
<tr><td><b>Mode</b></td><td colspan="2">EXEC Mode</td></tr>
<tr><td><b>Usage</b></td><td colspan="2">Display access management status and all entries or statistics or a specific entry.</td></tr>
<tr><td><b>Examples</b></td><td colspan="2">

Example#1 (show access management configuration)

show access management



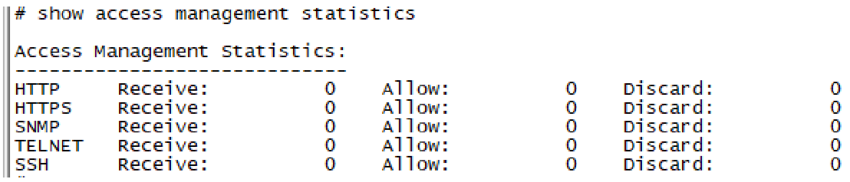
```
# show access management
Switch access management mode is disabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx VID  Start IP Address                End IP Address                 W S T
--- ---  ------------------------------- ------------------------------ - - -
1   4    192.168.0.40                    192.168.0.70                   Y Y Y
```

Example#2 (show access management statistics)

#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
```

</td></tr>
</table>

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.

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

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	
Usage	Configure a port VLAN ID for a trunk port. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as trunk with PVID 4) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk native vlan 4	

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	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.
Default	All VLANs are allowed (1-4095)	
Mode	Port List Interface Mode	
Usage	Configure allowed VLANs for a trunk port. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as trunk and exclude VLAN 10 and 30,31,32 from allowed VLANs) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode trunk (config-if)# switchport trunk allowed vlan except 10,30-32	

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	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	Configure a port VLAN ID for a hybrid port. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 4 as hybrid with PVID 5) # configure terminal (config)# interface GigabitEthernet 1/4 (config-if)# switchport mode hybrid (config-if)# switchport hybrid native vlan 5	

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. No matter the received frame is tagged or untagged, 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	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	Enable ingress filtering. Use the no version of the command to revert to default.	
Examples	Example#1 (configure port 3 as hybrid and enable ingress filtering) # configure terminal (config)# interface GigabitEthernet 1/3 (config-if)# switchport mode hybrid (config-if)# switchport hybrid ingress-filtering	

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	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	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 will become a member of all VLANs (1-4095).

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

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

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	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	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

9.10.1. STP Bridge Configuration Commands

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.

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	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.

	Parameter	Description
	<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	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 (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

	Parameter	Description
	link-type { point-to-point | shared | auto }	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. Default is auto.
	edge	Defines whether the port is connecting directly to edge devices. Default is non-edge.
	auto-edge	Enables auto edge detection on the port.
	restricted-role	If enabled causes the port not to be selected as Root port.
	restricted-tcn	If enabled causes the port not to propagate received topology change notifications to other ports.
	Bpdu-guard	If enabled causes the port to disable itself upon receiving valid BPDUs.
Default	N.A	
Mode	Port List Interface Mode	
Usage	Configure STP CIST settings for the specific physical and aggregated ports. Use the no version of the command to revert to default.	
Examples	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 a detailed status information on a STP bridge instance, along with port state for all active ports associated.

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

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

9.11. Port Mirroring

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. Monitor Session

Description - Enable Port Mirroring.

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

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

9.11.2. Port Configuration

Description - Configure port mirroring parameters.

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

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

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

9.11.3. Mirror Data Traffic and Tag with VLAN

Example 1: Tagging mirrored data traffic with a specific VLAN:

Description of the example Use Case:
Two Ports of the Switch are receiving (Port 1/1) and transmitting (Port 1/2) Data Traffic.
This Traffic needs to be mirrored and tagged with a specific VLAN to enable for example the Data Traffic to be monitored.

For Traffic to be mirrored and tagged with a VLAN it is required to use a Reflector Port (Port 1/5).
The Reflector Port uses a physical Port that results in losing the "normal" function of the configured Port.
One additional Port (Port 1/3) will be needed to function as the Destination Port for the tagged and Mirrored Data.

Example configuration for the described Use Case (Vlan 10=Data Traffic / Vlan 200=Mirrored Data Traffic):

```
vlan 1,10,200
!
monitor session 1 destination remote vlan 200 reflector-port GigabitEthernet 1/5
monitor session 1 source interface GigabitEthernet 1/1 rx
monitor session 1
no mac address-table learning vlan 200
```

The source interfaces can also be set up differently.
However, it is advisable to exclude the RMirror VLAN.

```
interface GigabitEthernet 1/1
switchport access vlan 10
!
interface GigabitEthernet 1/2
switchport access vlan 10
!
interface GigabitEthernet 1/3
switchport hybrid allowed vlan 200
switchport hybrid egress-tag all
switchport mode hybrid
!
interface GigabitEthernet 1/5
no mac address-table learning
no spanning-tree
!
```

9.12. System Information Management Commands

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

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

9.12.1. Read Phy Temperature

```
Show thermal-protect
```

9.12.2. Interface Status

The Interface status depends on the Ethernet port configuration. The following shows examples of 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.

The switch's NOS provides a set of MIBs that are used to configure the switch using SNMP by any SNMP browser. For information on the supported MIBs, visit Kontron's Customer Section.

For information on the supported MIBs, visit Kontron's Customer Section.

For the PTN and TSN Configuration Guides, visit Kontron's Customer Section.

9.14. Autoinstall Switch Configuration features using USB Dongle

9.14.1. Auto Install 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 feature the system

- checks if file on stick is different to current startup-config;
- if different, copies file from stick as new startup-config to system
- performs reboots

9.14.2. LED L1 Autoinstall Status

The status of autoinstall feature can be observed without logging into the system. The indication LED L1 reports switch application information, including the autoinstall status, see Table 9: Indication LED (L1, L2, L3).
After boot, LED L1 reports for 2 minutes, whether autoinstall synced startup-config on switch and USB stick.

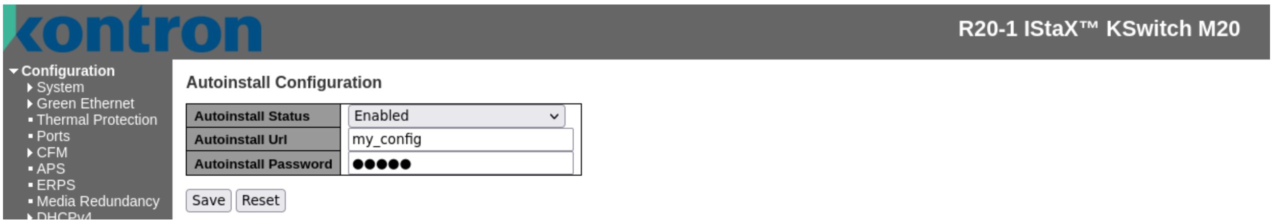
9.14.3. Enable Autoinstall Feature

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

Encrypted/Unencrypted Parameter:

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

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



Autoinstall Configuration

Autoinstall Status	Enabled
Autoinstall Url	my_config
Autoinstall Password	●●●●●

9.14.4. Disable Autoinstall Feature

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

9.14.5. Prepare USB Storage

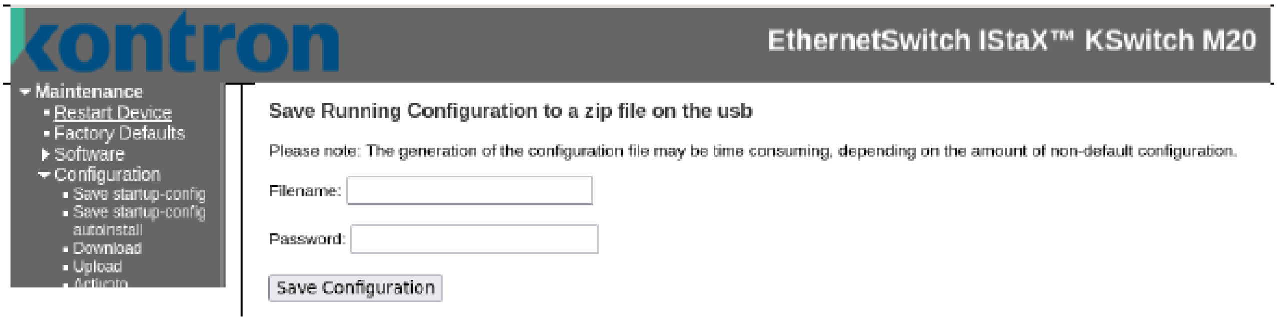
Run one time CLI command to format and partition (ext4) USB device.

```
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
```



Save Running Configuration to a zip file on the usb

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Filename:

Password:

Save Configuration

9.14.7. Query Autoinstall Status

```
EthernetSwitch# show autoinstall startup-config

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

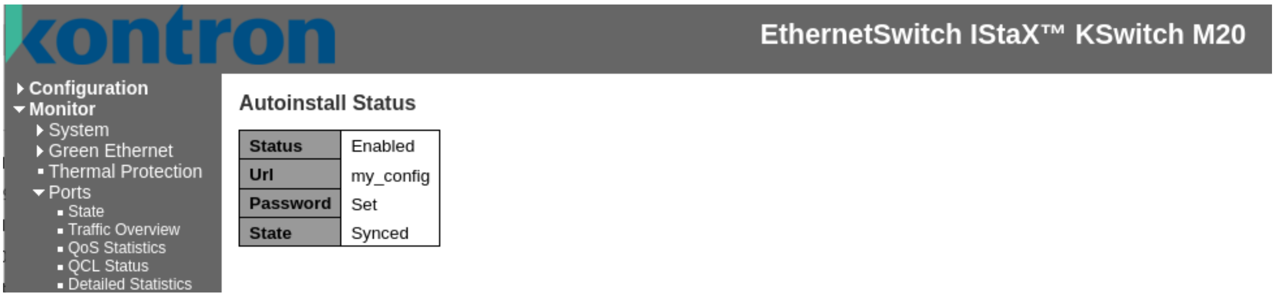
States:

- 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.

```
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)
```



Autoinstall Status

Status	Enabled
Url	my_config
Password	Set
State	Synced

9.14.8. Example 1: Prepare Autoinstall Setup Locally on Switch

For described use-case, autoinstall should also be enabled in 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-R20 and mount it on external Linux system with adapter cable.
In case changed switch settings are desired, 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.
```

Umount USB stick from external Linux system, connect it to KSwitch-R20 system.
Systems auto-mounter detects 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 R20 and External Linux System via Network

The switch CLI provides the possibility to copy files via network.
So also for environments where autoinstall files are generated on external Linux systems, it is not necessarily needed 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-R20

```
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 R20 and KSwitch R16 switch series are maintenance free with no user serviceable parts. Opening the switch may corrupt the switch's internal IP54 protection seal and invalidate the warranty. Return the switch to Kontron for maintenance and repair, see Chapter 11.1: Returning Defective Merchandise.

The switch may become hot during operation. Users must take adequate precautions before handling the switch.

⚠CAUTION

Handling and Operation

Handling and operation of the switch is permitted only for skilled personnel aware of the associated dangers, within a workplace that is access-controlled and fulfills all necessary technical and environmental requirements.

Hot Surface

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

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

NOTICE

Opening the switch is not permitted

Opening the switch may corrupt the switch's internal IP54 protection seal and is therefore not permitted. The switch contains no user serviceable parts. Therefore, users are not required to open the switch.

For any form of maintenance and repair, return the switch to Kontron, see Chapter 11.1: Returning Defective Merchandise.

10.1. USB Port Dongle

10.1.1. USB Port Dongel not Recognised

When connected to the USB port, the dongle is automatically recognized. If the dongle is not recognized:

- Check that the dongle is connected correctly and tightly screwed
- Check the Green status LED activity:
  - LED On - activity
  - LED Off- no activity
  - LED Blinking – data transfer

When data cannot be read or written, and the dongle is connected to the USB port:

- Ensure that the dongle has been formatted correctly. Note that different formats are incompatible. If required back up the data and reformat the dongle with a compatible format.

10.1.2. Autoinstall Switch Configuration

To autoinstall the switch configuration from an USB stick to KSwitch R20 or KSwitch R16 for easy switch configuration during possible field replacements by storing configuration information on external media, see Chapter 9.14: Autoinstall Switch Configuration features using USB Dongle.

10.2. Hardware Reset

To reset the switch, switch off by disconnecting the power properly, as described in Chapter 7.4: Switching Off. Then wait approximately 10 seconds before reconnecting the switch to the external DC power supply.

10.3. Software Interface Maintenance

To manage and configure the switch's software interface, refer to the relevant chapter(s) within Chapter 9/Software Interface.

10.3.1. Software Reset and Restore Switch

10.3.1.1. Reload Cold

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

reload cold

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

10.3.1.2. Reload Defaults Keep-IP

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

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

reload defaults keep-ip

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

10.3.1.3. Reload Defaults

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

The new semi factory default configuration is not automatically saved. Issue a command as "copy running-config startup-config" to make the new configuration change permanent.

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

reload defaults

	Parameter	Description
Parameter	-	-
Default	N.A	

	Parameter	Description
Mode	EXEC	
Usage	Use this command to restore to factory default	
Examples	# reload defaults	

10.3.2. Switch Configuration

10.3.2.1. Download Switch Configuration to TFTP-Server

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

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

	Parameter	Description
Parameter	-	-
Default	N.A	
Mode	EXEC	
Usage	Use this command to copy one of the switch configurations to TFTP Server	
Examples	Example #1 – copy running configuration to TFTP Server under name test Example #2 - save switch running configuration file to TFTP Server under name "test" # copy running-config tftp://192.168.0.40/test Example #2 – copy switch local configuration file named test1 to TFTP-Server under name "switch-test-config-file". #copy flash:test1 tftp://192.168.0.40/switch-test-config-file	

10.3.2.2. Upload Configuration File from TFTP-Server to Switch

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

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

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

10.3.2.3. Activate One of the Already Stored Configuration Files

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

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

copy flash:<file-name> running-config

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

10.3.2.4. Delete Configuration

Description – Delete configuration file from flash. To check the files stored in flash use "dir" command.
delete <flash:filename>

10.3.3. Software Update

10.3.3.1. Upload New Version

Description – Upload a new software version to the switch.

firmware upgrade <url_file>

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

10.3.3.2. Select Active Image

Description – Swap the active and alternative image.

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

firmware swap

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

10.4. Cleaning

Clean the switch when dirty to maintain the best thermal conditions for cooling.

NOTICE The switch is IP54 protected against dust in harmful quantities and water splashes on all sides. When cleaning, limit the use of liquid to ensure that no liquid enters the switch.

NOTICE Do not use an abrasive cloth or chemical substances to clean the switch, this may damage the lettering and chassis finish.

To clean the surface of the switch, perform the following:

1. Take precautions not to touch the switch’s cooling fins during operation.
2. Remove dust using a clean, soft brush and/or a clean, soft microfiber cloth only.
3. If lightly soiled, gently wipe the switch with a dry microfiber cloth.
4. Remove stubborn dirt using a microfiber cloth. Dampened with warm soapy water only and not with chemical substances.

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 product label, located on the switch’s rear side.

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 equipment to Kontron.

1. Visit the RMA Information website: https://www.kontron.com/en/support/rma-information
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 item, fill out the above information in the RMA Request form for each item. Send the completed RMA-Request form to the fax or email address given below at Kontron Europe GmbH. Kontron will provide an RMA-Number.
3. Kontron Europe GmbH
   RMA Support
   Phone: +49 (0) 821 4086-0
   Fax: +49 (0) 821 4086 111
   Email: service@kontron.com
4. The equipment for repair must be packed properly for shipping, considering shock and ESD protection.

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

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

12/ Storage and Transportation

The KSwitch R20 switch series must be stored or transported as described in this user guide.

12.1. Storage

If the switch is not in use for an extended period time, disconnect the power to the switch. If it is necessary to store the switch, then re-pack the switch as originally delivered to avoid damage. The storage facility must meet the switch's environmental storage 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 switch, use the original packaging, designed to withstand impact and adequately protect the switch. When packing or unpacking the switch always take shock and ESD protection into consideration and use an EOS/ESD safe working area.

13/ Warranty

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

1. Visit Kontron's Term and Conditions webpage.
   http://www.kontron.com/terms-and-conditions
2. Click on your region's General Terms and Conditions of Sale.

Opening the switch invalidates the warranty.

13.1.1. Limitation/Exemption from Warranty Obligation

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

- General safety instructions within this user guide.
- Type label information and specifications
- Warning labels on the product and warning symbols within this user guide.
- Information and hints within this user guide.

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

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.

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 indicte 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, and 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.

15/ Cyber Security

Cyber security is an important aspect to consider when installing, operating, maintaining and disposing of the product. 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, visit the Kontron Customer Section and refer to Kontron's Security White paper within General/Security Guidelines.

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 product:

- 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 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.

List of Acronyms

AWG	American Wire Gauge
CE	Conformitè Europëenne
CLI	Command Line Interface
COM	Communication port
DC	Direct Current
DWRR	Deficit-Weighted Round Robin
EMC	ElectroMagnetic compatibility
EOS	Electrical Over Stress
ESD	ElectroStatic Discharge
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FIFO	First In First Out
FRER	Frame Replication and Elimination for Reliability
GbE	Giga Bit Ethernet
GBT	Guard Band Time
GCE	Gate Control Entry
GCL	Gate Control List
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IOT	Internet of Things
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LED	Light Emitting Diode
LPC	Limited Power Source
MAC	Media Access Control
MDI	Media Dependent Interface
MIB	Managed Information Base
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Before Failure
NEBS	Network Equipment Building Systems
NOS	Network Operating System
NTP	Network Time Protocol
PD	Powered Device
PHY	PHYical interface
PoE	Power over Ethernet
PSE	Power Source Equipment
PTP	Precision Time Protocol

RMA	Return of Material Authorization
RoHS	Restriction of Hazardous Substances
RSTP	Rapid Spanning Tree Protocol
RTC	Real Time Clock
SDU	Service Data Unit
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
SQP	Strict priority Queuing
TAS	Time Aware Shaper
TFTP	Trivial File Transfer Protocol
TSN	Time Sensitive Network
UEFI	Unified Extensible Firmware Interface
UI	User Interface
UL	Underwriters Laboratories
USB	Universal Serial Bus
VLAN	Virtual Local Area network
WEEE	Waste Electrical and Electronic Equipment

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: 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