RAPTOR iMX350-Hardware Installation Guide

Intelligent Cyber Secure Platform

iMX350

Version: 1.41.1-1, Date: Mar 2024

Copyright Notice

© 2024 iS5 Communications Inc. All rights reserved.

No Part of this publication may be reproduced in any form without the prior written consent of iS5 Communications Inc. (iS5).

Trademarks

iS5Com is a registered trademark of iS5. All other trademarks belong to their respective owners.

Regulatory Compliance Statement

Product(s) associated with this publication complies/comply with all applicable regulations. For more details, refer to the Technical Specifications.

Warranty

iS5 warrants that all products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). iS5 will repair or replace products found to be defective within this warranty period including shipping costs. This warranty does not cover product modifications or repairs done by persons other than iS5-approved personnel, and this warranty does not apply to products that are misused, abused, improperly installed, or damaged by accident. Refer to the Technical Specifications for the actual warranty period(s) of the product(s) associated with this publication. Warranty certificate available at: https://is5com.com/warranty

Disclaimer

Information in this publication is intended to be accurate. iS5 shall not be responsible for its use or infringements on third-parties because of the use of this publication. There may occasionally be unintentional errors on this publication. iS5 reserves the right to revise the contents of this publication without notice.

Contact Information

iS5 Communications Inc. 5895 Ambler Dr., Mississauga, Ontario, L4W 5B7 Tel: 1+ 905-670-0004 Website: http://www.is5com.com/ Technical Support: E-mail: support@is5com.com Sales Inquiries:Phoenix Contact Sales Subsidiaries

End User License Agreement (EULA)

TERMS AND CONDITIONS FOR SOFTWARE PROGRAMS AND EMBEDDED SOFTWARE IN PRODUCTS

1) **EULA**

   *All products which consist of or include software (including operating software for hardware supplied by Supplier and software in object code format that is embedded in any hardware) and/or any documentation shall be subject to the End User License Agreement ("**EULA**") attached hereto as Exhibit A. Buyer shall be deemed to have agreed to be bound by all of the terms, conditions and obligations therein and shall ensure that all subsequent purchasers and licensees of such products shall be further bound by all of the terms, conditions and obligations therein. For software and/or documentation delivered in connection with these Terms and Conditions, that is not produced by Supplier and which is separately licensed by a third party, Buyer's rights and responsibilities with respect to such software or documentation shall be governed in accordance with such third party's applicable software license. Buyer shall, on request, enter into one or more separate "click-accept" license agreements or third party license agreements in respect thereto. Supplier shall have no further obligations with respect to such products beyond delivery thereof. Where Buyer is approved by Supplier to resell products, Buyer shall provide a copy of the EULA and applicable third party license agreements to each end user with delivery of such products and prior to installation of any software. Buyer shall notify Supplier promptly of any breach or suspected breach of the EULA or third party license agreements and shall assist Supplier in efforts to preserve Supplier's or its supplier's intellectual property rights including pursuing an action against any breaching third parties. For purposes of these terms and conditions: "software" shall mean scripts, programs, macros, computer programs, application programming and other interfaces, tools and other instructions and sets of instructions for hardware to follow, including SQL and other query languages, hypertext markup language ("**html**") and other computer mark-up languages; "**hardware**" shall mean mainframes, personal computers, servers, client/server stations, network equipment, routers, semi-conductor chips, communication lines and other equipment; and "**documentation**" shall mean documentation supplied by Supplier relating to the development, use, installation, implementation, integration, configuration, operation, modification, maintenance or support of any software.*

2) **INTELLECTUAL PROPERTY**

   *Buyer shall not alter, obscure, remove, cancel or otherwise interfere with any markings (including without limitation any trademarks, logos, trade names, or labelling applied by Supplier). Buyer acknowledges that Supplier is the sole owner of the trademarks used in association with the products and that Buyer has no right, title or interest whatsoever in such trademarks and any goodwill associated therewith and that all goodwill associated with such trademarks is owned by and shall enure exclusively to and for the benefit of Supplier. Further, Buyer shall not represent in any manner that it has acquired any ownership rights in such trademarks or other intellectual property of Supplier. Supplier will defend any claim against Buyer that any iS5Com branded product supplied under these Terms and Conditions infringes third party patents or copyrights (a "**Patent Claim**") and will indemnify Buyer against the final judgment entered by a court of competent jurisdiction or any settlements arising out of a Patent Claim, provided that Buyer: (1) promptly notifies Supplier in writing of the Patent Claim; and (2) cooperates with Supplier in the defence of the Patent Claim, and grants Supplier full and exclusive control of the defence and settlement of the Patent Claim and any subse-*

quent appeal. If a Patent Claim is made or appears likely, Buyer agrees to permit Supplier to procure for Buyer the right to continue using the affected product, or to replace or modify the product with one that is at least functionally equivalent. If Supplier determines that none of those alternatives is reasonably available, then Buyer will return the product and Supplier will refund Buyer's remaining net book value of the product calculated according to generally accepted accounting principles. Supplier has no obligation for any Patent Claim related to: (1) compliance with any designs, specifications, or instructions provided by Buyer or a third party on Buyer's behalf; (2) modification of a product by Buyer or a third party; (3) the amount or duration of use which Buyer makes of the product, revenue earned by Buyer from services it provides that use the product, or services offered by Buyer to external or internal Buyers; (4) combination, operation or use of a product with non-Supplier products, software or business processes; or (5) use of any product in any country other than the country or countries specifically authorized by Supplier.

3) **EXPORT CONTROLS AND SANCTIONS**

   a) In these Term and Conditions, "***Export Controls and Sanctions***" means the export control and sanctions laws of each of Canada, the US and any other applicable country, territory or jurisdiction including the United Nations, European Union and the United Kingdom, and any regulations, orders, guides, rules, policies, notices, determinations or judgements issued thereunder or imposed thereby.

   b) Supplier products, documentation and services provided under these Terms and Conditions may be subject to Canadian, U.S. and other country Export Controls and Sanctions. Buyer shall accept and comply with all applicable Export Control and Sanctions in effect and as amended from time to time pertaining to the export, re-export and transfer of Supplier's products, documentation and services. Buyer also acknowledges and agrees that the export, re-export or transfer of Supplier products, documentation and services contrary to applicable Export Controls and Sanctions may be a criminal offence.

   c) For greater certainty, Buyer agrees that (i) it will not directly or indirectly export, re-export or transfer Supplier products, documentation and services provided under these Terms and Conditions to any individual or entity in violation of any aforementioned Export Controls and Sanctions; (ii) it will not directly or indirectly export, re-export or transfer any such products, documentation and services to any country or region of any country that is prohibited by any applicable Export Controls and Sanctions or for any of the following end-uses, or in any of the following forms unless expressly authorized by any applicable government permit issued under or otherwise expressly permitted by applicable Export Controls and Sanctions:

      i) For use that is directly or indirectly related to the research, design, handling, storage, operation, detection, identification, maintenance, development, manufacture, production or dissemination of chemical, biological or nuclear weapons, or any missile or other delivery systems for such weapons, space launch vehicles, sounding rockets or unmanned air vehicle systems;

      ii) Technical information relating to the design, development or implementation of the cryptographic components, modules, interfaces, or architecture of any software; or

      iii) Source code or pseudo-code, in any form, of any of the cryptographic components, modules, or interfaces of any software.

   d) Buyer confirms that it is not (i) listed as a sanctioned person or entity under any Export Controls and Sanctions list of designated persons, denied persons or specially designated

nationals maintained by the Canadian Department of Foreign Affairs, Trade and Development, the Canadian Department of Public Safety and Emergency Preparedness, the U.S. Office of Foreign Assets Control of the U.S. Department of the Treasury, the U.S. Department of State, the U.S. Department of Commerce, United Nations Security Council, the European Union or any EU member state, HM's Treasury, or any other department or agency of any of the aforementioned countries or territories, or the United Nations or any other country's sanctions-related list; (ii) owned or controlled by such person or entity; or (iii) acting in any capacity on behalf of or for the benefit of such person or entity. Buyer also confirms that this applies equally to any of its affiliates, joint venture partners, subsidiaries and to the best of Buyer's knowledge, any of its agents or representatives.

Exhibit A: End User License Agreement

IMPORTANT – READ CAREFULLY: iS5 Communications Inc. ("**iS5Com**") licenses the iS5Com Materials (as defined below) subject to the terms and conditions of this end user license agreement (the "**EULA**"). BY SELECTING "ACCEPT" OR OTHERWISE EXPRESSLY AGREEING TO THIS EULA, BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, OR BY USING THE HARDWARE (AS DEFINED BELOW), ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS EULA BECOME LEGALLY BINDING ON THE CUSTOMER.This End User License Agreement (the "**EULA**") supplements the Terms and Conditions or such other terms and conditions between iS5Com or, if applicable, a reseller for iS5Com, and the Customer (as defined below) (in either case, the "**Contract**").

1) **DEFINITIONS**

   *"**Confidential Information**" means all data and information relating to the business and management of iS5Com, including iS5Com Materials, trade secrets, technology and records to which access is obtained hereunder by the Customer, and any materials provided by iS5Com to the Customer, but does not include any data or information which: (a) is or becomes publicly available through no fault of the Customer; (b) is already in the rightful possession of the Customer prior to its receipt from iS5Com; (c) is already known to the Customer at the time of its disclosure to the Customer by iS5Com and is not the subject of an obligation of confidence of any kind; (d) is independently developed by the Customer; (e) is rightfully obtained by the Customer from a third party; (e) is disclosed with the written consent of iS5Com; or (f) is disclosed pursuant to court order or other legal compulsion.*

   – "*Customer*" means the licensee of the iS5Com Software pursuant to the Contract.

   – "**iS5Com Documentation**" means Documentation supplied by or on behalf of iS5Com under the Contract relating to the development, use, installation, implementation, integration, configuration, operation, modification, maintenance or support of iS5Com Software, or iS5Com Firmware.

   – "**iS5Com Firmware**" means iS5Com Software in object code format that is embedded in iS5Com Hardware.

   – "**iS5Com Hardware**" means Hardware supplied by or on behalf of iS5Com under the Contract.

   – "**iS5Com Materials**" means, collectively, the iS5Com Software and the iS5Com Documentation.

- "**iS5Com Software**" means Software supplied by or on behalf of iS5Com under the Contract. For greater certainty, iS5Com Software shall include all operating Software for iS5Com Hardware, and iS5Com Firmware.

- "**Documentation**" means written instructions and manuals of a technical nature.

- "**EULA**" means this End User License Agreement.

- "**Hardware**" means hardware, mainframes, personal computers, servers, client/server stations, network equipment, routers, semi-conductor chips, communication lines and other equipment.

- "**Intellectual Property Rights**" means any and all proprietary rights provided under: (i) patent law; (ii) copyright law (including moral rights); (iii) trade-mark law; (iv) design patent or industrial design law; (v) semi-conductor chip or mask work law; or (vi) any other statutory provision or common law principle applicable to this EULA, including trade secret law, which may provide a right in either Hardware, Software, Documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how generally, or the expression or use of such Hardware, Software, Documentation, Confidential Information, ideas, formulae, algorithms, concepts, inventions, processes or know-how trade secret law; any and all applications, registrations, licenses, sub-licenses, franchises, agreements or any other evidence of a right in any of the foregoing; and all licenses and waivers and benefits of waivers of the intellectual property rights set out herein, all future income and proceeds from the intellectual property rights set out herein, and all rights to damages and profits by reason of the infringement of any of the intellectual property rights set out herein.

- "**Software**" means scripts, programs, macros, computer programs, application programming and other interfaces, tools and other instructions and sets of instructions for hardware to follow, including SQL and other query languages, hypertext markup language ("html") and other computer mark-up languages.

- "**Third Party License Terms**" means additional terms and conditions that are applicable to Third Party Software.

- "**Third Party Software**" means Software owned by any third party, licensed to iS5Com and sublicensed to the Customer.

- "**Update**" means a supplemented or revised version of iS5Com Software which rectifies bugs or makes minor changes or additions to the functionality of iS5Com Software and is designated by iS5Com as a higher release number from, for example, 6.06 to 6.07 or 6.1 to 6.2.

2) **LICENSE**

- **2.1 License Grant**

    The iS5Com hereby grants to the Customer, subject to any Third Party License Terms, a non-exclusive, non-transferable, non-sublicensable right and licence to use iS5Com Materials solely in object code format, solely for the Customer's own business purposes, solely in accordance with this EULA (including, for greater certainty, subject to Section 6.1 of this EULA) and the applicable iS5Com Documentation, and, in the case of iS5Com Firmware, solely on iS5Com Hardware on which iS5Com Firmware was installed, provided that Customer may only install iS5Com Software on such number of nodes expressly set out in the Contract.

- **2.2 License Restrictions**

Except as otherwise provided in Section 2.1 above, the Customer shall not: (a) copy iS5Com Materials for any purpose, except for the sole purpose of making an archival or back-up copy; (b) modify, translate or adapt the iS5Com Materials, or create derivative works based upon all or part of such iS5Com Materials; (c) assign, transfer, loan, lease, distribute, export, transmit, or sublicense iS5Com Materials to any other party; (d) use iS5Com Materials for service bureau, rent, timeshare or similar purposes; (e) decompile, disassemble, decrypt, extract, or otherwise reverse engineer, as applicable, iS5Com Software or iS5Com Hardware; (f) use iS5Com Materials in a manner that uses or discloses the Confidential Information of iS5Com or a third party without the authorization of such person; (g) permit third parties to use iS5Com Materials in any way that would constitute breach of this EULA; or (h) otherwise use iS5Com Materials except as expressly authorized herein.

– **2.3 Updates and Upgrades**

The license granted hereunder shall apply to the latest version of iS5Com Materials provided to the Customer as of the effective date of this EULA, and shall apply to any Updates and Upgrades subsequently provided to the Customer by iS5Com pursuant to the terms of this EULA. Customer shall only be provided with Updates and/or Upgrades if expressly set out in the Contract.

– **2.4 Versions**

In the event any Update or Upgrade includes an amended version of this EULA, Customer will be required to agree to such amended version in order to use the applicable iS5Com Materials and such amended EULA shall be deemed to amend the previously effective version of the EULA.

– **2.5 Third Party Software**

Customer shall comply with any Third Party License Terms.

3) **OWNERSHIP**

– **3.1 Intellectual Property**

Notwithstanding any other provision of the Contract, iS5Com and the Customer agree that iS5Com is and shall be the owner of all Intellectual Property Rights in iS5Com Materials and all related modifications, enhancements, improvements and upgrades thereto, and that no proprietary interests or title in or to the intellectual property in iS5Com Materials is transferred to the Customer by this EULA. iS5Com reserves all rights not expressly granted to the Customer under Section 2.1.

– **3.2 Firmware**

iS5Com and the Customer agree that any and all iS5Com Firmware in or forming a part of iS5Com Hardware is being licensed and not sold, and that the words "purchase," "sell" or similar or derivative words are understood and agreed to mean "license," and that the word "Customer" as used herein are understood and agreed to mean "licensee," in each case in connection with iS5Com Firmware.

– **3.3 Third Party Software**

Certain of iS5Com Software provided by iS5Com may be Third Party Software owned by one or more third parties and sublicensed to the Customer. Such third parties retain ownership of and title to such Third Party Software, and may directly enforce the Customer's obligations hereunder in order to protect their respective interests in such Third Party Software.

4) **CONFIDENTIALITY**

– **4.1 Confidentiality**

The Customer acknowledges that iS5Com Materials contain Confidential Information of iS5Com and that disclosure of such Confidential Information to any third party could cause great loss to iS5Com. The Customer agrees to limit access to iS5Com Materials to those employees or officers of the Customer who require access to use iS5Com Materials as permitted by the Contract and this EULA and shall ensure that such employees or officers keep the Confidential Information confidential and do not use it otherwise than in accordance with the Contract and this EULA. The obligations set out in this Section 4 shall continue notwithstanding the termination of the Contract or this EULA and shall only cease to apply with respect to such part of the Confidential Information as is in, or passes into, the public domain (other than in connection with the Customer's breach of this EULA) or as the Customer can demonstrate was disclosed to it by a third person who did not obtain such information directly or indirectly from iS5Com.

– **4.2 Irreparable Harm**

Without limiting any other rights or remedies available to iS5Com in law or in equity, the Customer acknowledges and agrees that the breach by Customer of any of the provisions of this EULA would cause serious and irreparable harm to iS5Com which could not adequately be compensated for in damages and, in the event of a breach by the Customer of any of such provisions, the Customer hereby consents to an injunction against it restraining it from any further breach of such provisions.

– **4.3 Security**

*Any usernames, passwords and/or license keys ("**Credentials**") provided to you by iS5Com shall be maintained by the Customer and its representatives in strict confidence and shall not be communicated to or used by any other persons. THE CUSTOMER SHALL BE RESPONSIBLE FOR ALL USE OF CREDENTIALS, REGARDLESS OF THE IDENTITY OF THE PERSON(S) MAKING SUCH USE, AND WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, IS5COM SHALL HAVE NO RESPONSIBILITY OR LIABILITY IN CONNECTION WITH ANY UNAUTHORIZED USE OF CREDENTIALS.*

5) **LIMITATION OF LIABILITY**

– **5.1 Disclaimer**

EXCEPT FOR THE EXPRESS WARRANTIES MADE BY IS5COM IN THE CONTRACT, (A) IS5COM MAKES NO AND HEREBY EXPRESSLY DISCLAIMS, AND THE PARTIES HERETO HEREBY EXPRESSLY WAIVE AND EXCLUDE TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS, AND THE CUSTOMER AGREES NOT TO SEEK OR CLAIM ANY BENEFIT THEREOF, IN EACH CASE, ALL WARRANTIES, CONDITIONS, REPRESENTATIONS OR INDUCEMENTS (AND THERE ARE NO OTHER WARRANTIES, CONDITIONS, REPRESENTATIONS OR INDUCEMENTS, ORAL OR WRITTEN, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, OF ANY KIND WHATSOEVER SET OUT HEREIN) WITH RESPECT TO THE IS5COM MATERIALS, INCLUDING AS TO THEIR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, DESIGN OR CONDITION, COMPLIANCE WITH THE REQUIREMENTS OF ANY APPLICABLE LAWS, CONTRACT OR SPECIFICATION, NON- INFRINGEMENT OF THE RIGHTS OF OTHERS, ABSENCE OF LATENT DEFECTS, OR AS TO THE ABILITY OF THE IS5COM MATERIALS TO MEET CUSTOMER'S REQUIREMENTS OR TO OPERATE OF ERROR

*FREE; AND (B) THE IS5COM MATERIALS ARE PROVIDED "**AS IS**" WITHOUT WARRANTY OR CONDITION OF ANY KIND.*

– **5.2 Limitation of Liability**

EXCEPT AS EXPRESSLY PROVIDED IN THE CONTRACT, IN NO EVENT SHALL IS5COM BE LIABLE TO THE CUSTOMER OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSE-QUENTIAL DAMAGES ARISING UNDER OR IN CONNECTION WITH THIS EULA EVEN IF ADVISE OF THE POSSIBILITY THEREOF. THIS LIMITATION SHALL APPLY IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND OR CLAIM, INCLUDING BREACH OF CONTRACT, NEGLI-GENCE, TORT OR ANY OTHER LEGAL THEORY, AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES AND/OR FAILURE OF THE ESSENTIAL PURPOSE OF THIS EULA.

6) **TERM**

– **6.1 Term**

Customer's right to use iS5Com Materials shall terminate at such time as set out in the Con-tract or upon termination or expiration of the Contract, in each case at which time this EULA shall be deemed to terminate.

– **6.2 Survival**

Each of Sections 1, 2.4, 3, 4, 5, 6.2, and 7 shall survive termination of the EULA.

7) **MISCELLANEOUS**

– **7.1 Miscellaneous**

This EULA is (together with, as applicable, any click-wrap license agreement or Third Party Li-cense Terms pertaining to the use of iS5Com Materials) the entire agreement between the Customer and iS5Com pertaining to the Customer's right to access and use iS5Com Materials, and supersedes all prior or collateral oral or written representations or agreements related thereto. Notwithstanding anything to the contrary contained in the Contract, to the extent of any inconsistency between this EULA and the Contract, or any such applicable click-wrap agreement, this EULA shall take precedence over the Contract and such click- wrap agree-ment. In the event that one or more of the provisions is found to be illegal or unenforceable, this EULA shall not be rendered inoperative but the remaining provisions shall continue in full force and effect. The parties expressly disclaim the application of the United Nations Conven-tion for the International Sale of Goods. This EULA shall be governed by the laws of the Prov-ince of Ontario, Canada, and federal laws of Canada applicable therein. In giving effect to this EULA, neither party will be or be deemed an agent of the other for any purpose and their re-lationship in law to the other will be that of independent contractors. Any waiver of any terms or conditions of this EULA: (a) will be effective only if in writing and signed by the party grant-ing such waiver, and (b) shall be effective only in the specific instance and for the specific pur-pose for which it has been given and shall not be deemed or constitute a waiver of any other provisions (whether or not similar) nor shall such waiver constitute a continuing waiver unless otherwise expressly provided. The failure of either party to exercise, and any delay in exercis-ing, any of its rights hereunder, in whole or in part, shall not constitute or be deemed a waiver or forfeiture of such rights, neither in the specific instance nor on a continuing basis. No single or partial exercise of any such right shall preclude any other or further exercise of such right or the exercise of any other right. Customer shall not assign or transfer this EULA or any of its rights or obligations hereunder, in whole or in part, without the prior written consent of

iS5Com. The division of this EULA into sections and the insertion of headings are for convenience of reference only and shall not affect the construction or interpretation of this EULA. References herein to Sections are to sections of this Agreement. Where the word "include", "includes" or "including" is used in this EULA, it means "include", "includes" or "including", in each case, "without limitation". All remedies provided for iS5Com under this EULA are non-exclusive and are in addition, and without prejudice, to any other rights as may be available to of iS5Com, whether in law or equity. By electing to pursue a remedy, of iS5Com does not waive its right to pursue any other available remedies. The parties acknowledge that they have required this Agreement to be written in English. Les parties aux présentes reconnaissent qu'elles ont exigé que la présente entente soit rédigée en anglais.

– **7.2 Subject to Change**

Terms and Conditions are subject to change. For the latest information please visit:
https://is5com.com/terms-and-conditions/

Preface

This guide is intended for use of network technical support skilled persons who are responsible for installation, commissioning, and maintenance of the device.

Alerts

WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.

CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.

DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.

NOTES provide additional information and details.

Temperature hazard − above TS2 limits. To be accessible by Skilled Persons only

Multiple power source - redundant power

Protective earthing conductor

Electrical hazard − above ES2 limits. To be accessible by Skilled Persons only

Related Documents

1)   RAPTOR Quick Start Guide
2)   RAPTOR WebUI Manuals
3)   RAPTOR CLI User Manuals
4)   RAPTOR Configuration Manuals

Training

Training is a key for customers to continue maintaining and using their iS5Com's device. Customers can select a standard training course or customized training courses at the iS5Com facility or a customer provided facility. Go to https://is5com.com/training/ to submit your request for training or contact an iS5Com Sales Representative.

iSUPPORT

PHONE SUPPORT

Support can be directed to iS5Com's Technical Action Center at https://is5com.com/isupport/ . You can also call Tech Support: +1 844-475-8324

SERVICE LEVEL AGREEMENTS

Service Level Agreements can be tailored to suit your needs with our standard Service Level Agreement packages or through customized solutions.

RETURN MANUFACTURING AUTHORIZATION

Return Manufacturing Authorization is easy and simplified for our customers. Contact the support team at https://is5com.com/isupport/ or call us to complete and submit your repair or replacement request through our Technical Action Centre.

Contents

1. Introduction

The RAPTOR® iMX350 is an Intelligent Cyber Secure Platform running the iBiome OS. The iBiome is an all-encompassing operating system that supports switching and routing on a single platform. RAPTOR has been designed for future scalability. Its modular system of field replaceable line blocks, hot swappable power supplies, and its ability to run third party software applications makes it a very flexible platform for today and the future.

In this document iMX350 and RAPTOR are used interchangeably.

Figure 1:   RAPTOR iMX350

1.1. Key Features and Benefits of RAPTOR iMX350

FEATURES		BENEFITS
Single platform function		The multi-service platform allows the user to connect various plug-in modules to meet their functional requirements.
Simplified GUI- easy to use		Allows easy configuration and monitoring with a web-based User Interface; eliminates the need for more complex terminal emulation programs; reduced cost of deployment; one platform—multiple functions; built-in LCD display provides easy access to information
Robust industrial design		-40°C to +85°C (-40°F to 185°F) operating temperature, no fans needed; IP 40
Power over Ethernet		The iMX350 may be factory equipped to support Power over Ethernet (PoE). The iMX350 can deliver up to 720 Watts of power, from an external PoE power supply, with up to 240 Watts per 8GRJ45P line module.

2. Line Modules

2.1. Line Modules for Slots 1-4

Part #		Slots 1-4 Line Module Description
BLK		Blank Module
4DB09		4 x Serial DB09 Interfaces, RS 232/422/485
IROC		Industrial Computing Module is in itself a configurable part and will be described further in its own section of the manual along with its configurable options. Only two iROCs may be installed in the RAPTOR at a time. Storage on the iROC is available as either 256 GB, 512 GB, 1 TB, or 2 TB *SSD* with 3K *P/E* (Program/Erase) cycles. The *SSD*s are industrial grade rated for a temperature range of -40°C to +85°C. They provide an SATA III 6 Gbps interface. The CPU is an Intel 3950, 4-core, 4-threads, 1.6GHz, and with 8GB LPDDR4 memory. The faceplate has a 1 Gbps network interface, *HDMI* port capable of 1080p, USB 2.0, USB 3.0 and RJ45 RS232 Console port. There is a reset button and two LEDs (Power and Alarm).

2.2. Line Modules for Slots 1-3 only

Part #		Slots 1 - 3 Line Modules Description
8GRJ45		8 X 10/100/1000Base-T(X) RJ45
8GRJ45P		8 X 10/100/1000Base-T(X) RJ45, Power over Ethernet (*PoE*) capable.
8GSFP		8 X 100/1000Base-X *SFP* (optical transceivers are not included)
4RJ4SFP		4 X 10/100/1000Base-T(X) RJ45 plus 4 X 100/1000Base-X *SFP* (optical transceivers are not included)

2.3. Line Module for Slot 4 only

Part #		Slot 4 Line Module Description
4TGSFP		4 X 1G/10GBase-X *SFP* (optical transceivers are not included)

2.4. Power Supply Options

Part #	Description	Nominal Range/ Operating Range
LV	Low Voltage Power Module	24 VDC, 2.5 A, 60 W / 10-36 VDC
MV	Medium Voltage Power Module	48 VDC, 1.25 A, 60 W / 36-72 VDC
HV	High Voltage Power Module	100-240 VAC, 50/60 Hz, 1 A, 60 VA; 100-240 VDC, 1A, 60W / 85-264 VAC; 88-300 VDC
HV2	High Voltage Power Module	100-240 VAC, 50/60 Hz, 1 A, 60 VA; 100-240 VDC, 1A, 60W / 85-264 VAC; 88-300 VDC

2.5. Line Modules Details

The line modules (*LM*) are as shown below:

iRM-8GRJ45 - 8 x 10/100/1000 Base -T(X) RJ45 (to be used in Slots 1, 2, and 3)

Both the right and left LEDs for each port behave identically. The green LED will be in an ON state when the link is up, and will flash when there is network activity. The LED will be OFF when the link is down.

iRM-8GRJ45P - 8 x 10/100/1000 Base -T(X) RJ45 (to be used in Slots 1, 2, and 3)

Both the right and left LEDs for each port behave identically. The green LED will be in an ON state when the link is up, and will flash when there is network activity. The LED will be OFF when the link is down.

NOTE: Users of the iRM-8GRJ45 line module should rely on the following diagram for port numbering.

Operating temperature is restricted to -40°C to +75°C

iRM-8GSFP - 8 x 100/1000Base-X *SFP* (to be used in Slots 1, 2, and 3)

The green LED for each port will be in an ON state when the link is up, and will flash when there is network activity. The LED will be OFF when the link is down.

iRM-2RBX - Support for 2 RedBoxes or 1 QuadBox (supported in slots 1-4)

The numbering convention for the different RedBoxes in the different line module slots are as follows:

Table 1:   Naming Convention for RedBoxes

Redundant Switch	LM1	LM2	LM3	LM4
First	Red 1	Red 3	Red 5	Red 7
Second	Red 2	Red 4	Red 6	Red 8

By default, both redundant switches of the HSR-PRP line card are connected to the main switch through the I-port. However, there may be cases when only one or no redundant switch is required. For these cases it is possible to disable redundancy on a redundant interface so that two Ethernet ports can be used instead, thereby by-passing the redundant switch.

Only half of the possible line card ports are routed to the HSR-PRP line card. It is therefore only possible to get four Ethernet ports to the connectors (or two 1G Ethernet ports in the case of LM4 as HSR-PRP line card does not support 10G). The following port combinations can be achieved for the four different slots:

Table 2: LM1 Line Card port description

LM1 Line Card	HSR-PRP				8GRJ45
Red 1 Redundancy	Enable	Enable	Disable	Disable	-
Red 2 Redundancy	Enable	Disable	Enable	Disable	-
Port 1	Red 1A	Red 1A	Gi 0/1	Gi 0/1	Gi 0/1
Port 2	Red 1B	Red 1B	Gi 0/2	Gi 0/2	Gi 0/2
Port 3	Red 2A	Gi 0/3	Red 2A	Gi 0/3	Gi 0/3
Port 4	Red 2B	Gi 0/4	Red 2B	Gi 0/4	Gi 0/4
Port 5	-	-	-	-	Gi 0/5
Port 6	-	-	-	-	Gi 0/6
Port 7	-	-	-	-	Gi 0/7
Port 8	-	-	-	-	Gi 0/8

Table 3: LM2 Line Card port description (Sheet 1 of 2)

LM2 Line Card	HSR-PRP				8GRJ45
Red 3 Redundancy	Enable	Enable	Disable	Disable	-
Red 4 Redundancy	Enable	Disable	Enable	Disable	-
Port 1	Red 3A	Red 3A	Gi 0/9	Gi 0/9	Gi 0/9
Port 2	Red 3B	Red 3B	Gi 0/10	Gi 0/10	Gi 0/10
Port 3	Red 4A	Gi 0/11	Red 4A	Gi 0/11	Gi 0/11
Port 4	Red 4B	Gi 0/12	Red 4B	Gi 0/12	Gi 0/12
Port 5	-	-	-	-	Gi 0/13

Table 3: LM2 Line Card port description (Continued) (Sheet 2 of 2)

LM2 Line Card	HSR-PRP				8GRJ45
Port 6	-	-	-	-	Gi 0/14
Port 7	-	-	-	-	Gi 0/15
Port 8	-	-	-	-	Gi 0/16

Table 4: LM3 Line Card port description

LM3 Line Card	HSR-PRP				8GRJ45
Red 5 Redundancy	Enable	Enable	Disable	Disable	-
Red 6 Redundancy	Enable	Disable	Enable	Disable	-
Port 1	Red 5A	Red 5A	Gi 0/17	Gi 0/17	Gi 0/17
Port 2	Red 5B	Red 5B	Gi 0/18	Gi 0/18	Gi 0/18
Port 3	Red 6A	Gi 0/19	Red 6A	Gi 0/19	Gi 0/19
Port 4	Red 6B	Gi 0/20	Red 6B	Gi 0/20	Gi 0/20
Port 5	-	-	-	-	Gi 0/21
Port 6	-	-	-	-	Gi 0/22
Port 7	-	-	-	-	Gi 0/23
Port 8	-	-	-	-	Gi 0/24

Table 5: LM4 Line Card port description

LM4 Line Card	HSR-PRP				4TGSFP
Red 7 Redundancy	Enable	Enable	Disable	Disable	-
Red 8 Redundancy	Enable	Disable	Enable	Disable	-
Port 1	Red 7A	Red 7A	Ex 0/1	Ex 0/1 (1G)	Ex 0/1
Port 2	Red 7B	Red 7B	-	-	Ex 0/2
Port 3	Red 8A	Ex 0/3 (1G)	Red 8A	Ex 0/3 (1G)	Ex 0/3
Port 4	Red 8B	-	Red 8B	-	Ex 0/4

The HSR-PRP line card has four combo ports consisting of four RJ45 and four SFP interfaces.

Each combo port has one RJ45 and one SFP interface. If an SFP module is detected, the SFP interface is the active combo port interface. If there is no SFP module inserted then the RJ45 interface remains active.

The IEC 62439-3 HSR-PRP standard also requires that Port-A is to the left of Port-B (Raptor) (or above in the case of MicroRaptor). With the line card being flipped up-side-down between odd and even slots the HSR-PRP line card could have either four RJ45 interfaces followed by four SFP slots or the other way round. To locate the correct interface, information can be obtained through the front-panel LCD:

- ◉ RJ45 or SFP link up (Red 5A and Red 8A)
- ◉ RJ45 or SFP link down (Red 5B and Gi 0/19)
- ◎ SFP can be inserted as RJ45 is being used (Gi 0/20, Ex 0/1)
- ◉ Port unavailable (RJ45 port when SFP is detected (Gi 0/19, Red 8A) or no connection possible (Ex 0/2))
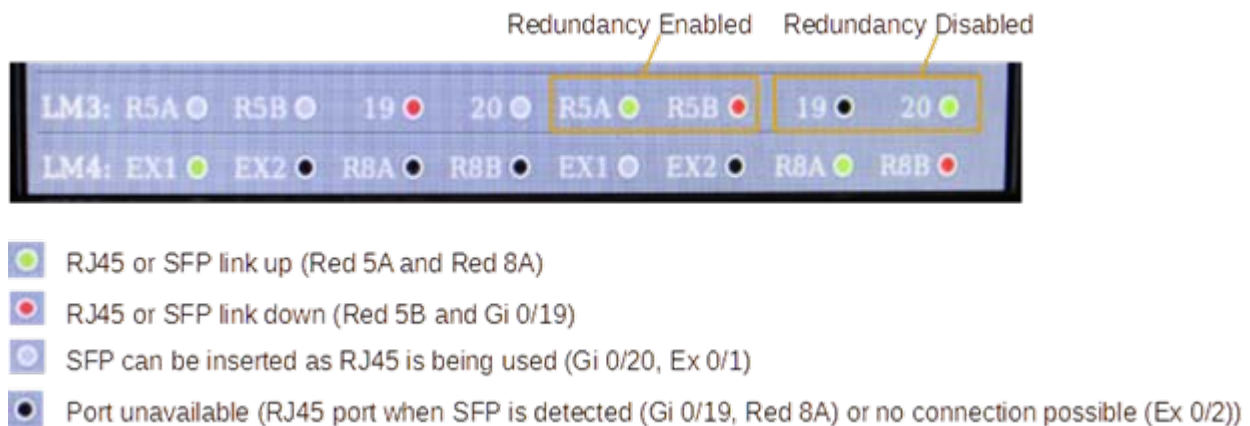
The CLI provides a redundancy map to indicate the active ports on the HSR/PRP module as well:

```
iS5comm# show interfaces redundant map

LM3
---
Redundancy switches:
        Red 5 - Enabled - I-port connected to Gi0/17
        Red 6 - By-passed
External connections:
Position:       1        2        3        4        5        6        7        8
                ---------------------------------------------------------------
Connector:    : SFP    : SFP    : SFP    : SFP    : RJ45   : RJ45   : RJ45   : RJ45   :
                ---------------------------------------------------------------
SFP Detected:   NO       NO       YES      NO       -        -        -        -
Port:           X        X        Gi0/19   X        Red-5A   Red-5B   X        Gi0/20

LM4
---
Redundancy switches:
        Red 7 - By-passed
        Red 8 - Enabled - I-port connected to Ex0/3
External connections:
Position:       1        2        3        4        5        6        7        8
                ---------------------------------------------------------------
Connector:    : RJ45   : RJ45   : RJ45   : RJ45   : SFP    : SFP    : SFP    : SFP    :
                ---------------------------------------------------------------
SFP Detected:   -        -        -        -        NO       NO       YES      YES
Port:           Ex0/1    X        X        X        X        X        Red-8A   Red-8B
iS5comm#
```

iRM-4RJ4SFP - 8 x 10/100/1000 Base -T(X) RJ45 plus 4 x 100/1000Base-X *SFP* (to be used in Slots 1, 2, and 3)

The green LEDs for each port will be in an ON state when the link is up, and will flash when there is network activity. The LEDs will be OFF when the link is down.

iRM-4TGSFP - 4 x 1G/10GBase-X *SFP* (only for Slot 4)

iRM-8SRJ45 - 8-port RJ45 RS232/422/485 (slots 1-4)
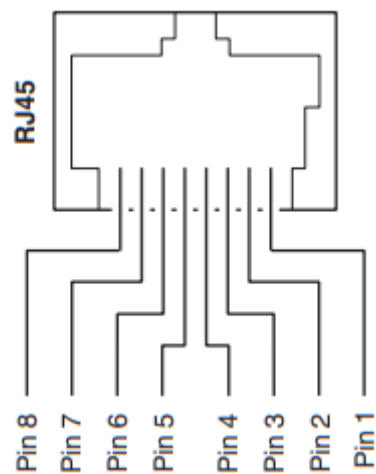

Figure 1: RJ45 Serial Pin Assignment

Table 6: Serial RJ45 Port Pin Configuration (Sheet 1 of 2)

RJ45 Pin	RS232 Mode	RS485-half mode	RS422/485 full mode
1			
2			
3	GND	GND	GND
4	GND	GND	GND
5	RX		RX+
6	TX	TX+/RX+	TX+
7	CTS		RX-

Table 6: Serial RJ45 Port Pin Configuration (Continued) (Sheet 2 of 2)

RJ45 Pin	RS232 Mode	RS485-half mode	RS422/485 full mode
8	RTS	TX-/RX-	TX-

iRM-4DB09 - 4-port DB09 RS232/422/485 (slots 1-4)

Figure 2: DB9 Serial Pin Assignment
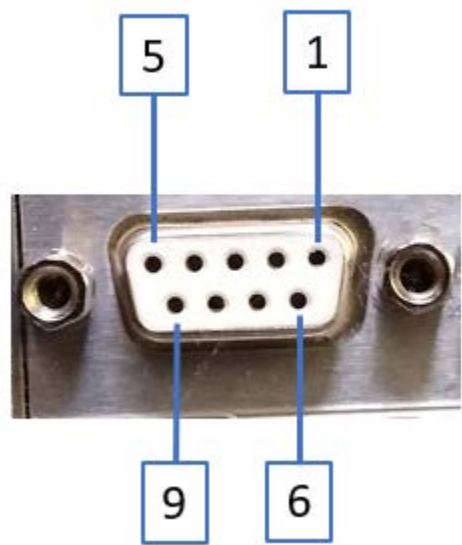
Table 7: Serial DB9 Port Pin Configuration (Sheet 1 of 2)

DB9 Pin	RS232 Mode	RS485-half mode	RS422/485 full mode
1			

Table 7: Serial DB9 Port Pin Configuration (Continued) (Sheet 2 of 2)

DB9 Pin	RS232 Mode	RS485-half mode	RS422/485 full mode
2	RX		RX+
3	TX	TX+/RX+	TX+
4			
5	GND	GND	GND
6	GND	GND	GND
7	RTS	TX-/RX-	TX-
8	CTS		RX-
9	GND	GND	GND

iRM-iROC - Computing Module

1. Ethernet Port
2. Reset
3. LEDs (Pwr & Alarm)
4. USB 3.0
5. USB 2.0
6. HDMI
7. Console Port
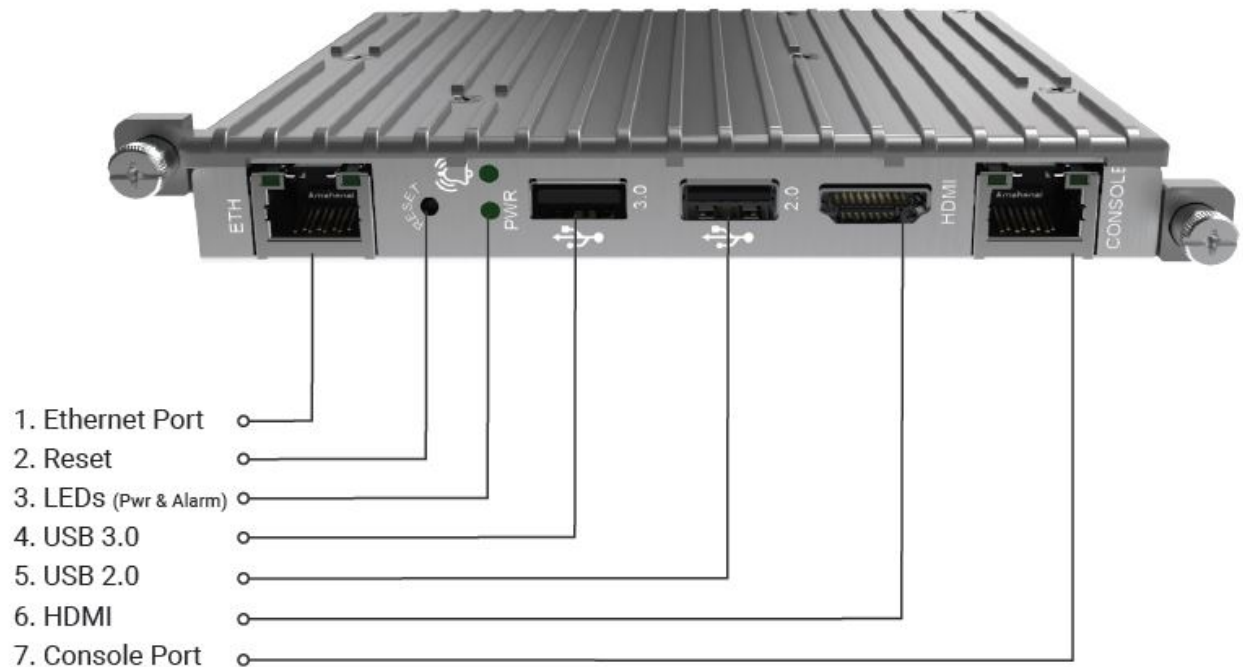
Operating temperature is restricted to -40°C to +70°C

This is an example of a label that is affixed to the iROC module.

Figure 3: This is an example of a label that is affixed to the iROC module.

The following table describes the iROC module configuration options.

Option	Order Code	Description
Model	iRM-iROC	iROC Computing Module, *HDMI* version 1.4 port supporting 1080p, USB 2.0 Port, USB 3.0 Port, RS 232 Console Port, 10/100/1000TX RJ45 Ethernet Port
CPU and Memory	01	Intel E3940, 4-core, 4-threads, 1.6 GHz, with 8GB LPDDR4 Memory.
Operating System	W11	Windows 11 Pro Operating System
	L01	Ubuntu Desktop v. 22.04.3 LTS
Storage	256	256 GB *SSD* with an operating temperature range of -40°C to +70°C. It has a SATA III 6 Gbps interface and 3K *P/E* cycles.
	512	512 GB *SSD* with an operating temperature range of -40°C to +70°C. It has a SATA III 6Gbps interface and 3K *P/E* cycles.
	1TB	1 TB Industrial SSD Storage temperature range of -40°C to +70°C. It has a SATA III 6Gbps interface and 3K *P/E* cycles.

Option	Order Code	Description
	2TB	2 TB Industrial SSD Storage temperature range of -40°C to +70°C. It has a SATA III 6Gbps interface and 3K *P/E* cycles.
Module Notes		The LEDs on the console port of the iROC are nonoperational at this time. Note that the USB can supply up to a maximum of 500 mA.

2.6. iROC Default Passwords

Table 8:

Operating System	Default User Name	Default Password
Windows 11	User configures this on first start	User configures this on first start
Ubuntu	user	user

2.7. iROC Network Interfaces on the iMX350

The following table describes the iROCs Ethernet connections and how they appear in Ubuntu.

Table 9:   (Sheet 1 of 2)

Connection	Ubuntu	Windows
Front-panel RJ45 Ethernet	Shows up as enp4s0	Shows up as Ethernet 4 (Intel(R) I211 Gigabit Network Connection)
Front-panel Console Port	RS232 Port that is managed by operating system and can be used in different ways.	RS232 Port that is managed by operating system and can be used in different ways.
Back-plane Ethernet connection 1	Shows up as enp1s0	Shows up as Ethernet 5(Intel(R) I210 Gigabit Backplane Connection)
Back-plane Ethernet connection 2	Shows up as enp2s0	Shows up as Ethernet 6(Intel(R) I210 Gigabit Backplane Connection)

Table 9: (Continued) (Sheet 2 of 2)

Connection	Ubuntu	Windows
Back-plane Ethernet connection 3	Shows up as enp3s0 (only available in LM4)	Shows up as Ethernet 7 (Intel(R) I210 Gigabit Backplane Connection) (only available in LM4)

Figure 4: iROC Console Port Pin Assignment
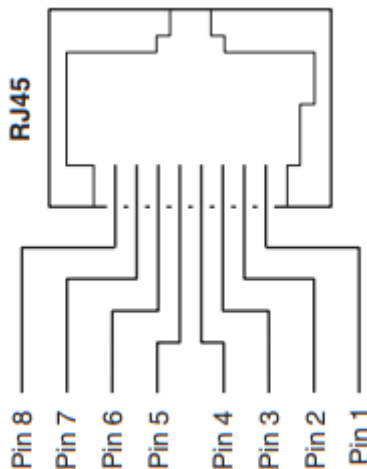
Table 10:

RJ45 Pin	RS232
1	
2	
3	TX
4	GND
5	GND
6	RX
7	
8	

This table describes how the iROC backplane connections are mapped to the switch.

Table 11: (Sheet 1 of 2)

iROC Slot Location	enp1s0/Ethernet 5	enp2s0/Ethernet 6	enp3s0/Ethernet 7
LM1	Gi0/1	Gi0/5	

Table 11:   (Continued) (Sheet 2 of 2)

iROC Slot Location	enp1s0/Ethernet 5	enp2s0/Ethernet 6	enp3s0/Ethernet 7
LM2	Gi0/9	Gi0/13	
LM3	Gi0/17	Gi0/21	
LM4	Ex0/1	Ex0/3	Ex0/4

2.8. Mechanical Drawing of a Line Module (generic)
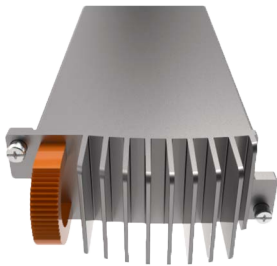
Figure 5:   Mechanical Drawing of a Line Module (generic)
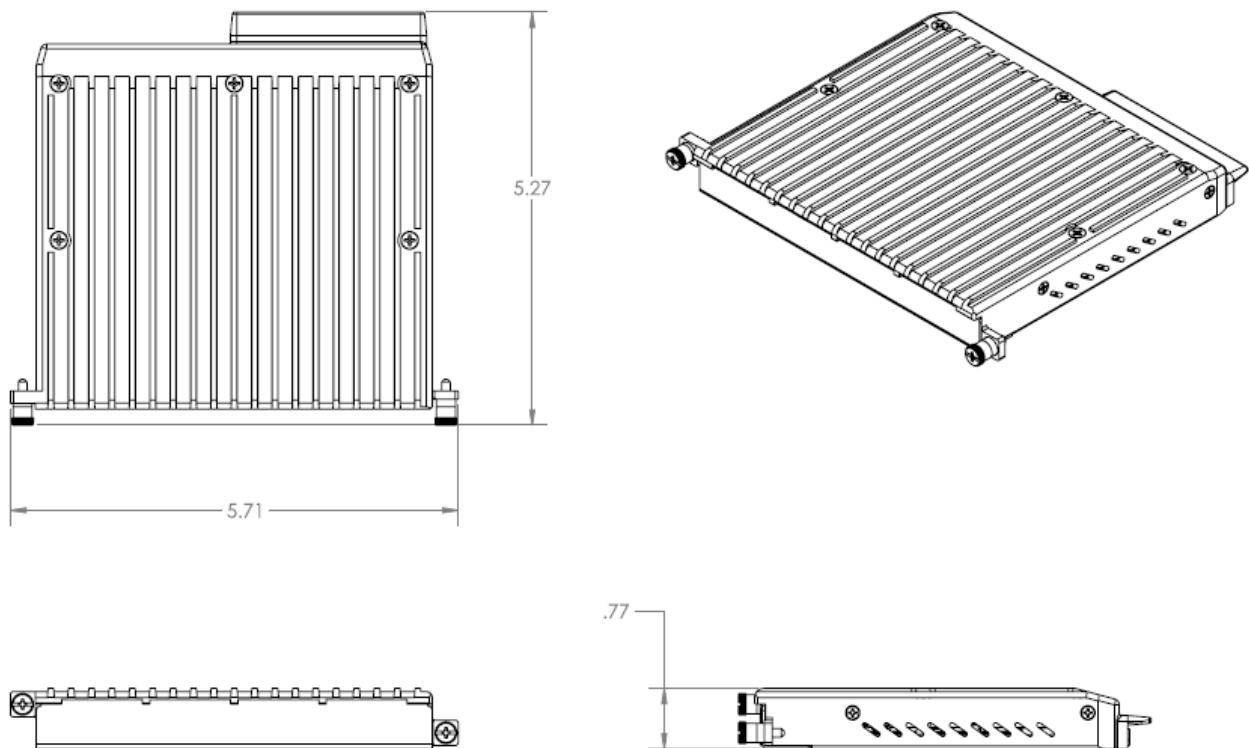
All dimensions are shown in inches.

3. Power Supply Modules

3.1. List of Power Supply Modules

Figure 1: Power Supply Module

PART #	DESCRIPTION	NOMINAL RANGE / OPERATING RANGE
LV	Low Voltage Power Module	24 VDC Nominal, 2.5 A, 60 W, 10-36 VDC Operating
LV2	Low Voltage Power Module	24 VDC Nominal, 2.5 A, 60 W, 10-36 VDC Operating
MV	Medium Voltage Power Module	48 VDC Nominal, 1.25 A, 60 W, 36-72 VDC Operating
MV2	Medium Voltage Power Module	48 VDC Nominal, 1.25 A, 60 W, 36-72 VDC Operating
HV	High Voltage Power Module	Nominal: 100-240 VAC at 50/60 Hz, 1 A, 60 VA, or 100-240 VDC, 1A, 60 W Operational: 85-264 VAC, or 88-300 VDC
HV2	High Voltage Power Module	Nominal: 100-240 VAC at 50/60 Hz, 1 A, 60 VA, or 100-240 VDC, 1A, 60 W Operational: 85-264 VAC, or 88-300 VDC

3.2. Mechanical Drawing of a Power Supply Module

Figure 2:   Mechanical Drawing of a Power Supply Module
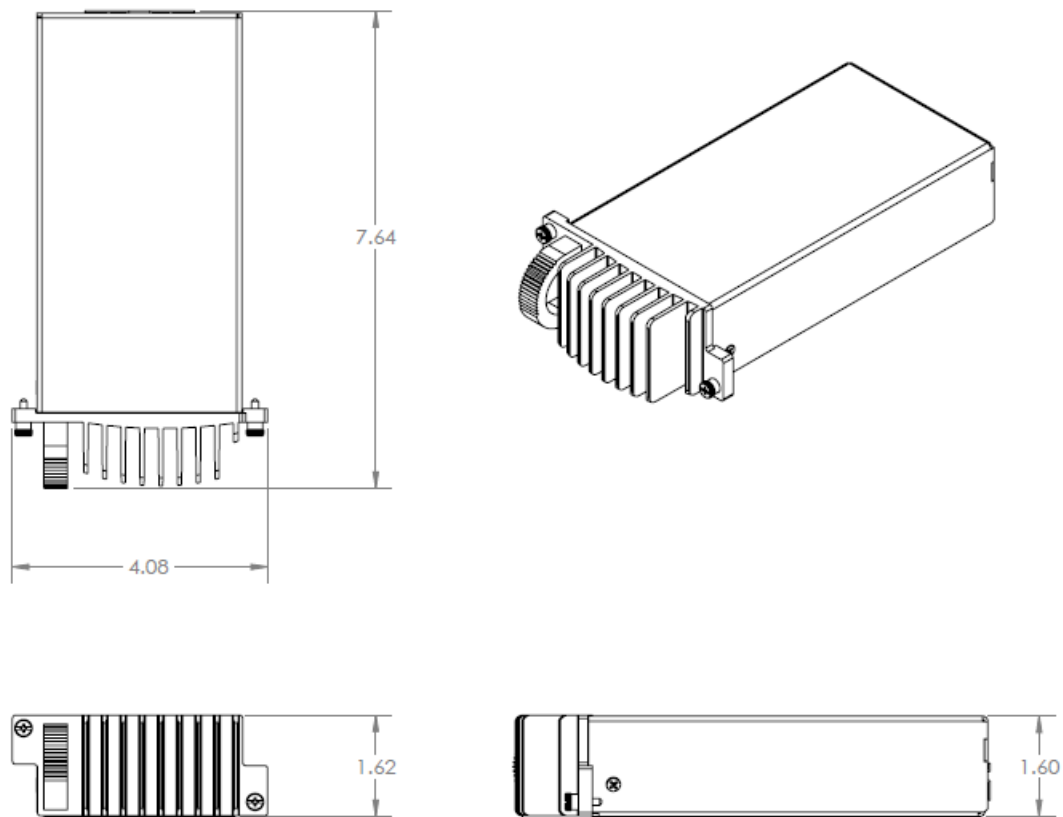
All power supply (*PS*) modules (LV, MV, HV, and HV2) have the same dimensions as shown above.

All dimensions are shown in inches.

4. Chassis

Figure 1: Front View of Chassis with a SD Card Cover

Figure 2: Mechanical Drawing of Chassis
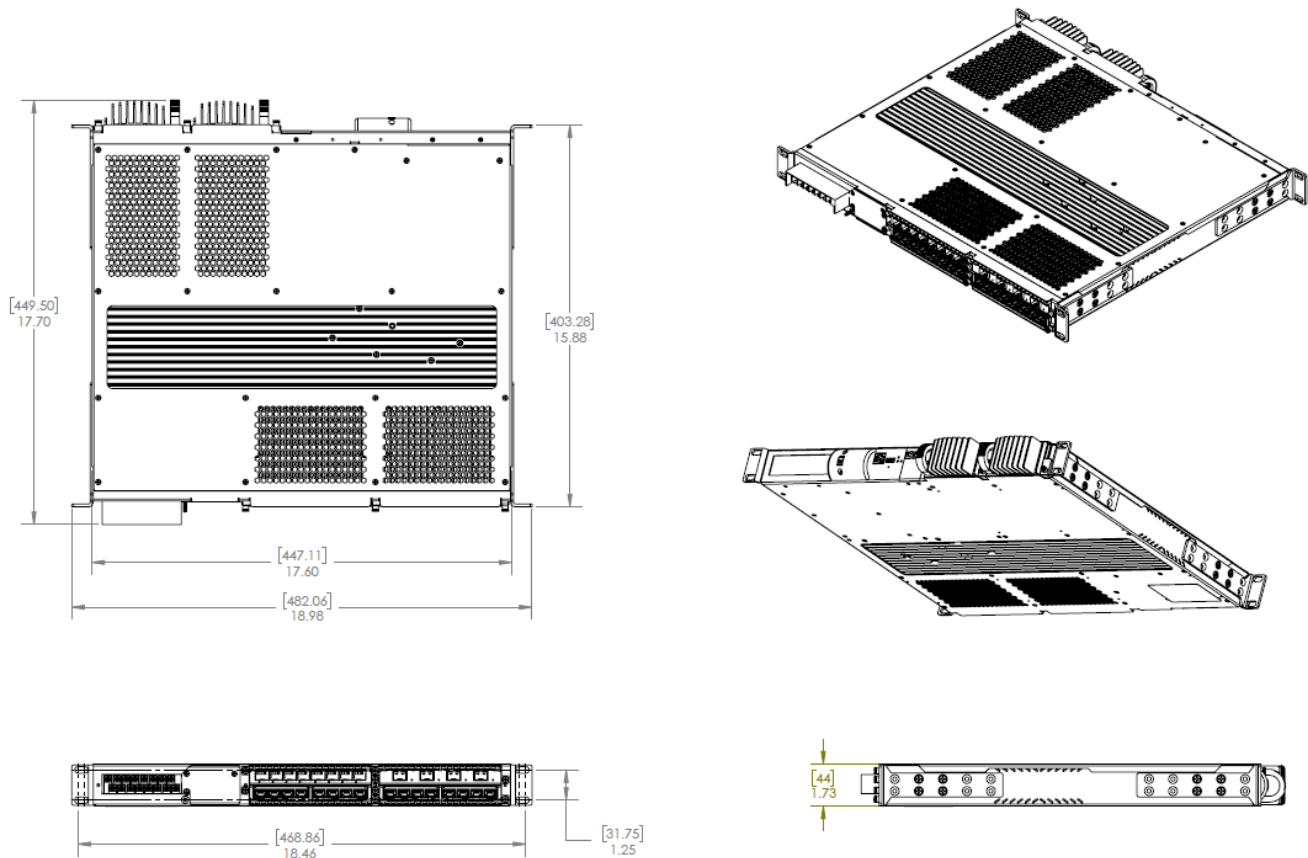
NOTE: All dimensions are shown in inches (millimeters).

5. RAPTOR Panels Description

This section contains views of the front and back panels of the RAPTOR. The locations of the power modules, interface module slots, and status indicators are shown.

RAPTOR supports the following slot types:

- Slot #1- 3 with up to 8 x 10/100/1000 RJ45s or 8 x 100/1000 SFPs
- Slot #4 with up to 4 x 10GB Base-X or 4 x 1 GB Base-X uplinks

The product label is located at the bottom of the unit.

Figure 1:   Product Label
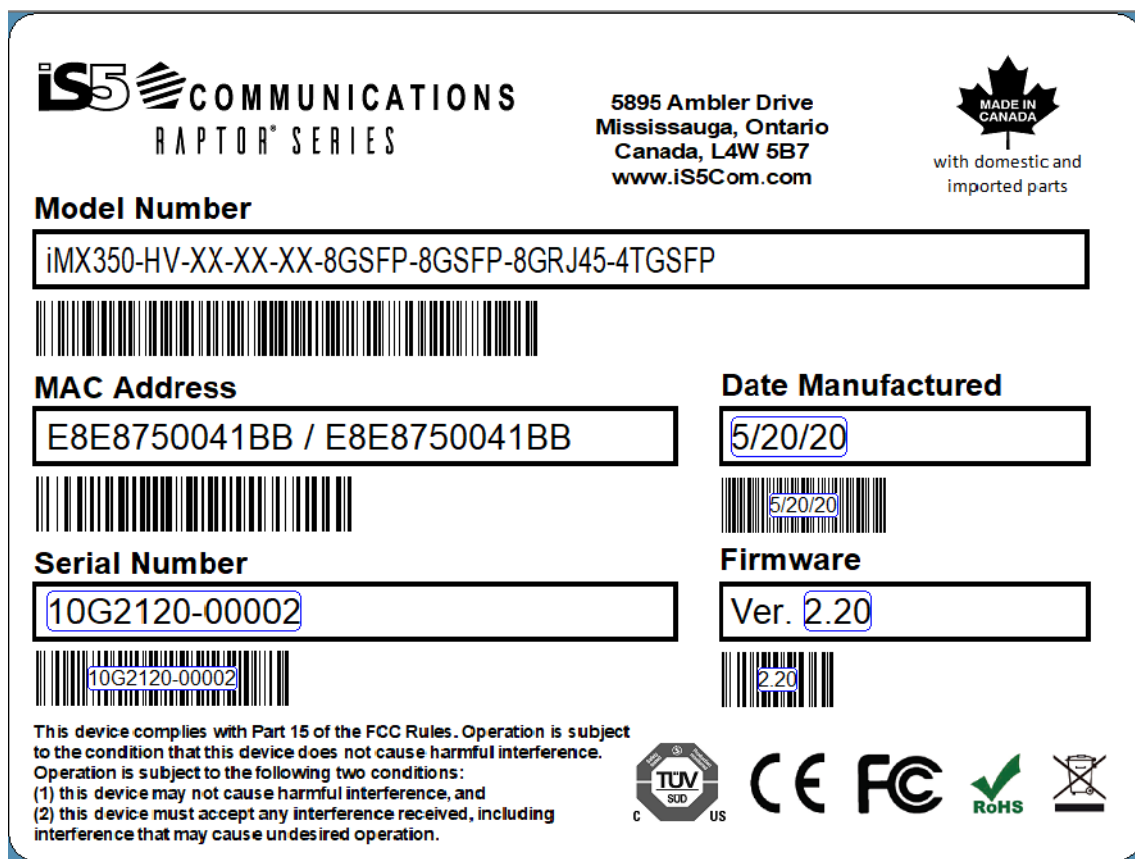
NOTE: The second MAC address is for future use.

5.1. Front Panel Elements

Figure 2: Front Panel Elements

1. SD CARD
2. Management Port
   (Factory Disabled)
3. RJ-45 serial console port
4. USB Port
5. Power Status LED
6. Power Supply 2 (PS2)
7. Power Supply 1 (PS1)

SD cover elements (a sample is shown on right) can vary.

1) **SD Card** port may be used to store Syslog files. SD#1 (top) is disabled by default. SD slot #2 (bottom) is available for customer use.

2) **Management Port**—this 10/100Base-T Ethernet port is used as an out-of-band factory service port. It is enabled by default and not available for user access.

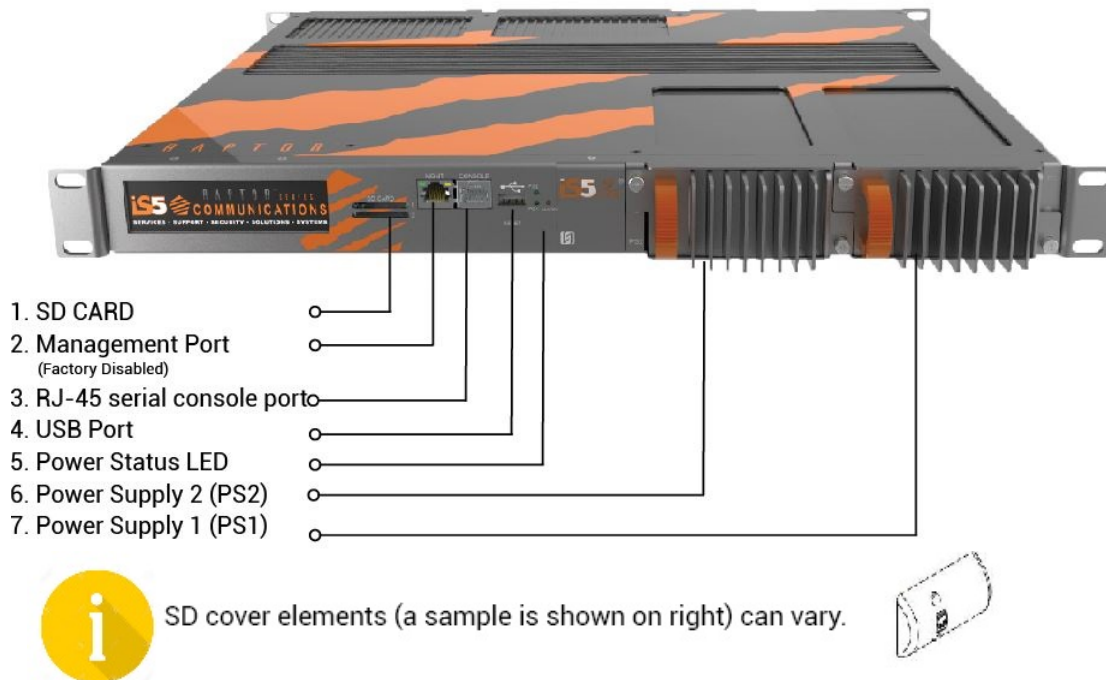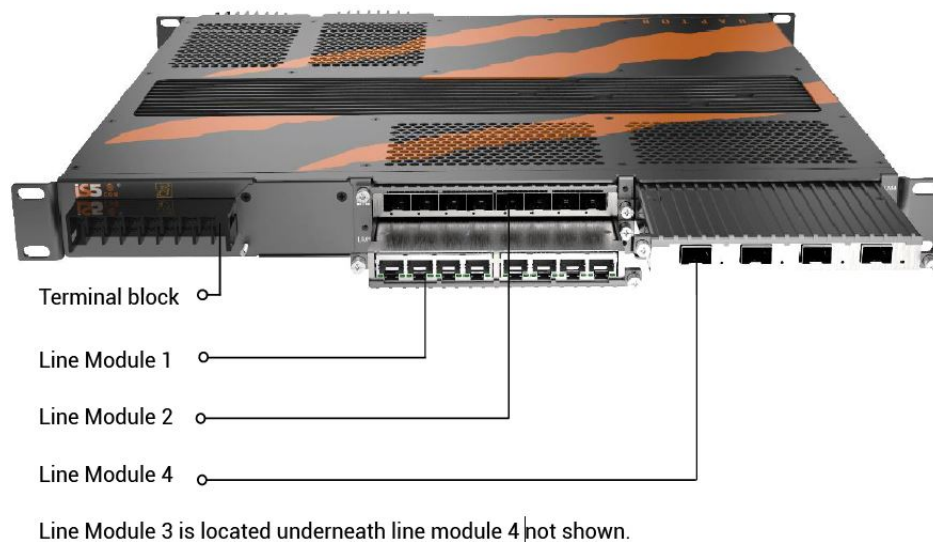3) **RS232 Serial Console Port**—this port is for interfacing directly with the device and accessing management functions via serial interface.

4) **USB Port** can be used to upgrade or back up the RAPTOR's software or configuration files.

5) **Power Status LEDs**—the light-emitting diodes (LED)s indicate the status of the power supply modules.

6) **Power Supply 2 (PS 2)**—both power supplies may be used for redundancy

7) **Power Supply 1 (PS 1)**—both power supplies may be used for redundancy.

8) **Reset Button (Not Shown)**—The Reset button is found directly under the USB Port. By pressing the reset button and then releasing it, the RAPTOR will reboot. By holding it for over two seconds and then releasing it, it will be possible to access debug functions on the console terminal. These debug functions should only be accessed in consultation with the iS5Com support team.

5.2. Back Panel Elements

Figure 3:   Back Panel Elements

Terminal block

Line Module 1

Line Module 2

Line Module 4

Line Module 3 is located underneath line module 4 not shown.

5.3. LED Indicators Summary

TYPE	DESRIPTION	Description
PS1	Power Status LED 1	Green: OK; No light: No power module installed
PS2	Power Status LED 2	Green: OK; No light: No power module installed
Alarm	Alarm Indicator LED	Indicates when an alarm condition exists; Off: Alarms cleared / acknowledged; Red: Alarm is on

All port status LEDs are as shown on LED display (see below).

Figure 4:   RAPTOR LED Display

5.4. Port Mapping

Figure 5 shows how the ports are numbered on the RAPTOR. This graphic was taken from the RAPTOR web user interface and is visible on most pages.

Figure 5:   Port layout on the RAPTOR

6. Mounting and Installing RAPTOR

The RAPTOR is designed for maximum mounting and display flexibility. It can be equipped with brackets that allow installation in a 48 cm (19 in) rack.

6.1. Prevention of ElectroStatic Discharge Damage

The device components are prone to ElectroStatic Discharge (*ESD*) damage. *ESD* damage, which can cause intermittent or complete component failures, can occur by voltages as low as 30 V. Potentially destructive static voltages can happen during handling of plastic or foam packing material or when moving components across plastic or carpets.

Some guidelines to minimize the potential for *ESD* damage are:

- Always use an *ESD* wrist strap when you are working with components that are subject to *ESD* damage, and make sure that *ESD* wrist strap is in direct contact with your skin.
- If a grounding strap is not available, then to ground yourself, touch the exposed bare metal of the device with the other hand immediately before inserting the component into the device.

> ⚠️ To ensure protection by the ESD strap, periodically check its resistance value.
>
> The measured value must be in the range between 1 and 10 MΩ.

- When handling any component that is subject to *ESD* damage and is to be removed from the device, make sure the equipment end of your *ESD* wrist strap is attached to the *ESD* point on the chassis.
- Avoid contact between the component that is subject to *ESD* damage and clothing. *ESD* voltages emitted from fabric can damage components.
- When removing or installing a component that is subject to *ESD* damage, always place its components upside on an antistatic surface, in an antistatic card rack, or in an antistatic bag. If you are returning a component, place it in an antistatic bag before packing it.

6.2. Before Rack Installation

- Ensure that you understand how to prevent *ESD* damage.
- Place the rack in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the structure.
- Remove the switch from the shipping package.

- Ensure that you have all necessary parts and tools needed to mount the switch on the rack.

Do not plan to use the device in a location where children are likely to be present.

6.3. Unpacking Device

- Inspect the package for damage before opening.
- Open the package and visually inspect all items for issues.
- Confirm that all items are available.

If there any missing or damaged items, contact iS5Com Support.

6.4. Prerequisites for Mounting Device on a Rack

Heat generated by the device is channeled outwards from the enclosure. For improved convectional airflow, make sure that there is at least one rack-unit of space or 44 mm (1.75 in) of space around all sides of the device or between the devices on the rack.

Forced airflow is not required. However, any increase in airflow will result in a reduction of ambient temperature and improve the long term reliability of the equipment mounted in the rack space.

6.5. General Procedure for Installing and Starting RAPTOR

- Review the Compliance Specification for any regulatory requirements.
- Check the equipment ratings, operating instructions and installation instructions before commissioning or maintenance.
- Mount the device.
- Connect the failsafe alarm relay.
- Connect power to the device and ground the device.
- Connect the device to the network.

• Configure the device.

This equipment is intended only for use in a restricted access area.

Caution: Access to Battery located inside the unit is prohibited.

CAUTION: Users are prohibited from accessing the battery. The switch is to be returned to the factory for proper disposition.

6.6. Electrical / Mechanical Hazards Prevention

• When installing the device in a closed or multi-device rack, be aware that the operating ambient temperature of the rack may be higher than the ambient temperature of the room. Make sure the rack is installed in a suitable environment that can withstand the maximum ambient temperature generated by the rack.

• Do not exceed the maximum number of devices or weight restrictions specified by the rack manufacturer.

• Do not overload the supply circuit. Refer to the overcurrent protection and power supply ratings specified by the rack manufacturer.

• Make sure the rack and all devices have a proper ground-to-Earth connection. Pay particular attention to power supply connections other than direct connections to the branch circuit (e.g. power strips). Ensure that the rack mount adapters are installed on the correct side of the chassis.

• The user shall be responsible for ensuring the integrity of any protective conductor connections before carrying out any other actions.

Electrocution hazard – risk of death, serious personal injury and/or damage to the device.

Caution – Access to wiring terminals and replaceable modules is restricted to Skilled Persons only.

6.7. Humidity and Dust Hazards

Do not store the switch in locations where it will be subject excessive dirt and dust and high humidity. Conformal coating is recommended for humid / moist applications.

6.8. Mounting RAPTOR on a Rack

Ensure that the rack mount brackets are installed on the correct side of the chassis.

Figure 1:   Mounting Raptor on a Rack

1. Raptor Unit
2. Mounting Bracket
3. Mounting Screws
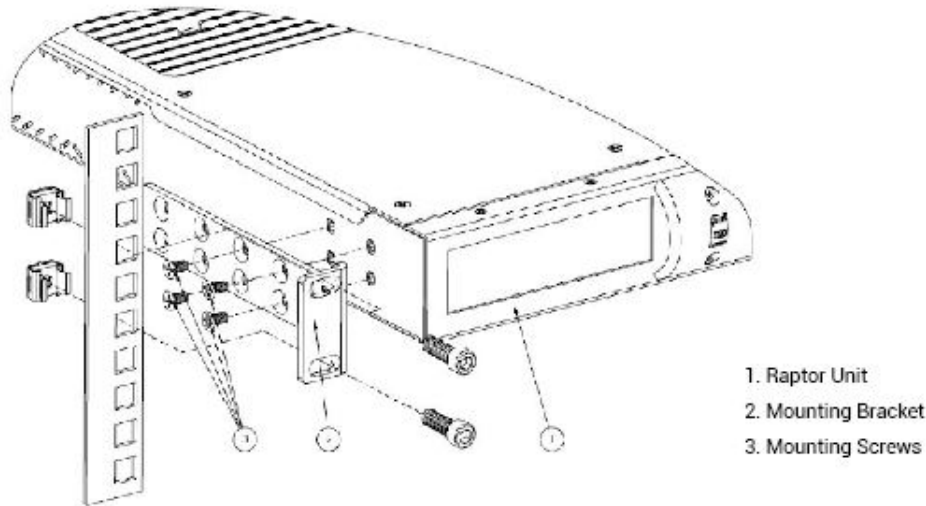
To secure the device to a standard 48 cm (19 in) rack, perform the following:

1)   Install the mounting brackets to RAPTOR using 4 x M4 x 0.7 screws on each side (screws will be provided with the switch). Use minimum of 2 brackets (4 brackets are included). Brackets are to be adjusted based on rack dimensions. Where only 2 brackets are used, screws should be installed in unused bracket holes, this will improve ingress protection.

2)   Place the switch in the rack by tilting the switch at an angle so that the ears will clear the mounting rails. Mount it on the rack using rack screws at the front and rear brackets.

Figure 2:   Mounting RAPTOR on a Rack
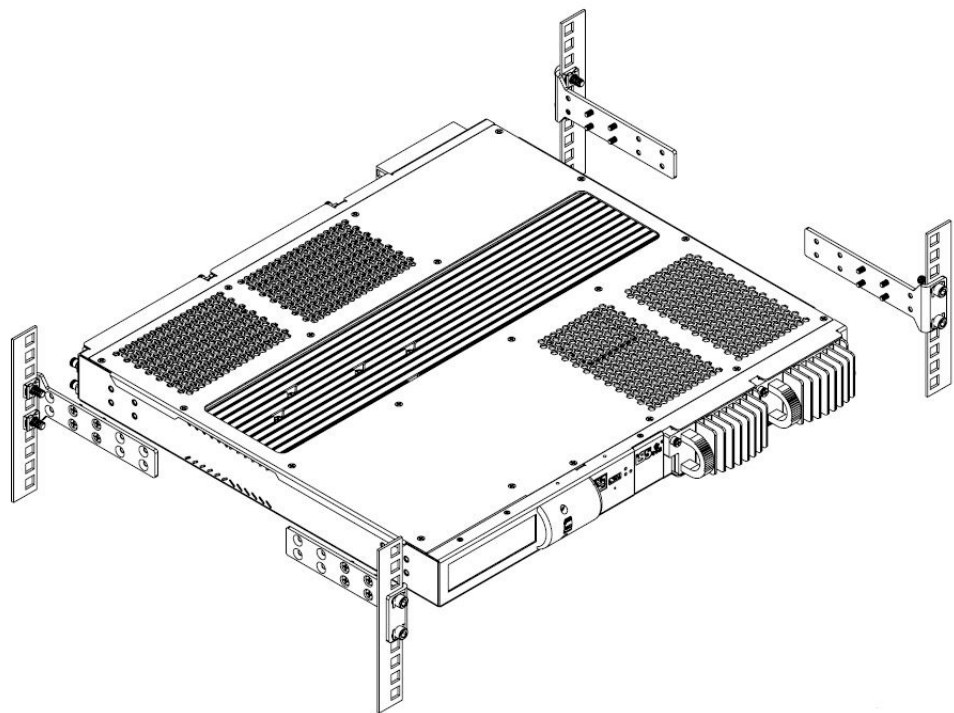
6.9. Equipment Needed for RAPTOR's Installation

PART #	QTY	DESCRIPTION
1	16 (included)	Mounting screw M 4 x 0.7
2	4 (included)	Mounting bracket
3	1 (not included)	Screwdriver

6.10. Panel Mounting the RAPTOR

A panel mount kit may be ordered separately that will permit the user to attach four (4) panel mount brackets to the RAPTOR. The RAPTOR may then be mounted to a flat panel.

PART #	QTY	DESCRIPTION
1900-0032	1	Panel Mount Bracket Kit for the iMX350/iMX950. The iMX Panel Mount Kit includes the following: 4x Mounting Brackets 8x Screws

6.11. Mounting Orientation of Panel Mount

The switch may be mounted with the line modules facing up or down, or the line modules facing either left or right.

 Four brackets are needed to secure the switch, with each bracket requiring two screws to secure it to the switch.
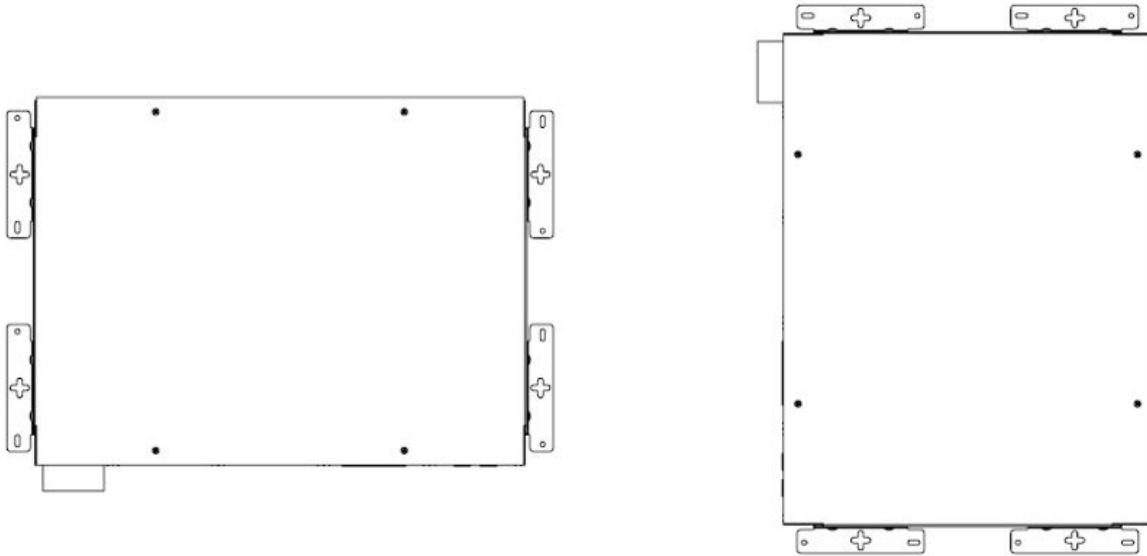
Figure 3:   Mounting orientation

The following illustration provides an example of how the brackets are affixed to the switch.
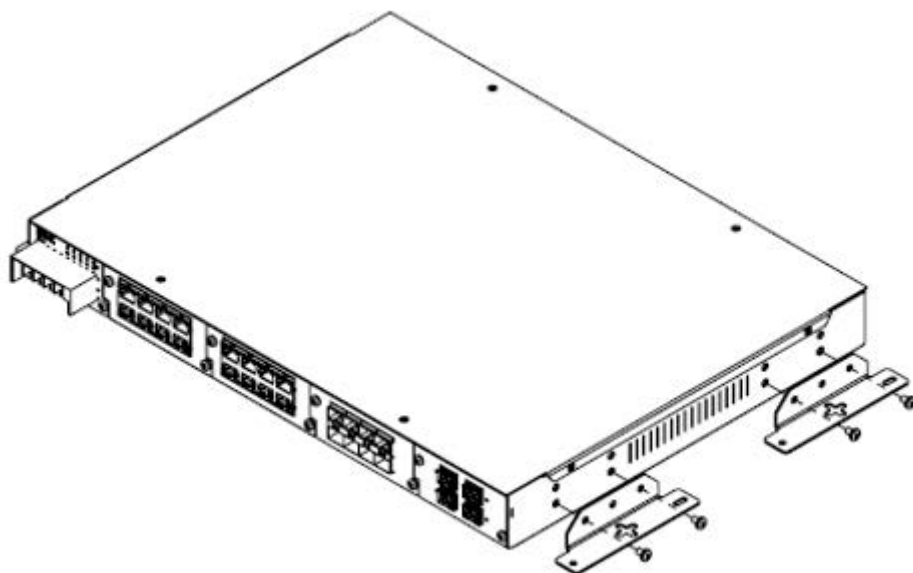
Figure 4:   Securing brackets to the switch. Two of the four brackets are shown.

7. Modules Installation

The RAPTOR supports two hot-swappable power supply modules (PS1 and PS2). The use of two power supply modules is recommended for providing redundancy and proper operation of the switch. The redundant power supplies should be connected to different power sources.

7.1. Power Supply Modules Installation

PREREQUISITE:

Equipment must be installed according to applicable local wiring codes and standards.

Electrical Hazard - Risk of damage to equipment.

Check the voltage input for each power supply module provided.

Figure 1:   Power Supply Modules

1. Raptor Unit

2. Deposition Sections

3. Power Supply Modules
(from left, shown PS2 and PS1)

4. Thumb Screws
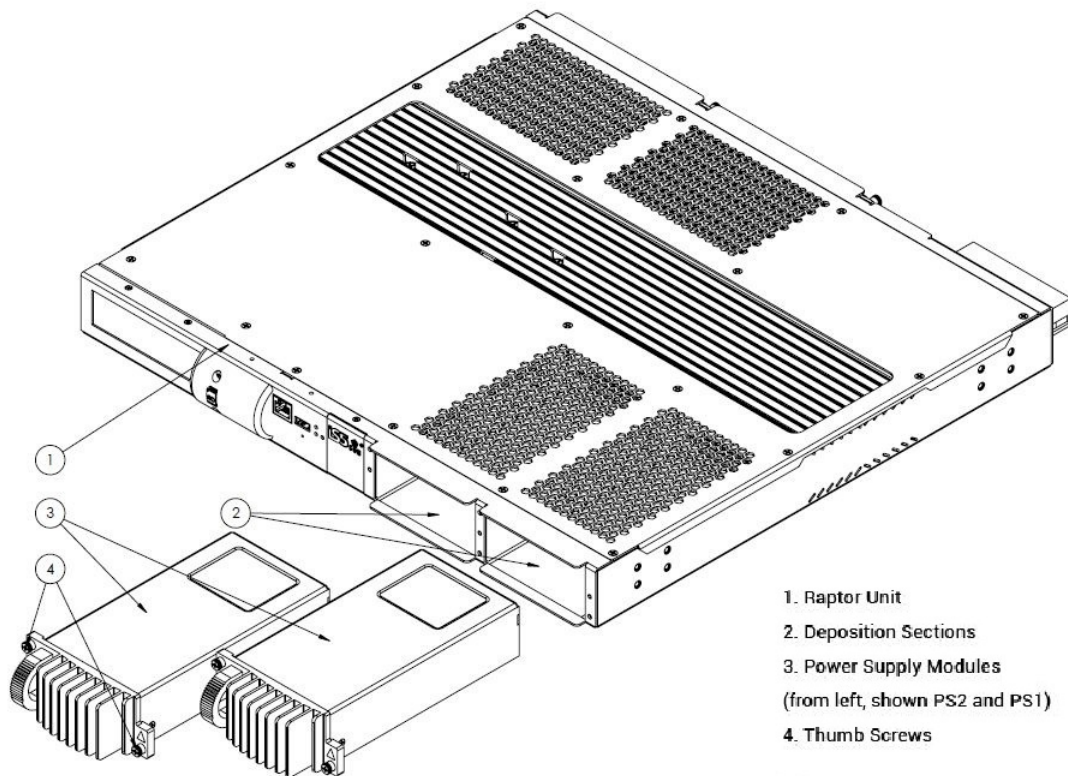
Figure 2:   Installing Power Supply Modules
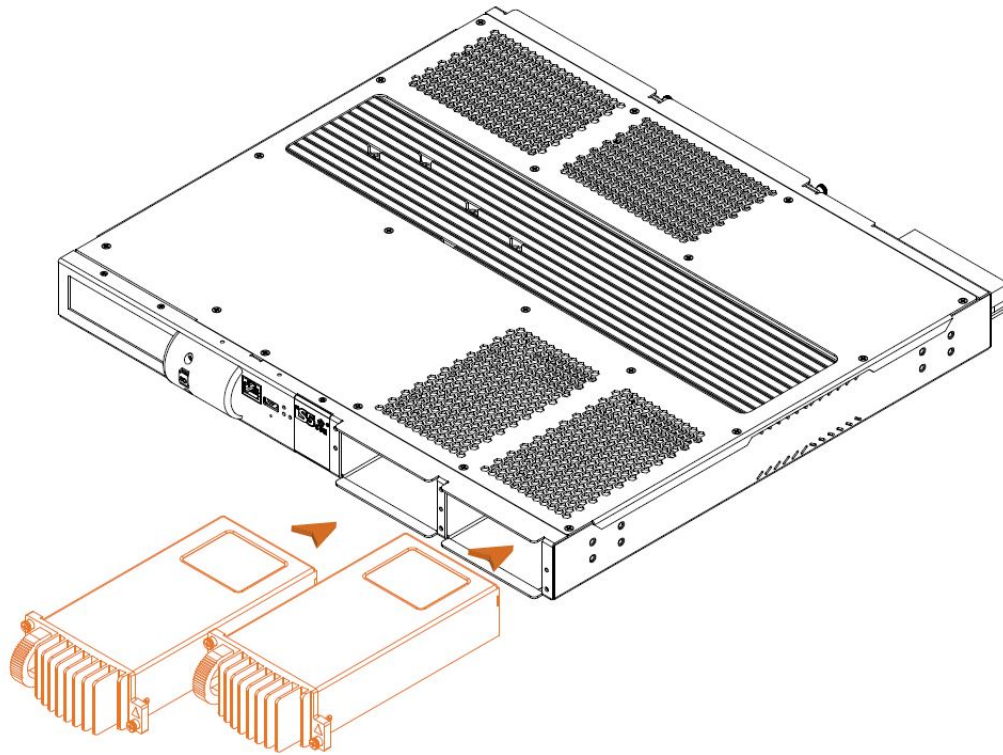
To install a power supply, perform the following:

1.   Check the label on the terminal block of the back panel so as to verify the voltage levels of power supplies PS1 and PS2.

2.   Insert the power supply modules in Power 1 and Power 2 slots respectively.

3.   Push and tighten every thumb screw until each power supply module is locked in position. The screws that are used for installation of the power supply and communication modules can be secured by thumb or screw. The torque applied on thumb screws using hand (without tools) is sufficient to secure them to the chassis. Please ensure that the screws are not over-torqued as it will lead to misalignment of pins on the interconnect. In case screwdriver is used then the applicable torque is approximately 0.6Nm.

4.   Turn on power to the device and confirm that the PS module is receiving and supplying power. This is indicated by PS1 and PS2 LEDs. If a LED's light is green, the PS module is receiving and supplying power.

7.2. Removal of Power Supply Modules from Chassis

CONTEXT: This section describes how to remove power modules from the Chassis.

Figure 3:   Removal of Power Supply Modules from Chassis
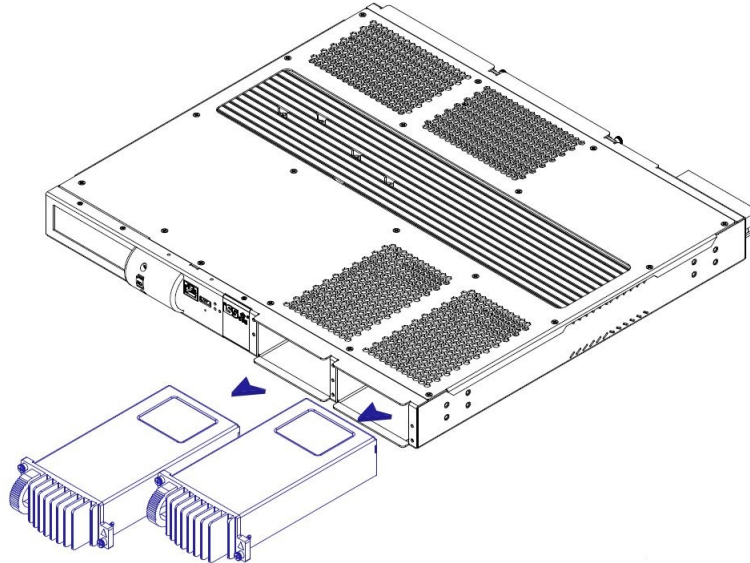
Danger of electrocution hazard exists.

To remove a PS module, perform the following steps:

1.   [Optional] If the device is installed in a rack, remove it from the rack.

2.   Loosen the screws securing the line module.

3.   Pull the module from its slot in the chassis.

4.   Install a new module or a blank module (to prevent accumulation of dust).

7.3. Lines Modules Installation

CONTEXT: This section describes how to install line modules.

Figure 4:   Line Modules Installation

1. Raptor Unit
2. Line Modules
3. Thumb Screws
4. Deposition sections
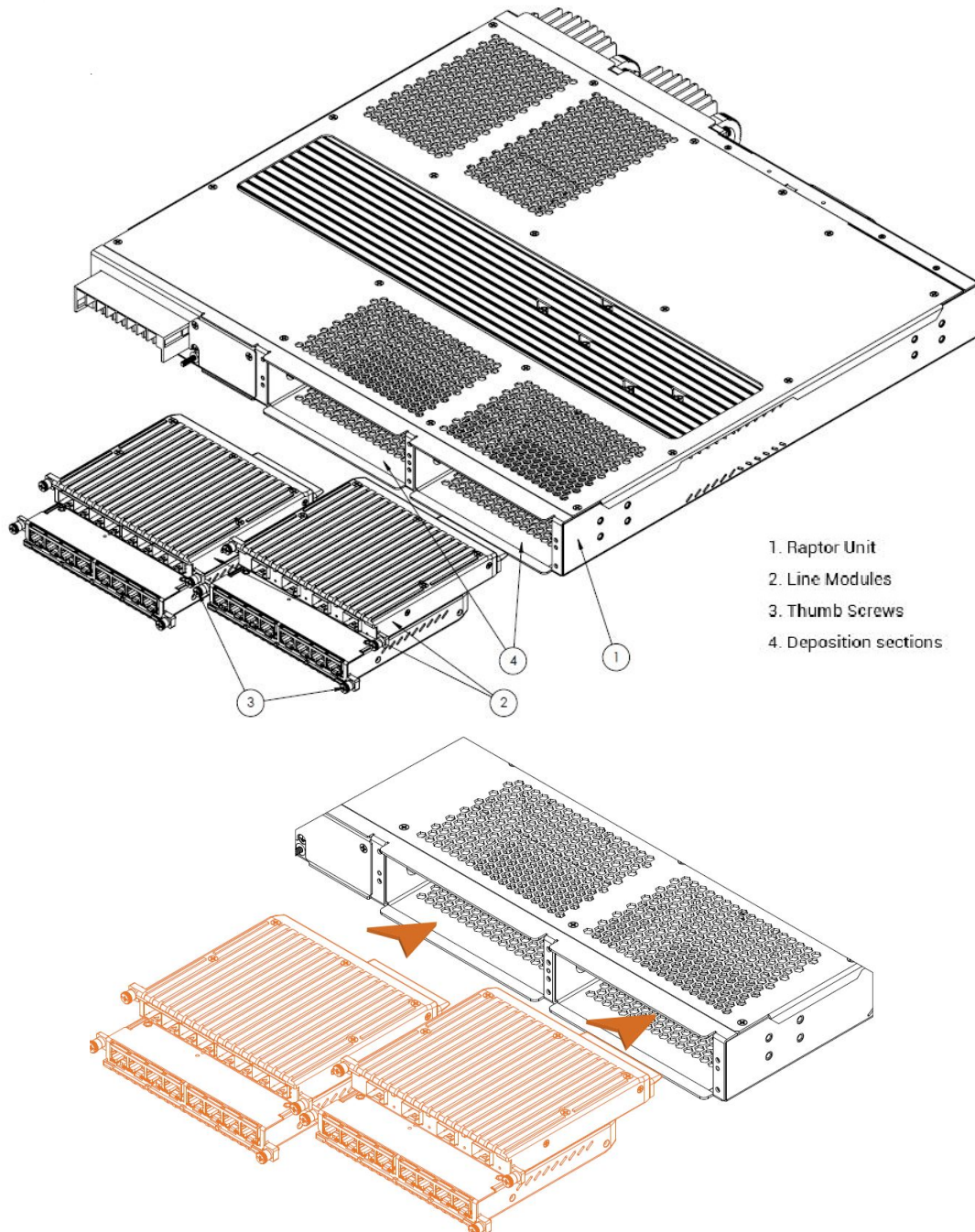
Check the Ordering Information for line modules to be installed.

1. Obtain all purchased line modules.

2. Check and insert them in the correct positions in the upper or lower slots of the deposition sections. Line modules 1 and 3 are to be inserted before line modules 2 and 4. The iRM-4TGSFP Module is reserved for the Slot 4 only. This module should be inserted prior to powering the module.

3. Push and turn every thumb screw until each line module is locked in position. The screws that are used for installation of the power supply and communication modules can be secured by thumb or screw. The torque applied on thumb screws using hand (without tools) is sufficient to secure them to the chassis. Please ensure that the screws are not over-torqued as it will lead to misalignment of pins on the interconnect. In case screwdriver is used, the applicable torque is approximately 0.6 Nm.

7.4. Removal of Line Modules from Chassis

CONTEXT: This section describes how to remove line modules.

**Figure 5:**   Removal of Line Modules from Chassis
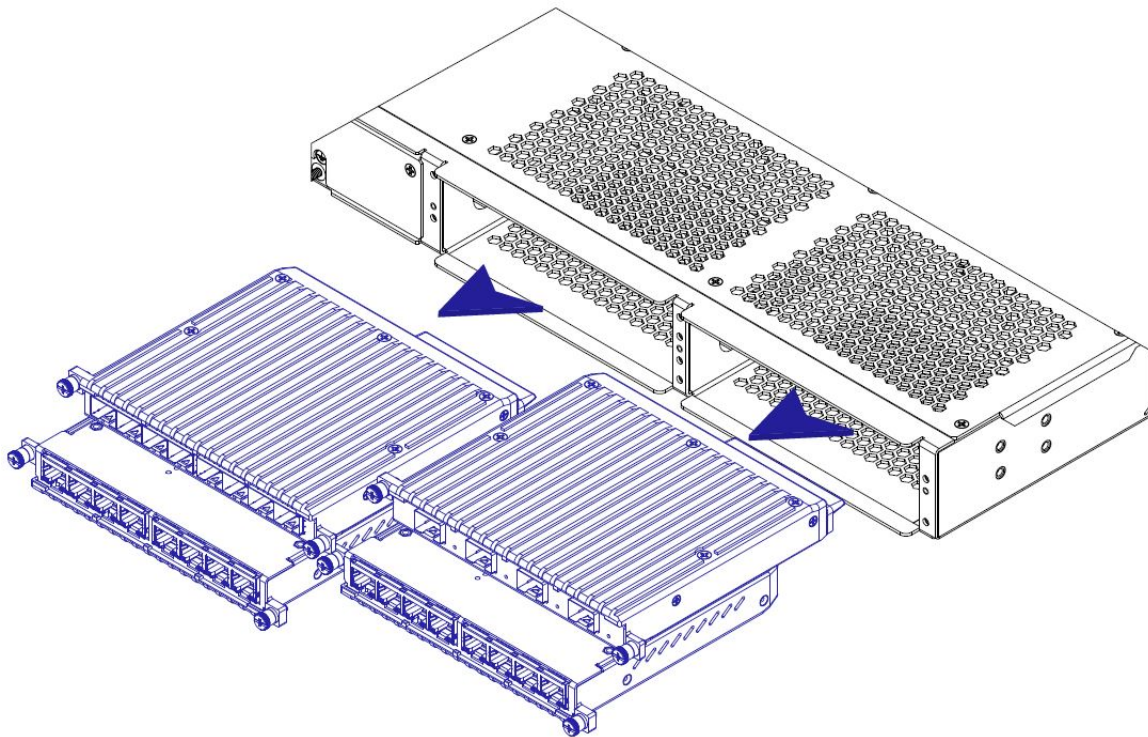
To remove a line module, perform the following steps:

1. [Optional] If the RAPTOR is installed in a rack, remove it from the rack.

2. Loosen the screws securing the line module.

3. Pull the module from its slot in the chassis. If all line modules are to be removed, first remove modules 2 and 4, and then modules 1 and 3.

7.5. iRM-4TGSFP Module Installation

CONTEXT: This section describes how to install a line module into slot 4.

Figure 6:   Removal of Line Modules from Chassis

1. Raptor Unit
2. Line Modules
3. Thumb Screws
4. Deposition sections
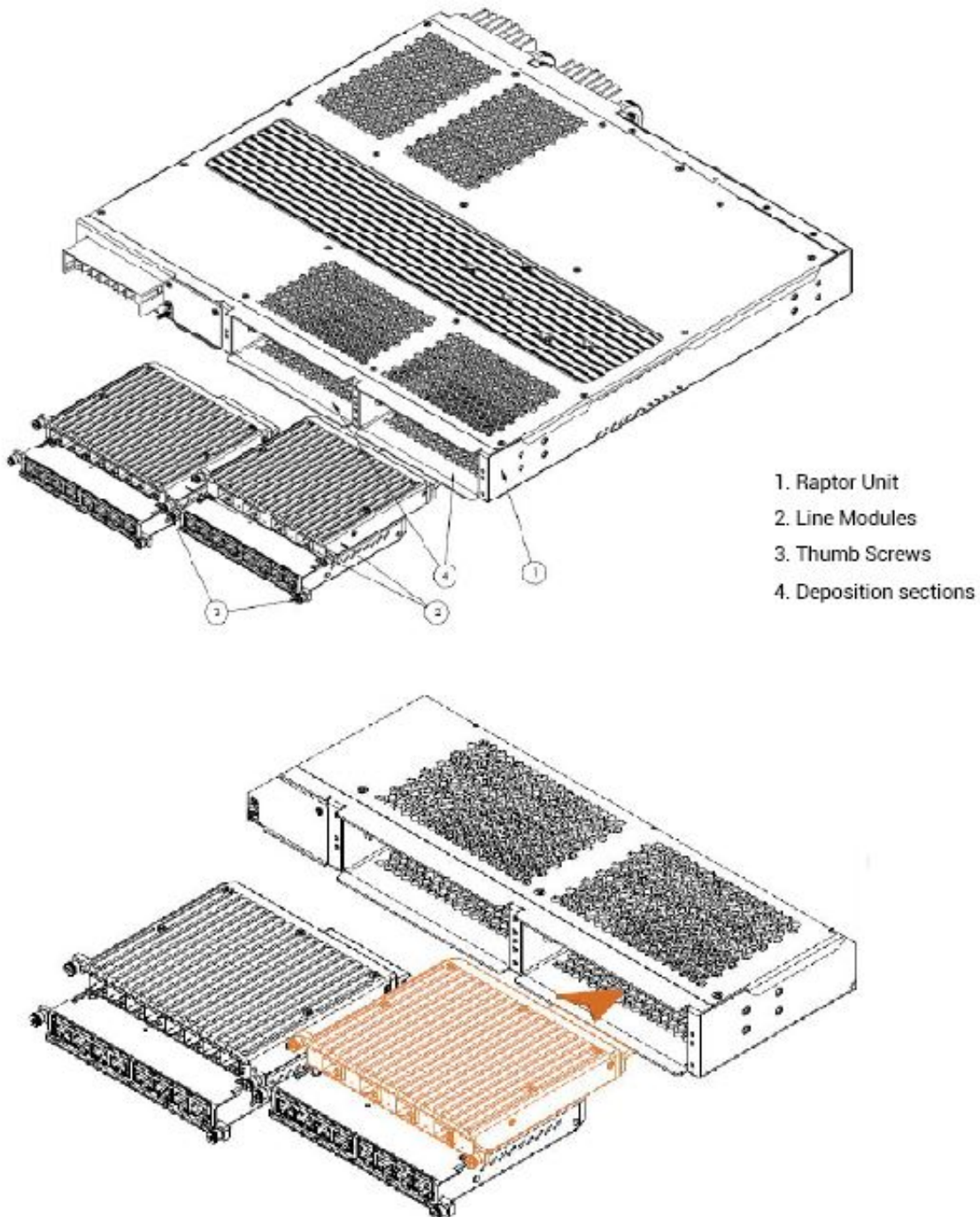
1.   4TGSFP line module should only be inserted into LM slot 4; it will not be fully inserted or function in any other slot.

7.6. Removal of iRM-4TGSFP Module

CONTEXT: This section describes how to remove a line module from slot 4.

Figure 7:   Removal of iRM-4TGSFP Module
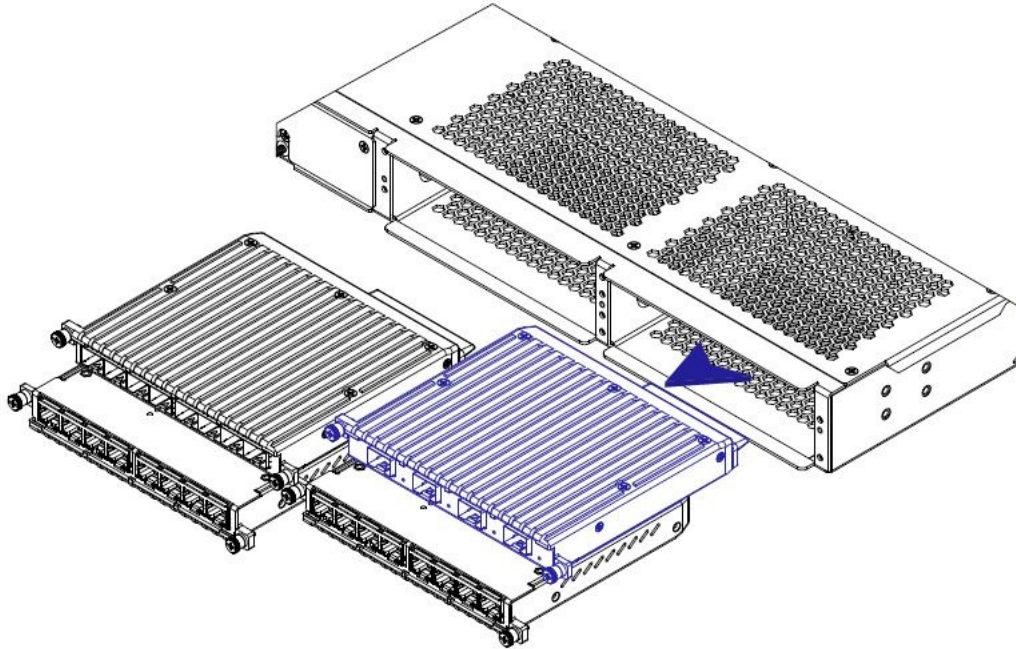
Removing and installing an Ethernet module can shorten its useful life!

Do not remove and insert the modules more often than is absolutely necessary.

1.   Loosen the screws securing the module. Remove the 4TGSFP module from Slot 4.

7.7. Inserting SD Card in SD Slot

CONTEXT: This section describes how to insert the SD Card into the RAPTOR.

Figure 8:   Inserting SD Card in SD Slot

1. Raptor Unit
2. SD Card
3. SD Card Cover
4. Mounting Screws
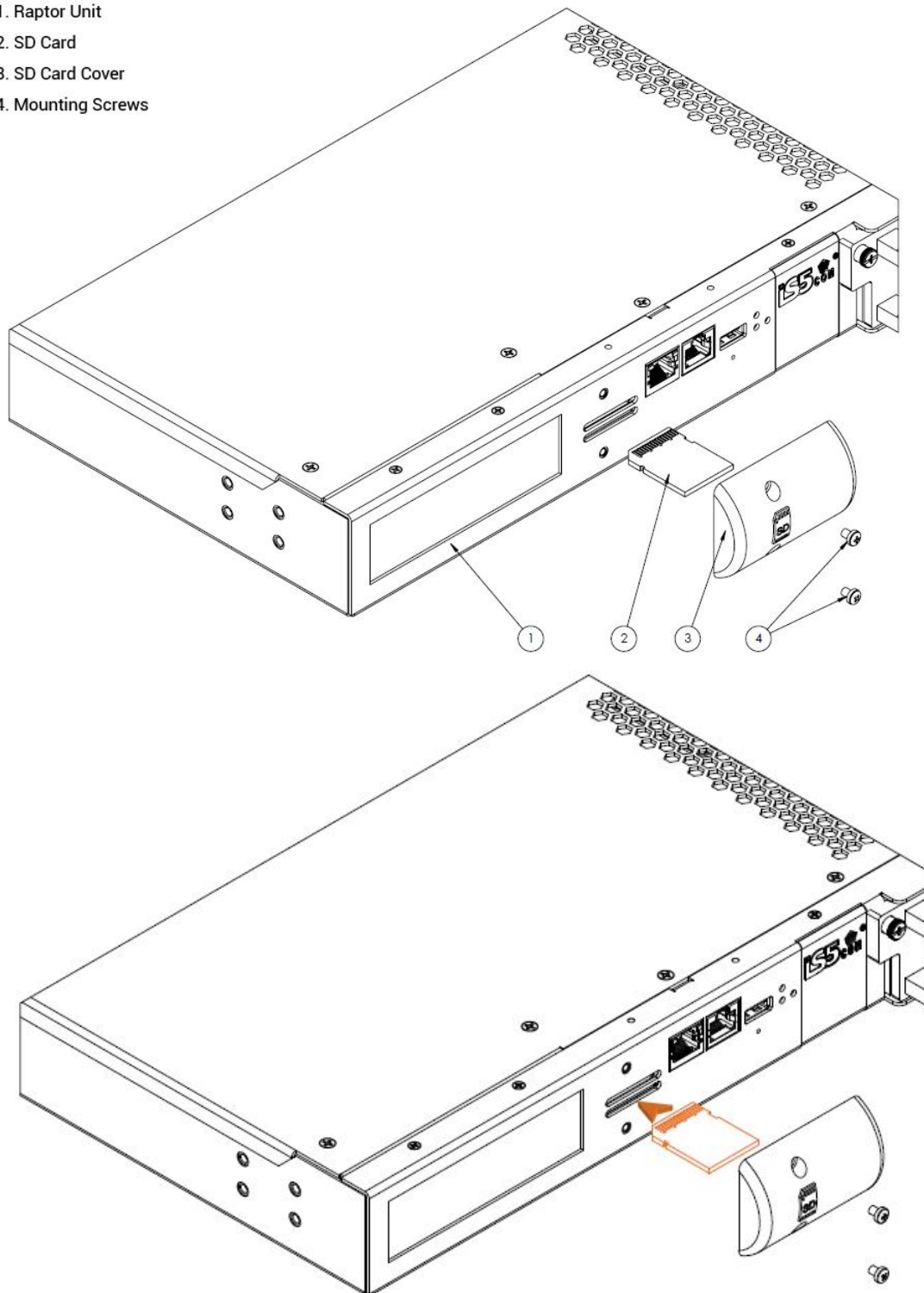
1.   Uninstall the SD card cover by removing the screws.

2.   Insert the SD card as shown into Slot 2 until a click is heard.

7.8. Removing SD Card

CONTEXT: This section describes how to remove the SD Card from the RAPTOR.

Figure 9:   Removing SD Card
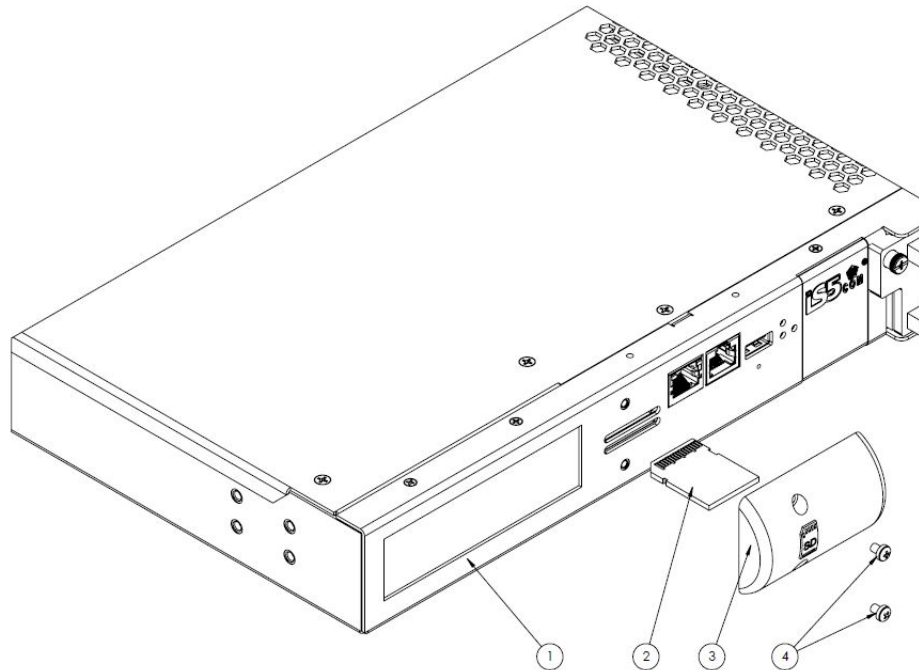
1.   Uninstall the SD card cover by removing the screws.

2.   Remove the SD card from the slot.

8. Electrical Wiring

RAPTOR supports dual redundant hot swappable power supplies—Power Supply 1 (PWR1) and Power Supply 2 (PWR2). The connections for PWR1 and PWR2 are located on the terminal block.

CONTEXT:

Electrocution hazard – risk of death, serious personal injury and/or damage to the device.

Electrical hazard – risk of damage to equipment. Do not connect AC power cables to a 24 or 48 power supply terminal block. Damage to the power supply may occur.

Caution – Access to wiring terminals and replaceable modules is restricted to Skilled Person only.

Multiple power source – redundant power. Disconnect all power sources.

Different power sources shall be used to achieve the redundancy of power supplies.

8.1. Power Inputs and Fault Relay

The relay contact of the terminal block connector is used to detect user-configured events. The switch provides fail open and fail close contacts to form relay circuits based on requirements. If the device is not powered, or if an active alarm is present, the relay de-energizes, therefore initiating the *NO* and *NC* states. The contacts are energized upon power up of the unit and remain energized unless a critical error occurs. One common application for this output is to raise an alarm if a power failure or removal of control power occurs.

CONTEXT: Summary

Table 1:   Relay States

Event	NO (Normally Open)	NC (Normally Closed)
No Alarm	Closed	Open
Alarm Present	Open	Closed

8.2. Connecting AC Power

PREREQUISITE: All equipment must be installed according to applicable local wiring codes and standards.

Always use cables that are rated for the operating ambient temperature of 85°C.

For 100-240 VAC rated equipment, protection for earth fault is provided by max. 20 A branch circuit from AC input in building installation. The protection in the building installation is relied upon for short-circuit backup protection.

- The specification for AC breaker is 5 A, 2P, 277 VAC (min) circuit breaker, thermomagnetic or equivalent type.
- The plug connector and wire gauge sizing is to be selected with appropriate design as per the Electrical code for a 60W, 1-phase device.

Note for IT power distribution systems:

1) This product is also designed for IT power distribution system with phase-to-phase voltage 230 V.

2) This equipment must be connected to an earthed mains socket-outlet.

Figure 1: AC Wiring Diagram
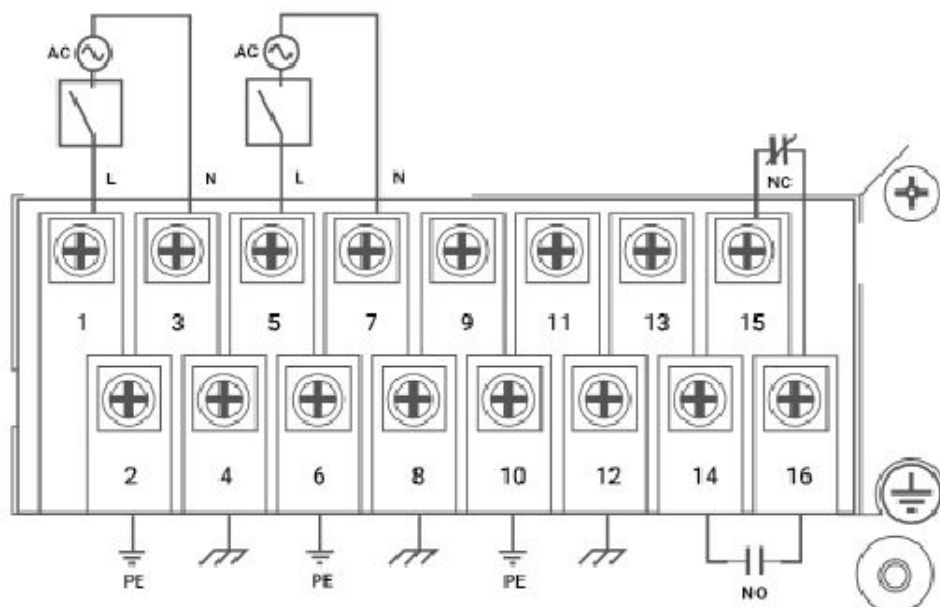
L—stands for Live   N—stands for Neutral

NO—Normally Open (open = open circuit = not creating a path for the current)

NC—Normally Closed (closed = short circuit = creating a path for the current)

PE—Protective Earth (earth Ground point in the electrical circuit)

To establish AC power connection with the power source turned off, follow the steps below. When following the instructions, refer to *AC Wiring Diagram*.

1. Remove the transparent plastic finger safe cover from the face of the terminal block.

If an AC power supply has been installed in PS1, perform steps 2 through 4.

2. Connect the ground from the first power source to GND1 terminal screw (pin 2).

3. Connect the Live from the first power source to the PWR1 V+/L terminal screw.

4. Connect the Neutral from the first power source to the PWR1 V-/N terminal screw.

If an AC power supply has been installed in PS2, perform steps 5 through 7.

5. Connect the ground from the second power source to GND2 terminal screw (pin 6).

6. Connect the Live from the first power source to the PWR2 V+/L terminal screw.

7. Connect the Neutral from the first power source to the PWR2 V-/N terminal screw.

To keep the wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

8. After wiring is completed, reinsert the transparent plastic finger safe cover back onto the face of the terminal block.

9. Connect pin 12 to the ground of the chassis.

8.3. Connecting DC Power

CONTEXT: This section explains how to connect the RAPTOR to a DC power supply.

Figure 2: DC Wiring Diagram
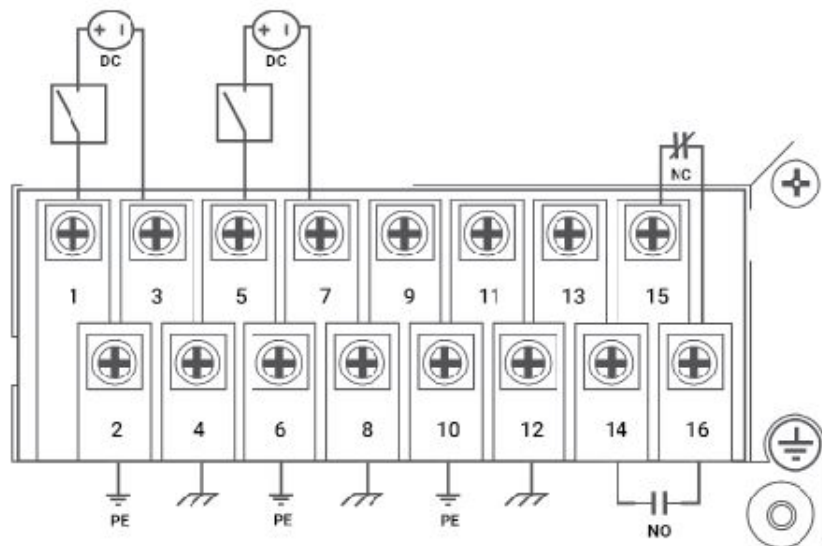
For 100-240 VDC rated equipment, an appropriately rated DC circuit breaker must be installed.

•   The specification for HV DC breaker is 5 A, 2P, 300 VDC (min) circuit breaker, thermomagnetic or equivalent type. A recommended option for this circuit breaker is Model No. CX2-B0-14-450-22A-13G, Molded Case Circuit Breaker, 2 P, 5 A, 250/500 VDC.

•   Wire gauge sizing is to be selected with appropriate design as per the Electrical Code for a 60 W, 1-phase device.

Equipment must be installed according to applicable local wiring codes and standards.

With the power source turned off, refer to figure *DC Wiring Diagram* and perform the following steps:

For a DC Power Supply in PS1, carry out steps 1 through 2.

1.   Connect the positive wire from the power source to the positive/live (+/L), screw #1, terminal on the terminal block.

2.   Connect the negative wire from the power source to the neutral/negative (-/N), screw #3, terminal on the terminal block.

If a DC Power Supply has been installed in PS2, perform the following steps.

3.   Connect the positive wire from the power source to the positive/live (+/L), screw #5, terminal on the terminal block.

4.   Connect the negative wire from the power source to the neutral/negative (-/N), screw #7, terminal on the terminal block.

After wiring is completed, perform the following:

5.   For screw terminal blocks, install the transparent plastic finger safety cover.

6.   Connect pin 12 to the ground of the chassis. The ground terminal is used as the ground conductor for surge and transient suppression circuitry internal to the unit.

8.4. Connecting Power over Ethernet (PoE) Power

CONTEXT: This section explains how to connect the RAPTOR to a DC power supply which provides power to the *PoE* ports.

Figure 3:   DC Wiring Diagram for *PoE* power
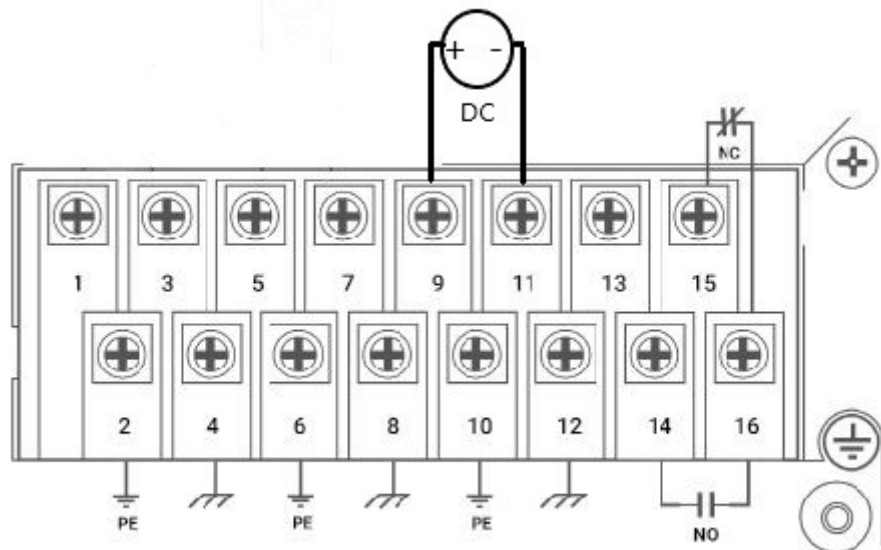
Power over Ethernet is a factory configured option for the iMX350/950 RAPTOR Switches. On devices where *PoE* has been factory configured, the terminal block label will indicate that screws #9 and #11 are to be used for *PoE* power.

For powering the *PoE* ports, a power source supplying 56 VDC and 13 A is recommended for a maximum of 720 Watts of *PoE* power. External DIN mount power supplies are recommended by iS5 Communications.

• Wire gauge sizing is to be selected with appropriate design as per the Electrical code for a 720 W, 1-phase device.

IS5 Communications recommends using the following power supplies for *PoE*.

Table 2: Recommended PoE Power Supplies

Part Number	Max Power	Nominal Input Voltage	Output Voltage
1900-0015	240 Watts	24 VDC	56 VDC
1900-0016	240 Watts	48 VDC	56 VDC
1900-0017	240 Watts	100 - 240 VAC / 110 - 250 VDC	56 VDC
1900-0018	480 Watts	100 - 240 VAC / 110 - 250 VDC	56 VDC

NOTE: PoE External Power Supplies support operating temperatures of -25°C to +70°C. Derating begins above +60°C. Power supplies may be wired in parallel to supply additional power to the PoE line modules.

Table 3: Phoenix Contact PoE Power Supplies

Phoenix Contact Part Number	Max Power	Nominal Input Voltage	Output Voltage
1110155 Web Page Link	240 Watts	100-240 VAC	56 VDC

NOTE: Phoenix Contact PoE External Power Supplies provide the necessary voltages to be used for PoE on the RAPTOR. Please visit power supply product web page to review specifications.

Equipment must be installed according to applicable local wiring codes and standards.

With all power sources connected to the terminal block and turned off, refer to figure *DC Wiring Diagram for PoE power*, and perform steps 1 through 2:

1. Connect the positive wire from the power source to the positive (+), screw #9, terminal on the terminal block.

2. Connect the negative wire from the power source to the negative (-), screw #11, terminal on the terminal block.

After wiring is completed, perform the following:

3. For screw terminal blocks, install the transparent plastic finger safety cover.

8.5. Connecting Ground Wire for Safety Precautions

CONTEXT: This section explains how to connect the ground wire to the RAPTOR.

Figure 4: Connecting Ground Wire

1. Chassis of Raptor

2. Grounding cable (provided by is5Com)

3. Grounding cable (provided by customer)

4. Nut (provided by is5Com)
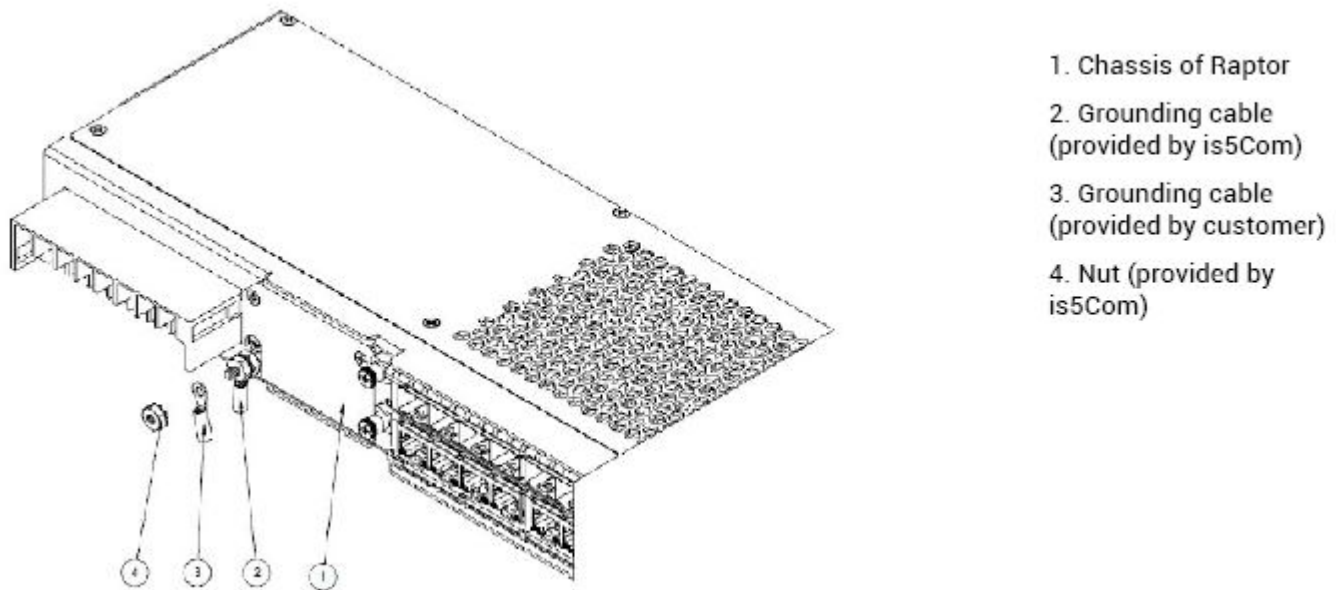
The earth ground connection must be verified by an electrical engineer or a service person skilled in electrical installation and grounding.

If the Raptor is used as cord-connected mains equipment, for reliable earthing, use it as:

♦ pluggable equipment type B, or

♦ stationary pluggable equipment type A in a location with equipotential bonding or with a permanently connnected protective earthing conductor.

ATTENTION: The user shall be responsible for ensuring the integrity of any protective conductor connections before carrying out any other actions.

ATTENTION: Wire gauge sizing is to be selected with the appropriate design as per the Electrical Code.

ATTENTION: Equipment must be installed according to applicable local wiring codes and standards.

ATTENTION: Protective earth connections should not be removed when the equipment is energized.

ATTENTION: It is the responsibility of the user to ensure that the equipment is installed, operated, and used for its intended function in the manner specified by the manufacturer. If this is not the case, then any safety protection provided by the equipment may be impaired.

1. Using a braided wire or another appropriate grounding wire, connect the chassis ground connection of the device.

9. Device Management

9.1. Serial Console

Figure 1: Serial Console

Connect a *PC* or terminal directly to the serial console to access the boot-time control and RAPTOR's interfaces. The serial console port provides access to the console interface.

The serial console port is RS232 with RJ45 connector with a console cable and port setup of 115200 bps, 8, N.

The serial console is intended to be used only as a temporary connection during initial configuration or troubleshooting.

Figure 2: RJ45 Serial Pin Assignment
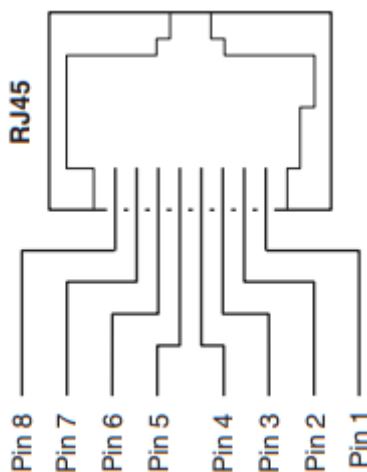
RS232 RJ-45 pin assignments are as follows:

PIN #	TYPE	ASSIGNMENT
1	RS232	*RTS*
2	RS232	
3	RS232	*TX*
4	RS232	*GND*
5	RS232	*GND*

PIN #	TYPE	ASSIGNMENT
6	RS232	*RX*
7	RS232	
8	RS232	*CTS*

9.2. Ethernet Ports & Communication Cabling

The RAPTOR comes with standard Ethernet ports. According to the link type, the switch uses CAT 3, 4, 5, and 5e *UTP* cables to connect to any other network devices (computers, servers, switches, routers, or hubs).

For RJ-45 cable specifications, refer to the following table.

CABLE	TYPE	MAXIMUM LENGHT
10BASE-T	Cat. 3, 4, 5 100 Ω *UTP*	100 m (328 ft)
100BASE-TX	Cat. 5 100 Ω *UTP*	100 m (328 ft)
1000BASE-T	Cat. 5/Cat. 5e 100 Ω *UTP*	100 m (328 ft)

9.3. RJ45 Ethernet Pin Assignments

With 10/100/1000BASE-T(X) cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

10/100 Base-T(X) RJ-45 pin assignments are as follows:

PIN #	TYPE	ASSIGNMENT
1	10/100 Base-T(X)	TD+
2	10/100 Base-T(X)	TD-
3	10/100 Base-T(X)	RD+
4	10/100 Base-T(X)	Not used
5	10/100 Base-T(X)	Not used
6	10/100 Base-T(X)	RD-
7	10/100 Base-T(X)	Not used
8	10/100 Base-T(X)	Not used

1000 Base-T RJ-45 pin assignments are as follows:

PIN #	TYPE	ASSIGNMENT
1	1000 Base-T	BI_DA+
2	1000 Base-T	BI_DA-
3	1000 Base-T	BI_DB+
4	1000 Base-T	BI_DC+
5	1000 Base-T	BI_DC-
6	1000 Base-T	BI_DB-
7	1000 Base-T	BI_DD+
8	1000 Base-T	BI_DD-

1000 Base-T MDI/MDI- X pin assignments are as follows:

PIN #	MDI PORT	MDI-X PORT
1	TD+ (transmit)	RD+ (receive)
2	TD- (transmit)	RD- (receive)
3	RD+ (receive)	TD+ (transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

1000 Base-T RJ-45 pin assignments are as follows:

PIN #	MDI PORT	MDI-X PORT
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+

PIN #	MDI PORT	MDI-X PORT
8	BI_DD-	BI_DC-

NOTE: "+" and "-" signs represent the polarity of the wires that make each wire pair.

9.4. Recommendations for Cables in High Electrical Noise

Constant electrical noise can be due to the predictable 50 or 60 Hz AC 'hum' from power circuits or harmonic multiples of power frequency close to the data communications cable.

Follow these recommendations for copper data cabling in high electrical noise environments:

- Data cable lengths should be as short as possible, preferably 3 m (10 ft) in length. Copper data cables should not be used for inter-building communications.
- Power and data cables should not be run in parallel for long distances, and they should be installed in separate conduits. Power and data cables should intersect at 90° angles when necessary to reduce inductive coupling.
- Ground loops which are major cause of noise propagation must be avoided.

9.5. SFP

The RAPTOR supports fiber optic ports that can connect to other devices using *SFP* (Small Form-factor Pluggable) modules. The fiber optical ports are MultiMode (*MM*) or SingleMode (*SM*) with *LC* connectors.

Always connect the *TX* port of Switch A to the *RX* port of Switch B.

Figure 3:   SFP
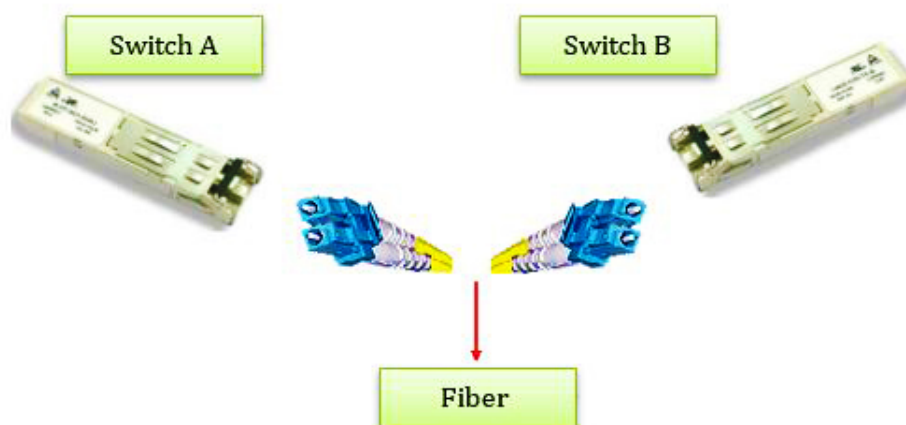
The *SFP* modules are available separately from the Accessories list.

9.6. Mechanical Dimensions of a SFP module

Figure 4: Mechanical Dimensions of a SFP module
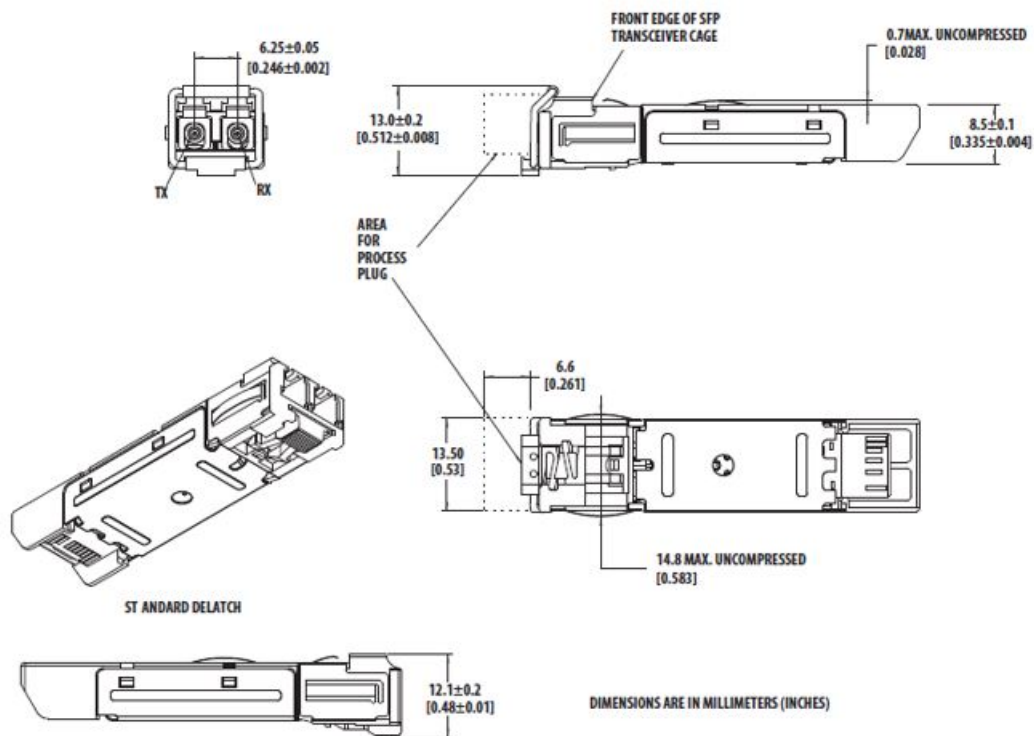
The dimensions are in millimeters (inches)

9.7. Differences between SM and MM Fibers

The main difference between *MM* and *SM* fibers is that the former has much larger core diameter. Typically, *MM* has a core diameter of 50 or 62.5 µm and a cladding diameter of 125 µm, while a typical *SM* fiber has a core diameter between 8 and 10 µm and a cladding diameter of 125 µm.

Figure 5:   SM and MM Fibers
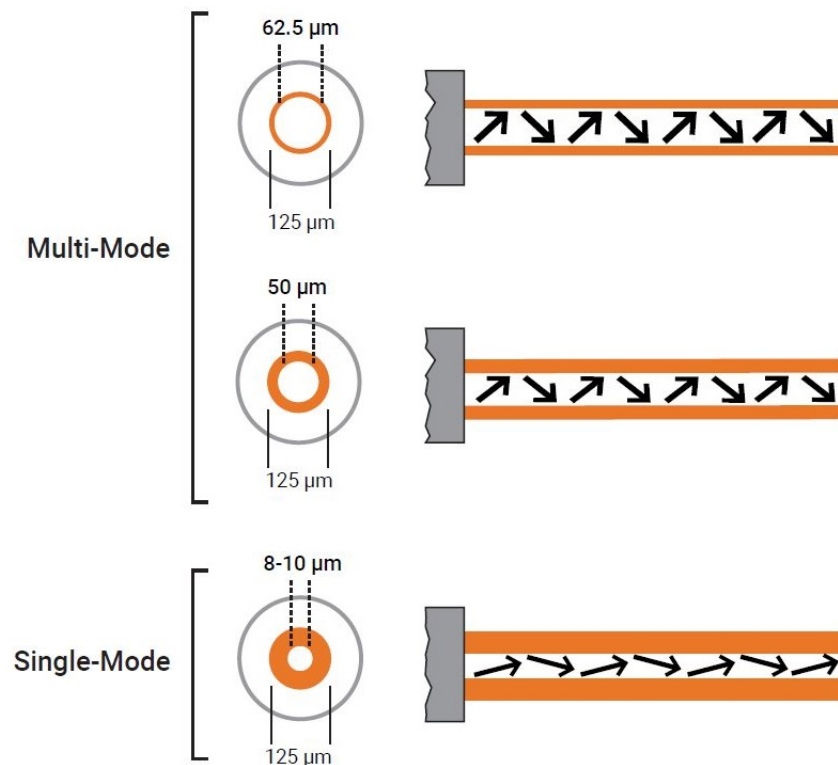
SM fibers are better suited for moving information across longer distances and are routinely used by tele-communications. In comparison, *MM* fibers are ideal for local networks due to their low cost and greater bandwidth.

> ⚠ Laser radiation might be emitted from disconnected fibers or connectors. Do not stare into cables.

9.8. General Fiber Optic Cables Handling Instructions

- Wear finger cots or gloves. Your hands may look clean, but dirt and oils on them can damage the fiber and contaminate connectors.
- Never use the fiber pigtail to pick up or support the weight of the device. Keep both the device and the optical connector together in your hand(s).
- The fiber is made of a very pure expensive glass. Treat it with the same care that would be used when handling expensive crystal glass.
- Do not allow kinks or knots to develop in the fiber. Do not pull on the fiber when kinks or knots are present. Pulling will only cause knots, kinks, and curls to tighten and exceed the minimum bend radius.
- Always use the correct tools for stripping and cleaving the fiber. It will save time and reduce breakage caused by scratches.
- Follow all *ESD* precautions.

10. Technical Specifications

10.1. Flexible Communications

Flexible Communications	
Number of slots for communications modules	Up to 4 slots

10.2. Ports

Ports	
Ethernet Network Ports	Slot #1 - 3—supports up to 8 x 10/100/1000 RJ45s or 8 x 100/1000 *SFP*s per slot Slot #4—supports up to 4 x 10GB Base-X or 4x1GB Base-X Uplinks
Serial Console Port	RS-232 in RJ-45 connector with console cable. 115200bps, 8, N, 1
USB Port / SD cards	USB 2.0 for software and configuration update
Other hardware features	Modular chassis with hot-swappable modules; redundant hot-swappable power supplies
Alarm	Fault Contact: relay output to carry capacity of 1 A at 24 VDC and 200mA at 125 VDC.

10.3. Technology

Technology	
MAC Table	16K
Priority Queues	8
Processing	Store and Forward
Switch Properties	Switching latency: 7 µs Switching bandwidth: 128 Gbps
Jumbo Frame	Up to 9216 bytes

10.4. Physical Characteristics

Physical Characteristics	
Enclosure	IP 20 Satin Coat Steel
Dimensions	482.05 (W) x 449.5 (D) x 44.00 (H) mm (18.98 x 17.70 x 1.73 inches)
Weight	9.8 kg (21.6 lbs.)

10.5. Power

Power	
Redundant Input power	Dual Power Supplies available in any combination of: • 24 VDC, 2.5 A (Nom.) • 48 VDC, 1.25 A (Nom.) • 100-240 VAC, 50/60 Hz, 100-240 VDC, 1 A (Nom.)
Power Consumption	• 60 W for DC Power Supplies • 60 VA for AC Power Supplies
Overload Current Protection	Fast Acting Fuse 3.15 A and 250 V (can only be replaced in the factory).
Class of Equipment	IEC 61140: Protection against electric shock Insulation Class - I (AC Mains) Insulation Class - III (DC Mains)

10.6. Power over Ethernet (PoE)

Power over Ethernet (PoE)	
Maximum *PoE* Power from Switch	720 Watts
Maximum *PoE* Power from iRM-8GRJ45P Line Module	240 Watts
Slots where *PoE* is supported	Slots 1, 2, and 3

Power over Ethernet (PoE)		
Notes		*PoE* is a factory-configured option for the iMX350 and iMX950. It requires an external power supply to provide power to the *PoE* ports.

11. Compliance Specifications

11.1. Product Safety Tests

Description	Specification	Level
IP Rating	IEC 61850-3 clause 6.6.2 IEC 60529 clause 6.11 ISO 20653:2013	IP20
Clearance and Creepage	IEC 61850-3 clause 6.6.1 IEC 62368-1, clause 6.4.2 & 5.4.3	Overvoltage Category II Pollution Degree II
Impulse Voltage	IEC 61850-3 clause 6.6.3 IEEE 1613 clause 5.3	5 kV on auxiliary power supply and digital inputs 1 kV on station bus ports
Dielectric Voltage	EC 61850-3 clause 6.6.4 IEEE 1613 clause 5.2	2 kV on auxiliary power supply and digital inputs 0.5 kV on station bus ports
Insulation Resistance	IEC 60255-27 clause 10.6.4.4	≥550MΩ at 500VDC
Protective Bonding	IEC 61850-3 clause 6.6.5	Less than 0.1 Ω
Flammability	IEC 61850-3 clause 6.6.6	V-1
Single Fault Condition	IEC 61850-3 clause 6.6.7	12 VDC
Product Safety Standards	IEC 62368-1	Product Safety Standard for Europe and North America

11.2. Electromagnetic Compatibility (EMC) Tests

Description	Specification	Level
European Compliance	EN 55032:2012 EN 55024:2010 CISPR 32:2012 CISPR 24:2010	Multimedia Class A Equipment
North America Compliance	FCC Part 15 Subpart B:2017 ICES-003:2017	Multimedia Class A Equipment

Description	Specification	Level
Radiated Emission	IEC 61850-3 clause 6.7.4 CISPR22 table 5/7	class A
Conducted Emission	IEC 61850-3 clause 6.7.4 CISPR22 table 1/3	class A
1 MHz Damped Oscillatory Wave	IEC 61850-3 clause 6.7.3 IEC 61000-4-18 EEE 1613 clause 6 IEEE 1613.1 clause 5	2.5 kV CM, 1.0 kV DM HV/Telec. 2.5 kV CM, 2.5 kV DM Zone A
Electrostatic Discharges	IEC 61850-3 clause 6.7.3 IEC 61000-4-2 IEEE 1613 clause 8 IEEE 1613.1 clause 8	8 kV contact, 15 kV air
Radiated Radio Frequency Magnetic Field	IEC 61850-3 clause 6.7.3 IEC 61000-4-3 IEEE 1613 clause 7 IEEE 1613.1 clause 7	20 V/m
Fast Transient/Burst	IEC 61850-3 clause 6.7.3 IEC 61000-4-4 IEEE 1613 clause 6 IEEE 1613.1 clause 5	4 kV
Surge	IEC 61850-3 clause 6.7.3 IEC 61000-4-5 IEC 1613.1 clause 6	AC Power Ports: • 4 kV LE • 2 kV LL DC Power Ports: • 4 kV LE • 2 kV LL • 2 kV LE (PoE 56VDC) • 1 kV LL (PoE 56VDC) Signal Ports: • 4 KV LE • 1 KV LE (PoE)
Conducted Disturbance Induced by RF Fields	IEC 61850-3 clause 6.7.3 IEC 61000-4-6 IEEE 1613.1 clause 9	0.15-80 MHz at 10 V 27, 68 MHz at 10 V

Description	Specification	Level
Main Frequency Voltage, Common-mode Disturbances	IEC 61850-3 clause 6.7.3 IEC 61000-4-16 IEEE 1613.1 clause 12	30 V; 60 s 300 V; 1 s
Power Frequency Magnetic Field	IEC 61850-3 clause 6.7.3 IEC 61000-4-8 IEEE 1613.1 clause 10	100 A/m cont.; 1000 A/m 1s
D.C. Voltage Dips	IEC 61850-3 clause 6.7.3 IEC 61000-4-29	60%; 0.1 s 30%; 0.1 s
A.C. Voltage Dips	IEC 61850-3 clause 6.7.3 IEC 61000-4-11	60%; 50 c 30%; 1c
D.C. Voltage Interruptions	IEC 61850-3 clause 6.7.3 IEC 61000-4-29	100%; 0.05 s
A.C. Voltage Interruptions	IEC 61850-3 clause 6.7.3 IEC 61000-4-11	100%; 5/50 c
D.C. Ripple	IEC 61850-3 clause 6.7.3 IEC 61000-4-17 IEEE 1613 clause 4.2	10% Ur_dc 5% content (different calculation method)
Damped Oscillatory Magnetic Field	IEEE 1613.1 clause 11 IEC 61000-4-10	100 A/m (peak)
Burden for DC Power Supply	IEC 61850-3, clause 6.8.2	60W
Inrush Current	IEC 61850-3, clause 6.8.1.2/6.8.2.2	100 VAC peak 15.4 A ≤ 5 ms 240 VAC peak 32.4 A ≤ 5 ms 100 VDC peak 19.4 A ≤ 1 ms 240 VDC peak 52.8 A ≤ 1 ms 24 VDC peak 131 A ≤ 1 ms 48 VDC peak 262 A ≤ 1 ms

11.3. Climatic Environmental Tests

Description	Specification	Level
Dry Heat Operational	IEC 61850-3 clause 6.9.3.1 IEC 60068-2-2, test Be	+85°C; 16 hours
Dry Heat Operational	IEEE 1613 clause 3.1.1	+85°C

Description	Specification	Level
Cold Operational	IEC 61850-3 clause 6.9.3.2 IEC 60068-2-1, test Ad	-40°C; 16 hours
Cold Operational	IEEE 1613 clause 3.1.1	-40°C
Dry Heat Storage	IEC 61850-3 clause 6.9.3.3 IEC 60068-2-2, test Bb	+85°C; 16 hours
Dry Heat Storage	IEEE 1613 clause 3.1.2	+85°C
Cold Storage	IEC 61850-3 clause 6.9.3.4 IEC 60068-2-1, test Ab	-40°C; 16 hours
Cold Storage	IEEE 1613 clause 3.1.2	-40°C
Damp Heat, Steady State	IEC 61850-3 clause 6.9.3.6 IEC 60068-2-78 test Cab	+40°C; 93%, 10 days
Damp Heat, Cyclic	IEC 61850-3 clause 6.9.3.7 IEC 60068-2-78 test Db IEEE 1613 clause 3.1.3	+25°C; 55°C 97%; 93% 6 cycles + 55°C

11.4. Mechanical Environmental Tests

Description	Specification	Level
Vibration Response	IEC 61850-3 clause 6.10.1 IEC 60255-21-1	0.5 g, 1 sweep cycle/axis, 3 axis, freq range 10-150Hz
Vibration Endurance	IEC 61850-3 clause 6.10.1 IEC 60255-21-1	1 g, 20 sweep cycle/axis, 3 axis, freq range 10-150Hz
Shock Response	IEC 61850-3 clause 6.10.2 IEC 60255-21-2	5 g, 11 ms duration/pulse, 6 pulses/axis, 3 axis
Shock Withstand	IEC 61850-3 clause 6.10.2 IEC 60255-21-2	15 g, 11 ms duration/pulse, 6 pulses/axis, 3 axis
Bump	IEC 61850-3 clause 6.10.2 IEC 60255-21-2	10 g, 16 ms duration/pulse, 2000 pulses/axis, 3 axis

Description	Specification	Level
Seismic, Single Axis Sweep	IEC 61850-3 clause 6.10.3 IEC 60255-21-3	Freq range: 1-35 Hz, Cross-over freq: 8-9 Hz Displacement: 3.5 mm[x], 1.5 mm [y] Acceleration: 1.0 g [x], 0.5 g [y] Number of sweep cycles per axis 1, number of axis 3
Vibration	IEEE 1613 clause 9	V.S.3
Shock	IEEE 1613 clause 9	100 mm

11.5. Altitude

Description	Specification	Level
Altitude	IEC 61850-3 section 4, table 1 IEC 61850-3 section 7.2, table 25	less than or equal to 2000 m 86 kPa to 106 kPa

GLOSSARY ENTRIES

802.1D

IEEE 802.1D is the Ethernet MAC bridges standard which includes Bridging, Spanning Tree and others. It is standardized by the IEEE 802.1 working group. It includes details specific to linking many of the other 802 projects including the widely deployed 802.3 (Ethernet), 802.11 (Wireless LAN) and 802.16 (WiMax) standards.

Bridges using virtual LANs (VLANs) have never been part of 802.1D, but were instead specified in separate standard, 802.1Q originally published in 1998.

By 2014, all the functionality defined by IEEE 802.1D has been incorporated into either IEEE 802.1Q (Bridges and Bridged Networks) or IEEE 802.1AC (MAC Service Definition).

802.1Q

IEEE 802.1Q, often referred to as DOT1Q or 1Q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. It is the most widely used encapsulation method for VLAN tagging.

802.1X

IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). 802.1X authentication requires a client, an authenticator, and an authentication server. The client is a device that wants to connect to the network.

802.1W

IEEE 802.1W feature provides rapid traffic reconvergence for point-to-point links within a few milliseconds (0-500 milliseconds), following the failure of bridge or bridge point. This reconvergence occurs more rapidly than the reconvergence provided by the 802.1F spanning Tree Protocol (STP) or by RSTP.

AAA

Authentication, Authorization and Accounting (AAA) functionalities. AAA are provided by TACACS+. TACACS+ is used because it provides independently separate and modular authentication, authorization, and accounting (AAA) facilities achieved by a single access control server (the TACACS+ daemon).

AARP

AppleTalk Address Resolution Protocol (AARP). The AARP maps computers' physical hardware addresses to their temporarily assigned AppleTalk network addresses. AARP is functionally equivalent to Address Resolution Protocol (ARP). The AARP table permits management of the address mapping table on the managed device. This protocol allows Apple computers' AppleTalk hosts to generate their own network addresses

ABR

Area Border Router (ABR)

ACK

ACK stands for acknowledgment. ACK is one of the TCP flags.

TCP flags are various types of flag bits present in the TCP header. Each of them has its own significance. They initiate connections, carry data, and tear down connections. The commonly used TCP flags are SYN, ACK, RST, FIN, URG, PSH.

- SYN (synchronize): Packets that are used to initiate a connection.
- ACK (acknowledgment): Packets that are used to confirm that the data packets have been received, also used to confirm the initiation request and tear down requests.
- RST (reset): Signify the connection is down or maybe the service is not accepting the requests.
- FIN (finish): Indicate that the connection is being torn down. Both the sender and receiver send the FIN packets to gracefully terminate the connection.
- PSH (push): Indicate that the incoming data should be passed on directly to the application instead of getting buffered.
- URG (urgent): Indicate that the data that the packet is carrying should be processed immediately by the TCP stack

ACL

An access-control list (ACL) is a list of permissions associated with a system resource (object). An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file object has an ACL that contains (Admin: read, write; guest 1: read), this would give Admin permission to read and write the file, and only give guest 1 permission to read it.

AES

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

AH

The Authentication Header (AH) protocol provides data origin authentication, data integrity, and replay protection. However, AH does not provide data confidentiality, which means that all of your data is sent in the clear.

AH ensures data integrity with the checksum that a message authentication code, like MD5, generates. To ensure data origin authentication, AH includes a secret shared key in the algorithm that it uses for authentication. To ensure replay protection, AH uses a sequence number field within the AH header. It is worth noting here, that these three distinct functions are often lumped together and referred to as authentication. In the simplest terms, AH ensures that your data has not been tampered with en route to its final destination.

Although AH authenticates as much of the IP datagram as possible, the values of certain fields in the IP header cannot be predicted by the receiver. AH does not protect these fields, known as mutable fields. However, AH always protects the payload of the IP packet.

The Internet Engineering Task Force (IETF) formally defines AH in Request for Comment (RFC) 4302, IP Authentication Header.

AO

Authentication Option (AO). TCP-AO specifies the use of stronger Message Authentication Codes (MACs), protects against replays even for long-lived TCP connections, and provides more details on the association of security with TCP connections than TCP MD5. TCP-AO is compatible with either a static Master Key Tuple (MKT) configuration or an external, out-of-band MKT management mechanism; in either case, TCP-AO also protects connections when using the same MKT across repeated

instances of a connection, using traffic keys derived from the MKT, and coordinates MKT changes between endpoints.

ARAP

Apple Remote Access Protocol (ARAP); the Apple Remote Access Protocol (ARAP) sends traffic based on the AppleTalk protocol across PPP links and ISDN switched-circuit networks. ARAP is still pervasive in the Apple market, although the company is attempting to transition into an Apple-specific TCP stack for use over a PPP link.

ARP

ARP (Address Resolution Protocol). The ARP is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given Internet layer address, typically an IPv4 address.

AS

Autonomous System (AS)

ASBR

Autonomous Border System Router (ASBR)

Asdot

Asdot format is used when the 4-byte ASN are represented by their decimal value e.g. 100.1. BGP uses AS numbers as a fundamental part of its routing process. Because conventional 2-byte public AS numbers were becoming exhausted, the IANA increased the AS numbers by introducing a 4-byte AS numbers. The Asdot notation to represent these AS numbers is as follows.
For values between 0 and 65535, Asdot notation is simply the decimal value of the AS number. These values take up to 16 bits to express in binary. Examples include:

- 5
- 25
- 196
- 65000
- 65535

For values above 65536, Asdot notation splits the 32 bit binary value into two 16 bit values. These values are represented as two decimal numbers separated by a dot. Examples include:

- 0.65536
- 15.418
- 65535.8520
- 65535.65535

You will notice that for values of up to 65535, the Asdot is the same as the Asplain notation, and for values of 65536 and above, the Asdot is the same as the Asdot+ notation.

ASN

Autonomous System Number (ASN)

BDR

BDR stands for Backup Designated Router.

BFD

Bidirectional Forwarding Detection (BFD) is a super fast protocol that is able to detect link failures within milliseconds or even microseconds. BFD runs independent from any other (routing) protocols. Once it's up and running, you can configure protocols like OSPF, EIGRP, BGP, HSRP, MPLS LDP etc. to use BFD for link failure detection instead of their own mechanisms. When the link fails, BFD will inform the protocol

BGP

BGP (Border Gateway Protocol) is an Inter AS (Autonomous Systems) Routing Protocol that manages the distribution of Network Layer Reachability Information (NLRI) across AS. It is used to build an AS connectivity graph that is used to prune routing loops and enforce policies at AS level

BGP

BGP-4 is an extension of BGP-3 (BGP version 3),and it is the current version of BGP. BGP4 was published as RFC 4271 in 2006. Its major enhancement is the support for Classless Inter-Domain Routing (CIDR) and use of route aggregation to decrease the size of routing tables. The new RFC allows BGP4 to carry a wide range of IPv4 and IPv6 "address families".

BIDIR-PIM

Bi-directional Sparse Mode (PIM-SM); Derived from PIM-SM, BIDIR-PIM builds and maintains a bidirectional RPT, which is rooted at the RP and connects the multicast sources and the receivers. Along the bidirectional RPT, the multicast sources send multicast data to the RP, and the RP forwards the data to the receivers. Each router along the bidirectional RPT needs to maintain only one (*, G) entry, saving system resources.

Another difference between PIM sparse mode and PIM bidirectional mode is that with sparse mode traffic only flows down the shared tree. Using PIM bidirectional mode, traffic will flow up and down the shared tree. When the multicast packets arrive at the RP, they will be forwarded down the shared tree (if there are receivers) or dropped (when we don't have receivers).

BMS

Best Master Clock (BMS); The ordinary clock executes the port state machine and BMC (Best Master Clock) algorithm to select the *PTP* port state.

BOOTP

The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. The BOOTP was originally defined in RFC 951.

BPDU

Bridge Protocol Data Units (BPDUs) are frames that contain information about the spanning tree protocol (STP). A switch sends BPDUs using a unique source MAC address from its origin port to a multicast address.

There are two kinds of BPDUs for 802.1D Spanning Tree:

- Configuration BPDU, sent by root bridges to provide information to all switches.
- TCN (Topology Change Notification), sent by bridges towards the root bridge to notify changes in the topology, such as port up or port down.

BPS

BPS (Bits-per-second)

BR

Border Router (BR)

BSD

Berkeley Software Distribution (BSD)

BSR

The bootstrap router (BSR) ensures that all routers in the PIM domain have the same RP cache as the BSR. You can configure the BSR to help you select an RP set from BSR candidate RPs. The function of the BSR is to broadcast the RP set to all routers in the domain. You select one or more candidate BSRs to manage the RPs in the domain. Only one candidate BSR is elected as the BSR for the domain.

This figure shows the BSR mechanism. Router A, the software-elected BSR, sends BSR messages out all enabled interfaces (shown by the solid lines in the figure). The messages, which contain the RP set, are flooded hop by hop to all routers in the network. Routers B and C are candidate RPs that send their candidate-RP advertisements directly to the elected BSR (shown by the dashed lines in the figure).

The elected BSR receives candidate-RP messages from all the candidate RPs in the domain. The bootstrap message sent by the BSR includes information about all of the candidate RPs. Each router uses a common algorithm to select the same RP address for a given multicast group.
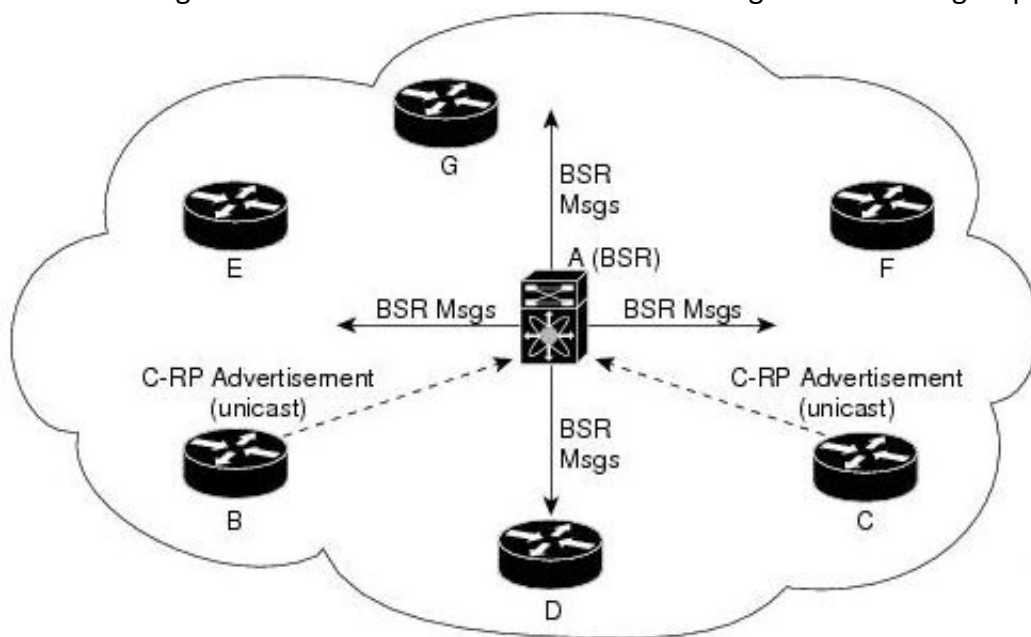
CA

Certificate Authorization (CA)

CBP

Customer Backbone Port (CBP)

CBS

Committed burst size (CBS). During periods of average traffic rates below the Committed information rate (CIR), any unused bandwidth capacity accumulates up to a maximum amount defined by the CBS. Short periods of bursting traffic (back-to-back traffic at averages rates that exceed the CIR) are also categorized as green provided that unused bandwidth capacity is available.

CEP

Customer Edge Port (CEP). The Customer Edge Port (CEP) and each Provider Edge Port are treated as separate Bridge Ports by the spanning tree protocol. If the C-VLAN component connects to the S-VLAN component with a single Provider Edge Port, and the associated service instance supports no more than two customer interfaces, then all frames (including Spanning Tree BPDUs) addressed to the Bridge Group Address may be relayed between the two Ports of the C-VLAN component without modification. Otherwise, the Spanning Tree Protocol Entity shall execute the Rapid Spanning Tree Protocol (RSTP, Clause 17 of IEEE Std 802.1D), as modified by the provisions of this subclause.

CFI

Canonical Format Identifier (CFI). If Drop Eligible Indicator (DEI) bit is enabled in 802.1ad header or has Canonical Format Identifier (CFI) bit enabled in 802.1q header on an arriving packet, such packets will be dropped using QoS.

MS-CHAP

CHAP stands for Challenge Handshake Authentication Protocol. MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol, CHAP. The protocol exists in two versions, MS-CHAPv1 (defined in RFC 2433) and MS-CHAPv2 (defined in RFC 2759). MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

CIDR

Classless Inter Domain Routing (CIDR).

CIR

Committed information rate (CIR) is defines the guaranteed bandwidth for traffic arriving at or departing from the interface under normal line conditions.

CIST

The Common and Internal Spanning Tree (CIST) is a collection of the ISTs in each MST region.

CLI

Command line interface (CLI) is a text-based interface that is used to operate software and operating systems while allowing the user to respond to visual prompts by typing single commands into the interface and receiving a reply in the same way

CLKIWF

CLKIWF is short for Clock InterWorking Function.

CoS

Output queue scheduling defines the class-of-service (CoS) properties of output queues. Based on certain types of traffic are preferred. The level of service is determined by the egress port queue to which the traffic is assigned. When traffic is queued for transmission, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in other queues for that port.

Some traffic is classified for service (i.e., packet marking) before it arrives at the switch. If you decide to use these classifications, you can map this traffic to egress queues by setting the CoS in the Queue table.

CPLD

A Complex Programmable logic device (CPLD) is a logic device with completely programmable AND/OR arrays and macrocells. Macrocells are the main building blocks of a CPLD, which contain complex logic operations and logic for implementing disjunctive normal form expressions. AND/OR arrays are completely reprogrammable and responsible for performing various logic functions.

CPU

The central processing unit (CPU) is the primary component of a computer that processes instructions. It runs the operating system and applications, constantly receiving input from the user or active software programs. It processes the data and produces output.

CRT

CRT stands for "Internet security certificate.

CSR

Certificate Signing Request (CSR)

CST

common spanning tree (CST); The common spanning tree (CST) that interconnects the MST regions and single spanning trees

CTS

CTS stands for Clear to Send. Request to Send (RTS)/CTS Flow Control is another flow control mechanism that is part of the RS232 standard.

CVID

The C-VID registration table is as follows:

Table 1:   C-VID registration table

C-VID Registration Table	Description
Cvid value	The value of the Customer VLAN id on the Customer edge port. (Table key)
Svid Value	The S-VLAN tag. Auto creates an S-VLAN component and the CNP and PNP and links the PEP of the C-VLAN component to the CNP.
Untagged-pep	A boolean indicating frames for this C-VLAN should be forwarded untagged through the Provider Edge Port (PEP).
Untagged-cep	A boolean indicating frames for this C-VLAN should be forwarded untagged through the Customer Edge Port (CEP).

CVLAN

Set of ports & inner VLANs (CVLAN); or C-VLAN or Customer Bridge (CB)

DB9

DB9 refers to a common connector type from the D-Subminiatures (D-Sub) connector family, which when introduced, was among the smallest connectors used on computer systems. DB9 houses 9 pins (for the male connector) or 9 holes (for the female connector). DB9 connectors were once very

common on PCs and servers. Today, the DB9 has mostly been replaced by more modern interfaces such as USB, PS/2, Firewire, and others.

DB25

The DB25 connector is an analog socket, with 25 pins, from the D-Subminiatures (D-Sub) connector family. The prefix "D" represents the D-shape of the connector shell. The DB25 connector is mainly used in serial and parallel ports, allowing asynchronous data transmission according to the RS-232 standard (RS-232C).

DCD

DCD stands Data Carrier Detect. The description is modem connected to another.

DEC

Digital Equipment Corporation (DEC)

DEI

Drop Eligible Indicator (DEI). If DEI bit is enabled in 802.1ad header or has Canonical Format Identifier (CFI) bit enabled in 802.1q header on an arriving packet, such packets will be dropped using QoS.

DES

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

DF

Designated Forwarder (DF).

DH

Diffie and Hellman (*DH*) describe a method for two parties to agree upon a shared secret number, called ZZ, in such a way that the secret will be unavailable to eavesdroppers. This method requires that both the sender and recipient of a message have key pairs (private and public). By combining one's private key and the other party's public key, both parties can compute the same shared secret number ZZ

DHCP

Dynamic Host Configuration Protocol (DHCP)

DITA

Darwin Information Typing Architecture (DITA); the DITA specification defines a set of document types for authoring and organizing topic-oriented information, as well as a set of mechanisms for combining, extending, and constraining document types.

D-LAG

Distributed Link Aggregation (D-LAG or DLAG)

DLF

The Destination Lookup Failure (DLF). When a packet arrives at the device and the device doesn't have an entry for the destination MAC address in its MAC address table, the packet is classified as a Destination Lookup Failure (DLF)

DM

DM stands for Dense Mode. Protocol-Independent Multicast Dense Mode (PIM-DM) uses dense multicast routing.

DNAT

Destination network address translation (DNAT) is a technique for transparently changing the destination IP address of an end route packet and performing the inverse function for any replies.

DNS

Domain Name System

DOT1Q

IEEE 802.1Q, often referred to as DOT1Q or 1Q, is the networking standard that supports virtual LANs (VLANs) on an IEEE 802.3 Ethernet network. It is the most widely used encapsulation method for VLAN tagging.

Dot1x

Dot1x Authentication is enabled when dot1x system-auth-control is enabled, and aaa authentication dot1x default is local. If you enable authentication on a port by using the default setting of dot1x port-control, which is force-authorized, it disables 802.1X authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client

DR

The Designated Router (DR) is the router that will forward the PIM join message from the receiver to the RP (rendezvous point).

DS

Differentiated Services (DS).

DS – Differentiated Service , DSCP – Differentiated Service Code Point, CU – Currently Unused
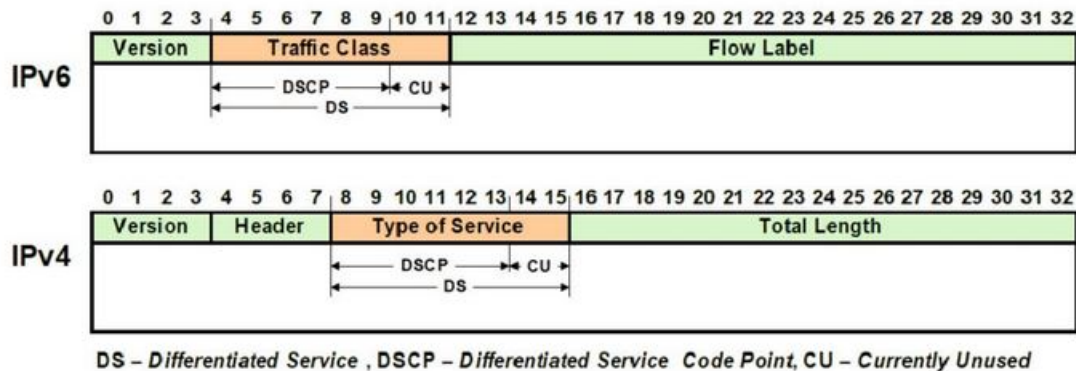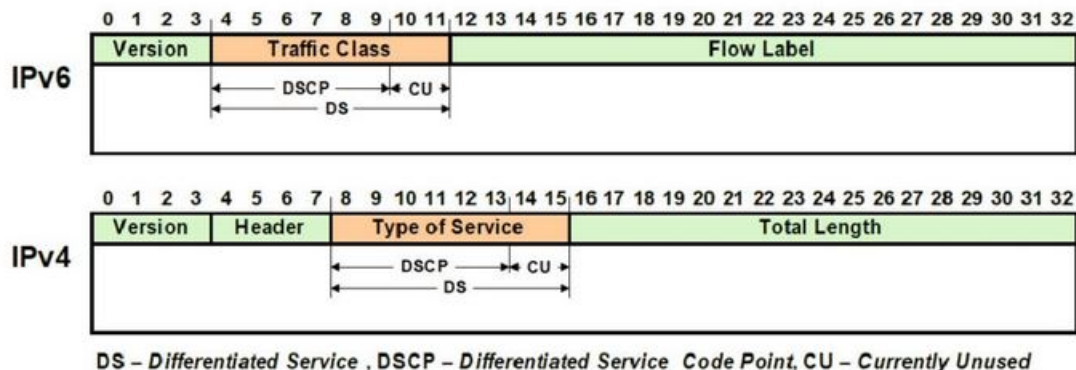
DSCP

A Differentiated Services Code Point (DSCP) is a packet header value that can be used to request (for example) high priority or best effort delivery for traffic.

DS – Differentiated Service , DSCP – Differentiated Service Code Point, CU – Currently Unused

DSR

DSR stands Data Set Ready. The description is ready to communicate.

DST

Daylight Saving Time (DST) is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year

DTR

DTR stands Data Terminal Ready. The description is ready to communicate.

DUT

Device under Test (DUT)

DVMRP

Distance Vector Multicast Routing Protocol (DVMRP)

E2E

End-to-end (E2E) transparent clock for Precision Time Protocol (PTP). With an E2Etransparent clock, only the residence time is included in the timestamp in the packet.

EAP

Extensible Authentication Protocol (EAP) is an authentication framework frequently used in network and Internet connections. EAP is usually tunnelled over RADIUS between the Authenticator and the Authentication Server. 802.1x uses EAP.
EAP is an authentication framework, not a specific authentication mechanism. Commonly used modern methods capable of operating in wireless networks include EAP-TLS, EAP-SIM, EAP-AKA, LEAP and EAP-TTLS. Requirements for EAP methods used in wireless LAN authentication are described in RFC 4017.
The Lightweight Extensible Authentication Protocol (LEAP) method was developed by Cisco Systems prior to the IEEE ratification of the 802.11i security standard.

EAPOL

Extensible Authentication Protocol (EAP) over LAN (EAPoL) is used between the Supplicant (software on your laptop) and the Authenticator (switch)

EBGP

External *BGP* (EBGP); EBGP runs between two BGP routers in different Autonomous System (AS).

EBS

The Excess Burst size (EBS) specifies how much data above the committed burst size (CBS) a user can transmit. The EBS is the size up to which the traffic is allowed to burst without being discarded. EBS allows for moderate periods of bursting traffic that exceeds both the committed information rate (CIR) and the committed burst size (CBS).

ECN

Explicit Congestion Notification (ECN)

EGP

Exterior Gateway Protocol (EGP) is a defunct routing protocol used in autonomous systems to exchange data between surrounding gateway sites. Border Gateway Protocol (BGP) supplanted EGP, widely utilized by research institutes, universities, government agencies, and commercial

companies (BGP). EGP is built on poll instructions to request update answers and periodic message exchange polling for neighbor reachability.

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is a network protocol that enables routers to exchange information more efficiently than earlier network protocols, such as Interior Gateway Routing Protocol (IGRP) or Border Gateway Protocol (BGP), and provides intelligent traffic sharing.

EIR

The excess information rate (EIR) specifies the rate above the CIR (committed information rate) at which traffic is allowed into the network and that may get delivered if the network is not congested. The EIR has an additional parameter associated with it called the excess burst size (EBS). The EBS is the size up to which the traffic is allowed to burst without being discarded.

ESD

ElectroStatic Discharge (ESD) is the sudden flow of electricity between two electrically charged objects caused by contact, an electrical short or dielectric breakdown. A buildup of static electricity can be caused by tribocharging or by electrostatic induction. The ESD occurs when differently-charged objects are brought close together or when the dielectric between them breaks down, often creating a visible spark.

EXEC

exec: Protocol
Commands that are invoked using the exec: protocol must be executable as standalone commands. Commands that are built into a command interpreter or other program cannot be executed directly, but must be executed (if possible) within the context of the application that provides them. For example, the following seed URL would not work on Microsoft Windows systems because the dir command is built into the Windows command interpreter (cmd.exe):
exec: dir e:\data
To use the exec protocol with commands that are built into the Windows command interpreter, you must do something as the following:
exec: cmd /c dir 'e:\data'

ESP

Encapsulation Security Protocol (ESP); the ESP protocol provides data confidentiality, and also optionally provides data origin authentication, data integrity checking, and replay protection. The difference between ESP and the Authentication Header (AH) protocol is that ESP provides encryption, while both protocols provide authentication, integrity checking, and replay protection. With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange.

EVB

Edge Virtual Bridge (EVB) is an IEEE standard that involves the interaction between virtual switching environments in a hypervisor and the first layer of the physical switching infrastructure. The EVB enhancements are following 2 different paths – 802.1qbg and 802.1qbh.

EVC

Ethernet Virtual Connection (EVC).

FCS

A frame check sequence (FCS) is an error-detecting code added to a frame in a communication protocol. Frames are used to send payload data from a source to a destination.

FDB

Forwarding Database (FDB)

FID

Filtering ID (FID)

FHRP

First Hop Redundancy Protocol (FHRP)

FPGA

The Field Programmable Gate Array (FPGA) is a programmable logic device that can have its internal configuration set by the firmware.

FTP

The File Transfer Protocol (FTP) is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).

GARP

GARP (Generic Attribute Registration Protocol) is a local area network (LAN) protocol that defines procedures by which end stations and switches can register and deregister attributes, such as network identifiers or addresses, with each other. Every end station and switch thus has a record, or list, of all the other end stations and switches that can be reached at any given time.
When an attribute for an end station or switch is registered or deregistered according to GARP, the set of reachable end stations and switches, called participants, is modified according to specific rules. The defined set of participants at any given time, along with their attributes, is a subset of the network topology called the reachability tree. Data frames are propagated only to registered end stations. This prevents attempts to send data to end stations that are not reachable.

GGP

Gateway-to-Gateway Protocol (GGP) is an obsolete protocol defined for routing datagrams between Internet gateways. It was first outlined in 1982. The GGP was designed as an IP datagram service similar to the TCP and the UDP.

GMRP

GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping.

GND

Ground

GPS

Global Positioning System

GR

Graceful Restart (GR)

GRE

Generic routing encapsulation (GRE) is an IP encapsulation protocol which is used to transport IP packets over a network. In GRE, an IP datagram is tunnelled (encapsulated) within another IP data-

gram.One great advantage of GRE is that it allows routing of IP packets between private IPv4 networks which are separated over public IPv4 Internet. GRE also supports encapsulating IPv4 broadcast and multicast traffic.

GVRP

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frame s with VLAN configuration data

HA

High Availability (HA)

HDMI

HDMI (High-Definition Multimedia Interface) is digital interface capable of transmitting high-quality and high-bandwidth streams of audio and video between devices

HOL

Head-Of-Line (HOL) blocking should be prevented on a port. HOL blocking happens when HOL packet of a buffer cannot be switched to an output port (i.e. HOL occurs when a line of packets is held up by the first packet).

HSR

High-availability Seamless Redundancy (HSR) is a network protocol for Ethernet that provides seamless failover against failure of any single network component. PRP and HSR are standardized by the IEC 62439 and are suited for applications that request high availability and no switchover time.

HTTP

Hyper Text Transfer Protocol (HTTP)

HTTPS

Hyper Text Transfer Protocol Secure (HTTPS)

IANA

Internet Assigned Numbers Authority (IANA)

IBGP

Internal BGP (iBGP) is the protocol used between the routers in the same autonomous system (AS). iBGP is used to provide information to your internal routers. iBGP requires all the devices in same AS to form full mesh neighborship or either of Route reflectors and Confederation for prefix learning.

ICMP

Internet Control Message Protocol

IDPR

Inter-domain Routing Protocol (IDPR). The objective of IDPR is to construct and maintain routes, between source and destination administrative domains, that provide user traffic with the requested services within the constraints stipulated for the domains transited.

IETF

Internet Engineering Task Force (IETF) is an open standards organization, which develops and promotes voluntary Internet standards, in particular the technical standards that comprise the Internet protocol suite (TCP/IP).

IGMP

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast and allows the network to direct multicast transmissions only to hosts that have requested them.

IGP

Interior Gateway Protocol (IGP) is a type of routing protocol used for exchanging routing table information between gateways (commonly routers) within an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.

IGRP

Interior Gateway Routing Protocol (IGRP) is a proprietary distance vector routing protocol that manages the flow of routing information within connected routers in the host network or autonomous system. The protocol ensures that every router has routing tables updated with the best available path. IGRP also avoids routing loops by updating itself with the changes occurring over the network and by error management.

IGS

The Internet Group Management Protocol (IGMP) Snooping (IGS) is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client). Essentially, IGS is a layer 2 optimization for the Layer 3 IGMP.

IKE

Internet Key Exchange (IKE)

IP

Internet Protocol (IP).

IPSec

IPSec (Internet Protocol Security) is a suite of protocols that provides security to Internet communications at the IP layer. The most common current use of IPSec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway); it can also provide end-to-end, or host-to-host, security.

IPv4

IPv4 and IPv6 are Internet protocol version 4 and Internet protocol version 6. IPv4 supports:

- IPv4 has a 32-bit address length
- IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
- IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method
- It Supports Manual and DHCP address configuration
- In IPv4 end to end, connection integrity is Unachievable
- It can generate 4.29×109 address space
- Fragmentation performed by Sender and forwarding routers
- In IPv4 Packet flow identification is not available
- In IPv4 checksum field is available
- It has broadcast Message Transmission Scheme

- In IPv4 Encryption and Authentication facility not provided
- IPv4 has a header of 20-60 bytes.

IPv6

IPv6 stands for Internet protocol version 6. An IPv6 address consists of eight groups of four hexa-decimal digits. Anexample of IPv6 address is as follows
3001:0da8:75a3:0000:0000:8a2e:0370:7334
there are different ypes of IPv6 addresses:

- Unicast addresses—it identifies a unique node on a network and usually refers to a single sender or a single receiver.
- Multicast addresses—it represents a group of IP devices and can only be used as the destination of a datagram.
- Anycast addresses—it is assigned to a set of interfaces that typically belong to different nodes.

IRDP

ICMP Router Discovery Protocol (IRDP) allows hosts to locate routers that can be used as a gateway to reach IP-based devices on other networks. When the device running IRDP operates as a router, router discovery packets are generated. When the device running IRDP operates as a host, router discovery packets are received. ICMP stands for Internet Control Message Protocol.

IRTP

Internet Reliable Transaction Protocol (IRTP) is a transport level host to host protocol designed for an Internet environment. It provides reliable, sequenced delivery of packets of data between hosts and multiplexes / demultiplexes streams of packets from/to user processes representing ports.

ISAKMP

Internet Security Association and Key Management Protocol (ISAKMP)

ISDN

Integrated Services Digital Network (ISDN)

ISL

ISL stands for Inter-Switch Link which is one of the VLAN protocols. The ISL is proprietary of Cisco and is used only between Cisco switches. It operates in a point-to-point VLAN environment and supports up to 1000 VLANs and can be used over Fast Ethernet and Gigabit Ethernet links only.

ISP

Internet service provider (ISP)

ISS

Intelligent Switch Solution (ISS).

IST

The Internal Spanning Tree (IST) instance receives and sends BPDUs to the CST. The IST can repre-sent the entire MST region as a CST virtual bridge to the outside world.

IVL

Independent VLAN Learning (IVL)

IVR

Inter VLAN Routing (IVR)

IWF

InterWorking Function (IWF).

KDF

Key Derivation Functions (KDFs); TCP-AO's Traffic_Keys are derived using KDFs. As per RFC5926, when invoked, a KDF generates a string of length Output_Length bit based on the Master_Key and context value. This result may then be used as a cryptographic key for any algorithm that takes anOutput_Length length key. A KDF MAY specify a maximum Output_Length parameter.

L2GP

Layer 2 Gateway Port (L2GP)

LA

Link Aggregation

LACP

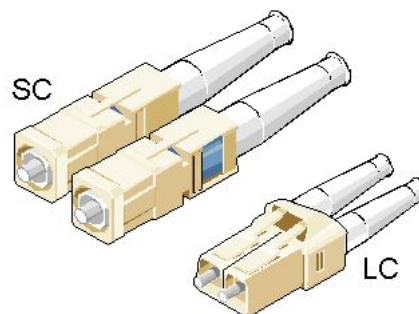Link Aggregation Control Protocol

LAG

Link Aggregation Group

LAN

Local Area Network

LC

LC (Lucent Connector) is a miniaturized version of the fiber-optic SC (Standard Connector) connector. It looks somewhat like the SC, but is half the size with a 1.25mm ferrule instead of 2.5mm.

SC and LC Connectors

LED

Light-emitting diode (LED) is a widely used standard source of light in electrical equipment.

LLDP

Link Layer Discovery Protocol (LLDP)

LM

Line Module (LM)

LSA

Link State Advertisement (LSA)

LSDB

link state database (LSDB)

LSR

Link State Routing (LSR)

MAC

Media access control (MAC) is a sublayer of the data link layer in the seven-layer OSI network reference model. MAC is responsible for the transmission of data packets to and from the network-interface card, and to and from another remotely shared channel.

MAU

Medium Attachment Unit (MAU)

MD5

Message Digest Algorithm 5 (MD5) is a cryptographic hash algorithm that can be used to create a 128-bit string value from an arbitrary length string.

A hash function provides encryption using an algorithm and no key. A variable-length plaintext is "hashed" into a (typically) fixed-length hash value (often called a "message digest" or simply a "hash"). Hash functions are primarily used to provide integrity; if the hash of a plaintext changes, the plaintext itself has changed.

Common older hash functions include Secure Hash Algorithm 1 (SHA-1), which creates a 160-bit hash and Message Digest 5 (MD5), which creates a 128-bit hash.

Although there has been insecurities identified with MD5, it is still widely used, and its most common use is to verify the integrity of files.

MDI

Media Independent Interface (MDI) and Media Independent Interface with Crossover (MDIX) are basically ports on a computer and a network switch, router, or hub, respectively.

MDIX

Media Independent Interface with Crossover (MDIX) and Media Independent Interface (MDI) are basically ports on a computer and a network switch, router, or hub, respectively.

MED

1) Media Endpoint Discovery (MED); LLDP does not contain the capability of negotiating additional information such as PoE management and VLAN assignments. This capability was added as an enhancement known as Media Endpoint Discovery or MED, resulting in the enhanced protocol LLDP-MED.The MED enhancement has been standardized by the Telecommunications Industry Association in standard number ANSI/TIA-1057.

2) Multi Exit Discriminator (MED) for routes received from different autonomous systems; MED is one of the parameters considered for selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

MHRP

Multipath Hybrid Routing Protocol (MHRP) is a multipath routing protocol for hybrid Wireless Mesh Network (WMN), which provides security and uses technique to find alternate path in case of route failure.

MIB

Management Information Base (MIB) is the hierarchical database used by the simple network management protocol (SNMP) to describe the particular device being monitored.

MIB OID

Management Information Base (MIB) is the hierarchical database used by the simple network management protocol (SNMP) to describe the particular device being monitored.

MIB Object IDentifier (OID), as known as a MIB object identifier in the SNMP, is a number assigned to devices in a network for identification purposes. OID numbering is hierarchical. Using the IETF notation of digits and dots, resembling very long IP addresses, various registries such as ANSI assign high-level numbers to vendors and organizations. They, in turn, append digits to the number to identify individual devices or software processes.

MIC

Media redundancy Interconnection Client (MIC) is a member node of a MRP Interconnect ring.

MIM

Media redundancy Interconnection Manager (MIM) is a node in a MRP Interconnect ring which acts a redundancy manager.

MLDS

Multicast Listener Discovery Snooping (MLDS) constrains the flooding of IPv6 multicast traffic on VLANs. When MLDS is enabled on a VLAN, adevice examines MLD messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. On the basis of what it learns, the device then forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

MKT

Master Key Tuple (MKT). TCP-AO uses cryptographic algorithms to convert MKTs, which can be shared across connections, into unique traffic keys for each connection.

MM

MultiMode (MM) Mode is in optical fiber with a larger core than singlemode fiber. Typically, MM has a core diameter of 50 or 62.5 μm and a cladding diameter of 125 μ.

MIC

Media redundancy Interconnection Client (MIC) is a member node of a MRP Interconnect ring.

MPLS

Multiprotocol Label Switching (MPLS) is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows. The labels identify virtual links (paths) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols, hence the "multiprotocol" reference on its name.

MRA

Media Redundancy Automanager (MRA). To configure a Media Redundancy Automanager (MRA), the node or nodes elect an MRM by a configured priority value.

MRC

Media Redundancy Client (MRC) is a member node of a MRP ring.

MRM

Media Redundancy Manager (MRM) is a node in the network which acts a redundancy manager.

MRP

Media Redundancy Protocol (MRP) is a networking protocol designed to implement redundancy and recovery in a ring topology.

MSR

1) MSR (MIB Save and Restore).

2) Model-Specific Register (*MSR*)

MST

MST (Multiple Spanning Tree) is the version of STP that allows multiple VLANs to a single instance. It is the standard based protocol defined with IEEE 802.1s. Unlike other spanning tree protocols, in which all the spanning tree instances are independent, MST establishes and maintains IST, CIST, and CST spanning trees.

MSTI

Multiple spanning trees, called MSTIs; inside an MST region, multiple spanning trees, called MSTIs, are calculated. Among these MSTIs, MSTI 0 is the IST.

MSTP

Multiple Spanning-Tree Protocol

MTU

Maximum Transmission Unit (MTU)

MVLAN

Multicast VLANs (MVLAN)

NAP

Network Access Protection (NAP)

NAPT

Network address port translation (NAPT) is a variation of the traditional *NAT*. NAPT extends the notion of translation one step further by also translating transport identifiers (e.g., TCP and UDP port numbers, ICMP query identifiers).

NAS

The Network Access Server (NAS) is the front line of authentication – it's the first server that fields network authentication requests before they pass through to the RADIUS. The NAS Identifier (NAS-ID) is a feature that allows the RADIUS server to confirm information about the sender of the authentication request.

NAT

Network address translation (NAT) is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

NBMA

NBMA (Non Broadcast Multi Access)

NBNS

NetBIOS Name Server where NetBIOS stands for Network Basic Input / Output System.

NC

NC (normally closed) is a closed (short) circuit creating a path for the current.

ND

Neighbor Discovery (ND); the Virtual Router Redundancy Protocol (*VRRP*) for IPv6 provides a much faster switchover to an alternate default router than can be obtained using standard neighbor discovery (ND) procedures.
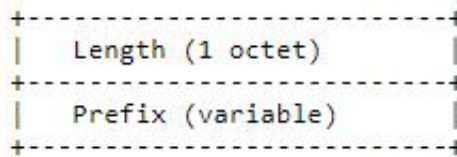
NETBIOS

Network Basic Input / Output System (NETBIOS)

NIP

This set of fields are a vector of N IP unicast addresses, where the value N corresponds to the Number or Sources (N) field.

NLRI

Network Layer Reachability Information (NLRI). The Network Layer Reachability information is encoded as one or more 2-tuples of the form <length, prefix>, whose fields are described below.

```
+---------------------------+
|     Length (1 octet)      |
+---------------------------+
|     Prefix (variable)     |
+---------------------------+
```

NMS

Network Management System (NMS)

NO

NO (normally open) is an open circuit not creating a path for the current.

NPS

Network Policy Server (NPS)

NSSA

Not-so-stubby Area (NSSA)

NTP

Network Time Protocol (NTP)

NVP

Network Voice Protocol (NVP) was a pioneering computer network protocol for transporting human speech over packetized communications networks. It was an early example of Voice over Internet Protocol technology.

NVRAM

Non-volatile random-access memory (NVRAM) is random-access memory that retains data without applied power. This is in contrast to dynamic random-access memory (DRAM) and static random-access memory (SRAM), which both maintain data only for as long as power is applied, or such forms of memory as magnetic tape, which cannot be randomly accessed but which retains data indefinitely without electric power.

OID

Object IDentifier

ORF

Outbound Route Filter (ORF); the BGP Prefix-Based ORF feature uses BGP ORF send and receive capabilities for minimizing the number of BGP updates that are sent between BGP peers. Configuring this feature can help reduce the amount of system resources required for generating and processing routing updates by filtering out unwanted routing updates at the source.

OSPF

Open Shortest Path First routing protocol

OUI

organization unique identifiers (OUI)s. LLDP enables defining optional *TLV* units by using organiza-tion unique identifiers (OUIs) or organizationally-specific TLVs. An OUI identifies the category for a *TLV* unit depending on whether the OUI follows the IEEE 802.1 or IEEE 802.3 standard.

P2P

Peer-to-peer (P2P) transparent clock for Precision Time Protocol (PTP).

PAE

Port Access Entity (PAE). 802.1X-2001 defines two logical port entities for an authenticated port—the "controlled port" and the "uncontrolled port". The controlled port is manipulated by the 802.1X PAE (Port Access Entity) to allow (in the authorized state) or prevent (in the unauthorized state) network traffic ingress and egress to/from the controlled port. The uncontrolled port is used by the 802.1X PAE to transmit and receive EAPOL frames.

PAP

Password Authentication Protocol (PAP) is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users. PAP stops working after establishing the authentication; thus, it can lead to attacks on the network.

PBB

Provider backbone bridging (PBB) extends Layer 2 Ethernet switching to provide enhanced scal-ability, quality-of-service (QoS) features, and carrier-class reliability.

PC

Personal Computer

PCB

Provider Core Bridge (PCB) or S-VLAN Bridge; PCB integrates only one S-VLAN component. It is capable of providing single service on a port.

PDU

A Protocol Data Unit (PDU) is a single unit of information transmitted among peer entities of a computer network. A PDU is composed of protocol-specific control information and user data.

P/E

Program/Erase (P/E). Writing a byte to flash memory involves two steps: Program and Erase (P/E). P/E cycles can serve as a criterion for quantifying the endurance of a flash storage device.

PEB

Provider Edge Bridge (PEB); Provider Edge Bridge integrates one S-VLAN component with zero or many C-VLAN components as well as integrates each C-VLAN (up to 4094 C-VLANs) individually with a different S-VLAN (up to 4094 S-VLANs).

PEM

PEM (originally "Privacy Enhanced Mail") is the most common format for X.509 certificates, CSRs, and cryptographic keys. A PEM file is a text file containing one or more items in Base64 ASCII encoding, each with plain-text headers and footers (e.g. -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----). A single PEM file could contain an end-entity certificate, a private key, or multiple certificates forming a complete chain of trust. Most certificate files downloaded from SSL.com will be in PEM format

PEP

Provider Edge Port (PEP). The Customer Edge Port and each Provider Edge Port are treated as separate Bridge Ports by the spanning tree protocol. If the C-VLAN component connects to the S-VLAN component with a single Provider Edge Port, and the associated service instance supports no more than two customer interfaces, then all frames (including Spanning Tree BPDUs) addressed to the Bridge Group Address may be relayed between the two Ports of the C-VLAN component without modification. Otherwise, the Spanning Tree Protocol Entity shall execute the Rapid Spanning Tree Protocol (RSTP, Clause 17 of IEEE Std 802.1D), as modified by the provisions of this subclause.

PFS

Perfect Forward Secrecy (PFS) means that a piece of an encryption system automatically and frequently changes the keys it uses to encrypt and decrypt information, such that if the latest key is compromised, it exposes only a small portion of the user's sensitive data.
If PFS is specified in the IPSec policy, a new Diffie-Hellman exchange is performed with each quick mode, providing keying material that has greater entropy (key material life) and thereby greater resistance to cryptographic attacks. Each Diffie-Hellman exchange requires large exponentiations, thereby increasing CPU use and exacting a performance cost.

PHB

PHB (Per Hop Behavior) is a term used in differentiated services (DiffServ) or multiprotocol label switching (MPLS). It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PHY

A PHY, an abbreviation for "physical layer", is an electronic circuit, usually implemented as an integrated circuit, required to implement physical layer functions of the OSI model in a network interface controller. A PHY connects a link layer device (often called MAC as an acronym for medium access control) to a physical medium such as an optical fiber or copper cable. A PHY device typically includes both physical coding sublayer (PCS) and physical medium dependent (PMD) layer functionality. PHY may also be used as a suffix to form a short name referencing a specific physical layer protocol, for example M-PHY.

PIM

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols. PIM is not dependent on a specific unicast routing protocol; it can make use of any unicast routing protocol in use on the network. PIM does not build its own routing tables. PIM uses the unicast routing table for reverse-path forwarding.
There are four variants of PIM:

- PIM Sparse Mode (PIM-SM) explicitly builds unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM generally scales fairly well for wide-area usage.

- PIM Dense Mode (PIM-DM) uses dense multicast routing. It implicitly builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present. PIM-DM is straightforward to implement but generally has poor scaling prop-

erties. The first multicast routing protocol, DVMRP used dense-mode multicast routing. See the PIM Internet Standard RFC 3973.

- Bidirectional PIM (Bidir-PIM) explicitly builds shared bi-directional trees. It never builds a shortest path tree, so may have longer end-to-end delays than PIM-SM, but scales well because it needs no source-specific state. See Bidirectional PIM Internet Standard RFC 5015, 70–73 .

- PIM Source-Specific Multicast (PIM-SSM) builds trees that are rooted in just one source, offering a more secure and scalable model for a limited number of applications (mostly broadcasting of content). In SSM, an IP datagram is transmitted by a source S to an SSM destination address G, and receivers can receive this datagram by subscribing to channel (S,G). See informational RFC 3569

Bidirectional (Bidir) *PIM*

Bidirectional PIM (Bidir-PIM) explicitly builds shared bi-directional trees. It never builds a shortest path tree, so may have longer end-to-end delays than PIM-SM, but scales well because it needs no source-specific state. See Bidirectional PIM Internet Standard RFC 5015, 70–73.

PIM-DM

Protocol-Independent Multicast Dense Mode PIM-DM) uses dense multicast routing. It implicitly builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present. PIM-DM is straightforward to implement but generally has poor scaling properties.

PIM-SM

Protocol-Independent Multicast Sparse Mode (PIM-SM) explicitly builds unidirectional shared trees rooted at a rendezvous point (RP) per group, and optionally creates shortest-path trees per source. PIM-SM generally scales fairly well for wide-area usage.

PING

Packet INternet Groper (PING or Ping)

PIP

Provider Instance Port (PIP)

PIR

Peak Information Rate (PIR) is a burstable rate set on routers and/or switches that allows throughput overhead. Related to committed information rate (CIR) which is a committed rate speed guaranteed/capped.

PMBR

PIM Multicast Border Router (PMBR)

PMTU

Path Maximum Transmission Unit (PMTU)

PNAC

Port Based Network Access Control (PNAC), or 802.1X, authentication requires a client, an authenticator, and an authentication server. The client is a device that wants to connect to the network.

PNP

Provider Network Ports (PNP)

PoE

Power over Ethernet (PoE) is distributing power over an Ethernet network. Because the power and signal are on the same cable, PoE enables remote network devices such as ceiling-mounted access points, surveillance cameras and LED lighting to be installed far away from AC power sources.

PPP

- Point-to-Point Protocol (PPP); The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the data link layer (L2) protocol—for example, Point-to-Point Protocol (PPP) in the case of many dial up or DSL providers or posted in an HTTPS secure web form.

- Protocol Packet Processing (PPP)

PPVID

Port and Protocol *VLAN* ID (PPVID)

PRP

Parallel Redundancy Protocol (PRP) is a network protocol standard for Ethernet that provides seamless failover against failure of any network component. This redundancy is invisible to the application.PRP nodes have two ports and are attached to two separated networks of similar topology. This is in contrast to the companion standard HSR (IEC 62439-3 Clause 5), with which PRP shares the operating principle.

PS

Power Supply

PTP

Precision Timing Protocol

PVID

Port *VLAN* ID (PVID)

PVLAN

Private VLAN (PVLAN); Private VLAN, also known as port isolation, is a technique in computer networking where a VLAN contains switch ports that are restricted such that they can only communicate with a given uplink. The restricted ports are called private ports

PVRST

Per VLAN Rapid Spanning-Tree

PVRSTP

Per VLAN Rapid Spanning-Tree Protocol

PW

An Ethernet pseudowire (PW) is used to carry Ethernet/802.3 Protocol Data Units (PDUs) over an MPLS network. See RFC 4448 for details.

Q-in-Q

802.1Q tunneling (Q-in-Q) is a technique often used by Ethernet providers as a layer 2 VPN for customers. During 802.1Q (or dot1q) tunneling, the provider will put an 802.1Q tag on all the frames that it receives from a customer with a unique VLAN tag. By using a different VLAN tag for each customer we can separate the traffic from different customers and also transparently transfer it throughout the service provider network.

QoS

Quality of Service (QoS) refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. QoS defines the ability to provide different priorities to different applications, users, or data flows or the ability to guarantee a certain level of performance to a data flow.

QRV

Querier's Robustness Variable (QRV).

RADIUS

Remote Authentication Dial-In User Service

RAM

Random-access memory (RAM) is a form of computer memory that can be read and changed in any order, and typically is used to store working data and machine code.

RARP

The Reverse Address Resolution Protocol (RARP) is an obsolete computer communication protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.

RBAC

Role Based Authentication (RBAC)

RED

1) Random early detection (RED) is where a single queue may have several different sets of queue thresholds.

2) Redundant interface (RED) or Red (e.g. RED 1 or RED 2).

RFD

A flapping route is an unstable route that is advertised and withdrawn over and over again. Every time a flap occurs, a BGP UPDATE message is sent. When routers have to process many BGP UPDATE messages, their CPU load increases.
BGP route dampening can be used to prevent installing flapping BGP routes and forwarding them to other BGP routers. This decreases the CPU load of routers and increases network stability. Nowadays, routers are powerful enough to process BGP updates so dampening isn't considered a best practice anymore
RFP has 5 attributes - the default values are shown

- Penalty
- Suppress-Limit - 2000
- Half-Life - 900 secs
- Reuse limit - 750
- Maximum Suppress-Limit -3600 secs (60 min)

When the route exceeds the suppress limit, the route is dampened.Once the route is dampened, the router won't install the route in the routing table nor advertise it to other BGP neighbor.
If for example the penalty is 4000 and the half-life time is 15 minutes. After 15 minutes the penalty will be 2000, after another 15 minutes, the penalty is 1000, and after another 15 minute, the penalty is 500. Once the penalty is below the reuse limit of 750, the route can be used again and

advertised to other BGP routers. When the penalty is below 50% of the reuse limit, the penalty is removed from the route.

The maximum suppress limit ensures that a route won't be dampened forever. The maximum suppress time is 3600 secs or 60 minutes by default.

RFL

Route Reflector Client (RFL); The route reflector allows all IBGP speakers within your autonomous network to learn about the available routes without introducing loops

RIB

Routing Information Base (RIB); Routing and routing functions in enterprise and carrier networks are typically performed by network devices (routers and switches) using an RIB. Protocols and configuration push data into the RIB and the RIB manager installs state into the hardware for packet forwarding.

RIP

RIP (Routing Information Protocol) sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers about the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses a hop count as a way to determine network distance. Each host with a router in the network uses the routing table information to determine the next host to route a packet for a specified destination.

RMON

Remote network monitoring (RMON) is the process of monitoring network traffic on a remote Ethernet segment for detectingnetwork issues such as dropped packets, network collisions, and traffic congestion

RP

Rendezvous point (RP)

RPF

RPF stands for Reverse Path Forwarding. PIM uses reverse-path forwarding (RPF) to prevent multicast routing loops by leveraging the unicast routing table on the virtual router. When the virtual router receives a multicast packet, it looks up the source of the multicast packet in its unicast routing table to see if the outgoing interface associated with that source IP address is the interface on which that packet arrived. If the interfaces match, the virtual router duplicates the packet and forwards it out the interfaces toward the multicast receivers in the group. If the interfaces don't match, the virtual router drops the packet. *This is called a RPF failure.*

RPT

Root Part Tree (RPT)

RRD

Route Redistribution (RRD)

RSVP

Resource Reservation Protocol (RSVP) is a transport layer protocol designed to reserve resources across a network using the integrated services model. RSVP operates over an IPv4 or IPv6 and provides receiver-initiated setup of resource reservations for multicast or unicast data flows.

RS-232

RS-232 is a short range connection between a single host and a single device (such as a PC to a modem) or another host (such as a PC to another PC). The standard uses a single TX line, a single RX line, numerous modem handshaking lines and a ground line with the option of DB9 and DB25 connectors. A minimal 3-wire RS-232 connection consists only the TX, RX, and ground lines, but if flow control is required a minimal 5-wire RS-232 is used adding the RTS and CTS lines. The RS-232 standard has been commonly used in computer serial ports and is still widely used in industrial communication devices.

RS-422

RS-422 was meant as a replacement for RS-232 as it offered much higher speeds, better immunity to noise and allow for longer cable lengths making it better suited to industrial environments. The standard uses the same signals as the RS-232 standard, but used differential twisted pair so requires double the number of wires as RS-232. Connectors are not specified in the standard so block or DB connectors are commonly used. RS-422 cannot implement a true multi-point communications network since there can be only one driver on each pair of wires. However, one driver can fan-out to up to ten receivers.

RS-485

RS-485 standard addresses some short coming of the RS-422 standard. The standard supports inexpensive local networks and multidrop communication links, using the same differential signalling over twisted pairs as RS-422. The main difference being that in RS-485 drivers use three-state logic allowing the individual transmitters to deactivate while not transmitting, while RS-422 the transmitter is always active therefore holding the differential lines. Up to 32 devices can be connected, but with repeaters a network with up to 256 devices can be achieved. RS-485 can be used in a full-duplex 4-wire mode or half-duplex 2-wire mode. With long wires and high baud-rates it is recommended that termination resistors are used at the far ends of the network for signal integrity

RST

RST stands for reset. RST is one of the TCP flags.
TCP flags are various types of flag bits present in the TCP header. Each of them has its own significance. They initiate connections, carry data, and tear down connections. The commonly used TCP flags are SYN, ACK, RST, FIN, URG, PSH.

* SYN (synchronize): Packets that are used to initiate a connection.

* ACK (acknowledgment): Packets that are used to confirm that the data packets have been received, also used to confirm the initiation request and tear down requests.

* RST (reset): Signify the connection is down or maybe the service is not accepting the requests.

* FIN (finish): Indicate that the connection is being torn down. Both the sender and receiver send the FIN packets to gracefully terminate the connection.

* PSH (push): Indicate that the incoming data should be passed on directly to the application instead of getting buffered.

* URG (urgent): Indicate that the data that the packet is carrying should be processed immediately by the TCP stack.

RSTP

Rapid Spanning-Tree Protocol

RT

Route Target (RT) value; RT can be used to share routes among them. We can apply route targets to a VRF to control the import and export of routes among it and other VRFs. When you configure RT import, it imports all prefixes that match the configured RT value as one of the attributes in the BGP update. So in any-any VRF, it is common to see all PE configured with same RT value

RTM

Routing Table Manager (RTM). The RTM is the central repository of routing information for all routing protocols that operate under the routing and remote access service (RRAS). It provides routing information to all interested clients, such as routing protocols, management programs, and monitoring programs. The RTM also determines the best route to each destination network that is known to the routing protocols. The determination of this route is based on routing protocol priorities and on the metrics associated with the routes.

RTS

Request to Send (RTS)/CTS Flow Control is another flow control mechanism that is part of the RS232 standard.

RX

Receive

SA

Security Associations (SA). A SA is a relationship between two or more entities that describes how the entities will utilize security services to communicate securely. In endpoint-to-endpoint Transport Mode, both end points of the IP connection implement IPSec.

SAN

Singly attached nodes (SAN); singly attached nodes don't have the same redundancy as the doubly attached nodes since they still have just one connection that could fail.

SEM

State Event Machines (SEM)

SFP

SFP (Small Form-factor Pluggable) is a small transceiver that plugs into the SFP port of a network switch and connects to fibre channel and gigabit Ethernet (GbE) optical fiber cables at the other end. The SFP converts the serial electrical signals to serial optical signals and vice versa. SFP modules are hot swappable and contain ID and system information for the switch.

SFTP

SSH File Transfer Protocol (SFTP)

SHA

Secure Hash Algorithm is the name of a series of hash algorithms.
A hash function provides encryption using an algorithm and no key. A variable-length plaintext is "hashed" into a (typically) fixed-length hash value (often called a "message digest" or simply a "hash"). Hash functions are primarily used to provide integrity; the hash of a plaintext changes, the plaintext itself has changed.
Common older hash functions include Secure Hash Algorithm 1 (SHA-1), which creates a 160-bit hash and Message Digest 5 (MD5), which creates a 128-bit hash.

SIP

Session Initiation Protocol (SIP) is mostly well known for establishing voice and video calls over the Internet. To initiate such sessions, SIP uses simple request and response messages. For example, the INVITE request message is used to invite a user to begin a session and ACK confirms the user has received the request. The response code 180 (Ringing) means the user is being alerted of the call and 200 (OK) indicates the request was successful. Once a session has been established, BYE is used to end the communication.

SISP

Switch Instance Shared Port (SISP)

SLA

Service-level agreements (SLA).

SLIP

Serial Line Internet Protocol (SLIP); SLIP is the predecessor protocol of Point-to-Point Protocol (PPP). SLIP does not provide authentication, is a static IP addressing assignment, and data is transferred in synchronous form.

SM

State Machine

SNAT

Static Network Address Translation (SAT, SNAT) performs one-to-one translation of internal IP addresses to external ones.

SNMP

Simple Network Management Protocol

SNTP

Simple Network Time Protocol (SNTP)

SPT

Shortest path tree (SPT) is used for multicast transmission of packets with the shortest path from sender to recipients.

SR

State Refresh (SR) message. For a given (S,G) tree, SR messages will be originated by all routers that use an interface directly connected to the source as the RPF interface for the source. Ref: IETF "State Refresh in PIM-DM"

SRM

State Refresh Message (SRM). For a given (S,G) tree, SRM will be originated byall routers that use an interface directly connected to the source as the RPF interface for the source. Ref: IETF "State Refresh in PIM-DM"

SSD

SSD (Solid State Drive) is an all-electronic, non-volatile random access storage drive.

SSH

(Secure SHell) is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs on all platforms. Also serving as a secure client/server connection for applications such as database access and email, SSH supports a variety of authentication methods.

SSL

Secure Sockets Layer

SSM

Source-Specific Multicast (SSM)

SST

Single Spanning Tree (SST); SST is formed in either of the following situations:

- A switch running STP or RSTP belongs to only one spanning tree.
- An MST region has only one switch.

STP

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on bridges and switches. The specification for STP is IEEE 802.1D. The main purpose of STP is provide path redundancy while preventing undesirable loops in the network.

SVL

Shared VLAN Learning (SVL)

S-VLAN

Stacked VLAN (S-VLAN)

TAC

Taxonomy Access Control (TAC) allows the user administrator to control access to nodes indirectly by controlling which roles can access which categories.

TACACS

Terminal Access Controller Access-Control System

TAI

International Atomic Time (TAI); if the port is in the master state, the local clock is synchronized to an external source of time traceable to TAI (International Atomic Time) and UTC (Universal Coordinated Time) such as GPS (Global Positioning System) system.

TB

Token Bucket (TB). The TB algorithm is based on an analogy of a fixed capacity bucket into which tokens, normally representing a unit of bytes or a single packet of predetermined size, are added at a fixed rate. When a packet is to be checked for conformance to the defined limits, the bucket is inspected to see if it contains sufficient tokens at that time. If so, the appropriate number of tokens, e.g. equivalent to the length of the packet in bytes, are removed ("cashed in"), and the packet is passed, e.g., for transmission. The packet does not conform if there are insufficient tokens in the bucket, and the contents of the bucket are not changed.

TC

TC (Topology Change); once the Root Bridge is aware of a change in the topology of the network, it sets the Topology Change (TC) flag on the sent BPDs.

TCN

TCN (Topology Change Notification), a kind of BPDU, is sent by bridges towards the root bridge to notify changes in the topology, such as port up or port down.

TCP

Transmission Control Protocol

TCP-AO

TCP-AO MKT (Transmission Control Protocol Authentication Option). TCP-AO uses cryptographic algorithms to convert MKTs, which can be shared across connections, into unique traffic keys for each connection.

TCP-AO MKT

TCP-AO MKT (Transmission Control Protocol Authentication Option Master Key Tuple). TCP-AO uses cryptographic algorithms to convert MKTs, which can be shared across connections, into unique traffic keys for each connection.

TFTP

Trivial File Transfer Protocol

TLS

Transport Layer Security (TLS), the successor of the now-deprecated Secure Sockets Layer (SSL), is a cryptographic protocol designed to provide communications security over a computer network.

TLV

type, length, and value (TLV) traces

TN

Telnet (TN) is a networking protocol and software program used to access remote computers and terminals over the Internet or a TCP/IP computer network. Upon providing correct login and sign-in credentials, a user may access a remote system's privileged functionality. Telnet sends all messages in clear text and has no specific security mechanisms.

TOS

Type of Service (TOS). IP packets have a field called the Type of Service field (also known as the TOS byte).
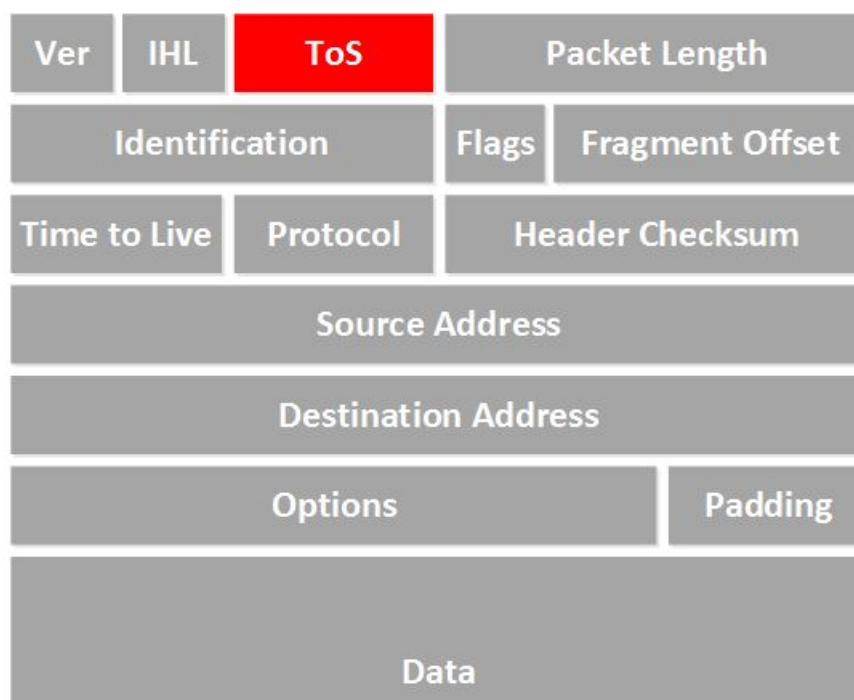
TPID

Tag Protocol Identifier (TPID)

TTL

TTL (time to live). Under IP, TTL is an 8-bit field. In the IPv4 header, TTL is the 9th octet of 20. In the IPv6 header, it is the 8th octet of 40. The maximum TTL value is 255, the maximum value of a single octet. A recommended initial value is 64.

TX

Transmit

UAP

Uplink Access Port (UAP); when a tagged LLDP is enabled, the LLDP packets with destination address as 'nearest bridge address (01-80-c2-00-00-0E)' will be replicated for all S-Channels emulated over that UAP.

UART

UART (Universal Asynchronous Transmitter Receiver) is the most common protocol used for full-duplex serial communication.It is a single LSI (large scale integration) chip designed to perform asynchronous communication. This device sends and receives data from one system to another system.

UDP

User Datagram Protocol

UFD

Uplink failure detection (UFD)

URM

Unified Route Map (URM)

USM

USM stands for User based Security Model; USM (User based Security Model) and VACM (View-based Access Control Model) are the main features added as a part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees.

UTC

Coordinated Universal Time (UTC); If the port is in the master state, the local clock is synchronized to an external source of time traceable to TAI (International Atomic Time) and UTC (Universal Coordinated Time) such as GPS (Global Positioning System) system.

UTP

Unshielded Twisted Pair (UTP) is a pair of wires that are twisted around each other to minimize interference. Ethernet cables are common example of UTP wires.

UUID

A Universally Unique IDentifier (UUID) is a 128-bit domain UUID unique to a MRP domain/ring. All MRP instances belonging to the same ring must have the same domain ID.

VACM

VACM stands for View-based Access Control Model); USM (User based Security Model) and VACM (View-based Access Control Model) are the main features added as a part of the SNMPv3 specification. USM provides both encryption and authentication of the SNMP PDUs, while VACM specifies a mechanism for defining access policies for different users with different MIB trees.

Varbind

A Variable Binding (Varbind) represents a set of Oid/Value pairs. Individual Variable Bindings are stored in the Vb class. Individual Variable Bindings are stored in the Vb class.

Create a variable binding and add the Object identifier in string format:

Vb vb = new Vb("1.3.6.1.2.1.1.1.0")

Create a variable binding and add the Object identifier in Oid format:

Oid oid = new Oid("1.3.6.1.2.1.1.1.0");

Vb vb = new Vb(oid);

VFI

Virtual Forwarding Interface (VFI)

VID

Management VLAN ID (VID)

VINES

Virtual Integrated Network Service (VINES)

VLAN

Virtual Local Area Network (VLAN) is a logical subgroup within a local area network that is created via software rather than manually moving cables in the wiring closet.

VPN

Virtual Private Network (*VPN*)

VRF

Virtual Routing and Forwarding (VRF). In IP-based computer networks, VRF is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. One or more logical or physical interfaces may have a VRF and these VRFs do not share routes; therefore, the packets are only forwarded between interfaces on the same VRF. VRFs are the TCP/IP layer 3 equivalent of a VLAN. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other.

VRRP

VRRP (Virtual Router Redundancy Protocol) is an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the VRRP router(s) on a LAN, allowing several routers on a multi-access link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP setup, one router is elected as the virtual router master, and the other routers are acting as backups in case of the failure of the virtual router master. VRRP is designed to eliminate the single point of failure inherent in the static default routed environment

VSA

Vendor Specific Attribute (VSA)

WAN

A wide area network is a telecommunications network that extends over a large geographic area for the primary purpose of computer networking.

Web UI

Web User Interface (Web UI) is a control panel in a device presented to the user via the Web browser. Network devices such as gateways, routers, and switches typically have such control panel

that is accessed by entering the IP address of the device into a Web browser in a computer on the same local network.

WINS

Windows Internet Naming Service (WINS)

WRED

WRED (Weighted Random Early Detection) is a queueing discipline for a network scheduler suited for congestion avoidance. It is an extension to random early detection (RED) where a single queue may have several different sets of queue thresholds.

WRR

Weighted Round Robin (WRR) is one of the scheduling algorithms used by the device. In WRR, there is a number of queues and to every queue is assigned weight (w). In a classical WRR, the scheduler cycles over the queues, and when a queue with weight w is visited, the scheduler can send consequently a burst of up *to w* packets. This works well for packets with the same size.

XNS

Xerox Network Systems (XNS)

Index