MicroRAPTOR - Quick Start Guide

Intelligent Cyber Secure Platform

iMR320

Version: 1.14.10-2, Date: October 2022

iS5 COMMUNICATIONS
SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

© 2022 iS5 Communications Inc. All rights reserved.

Copyright Notice

© 2022 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 // Fax: 1+ 289-401-5206 Website: http://www.is5com.com/ Technical Support: E-mail: support@is5com.com Sales Contact: E-mail: sales@is5com.com

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 CONSEQUENTIAL 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, NEGLIGENCE, 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 Contract 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 License 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 agreement. 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 Convention for the International Sale of Goods. This EULA shall be governed by the laws of the Province 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 relationship 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 granting such waiver, and (b) shall be effective only in the specific instance and for the specific purpose 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 exercising, 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/

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

MicroRAPTOR - Quick Start Guide i

Copyright Notice ii

End User License Agreement (EULA) iii

iSUPPORT xi

Chapter: 1 **Introduction** 1
Purpose and Scope 1

Chapter: 2 **Console Port: Logging into the MicroRAPTOR** 2

Chapter: 3 **SSH: Logging into the MicroRAPTOR** 10

Chapter: 4 **Command Line: Switch Name** 14

Chapter: 5 **Command Line: Switch Prompt** 15

Chapter: 6 **Command Line: IP Address Configuration** 16

Chapter: 7 **Command Line: Admin Password** 17

Chapter: 8 **Command Line: Save and Restore Configuration** 18

Chapter: 9 **Command Line: Upgrading the MicroRAPTOR using a USB** 19

Chapter: 10 **Command Line: Upgrading the MicroRAPTOR using TFTP** 23

Chapter: 11 Command Line: Upgrading the MicroRAPTOR using SFTP 26

Chapter: 12 Web Interface: Logging into the MicroRAPTOR 28

Chapter: 13 Web Interface: System Settings 33

Chapter: 14 Web Interface: IP Address and Default Routes 34

Chapter: 15 Web Interface: User Password 37

Chapter: 16 Web Interface: Save and Restore Configurations 38

Chapter: 17 Web Interface: Upgrade the MicroRAPTOR using USB 42

Chapter: 18 Web Interface: Upgrade the MicroRAPTOR using TFTP 45

Chapter: 19 Web Interface: Upgrade the MicroRAPTOR using SFTP 48

Index i

1. Introduction

The Quick Start Guide provides instruction for first time users on how to login to the MicroRAPTOR through the *WebUI*, Console or *SSH* interfaces, how to backup and restore configurations, and how to upgrade the device.

This document explains how to use Command Line Interface (*CLI*) interface and Web user interface (*WebUI*) to perform the following tasks:

- Login to the MicroRAPTOR
- Create an *IP* address for *VLAN* #1
- Set password, switch name, banner name, and prompt
- Save configuration
- Restore configuration
- Upgrade the MicroRAPTOR

1.1. Purpose and Scope

This document covers the startup procedures and specifies the basic configuration commands. For more information or support, email support@is5com.com.

This document has been validated against the following product.

Product	Firmware Version
iMR320	1.14.10-2

2. Console Port: Logging into the MicroRAPTOR

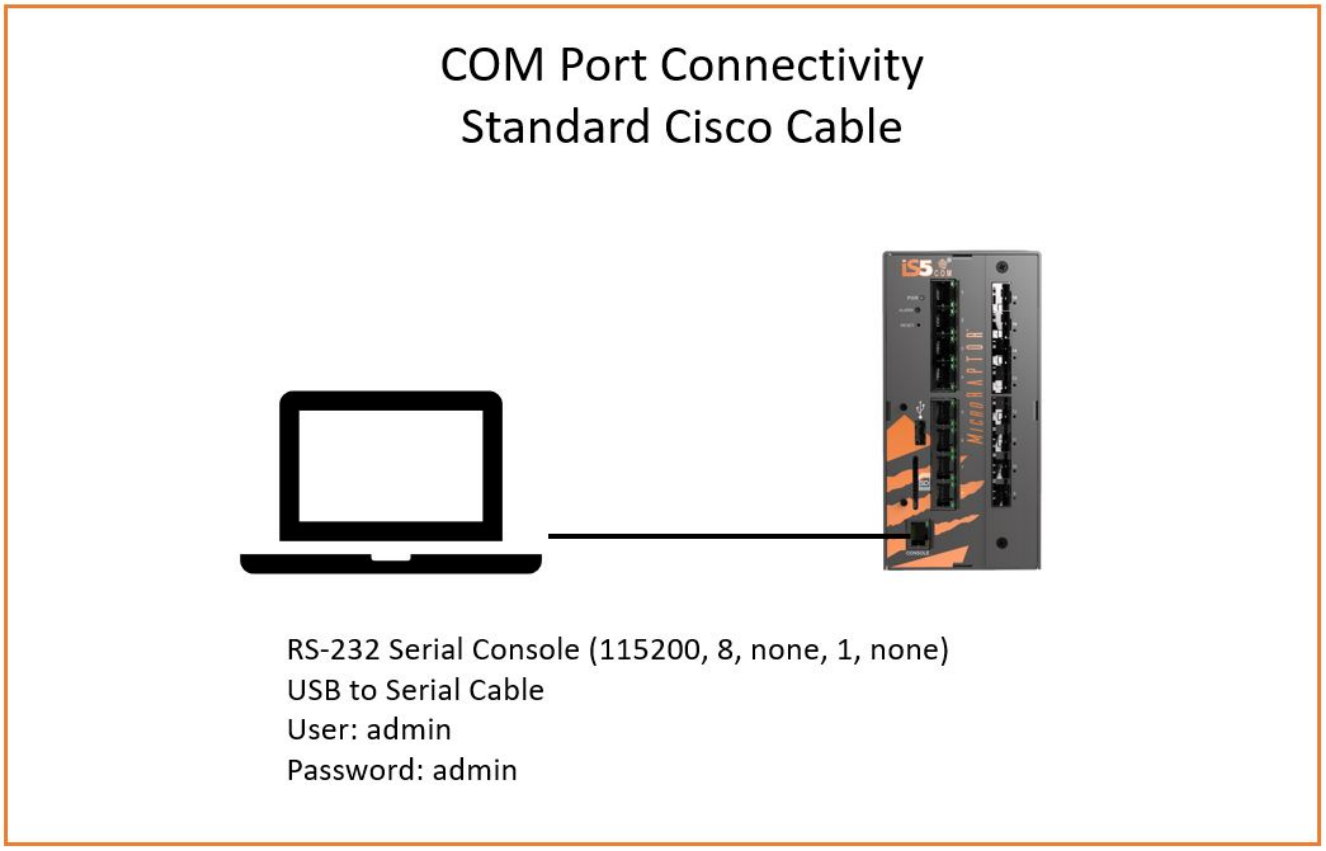
The following sections describe how the serial console interface on the MicroRAPTOR is used to configure an *IP* Address, save a configuration, and upgrade the firmware.

1. On a laptop, install a terminal emulator. A popular option is Putty.
   a. A link to download Putty is: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

MicroRAPTOR

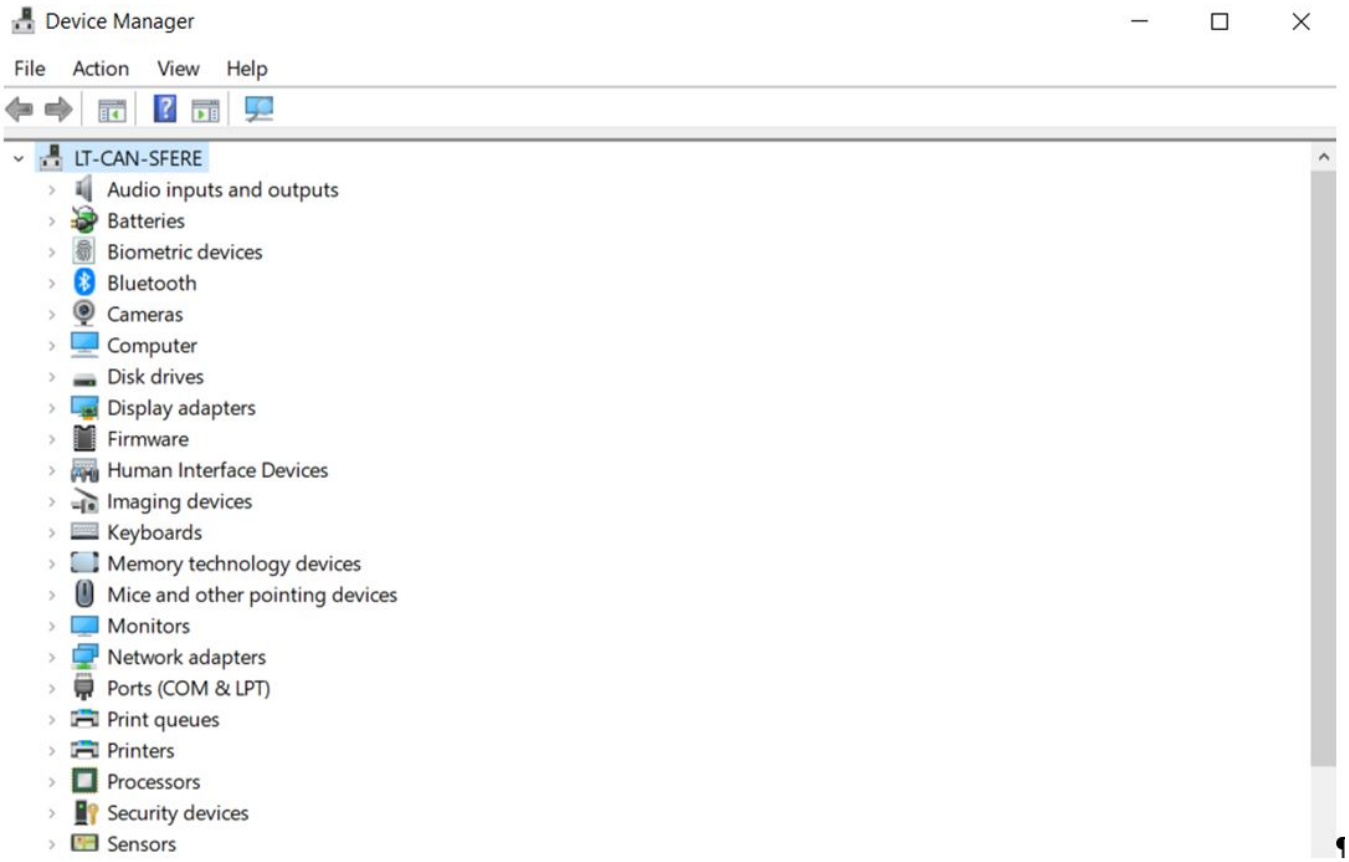
NOTE: The connection details and the Console ports are shown below. A Cisco Console cable is used to connect between the PC and the

console port.



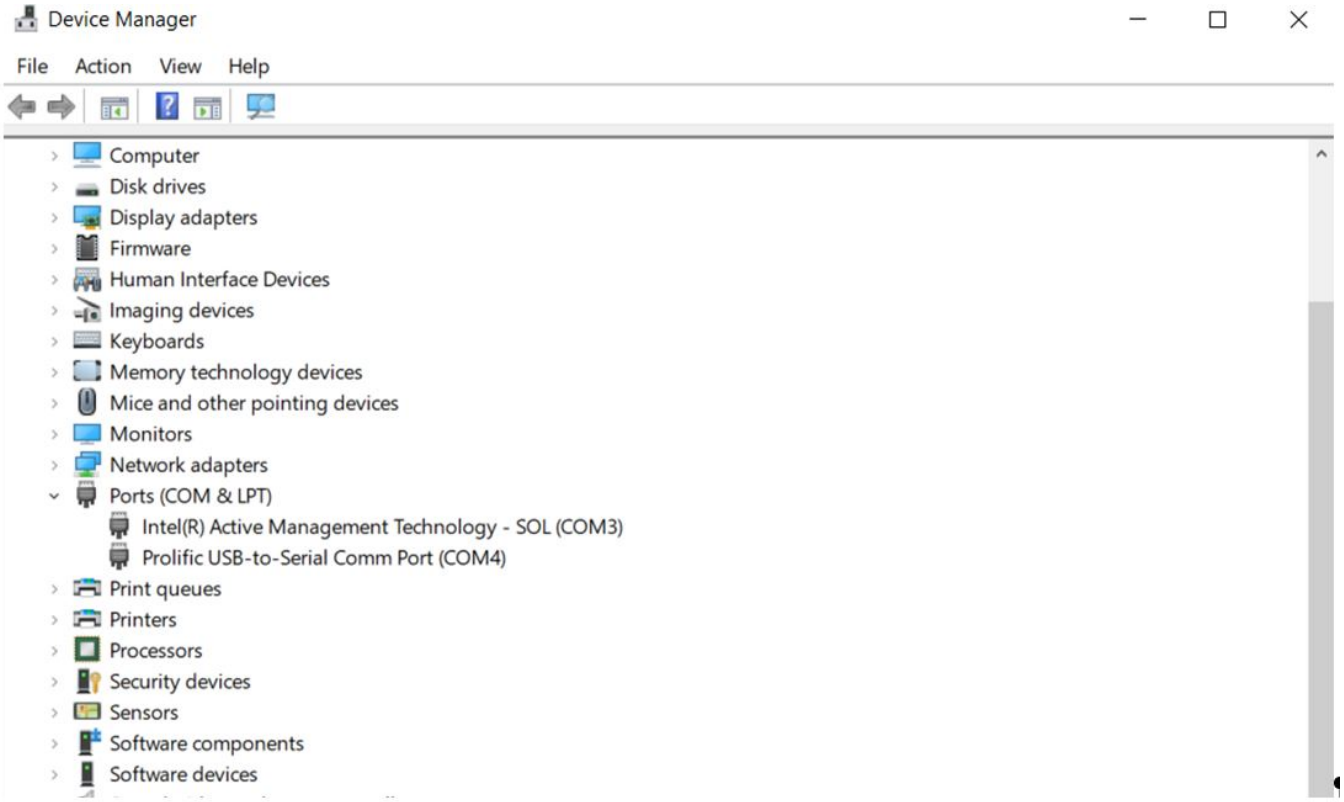
2. Form a serial connection from your computer to the console port of the MicroRAPTOR, by attaching the console port to the USB port of your laptop or PC and the RJ45 termination to the console port on the MicroRAPTOR.
3. To determine the communications port being used on your computer, open **Device Manager** on your PC or laptop.
   a. Open **Device Manager.**

      RESULT: The Device Manager window appears.



b. Navigate to **Ports** to determine which COM number the serial connection is using. You may have to unplug and reinsert the USB connection on your PC to make a determination of which COM number has been assigned to your serial connection.

RESULT: When the Ports leaf is exanded it will appear similar to the image below.



4. Putty can be configured by selecting the type of connection, entering the port number, and setting the baud rate.
   a. Additional serial parameters can be configured in Putty by selecting the **Serial** category found at the bottom of the **Category** panel.

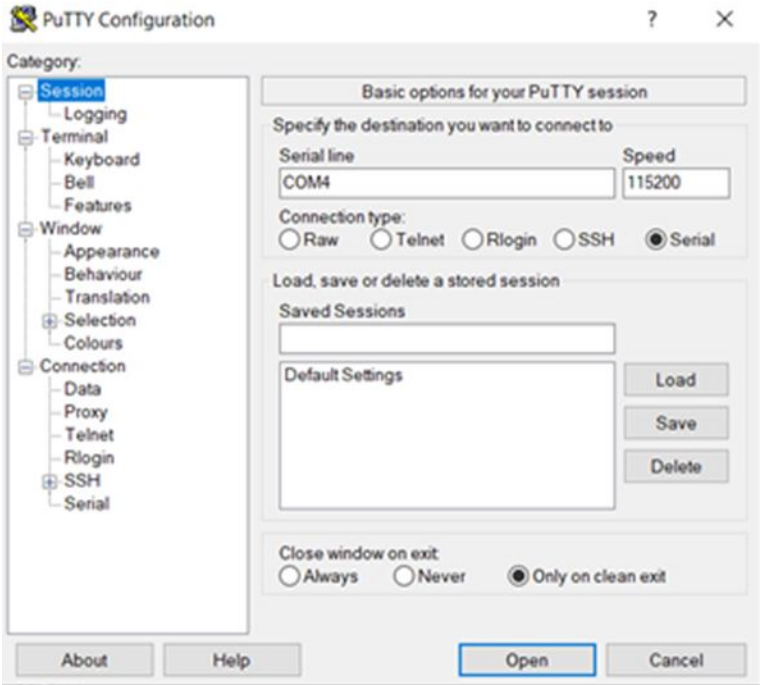
NOTE: *The serial port configuration is as follows:*

- Baud rate: 115200
- Data: 8
- Parity: none
- Stop: 1

- Flow Control: none

b. You should confirm in Putty's user interface that it has been configured with the appropriate Baud rate, Data, Parity, stop and flow control values.

STEP RESULT: The following image provides an image of the port and baud rate being set.

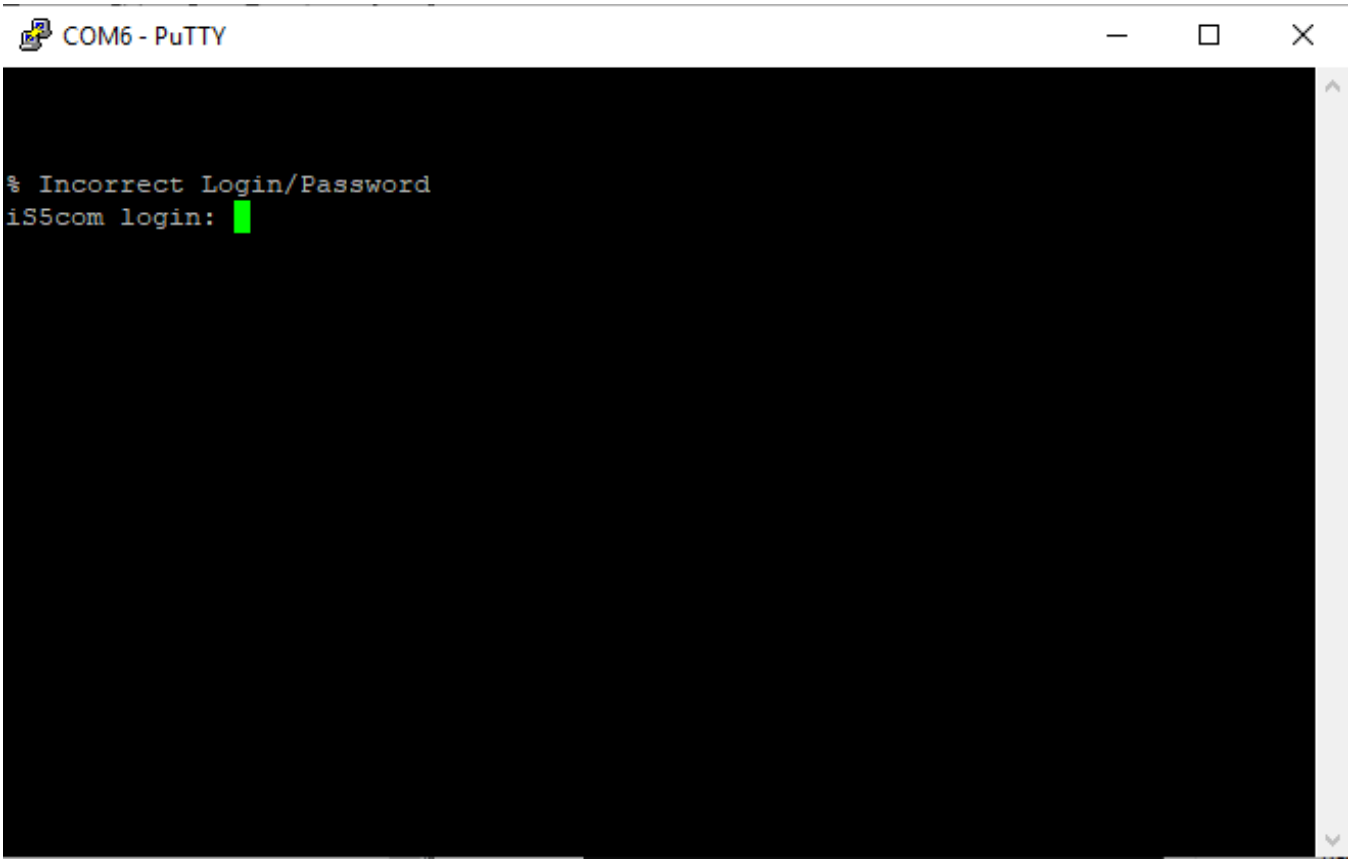


5. Click **Open** to launch a terminal.

   STEP RESULT: A blank terminal window will appear.

6. Press **Enter.**

   STEP RESULT: The login prompt will apear.



7. To access the command line interface *CLI* shell, at the MicroRAPTOR login prompt, use the user name **admin** and password **admin**.

   STEP RESULT: If this is the first login to the device, then you will be prompted to change the password.

   ```
   % Password must be reset. Please change the password
   Enter old password:
   ```

8. Enter the old password which is **admin**.

   STEP RESULT: You will now be prompted for a new password.

   ```
   Enter new password:
   ```

NOTE: The new password must meet the following criteria:

```
Password length should be in the range of 8 - 20 !! characters
Password should contain at least 1 lowercase characters !!
Password should contain at least 1 uppercase characters !!
Password should contain at least 1 numerical characters !!
Password should contain at least 1 special characters !!
New Password must be different from previous password
```

9. Enter the new password.

   STEP RESULT: You will be prompted to confirm the new password.

   ```
   Re-enter new password:
   ```

10. Re-enter the new password.

    STEP RESULT: The console prompt will appear.

    ```
    iS5comm#
    ```

RESULT:

You have logged into the MicroRAPTOR via the console port.

3. SSH: Logging into the MicroRAPTOR

This section describes how an *SSH* session can be established between a laptop and the MicroRAPTOR.

CONTEXT:

MicroRAPTOR can be configured through an *SSH*

Interface from a terminal emulator such as Putty. The command line interface allows the user to control various parameters at the system and protocol level.

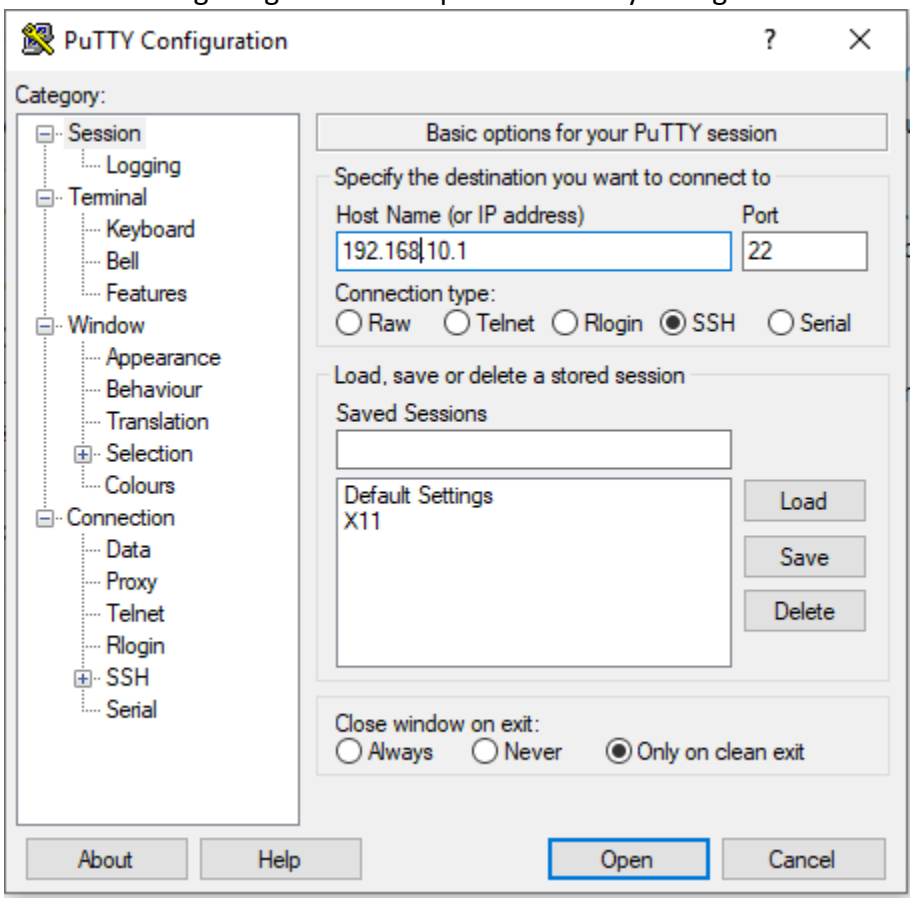
Before configuring the MicroRAPTOR from a PC, confirm accessibility of MicroRAPTOR's firmware by pinging it from the PC.

1. On a laptop, install a terminal emulator. A popular option is Putty.
   a. A link to download Putty is: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. An Ethernet cable must connect the MicroRAPTOR's switch ports and a computer. The computer interface should be assigned an *IP* address on the 192.168.10.0/24 network.

   FOR EXAMPLE: An address of 192.168.10.100 with a subnet mask of 255.255.255.0 is one such suitable combination of an *IP* address and submask to be assigned for the computer to be used in the connection.

3. Open Putty, select the connection type of *SSH*, and provide the default *IP* address of the MicroRAPTOR of 192.168.10.1. Then, click **Open.**

FOR EXAMPLE: The following image is an example of the Putty configuration screen.



STEP RESULT: A login prompt will appear on a terminal screen after **Open** is pressed.

4. To access the command line interface *CLI* shell, at the login prompt, use the user name **admin** and password **admin**.

   STEP RESULT: If this is the first login to the device, you will be prompted to change the password.

   ```
   % Password must be reset. Please change the password
   Enter old password:
   ```

5. Enter the old password which is **admin**.

   STEP RESULT: You will now be prompted for a new password.

   ```
   Enter new password:
   ```

NOTE: The new password must meet the following criteria:

```
Password length should be in the range of 8 - 20 !! characters
Password should contain at least 1 lowercase characters !!
Password should contain at least 1 uppercase characters !!
Password should contain at least 1 numerical characters !!
Password should contain at least 1 special characters !!
New Password must be different from previous password
```

6. Enter the new password.

   STEP RESULT: You will be prompted to confirm the new password.

   ```
   Re-enter new password:
   ```

7. Re-enter the new password.

   STEP RESULT: The console prompt will appear.

   `iS5comm#`

RESULT:

You have logged into the MicroRAPTOR via a *SSH* connection.

4. Command Line: Switch Name

This section will document how to configure the MicroRAPTOR's name.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the console cable or through *SSH*.

1. Configure the switch name.

   FOR EXAMPLE: At the command prompt type:

   ```
   iS5comm# configure terminal
   iS5comm(config)# set switch-name XYZ
   iS5comm(config)# exit
   ```

   STEP RESULT: The switch name has been changed to **XYZ**

5. Command Line: Switch Prompt

This section will document how to change the command line prompt.

PREREQUISITE:

In order to perform the tasks in this section you will have already logged into the MicroRAPTOR via the console cable or through *SSH*.

1. Configure the switch prompt.

   FOR EXAMPLE: At the command prompt type:

   ```
   iS5comm# configure terminal
   iS5comm(config)# set prompt-name Prompt-XYZ
   Prompt-XYZ(config)# exit
   ```

   STEP RESULT: The command line prompt has been changed to **Prompt-XYZ**

6. Command Line: IP Address Configuration

This section will document the configuration of an IP Address and a default route.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the console cable or through *SSH*.

Speak with your Network Administrator to determine the values of the following parameters:

- IP Address
- IP Address Mask
- Default Route

These values will be needed to configure the MicroRAPTOR.

1. Configure the IP Address.

   FOR EXAMPLE: At the command prompt type:

   ```
   iS5comm# configure terminal
   iS5comm(config)# interface vlan 1
   iS5comm(config-if)# ip address <IP Address> <IP Address Mask>
   iS5comm(config-if)# no shutdown
   iS5comm(config-if)# exit
   iS5comm(config)# exit
   ```

   STEP RESULT: The IP Address for the MicroRAPTOR has been set.

2. Configure the default route.

   FOR EXAMPLE: At the command prompt type:

   ```
   iS5comm# configure terminal
   iS5comm(config)# ip route 0.0.0.0 0.0.0.0 192.168.32.254
   iS5comm(config)# exit
   ```

   STEP RESULT: The default route has been set to **192.168.32.254**.

7. Command Line: Admin Password

This section will document how to set the administrator password.

PREREQUISITE:

In order to perform the tasks in this section you will have already logged into the MicroRAPTOR via the console cable or through *SSH*.

1. Configure the administrator password.

   FOR EXAMPLE: At the command prompt type:

   ```
   iS5comm# configure terminal
   iS5comm(config)# username admin password Abcd123! privilege 15
   confirm-password Abcd123!
   iS5comm(config)# exit
   ```

   STEP RESULT: The password has been changed to **Abcd123!**

   NOTE: The password by default must consist of a minimum of 8 characters. The characters must consist of a minimum of 1 lowercase, 1 uppercase, 1 number and 1 special character

   !@#$%^&*()_+-:”;’{}[]|\~

   NOTE: Password complexity rules may be changed by the administrator using the system commands.

8. Command Line: Save and Restore Configuration

This section will document how to save and restore the MicroRAPTOR configuration.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the console cable or through *SSH*.

1. Save the running configuration to flash memory.

   FOR EXAMPLE: At the command prompt type:

   ```
   iS5comm# write startup-config
   ```

   STEP RESULT: The following will appear on the terminal when logged in via the console port.

   ```
   Building configuration ...
   [OK]
   ```

   The prompt will reappear and the configuration will now be saved in flash memory.

2. Optionally, you could save the configuration to USB. Insert a USB drive into the MicroRAPTOR and type the following:

   FOR EXAMPLE: iS5comm# copy startup-config usb

   STEP RESULT: The following text will appear followed by a prompt:

   ```
   Configuration is copied to USB
   ```

3. Optionally, you could restore a configuration that was saved to a USB.

   a. Insert the USB thumb drive into the MicroRAPTOR and type the following:

      FOR EXAMPLE: *iS5comm#* copy usb startup-config

      RESULT: The following text will appear followed by a prompt:

      Configuration is restored from USB

      File Copied Successfully

   b. For the configuration to be applied, the MicroRAPTOR needs to be reloaded.

      FOR EXAMPLE: *iS5comm#* reload

      RESULT: Are you sure you want to reload the device? (Y/N) [N]?

   c. Confirm that you would like to reload the device by typing **Y**.

      RESULT: The *MicroRAPTOR* will be reloaded.

   STEP RESULT: The MicroRAPTOR will be reloaded with the configuration that was restored from the USB.

9. Command Line: Upgrading the MicroRAPTOR using a USB

This section will document how to upgrade the firmware on the MicroRAPTOR. This process takes approximately 5 minutes to execute.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via an *SSH* connection or through the console port. For all upgrades it is recommended that user's backup their current running configuration prior to commencing the upgrade process.

Valid Upgrade Paths

If the release that your device is running is not listed in the Supported Upgrade Paths table, it is recommended that the support team is contacted for more detailed instructions.

1. Optionally, you may choose to upgrade the MicroRAPTOR firmware.
   a. Rename the upgrade software file to “firmware-upgrade.tgz” and copy the file to the USB stick.
   b. Insert USB stick into front panel USB connector.
   c. Type the following:

      FOR EXAMPLE: *iS5comm#* firmware upgrade usb firmware_upgrade.tgz

   STEP RESULT: The upgrade process will begin, text similar the following will begin scrolling on the

terminal:

```
USB device access:  /dev/sdb1
Copying firmware upgrade package ...
'/mnt/usb/firmware_upgrade.tgz' -> '/mnt/shared/firmware_upgrade.tgz'
Firmware upgrade package is copied successfully
Software upgrade ................... Started
######## Raptor firmware upgrade  ########
Raptor boot status: secondary
Firmware revision       :
1.3.04.125-2020.05.07_is5
BSP=00.00.001-2018.05.10
FPGA=3.20
DRAGONITE=2.11
IBIOME=1.3.04
FACTORY=IS5
PRODUCT=iMX
hgid=2bed6e3e4469
Disable SWITCH
Extraction upgrade package ..... DONE
Upgrade package revision:
1.3.04.125-2020.05.07_is5
BSP=00.00.001-2018.05.10
FPGA=3.20
DRAGONITE=2.11
IBIOME=1.3.04
FACTORY=IS5
PRODUCT=iMX
hgid=2bed6e3e4469
Verification upgrade package ... DONE
Verification upgrade package for compatibility ... Upgrading primary instance
BSP FIT upgrade ................ DONE
FPGA upgrade ................... DONE
Application partition upgrade .. DONE
Copy initcfg.txt to config part. DONE
##########################################
Upgrade primary instance is successful
##########################################
##########################################
Switch partition ............... DONE
##########################################
Software upgrade ................... Completed
Device is going to reboot ......
```

2. Allow the MicroRAPTOR to reboot, the U-Boot menu will appear. Do not interact with it.

   STEP RESULT: Do not interact with this menu and the boot process will proceed automatically.

```
*** U-Boot Boot Menu ***

   Continue to boot
   Reset
   Restore to factory Default and boot
   Restore Users only to factory Default and boot
   Recovery boot
   Disable watchdog
   Enable watchdog
   Disable silent boot

Hit any key to stop autoboot:  7
Press UP/DOWN to move, ENTER to select
```

   The clock will expire and the upgrade will proceed without user intervention.

   The upgrade process will terminate at a user prompt.

```
                RAPTOR iBiome OS
MSR: Jun  3 00:08:54 2020 Restoration successfully completed
iS5com login:
```

3.

RESULT:

The MicroRAPTOR has been upgraded and users may now login to it.

10. Command Line: Upgrading the MicroRAPTOR using TFTP

This section will document how to upgrade the firmware on the MicroRAPTOR. This process takes approximately 5 minutes to execute.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via an *SSH* connection or through the console port. For all upgrades it is recommended that user's backup their current running configuration prior to commencing the upgrade process.

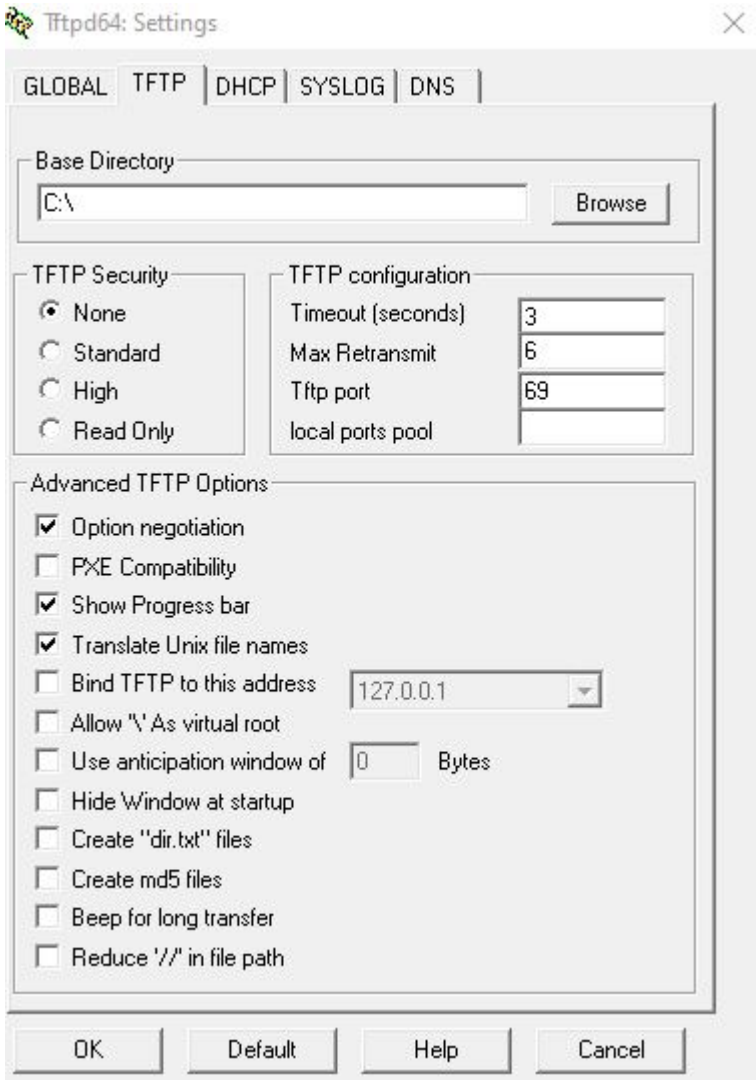
A TFTP server must be installed on a device with network connectivity to the MicroRAPTOR. There are a number of commercial and free TFTP server options available. For this example Tftpd64 was used as the server. It may be downloaded from this site: https://pjo2.github.io/tftpd64/

Valid Upgrade Paths

If the release that your device is running is not listed in the Supported Upgrade Paths table, it is recommended that the support team is contacted for more detailed instructions.

1. Install the TFTP server on a machine that has network connectivity to the MicroRAPTOR.
2. Configure the TFTP server such that its base directory contains the firmware file you wish to upload. Depending on the server software you are using there may be more settings that need to be configured.

   FOR EXAMPLE: This is a screen shot of theTftpd64 settings screen.



3. Optionally, you may choose to upgrade the MicroRAPTOR firmware.
   a. Copy the upgrade software file to the base directory on your TFTP server.
   b. Login to the MicroRAPTOR.
   c. Type the following, you will have to change the IP address and filename for your particular needs.:

      FOR EXAMPLE: *iS5comm#* firmware upgrade tftp://192.168.0.7/firmware_upgrade.tgz

   STEP RESULT: The upload process will begin and progress will be shown on the terminal.

   The upgrade will begin once the download is complete.

4. The MicroRAPTOR will reboot as part of the upgrade process.

   STEP RESULT: The upgrade process will terminate at a user prompt.

```
                 RAPTOR iBiome OS
MSR: Jun  3 00:08:54 2020 Restoration successfully completed
iS5com login:
```

5.

RESULT:

The MicroRAPTOR has been upgraded and users may now login to it.

11. Command Line: Upgrading the MicroRAPTOR using SFTP

This section will document how to upgrade the firmware on the MicroRAPTOR. This process takes approximately 5 minutes to execute.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via an *SSH* connection or through the console port. For all upgrades it is recommended that user's backup their current running configuration prior to commencing the upgrade process.

A SFTP server must be installed on a device with network connectivity to the MicroRAPTOR. There are a number of commercial and free SFTP server options available. For this example the Rebex Tiny SFTP Server was used as the server. It may be downloaded from this site:
https://www.rebex.net/tiny-sftp-server/

Valid Upgrade Paths

If the release that your device is running is not listed in the Supported Upgrade Paths table, it is recommended that the support team is contacted for more detailed instructions.

1. Install the SFTP server on a machine that has network connectivity to the MicroRAPTOR.
2. Configure the SFTP server such that its base directory contains the firmware file you wish to upload. Depending on the server software you are using there may be more settings that need to be configured. The Rebex SFTP server uses a configuration file, RebexTinySftpServer.exe.config, which the user must modify. Please note that the free Rebex is not full featured and the professional option may be more suitable for a commercial deployment. The link is here:
   https://www.rebex.net/tiny-sftp-server/
3. Optionally, you may choose to upgrade the MicroRAPTOR firmware.
   a. Copy the upgrade software file to the base directory on your TFTP server.
   b. Login to the MicroRAPTOR.
   c. Type the following, you will have to change the IP address and filename for your particular needs.:

      FOR EXAMPLE: *iS5comm#* firmware upgrade sftp://tester:password@192.168.0.7//firmware_upgrade.tgz

   STEP RESULT: The upload process will begin and progress will be shown on the terminal.

   The upgrade will begin once the download is complete.

4. The MicroRAPTOR will reboot as part of the upgrade process.

   STEP RESULT: The upgrade process will terminate at a user prompt.

```
                RAPTOR iBiome OS
MSR: Jun  3 00:08:54 2020 Restoration successfully completed
iS5com login:
```

5.

RESULT:

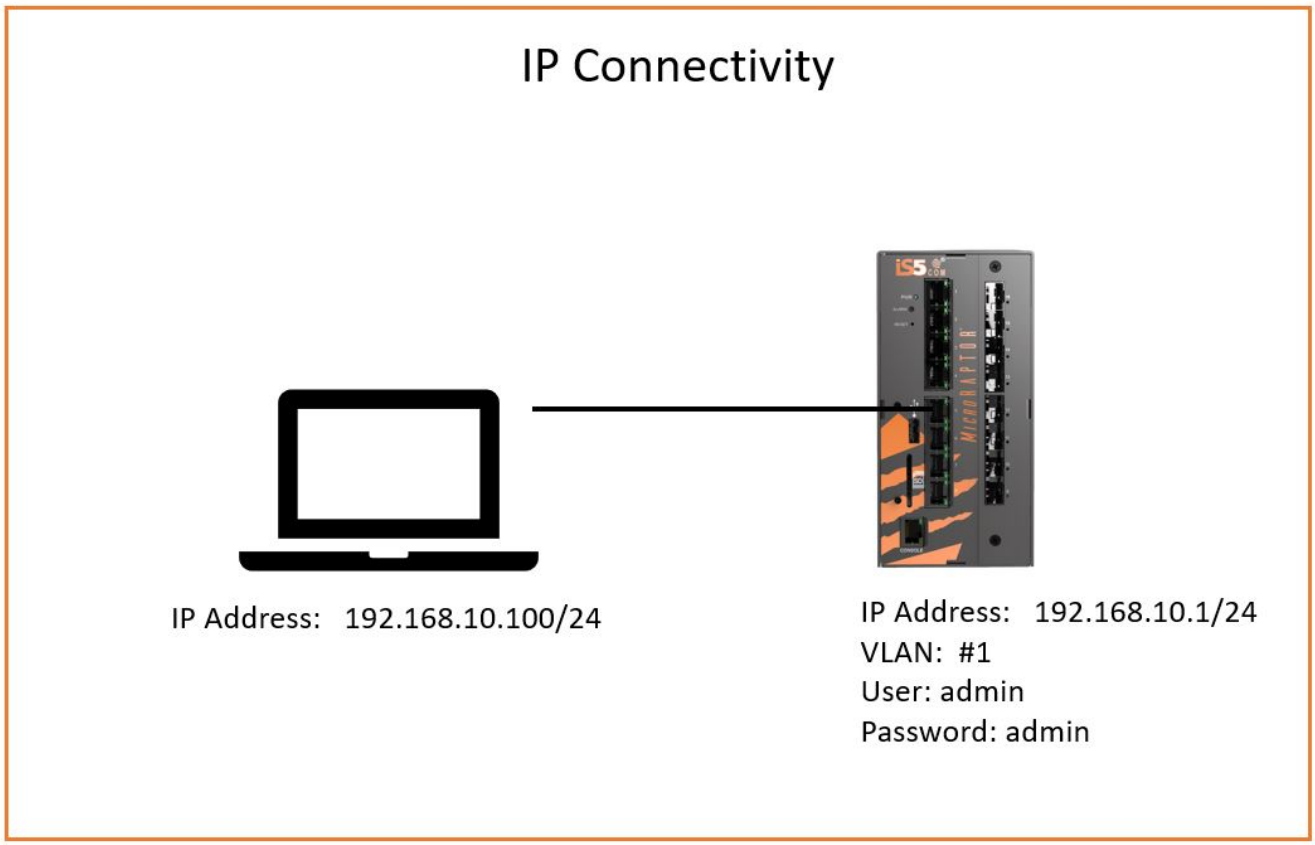
The MicroRAPTOR has been upgraded and users may now login to it.

12. Web Interface: Logging into the MicroRAPTOR

This section describes how to login to the MicroRAPTOR via the *Web UI* (Web User Interface).

PREREQUISITE:

Figure 1: Ethernet / IP Connectivity



CONTEXT:

MicroRAPTOR can be configured through Web User Interface (*Web UI*) from web browsers. The *Web UI* allows the user to control various parameters at the System and Protocol level.

Before configuring the Raptor from a PC, confirm accessibility of MicroRAPTOR's firmware by pinging it from the PC.

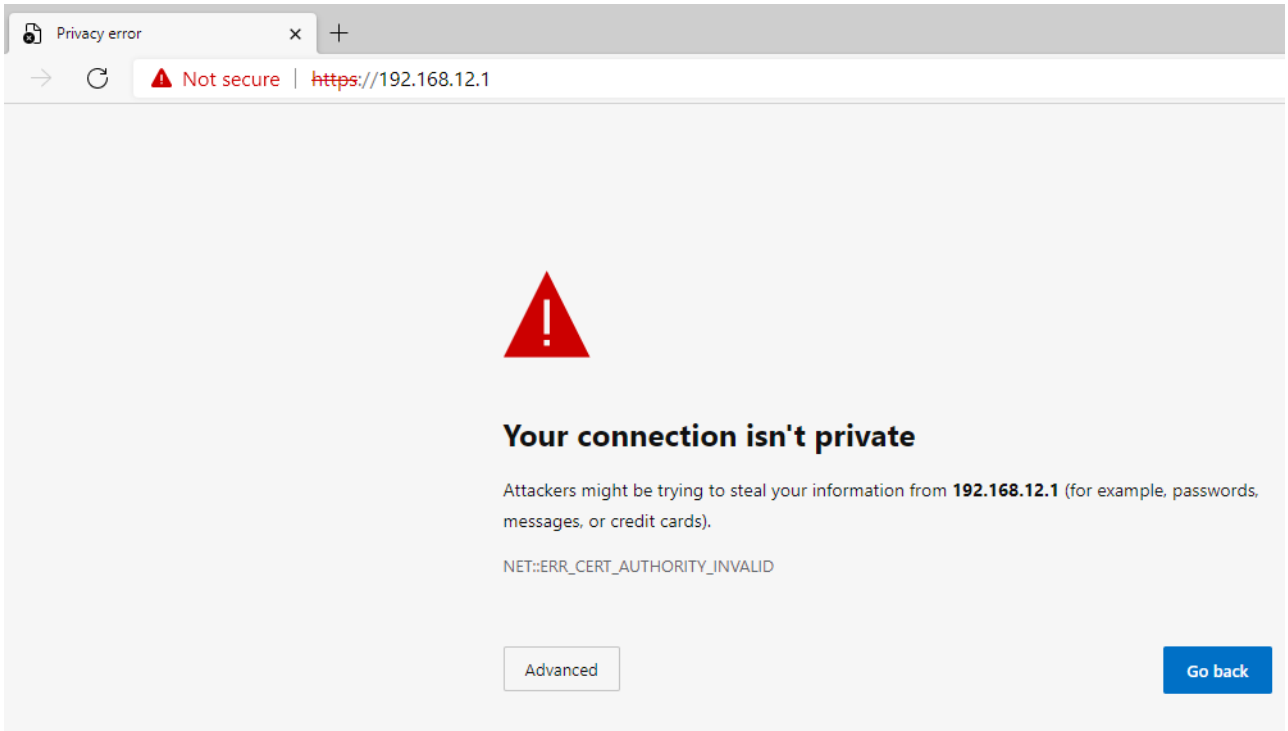
1. An Ethernet cable must connect the switch and a computer. The computer interface should be assigned an IP address on the 192.168.10.0/24 network. This is summarized in *Figure 1*.

   FOR EXAMPLE: An address of 192.168.10.100 with a subnet mask of 255.255.255.0 is one such suitable combination of an IP address and submask to be assigned for the computer to be used in the connection.

2. Launch a web browser to enter the MicroRAPTOR's default IP address. The IP address of the MicroRAPTOR's interface is 192.168.10.1. The https protocol is now the default protocol.

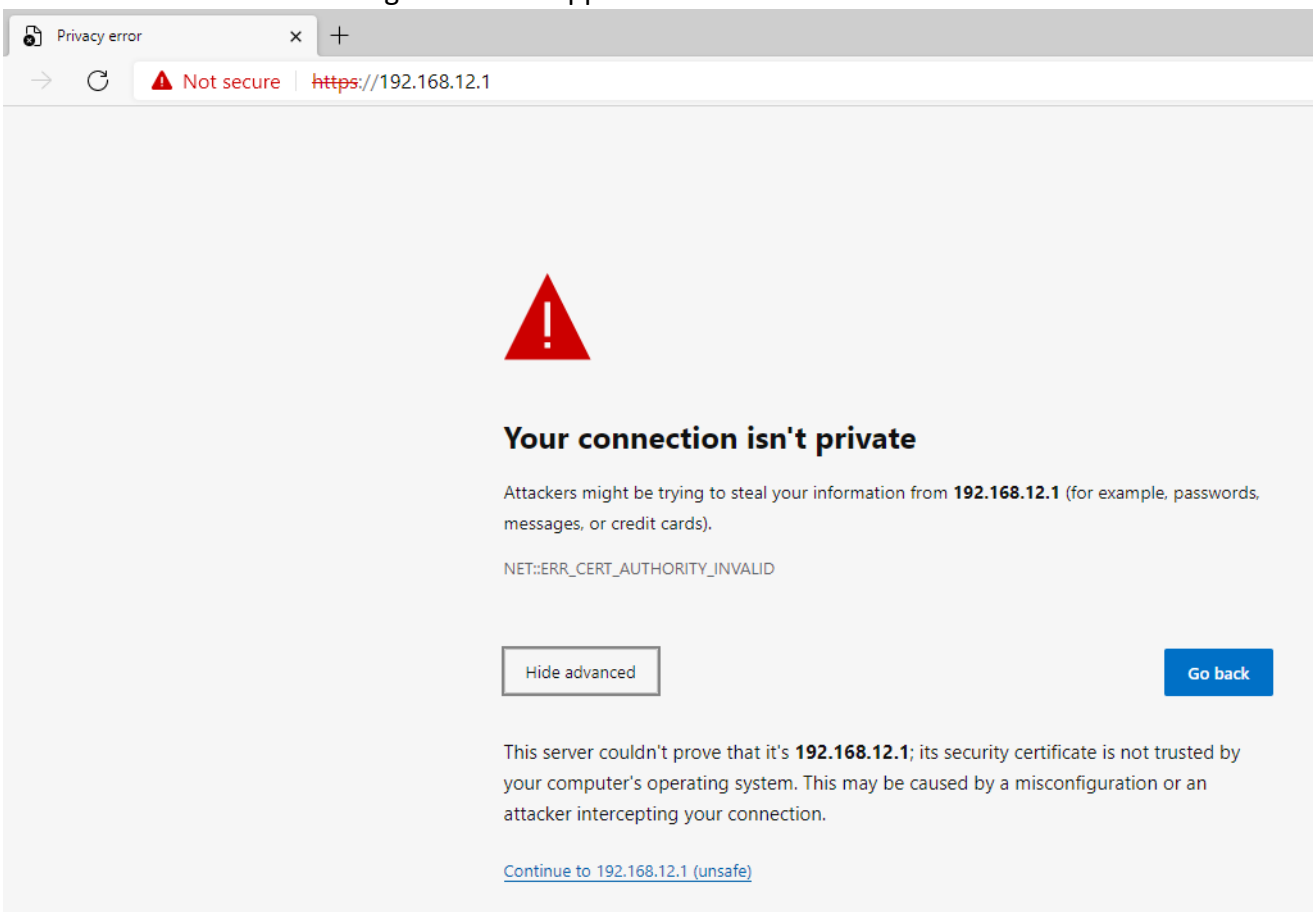
   FOR EXAMPLE: https://192.168.0.1

   STEP RESULT: Warnings from the browser about the web site having an invalid certificate may appear. On the Edge Browser, the following will appear. If the warnings do not appear, skip ahead to Step *4*.



3. Click the **Advanced** button.

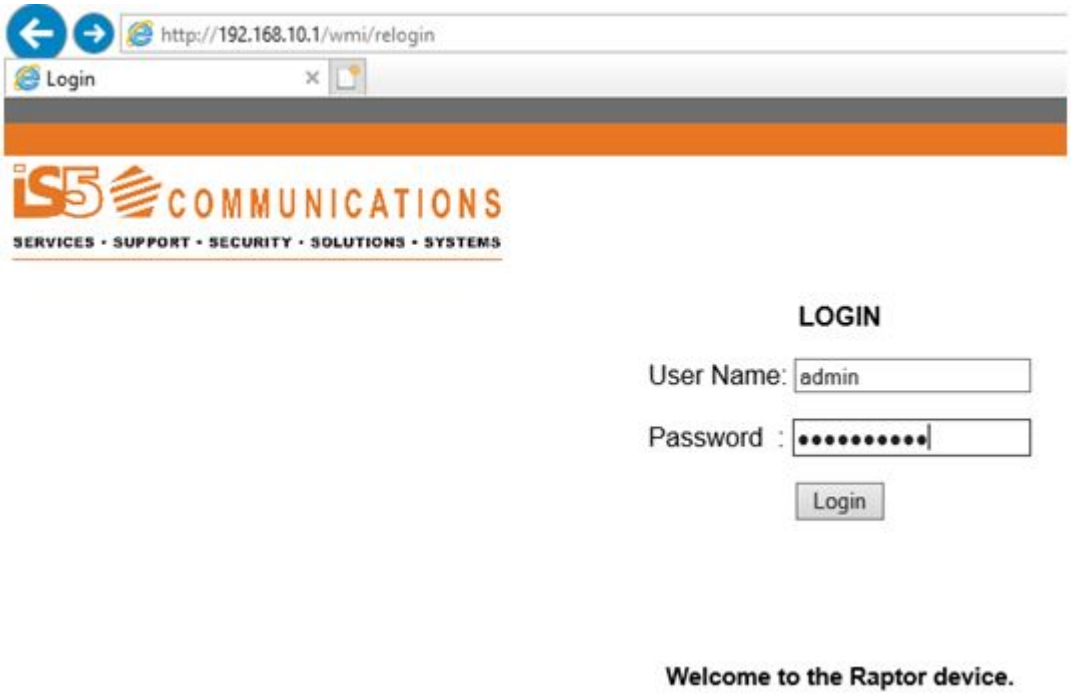
   STEP RESULT: The following screen will appear.



4. Launch a web browser to enter the MicroRAPTOR's default IP address. The IP address of the MicroRAPTOR's interface is 192.168.10.1. Enter **https**://192.168.10.1 into the browser's address bar.

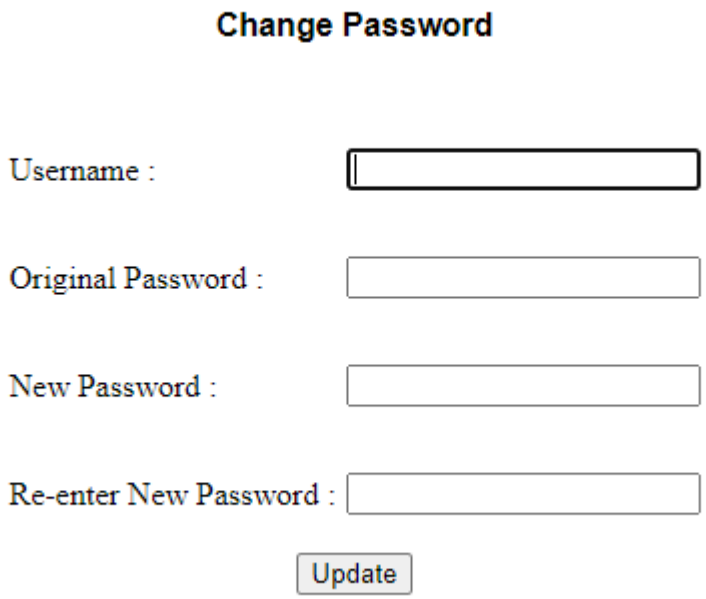
   STEP RESULT: The **Login** page appears.

Figure 2: Login Page



5. Enter the **User Name** “admin” and **Password** “admin” and click **Login.**

   STEP RESULT: If this is the first login to the device the user will be prompted to change the password.



NOTE: The new password must meet the following criteria:

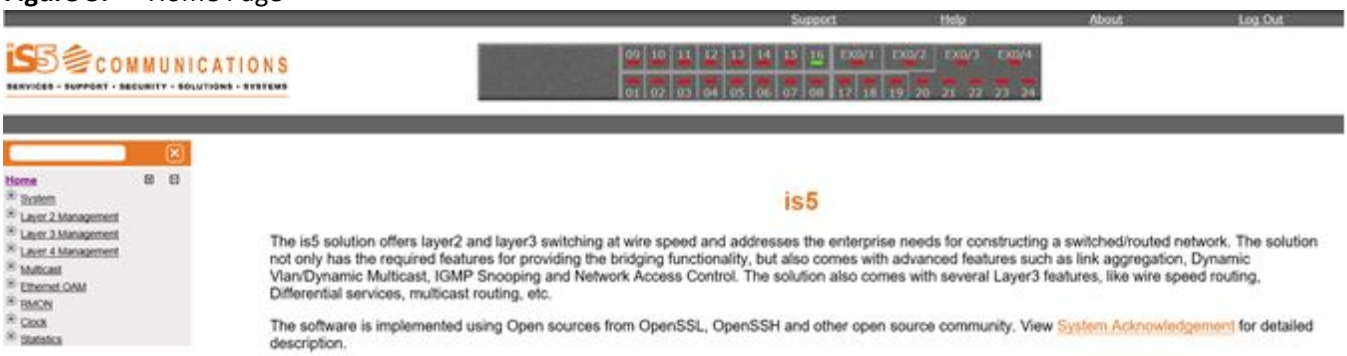
```
Password length should be in the range of 8 - 20 !! characters
Password should contain at least 1 lowercase characters !!
Password should contain at least 1 uppercase characters !!
```

```
Password should contain at least 1 numerical characters !!
Password should contain at least 1 special characters !!
New Password must be different from previous password
```

6. Enter the **User Name** “admin” and **Password** “admin” and then a new password in the **New Password** and **Re-enter New Password** fields. Then click **Update.**

   STEP RESULT: The home page will appear.

Figure 3: Home Page



RESULT:

You have logged into the MicroRAPTOR via the *Web UI*.

13. Web Interface: System Settings

This section will document how to configure common MicroRAPTOR system settings.

PREREQUISITE:

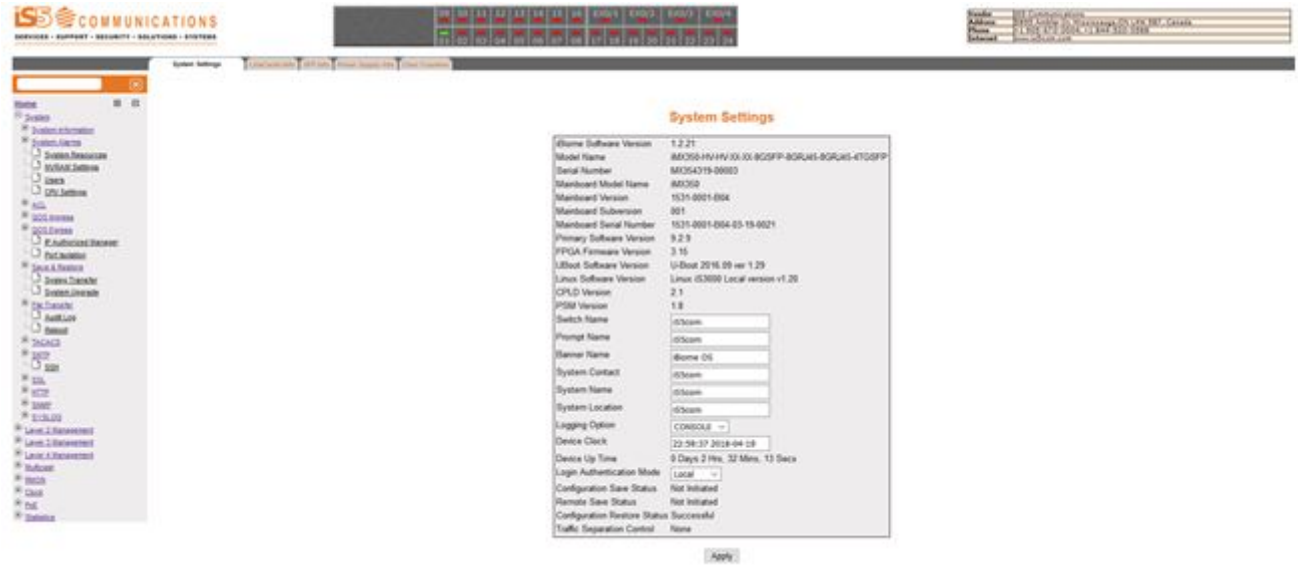
To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the *Web UI*.

1. Navigate to the **System Settings** page.

   FOR EXAMPLE: In the Home page, go to **System > System Information > System Settings**

   STEP RESULT: The following screen will appear.

Figure 1: System Settings



2. At this point you may change the values of any of the following fields.
   - **Switch Name**—enter the name for identifying the device. The default value is iS5. This value range is a string of size 15.
   - **Prompt Name**—enter the prompt name to be used. The default value is iS5.
   - **Banner Name**—enter the banner name to be used. The default value is MicroRAPTOR iBiome OS.
   - **System Contact**—enter the contact person details for this managed node. This value range is a string of size 50. The default value is iS5com.
   - **System Name**—enter the system name. The default value is iS5com.
   - **System Location**—enter the physical location of this node. This value range is a string of size 50. The default value is iS5com.

3. Click **Apply** to make your changes effective.

RESULT:

The system settings have been changed.

14. Web Interface: IP Address and Default Routes

This section will explain how to set the IP Address on the MicroRAPTOR and create a default route.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the *Web UI*.

Speak with your Network Administrator to determine the values of the following parameters:

- IP Address
- IP Address Mask
- Default Route

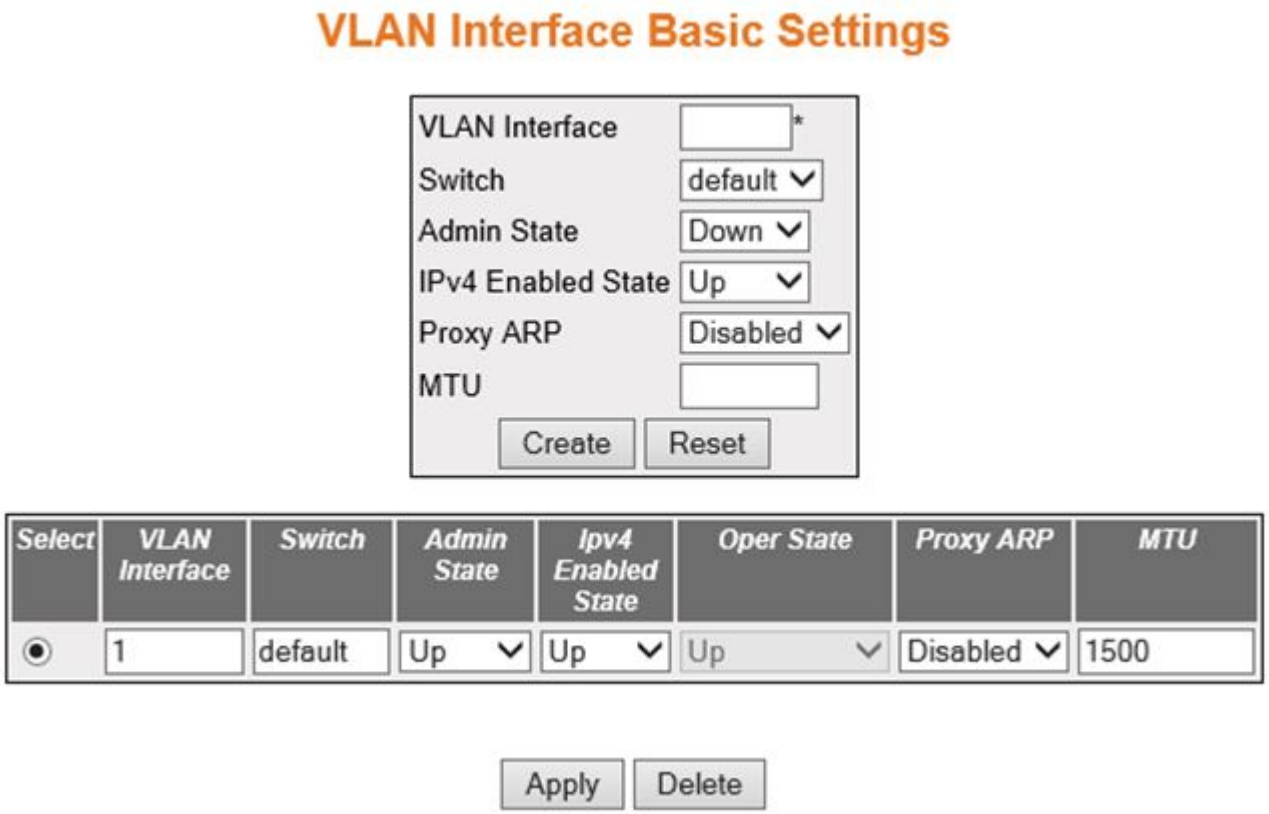
These values will be needed to configure the MicroRAPTOR.

1. Configure the *VLAN* settings by first navigating to the *VLAN* settings screen.

   FOR EXAMPLE: Go to **Layer 3 Management > IP > VLAN Interface.**

   STEP RESULT: The following screen will appear.

   VLAN Interface Basic Settings



2. Configure the values as follows:
   – **Select**—select the *VLAN* Interface for which configuration needs to be modified or deleted. In this case it will be *VLAN* interface #1.

- **VLAN Interface**—enter “1”.
- **Switch**—default.
- **Admin State**—select “UP” from the drop down list.
- **Operating State**—choose UP.
- **Proxy ARP**—select the Proxy *ARP* admin status for the interface. The default option is Disabled. Select **Disabled.**
- **MTU**—enter 1500

3. Click **Apply**.

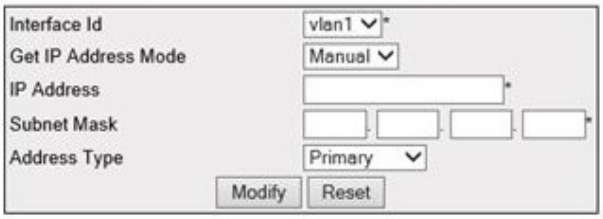
   STEP RESULT: The *VLAN* is now configured.

4. Configure the *PIv4* settings of the *VLAN* by first navigating to the *PIv4* Settings Page.

   FOR EXAMPLE: Go to **Layer 3 Management > IP > IPv4 AddrConf. IPv4 Interface Settings**

   STEP RESULT: The following page will appear:

   IPv4 Interface Settings



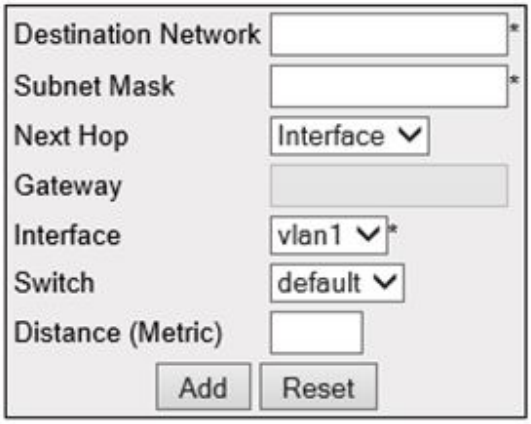
5. If you wish to change the *IP* address and subnet, enter new values in those fields and then click **Modify.**

   STEP RESULT: The *IP* address of *VLAN* 1 will have changed.

6. Configure the *IP* routes.

   FOR EXAMPLE: For *IP* Route Configuration, go to **Layer 3 Management > IP > IP Route. IP Route Configuration** appears.

IP Route Configuration



Select	Destination Network	Subnet Mask	Gateway	Interface	Switch	Distance (Metric)	Routing Protocol
◉	192.168.10.0	255.255.255.0	0.0.0.0	vlan1	default	0	Connected

Apply Delete

7. You will need two routes: one route to your network and a default route to your control center. Once these routes are established, a remote user can configure the switch for proper configuration.
   a. You will need to configure *VLAN* 1 to use the default gateway. This route may already be in your list. The destination network should be the network for the *IP* Address configured in section 0, the subnet mask, the interface should be “vlan1”, the switch option should be “default”, and the distance should be “0”. Click **Add.**
   b. Configure the default gateway. The destination network should be 0.0.0.0, the subnet mask should be 0.0.0.0, and the gateway should be the gateway router IP address. Consult with your administrator if you do not know this value. Leave the interface blank. The switch should be “default” and the distance should be “1”. Click **Add.**
   c. Click **Apply**

   STEP RESULT: You should see a screen similar to the following:

Select	Destination Network	Subnet Mask	Gateway	Interface	Switch	Distance (Metric)	Routing Protocol
○	0.0.0.0	0.0.0.0	192.168.13.254		default	1	Static
◉	192.168.13.0	255.255.255.0	0.0.0.0	vlan1	default	0	Connected

Apply Delete

RESULT:

The *IP* address and default routes have been configured on MicroRAPTOR.

15. Web Interface: User Password

This section will explain how to change a users password.

PREREQUISITE:

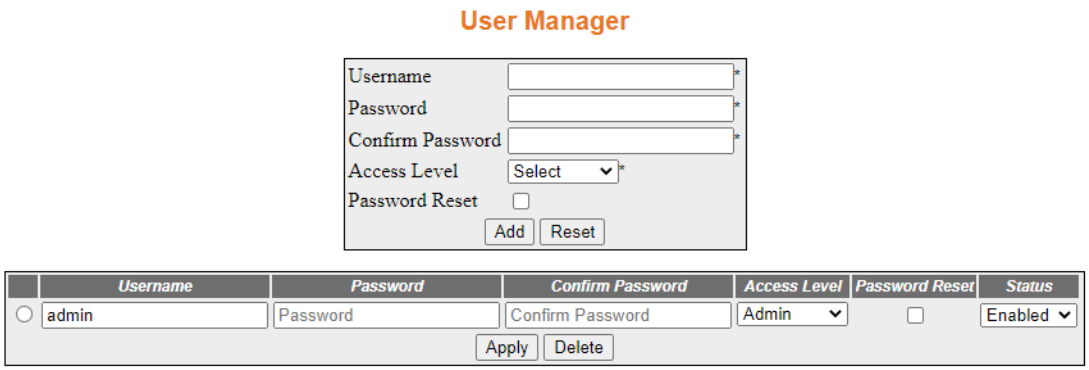
To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the *Web UI*.

1. Navigate to the **Users** page.

   FOR EXAMPLE: In the Home Page, go to **System > Users**

   STEP RESULT: The following screen will appear.

Figure 1: User Manager



2. Click the **admin** radial button.

   STEP RESULT: The username and password fields, starred out, will be populated on the panel above the radial selection.

3. Change the password in the **Password** and **Password Verification** fields.

4. Click **Apply** button.

RESULT:

The admin password has been changed.

16. Web Interface: Save and Restore Configurations

This section will describe how to save and restore the MicroRAPTOR's configuration.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the *Web UI*.

1. To save the configuration to flash memory, perform the following.
   a. Navigate to the **Save Configuration** screen.

      FOR EXAMPLE: In the Home page, go to ***System > Save and Restore > Save***

      RESULT: The following web page will appear.

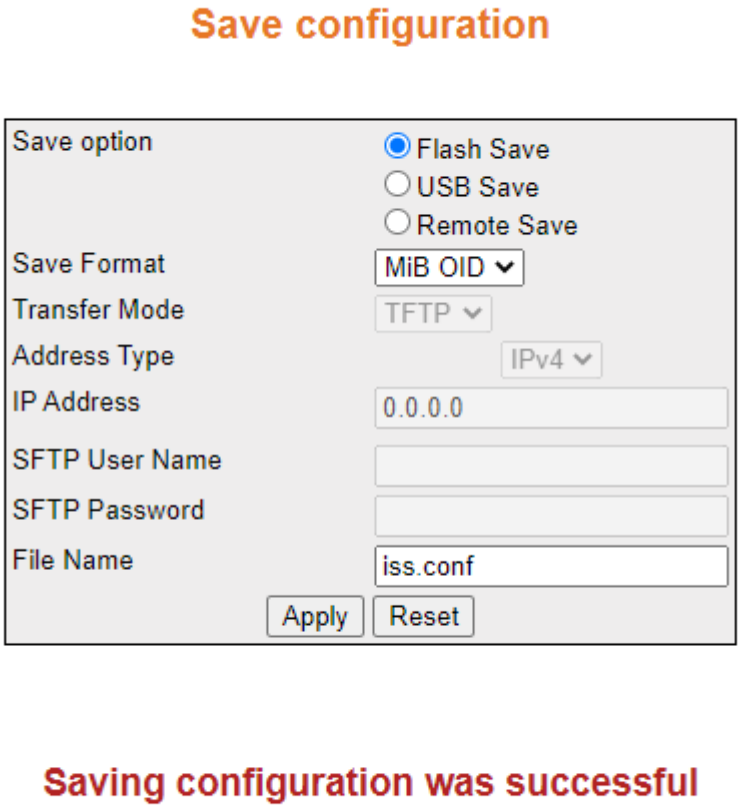
   b. Set the fields as follows:
      - **Save option**—select Flash Save.
      - **Save Format**—select either *MIB OID* or Script. Script format is human- readable and is the default option.

- **File Name**—default file name where the switch configurations are saved is iss.conf. Use the default file name.

c. Click **Apply** to save the changes.

STEP RESULT: The running configuration will now be saved to flash memory. Without saving to flash, the configuration will be lost in the event of a power cycle or device reset. The following screen will appear when the save configuration process is complete:

Save Configuration



2. To save the configuration to USB, perform the following.
   a. Navigate to the Save Configuration screen.

      FOR EXAMPLE: In the Home page, go to ***System > Save and Restore > Save***

      RESULT: The following web page will appear.

   b. Set the fields as follows:
      - **Save option**—select USB Save.
      - **Save Format**—select either *MIB OID* or Script. Script format is human- readable.
      - **File Name**—default file name where the switch configurations are saved is iss.conf. Use the default file name.
   c. Insert the USB thumb drive into the USB port on the front of the MicroRAPTOR.
   d. Click **Apply** to save the changes.

   STEP RESULT: The current configuration will be saved to USB.

3. To Restore a Configuration from USB.
   a. Navigate to the **Restore** page.

      FOR EXAMPLE: Go to ***System > Save and Restore > Restore.***

      RESULT: The ***Startup Configuration Restore Source***page appears.

Figure 1: Startup Configuration Restore Source

   b. Set the fields as follows:
      - **Save option**—select USB Save.

- **Save Format**—select either *MIB OID* or Script. Script format is human- readable.
- **File Name**—default file name where the switch's configurations are saved is iss.conf. Use the default file name.

c. Insert the USB thumb drive into the USB port on the front of the MicroRAPTOR.

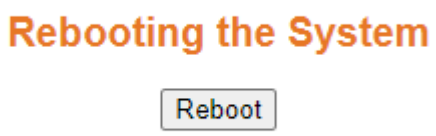
d. Click **Apply** to save the changes.

RESULT: The *MicroRAPTOR* will restore the configuration on the USB.

e. For the changes to take effect, the RAPTOR must be rebooted. Navigate to the reboot screen.

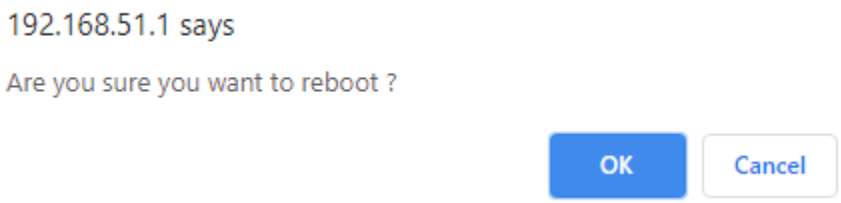
FOR EXAMPLE: Go to ***System > Reboot.***

RESULT: The following screen will appear.



f. Click **Reboot** .

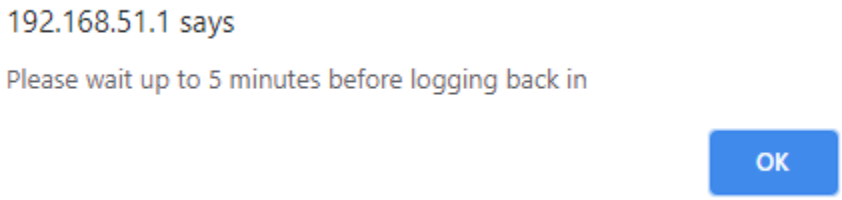
RESULT: A confirmation window will appear.



NOTE: *The IP address will depend on the address of the MicroRAPTOR.*

g. Click **OK**.

RESULT: A second confirmation window will appear.



NOTE: *The IP address will depend on address of the MicroRAPTOR.*

h. Click **OK**.

STEP RESULT: The MicroRAPTOR will reboot and the restored configuration will take effect.

17. Web Interface: Upgrade the MicroRAPTOR using USB

This section will explain how to upgrade the MicroRAPTOR firmware. This process takes approximately 5 minutes to execute.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the *Web UI*.

For all upgrades, it is recommended that user's backup their current running configuration prior to commencing the upgrade process.

Valid Upgrade Paths

If the release that your device is running is not listed in the Supported Upgrade Paths table, it is recommended that the support team is contacted for more detailed instructions.

1. To Upgrade a Configuration from USB navigate to the Upgrade page.

   FOR EXAMPLE: Go to **System > System Upgrade**

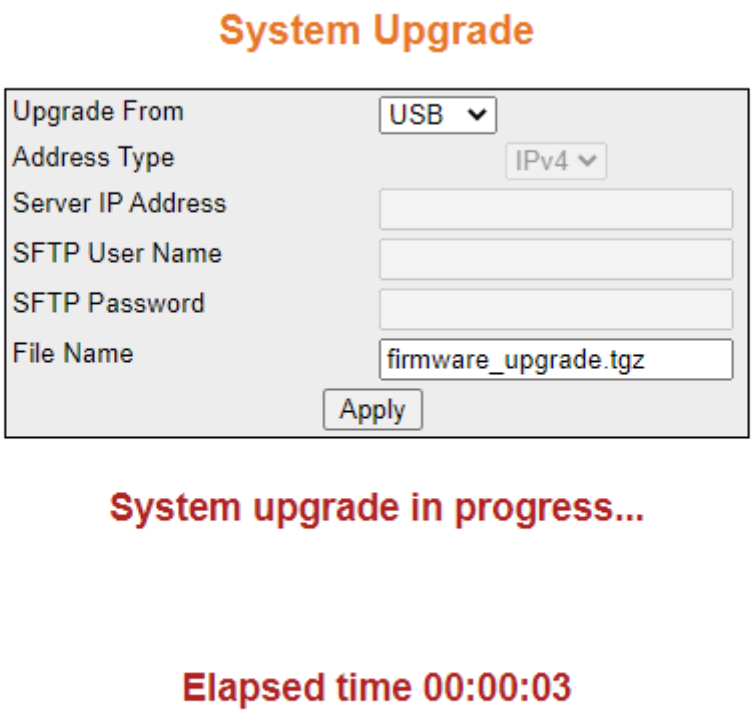
   STEP RESULT: The upgrade page appears:

   System Upgrade

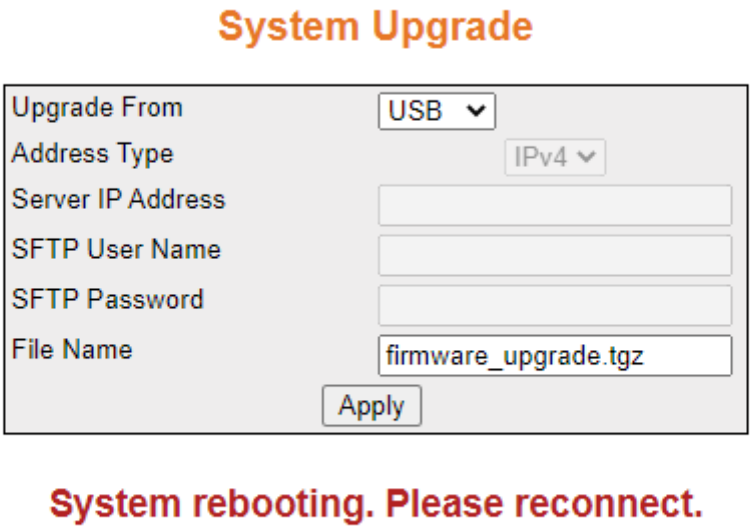
2. Set the fields as follows:
   - **Upgrade From** field—select USB.
   - **File Name**—enter the file name to be loaded from the USB.

3. Click **Apply** to upgrade the MicroRAPTOR.

   STEP RESULT: A timer will appear providing the elapsed time since the upgrade started. The screen will appear similar to the following:



The screen will eventually change to the following:



The MicroRAPTOR firmware will be upgraded and reloaded automatically. After about 5 minutes the device will be ready for users to login to it.

4.

RESULT:

The MicroRAPTOR upgrade is complete.

18. Web Interface: Upgrade the MicroRAPTOR using TFTP

This section will explain how to upgrade the MicroRAPTOR firmware. This process takes approximately 20 minutes to execute when there is a fast network connection between the TFTP server and the MicroRAPTOR.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the *Web UI*.

For all upgrades, it is recommended that user's backup their current running configuration prior to commencing the upgrade process.

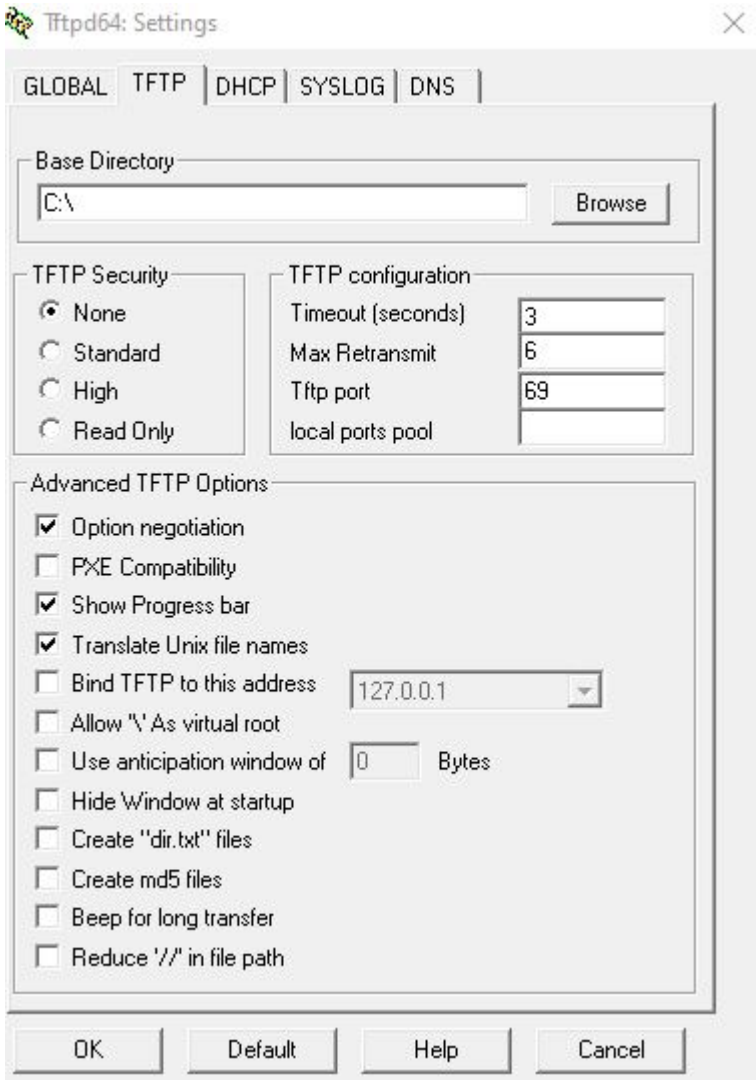
A TFTP server must be installed on a device with network connectivity to the MicroRAPTOR. There are a number of commercial and free TFTP server options available. For this example Tftpd64 was used as the server. It may be downloaded from this site: https://pjo2.github.io/tftpd64/

Valid Upgrade Paths

If the release that your device is running is not listed in the Supported Upgrade Paths table, it is recommended that the support team is contacted for more detailed instructions.

1. Install the TFTP server on a machine that has network connectivity to the MicroRAPTOR.
2. Configure the TFTP server such that its base directory contains the firmware file you wish to upload. Depending on the server software you are using there may be more settings that need to be configured.

   FOR EXAMPLE: This is a screen shot of theTftpd64 settings screen.



3. To Upgrade a Configuration from TFTP navigate to the Upgrade page.

   FOR EXAMPLE: Go to **System > System Upgrade**

   STEP RESULT: The upgrade page appears:

   System Upgrade

4. Set the fields as follows:
   - **Upgrade From** field—select TFTP.
   - **File Name**—enter the file name to be downloaded from the TFTP Server.
   - **Server IP Address**—enter the IP address of the TFTP server.

   STEP RESULT:

   The MicroRAPTOR will be upgraded and reloaded automatically. After about 5 minutes the device will be ready for users to login to it.

5. Click **Apply** to upgrade the MicroRAPTOR.

   STEP RESULT: A timer will appear providing the elapsed time since the upgrade started. The screen will appear similar to the following:

   The screen will eventually change to the following:

6.

RESULT:

The MicroRAPTOR upgrade is complete.

19. Web Interface: Upgrade the MicroRAPTOR using SFTP

This section will explain how to upgrade the MicroRAPTOR firmware. This process takes approximately 20 minutes to execute when there is a fast network connection between the TFTP server and the MicroRAPTOR.

PREREQUISITE:

To perform the tasks in this section, you will have already logged into the MicroRAPTOR via the *Web UI*.

For all upgrades, it is recommended that user's backup their current running configuration prior to commencing the upgrade process.

A SFTP server must be installed on a device with network connectivity to the MicroRAPTOR. There are a number of commercial and free SFTP server options available. For this example the Rebex Tiny SFTP Server was used as the server. It may be downloaded from this site:
https://www.rebex.net/tiny-sftp-server/

Valid Upgrade Paths

If the release that your device is running is not listed in the Supported Upgrade Paths table, it is recommended that the support team is contacted for more detailed instructions.

1. Install the SFTP server on a machine that has network connectivity to the MicroRAPTOR.
2. Configure the SFTP server such that its base directory contains the firmware file you wish to upload. Depending on the server software you are using there may be more settings that need to be configured. The Rebex SFTP server uses a configuration file, RebexTinySftpServer.exe.config, which the user must modify. Please note that the free Rebex is not full featured and the professional option may be more suitable for a commercial deployment.

3. To Upgrade a Configuration from TFTP navigate to the Upgrade page.

   FOR EXAMPLE: Go to **System > System Upgrade**

   STEP RESULT: The upgrade page appears:

   System Upgrade

4. Set the fields as follows:
   - **Upgrade From** field—select SFTP.
   - **File Name**—enter the file name to be downloaded from the SFTP Server.
   - **Server IP Address**—enter the IP address of the SFTP server.
   - **SFTP User Name**—enter the User Name of the SFTP server.
   - **SFTP Password**—enter the Password of the SFTP server.

   STEP RESULT:

5. Click **Apply** to upgrade the MicroRAPTOR.

   STEP RESULT: A timer will appear providing the elapsed time since the upgrade started. The screen will appear similar to the following:

   The screen will eventually change to the following:

   The MicroRAPTOR will be upgraded and reloaded automatically. After about 5 minutes the device will be ready for users to login to it.

6.

RESULT:

The MicroRAPTOR upgrade is complete.

GLOSSARY ENTRIES

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.

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

IP

Internet Protocol (IP).

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.

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.

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.

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.

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.

Index

C

Command Line
- Admin Password 17
- IP Address Configuration 16
- Save and Restore Configuration 18
- Switch Name 14
- Switch Prompt 15
- Upgrading the 19, 23, 26

Configure
- Admin Password 17
- Default route 16
- IP Address 16

Console Port 2
- Logging into the 2

D

Device Manager 4

I

Installing terminal emulator
- Putty 2, 10

P

Passwords for initial login 8

Passwords for iS5Com initial login 12

Putty
- Session Configuration 6, 11

R

Return Manufacturing Authorization xi

S

Service Level Agreements xi

SSH
- Logging into 10
- new password criteria 12

V

Valid Upgrade Paths 42, 45, 48

W

Web Interface
- Ethernet/IP Connectivity 28
- Home Page 32
- IP Address and Default Routes 34
- IP Route Configuration 36
- IPv4 Interface Settings 35
- Logging into the 28
- Login Page 30
- Rebooting the System 41
- Save and Restore Configurations 38
- Save Configuration 39
- Startup Configuration Restore Source 40
- System Settings 33
- System Upgrade 42, 47, 49
- Upgrade the RAPTOR 42, 45, 48
- User Password 37
- VLAN Interface Basic Settings 34