Switches

Ruckus ICX Switches

- Initial/Basic Setup of an ICX Switch
- Upgrading ICX Firmware via USB
- Upgrading ICX Firmware via TFTP
- Clouding an ICX Switch
- Recovering Software Image
- Recovering from a Lost Password
- ICX Spanning Tree Commands
- RSTP for PtP Link(s) Configuration Guide
- How to Configure RSTP (802.1w) and Implement Spanning Tree Best Practices on ICX Switches

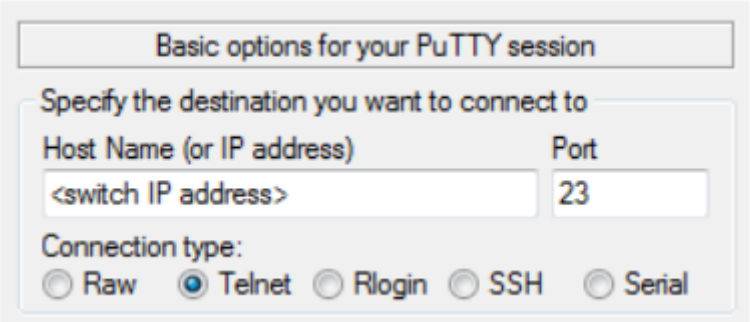
Initial/Basic Setup of an ICX Switch

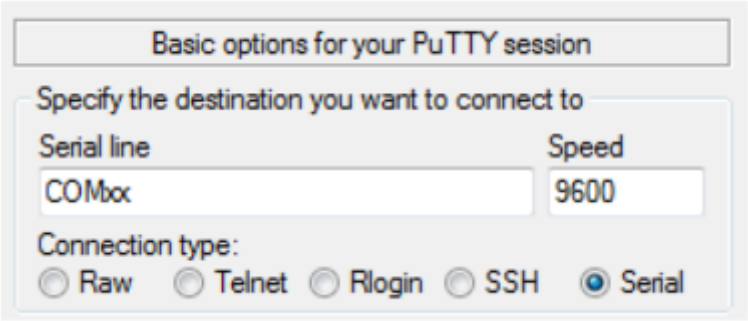
Introduction

Direct management of ICX switches can be performed either via a command-line interface (CLI) or via a web GUI. By default, only the CLI is enabled. This guide explains how to access the CLI, enable the web GUI, and secure all configuration access methods. The web GUI allows full configuration and monitoring of Layer 2 functions, QoS, ACL, authentication, PoE, performing software updates, and much more.

Introduction to the CLI

Start by powering up the switch, and connect a serial cable to the console port on the switch. Once this connection has been made to the switch, a command-line interface (CLI) session can be initiated via a terminal emulation program such as PuTTY (www.putty.org). When PuTTY is started, use the following settings depending on whether you are connecting via Telnet or a serial interface:





Once connected to the switch, the interface will present a console prompt.

Securing the Web, Serial, and Telnet Interfaces

IMPORTANT

As of version 80.9x the first thing you will be forced to do when you login to the switch via CLI is change the default password for the default user 'super'.

When you follow the instructions below you will reach the command line ' username <username> password <password>'

If your username differs from the default 'super' you will be creating an additional user account. With this in mind, you may want to remove the 'super' account. Particularly if you have put in a memorable/simple password in for the sake of logging into the unit (you may have put '12345678' or 'password' in to initially login).

To remove an account enter the following command at the config level:

device(config)#no user <username>

You can see what users have been created by running the following command at enable level:

device#show users

The following commands enable web access and secure the web GUI and serial interfaces with a default username and password of your choice.

IMPORTANT

The following commands were used on version **SPS08090k** (stable release as of August 2022). Upgrading/downgrading from the release may result in unrecognised commands.

device>enable
device#conf t
device(config)#crypto-ssl certificate generate
device(config)#aaa authentication web-server default local
device(config)#aaa authentication login default local
device(config)#enable telnet authentication
device(config)#username **XXXX** password **XXXX**
device(config)#enable super-user-password **XXXX**
device(config)#enable aaa console
device(config)#no telnet server
device(config)#web-management https

device(config)#no user super
device(config)#wr me

The password can be changed by repeating the username <username> password <password> command or via the web interface under Configure > System > Management > User Account.

Cut and paste the following command set at the user EXEC prompt to apply the complete configuration outlined above and set a default username of **super** with a password of **sp-admin** and an enable password of **password**

enable
conf t
crypto-ssl certificate generate
aaa authentication web-server default local
aaa authentication login default local
enable telnet authentication
username super password sp-admin
enable super-user-password password
enable aaa console
no telnet server
web-management https
no user super
wr me

Access to the web interface is now possible, and all access methods are protected by a username and password.

IMPORTANT

To ensure that your switches are secure from unauthorized access, always set a secure password. Never leave a switch with the default brocade/brocade or super/sp-admin settings provided above.

Accessing the Web Interface

To access the device by web interface simply browse to the dynamic IP the switch obtains (by default the switch is DHCP) or add a static IP address to the device**.** For example, if you wanted to access the switch based on a static IP address of 192.168.2.100/24 and a gateway address of 192.168.2.1 you would need to do the following;

device> enable

device# conf t

device(config)# ip address 192.168.2.100 255.255.255.0

device(config)# ip default-gateway 192.168.2.1

device(config)# wr mem

device(config)# exit

device#

You should now be able to browse to 192.168.2.100 via a web browser.

Upgrading ICX Firmware via USB

Introduction

Following best practices and for some features to work the firmware of the ICX switches must be upgraded for mostly all scenarios. This guide serves as a step-by-step guide to upgrading the firmware.

You will need:

- ICX Switch
- PC/Laptop
- USB
- Console Cable
- Ethernet Cable
- Firmware image

Method

It is highly recommended you follow the Initial/Basic Setup of an ICX Switch guide.

This will give you access to the switch which you may find easier to understand the upgrade process.

For the purpose of this guide, I shall start the procedure assuming that the initial setup has been completed.

Step 1)

Download and extract the software required.

Downloads can be found here: https://support.ruckuswireless.com/software N.B. you will need Ruckus credentials to obtain the software.

Step 2)

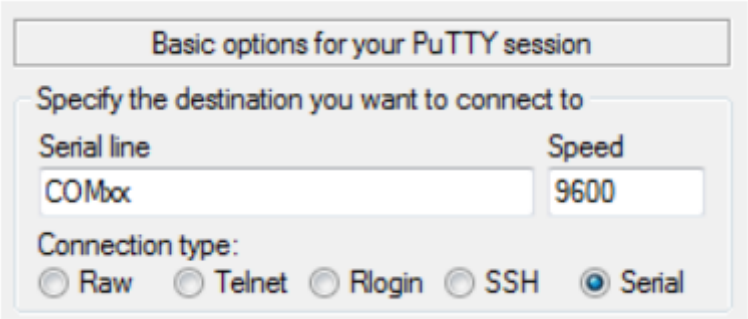
Copy the firmware to the USB root directory.

Step 3)

Start by powering up the switch, and connect a serial cable to the console port on the switch.

Once this connection has been made to the switch, a command-line interface (CLI) session can be initiated via a terminal emulation program such as PuTTY (www.putty.org).

When PuTTY is started, use the following settings to connect via serial interface:



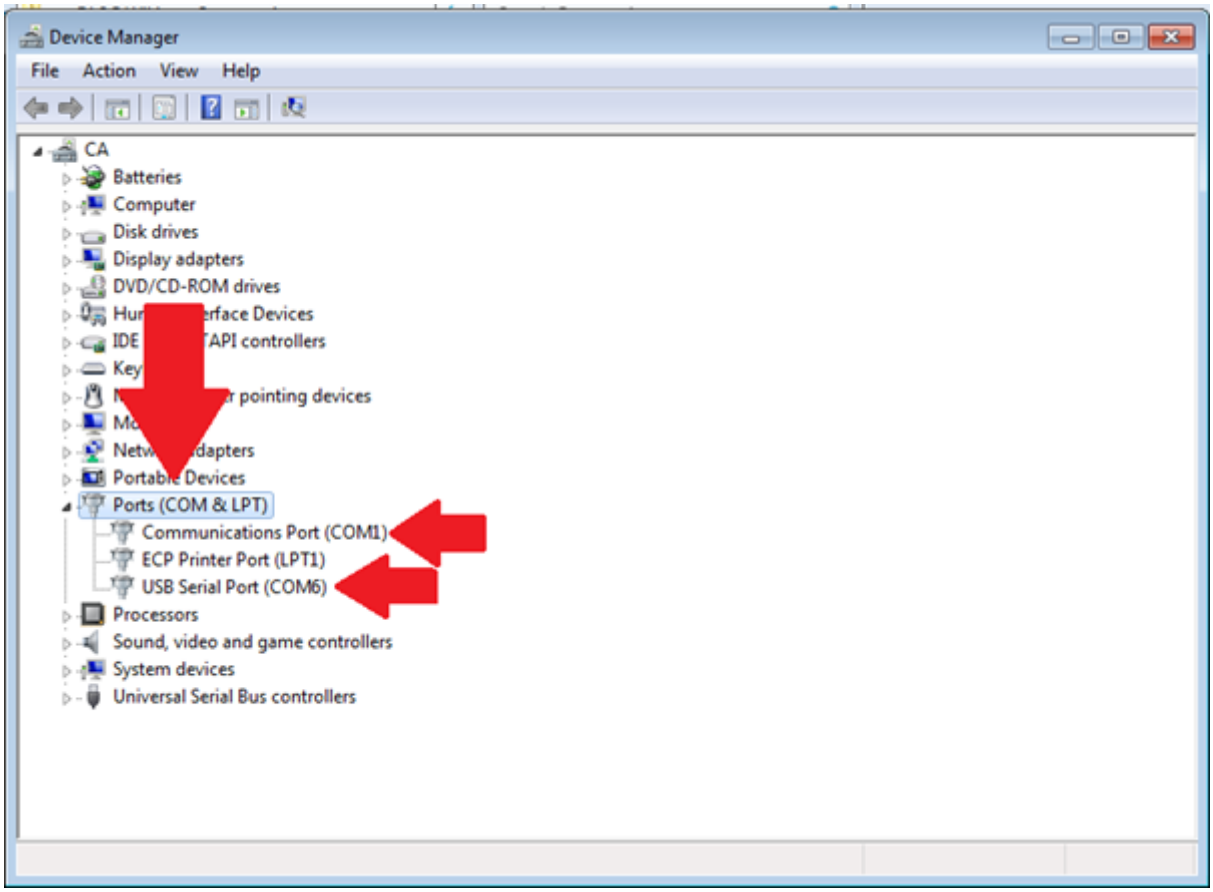
Select Serial

Speed: 9600

Serial line: COMxx

xx being the COM port your device is connected to.

To find which COM port. Open Device Manager under Ports it will be listed USB Serial Port(COMxx)



Once connected to the switch, the interface will present a console prompt.

Step 4)

Plug the USB into the ICX switch

Step 5)

The following commands will copy the firmware to Primary and then to secondary

- ICX5150-24P Switch# Copy disk0 flash SPSxxxxxdufi.bin primary

Note xxxxx is the firmware version.

```
ICX7150-24P Switch#Copy disk0 flash ICX7150/Images/SPS08090dufi.bin primary
```

(When completed you should get a **Flash Done** message)

- ICX5150-24P Switch# Copy disk0 flash SPSxxxxxdufi.bin secondary

Note xxxxx is the firmware version.

```
ICX7150-24P Switch#Copy disk0 flash ICX7150/Images/SPS08090dufi.bin secondary
```

(When completed you should get a **Flash Done** message)

Once the firmware is completed you need to reboot the switch for changes to come into effect. Type the command:

Reload

You will be asked if you are sure of doing so, confirm it by typing:

Y

Step 6)

Log into the switch. Once logged in check the firmware version.

Show version or abbreviated to **sh fl**

If the bootroms do not match enter the following commands

copy fl fl following by *primary* or *secondary* depending on which bootrom partition has not updated.

For example

copy fl fl primary

(this will update the primary bootrom image with an image from the bootrom secondary partition)

Upgrading ICX Firmware via TFTP

Introduction

Following best practices and for some features to work the firmware of the ICX switches must be upgraded for mostly all scenarios. This guide serves as a step-by-step guide to upgrading the firmware.

You will need:

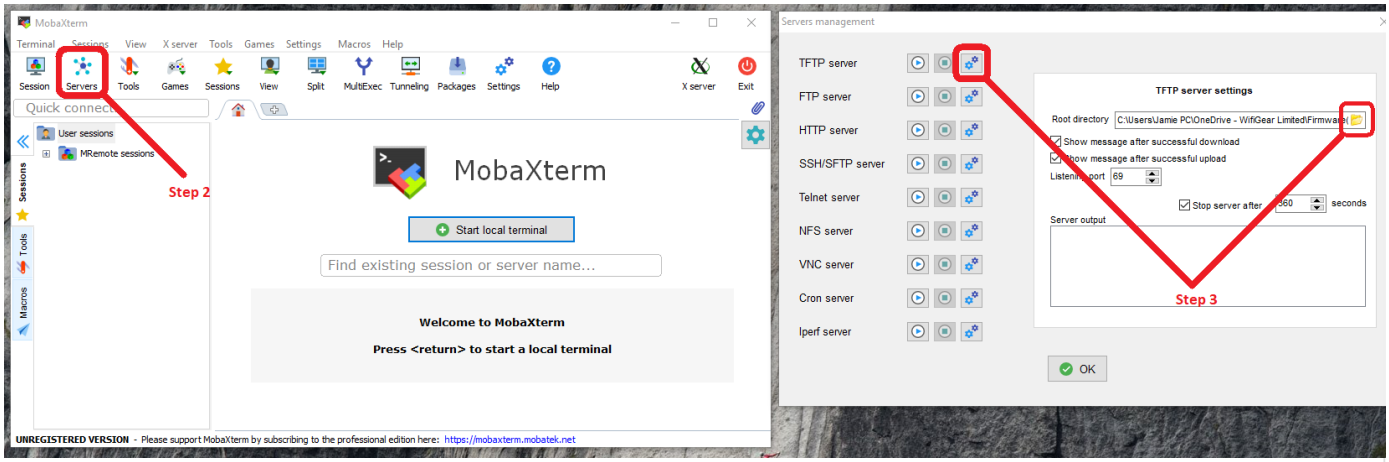
- ICX Switch
- PC/Laptop
- TFTP Server Software
- Console Cable
- Ethernet Cable
- Firmware image

Method

Step 1) Download and extract the software required. Downloads can be found here: https://support.ruckuswireless.com/software N.B. you will need Ruckus credentials to obtain the software.

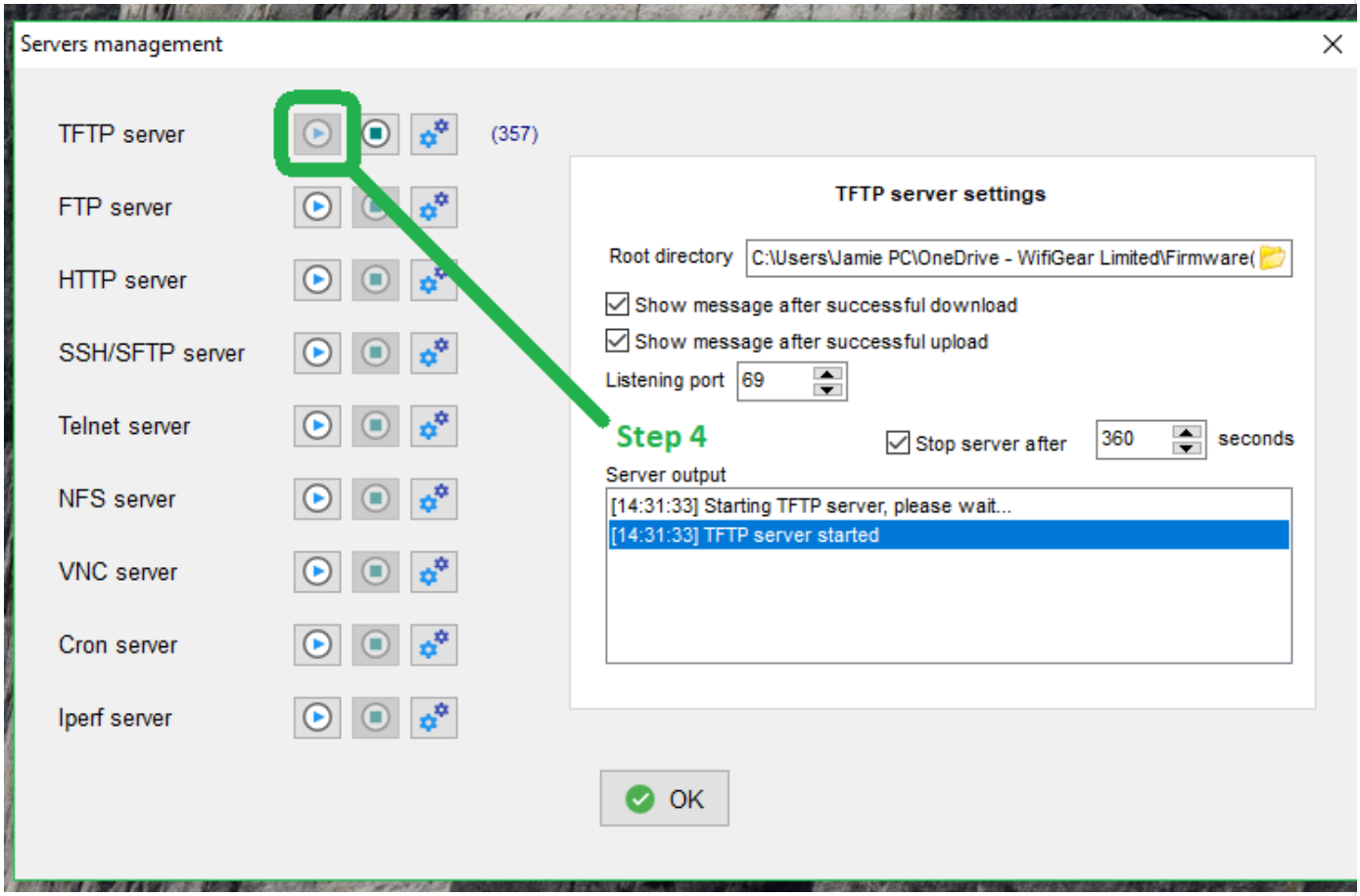
Step 2) Start up a TFTP Server. For this guide I will be using MobaXterm. Once running, click 'Servers'. A new page will load up.

Step 3) Click the 'Configuration' box under TFTP and select the file path of the ***firmware images***



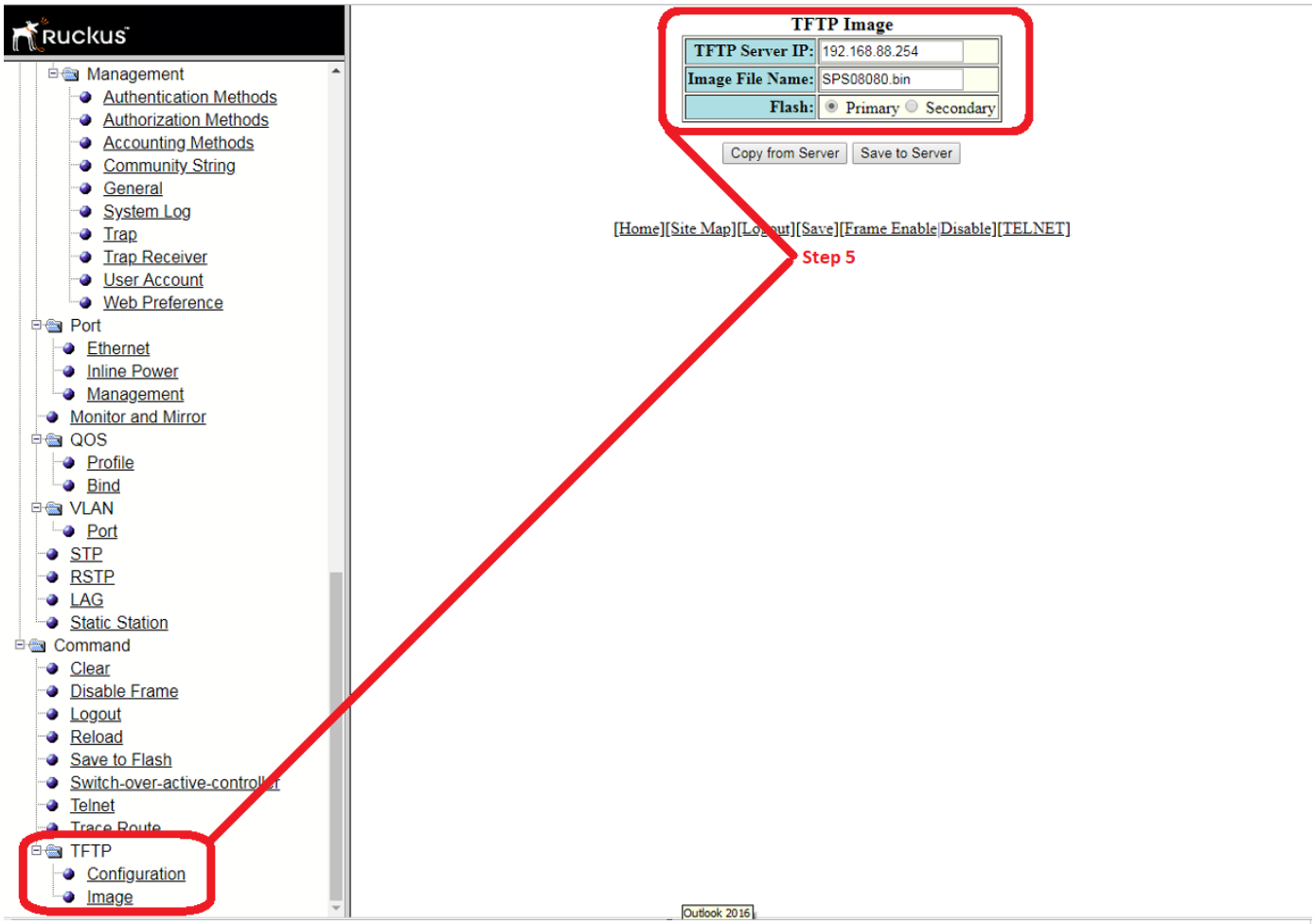
Step 4) Once the information has been entered correctly, start the server by clicking the 'Play' icon.

Be aware there is a default 360-second timeout in which to carry out the next steps before the TFTP server closes.



Step 5) Log in to the ICX Switch via web browser and browse to: TFTP > Image

You will need to enter the IP address of the server (in this case the computers IP address) and the **file name, including the extension.



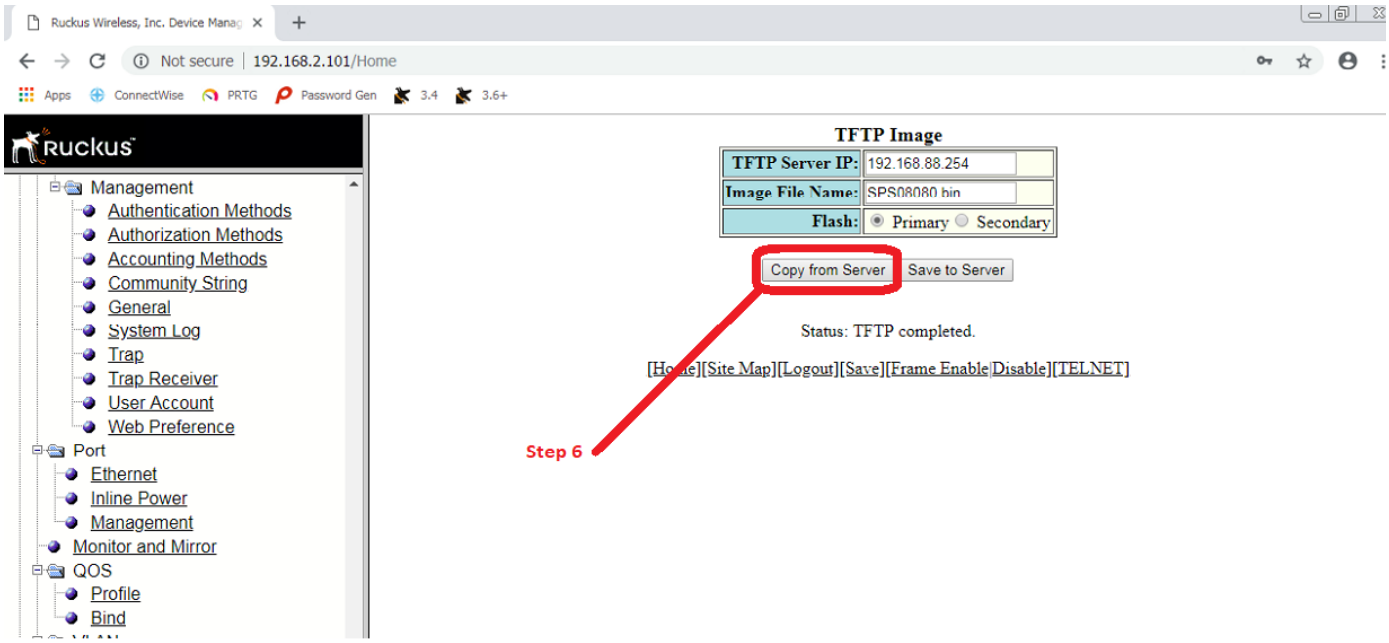
The file required will be under 'Images' and not 'Firmware'.

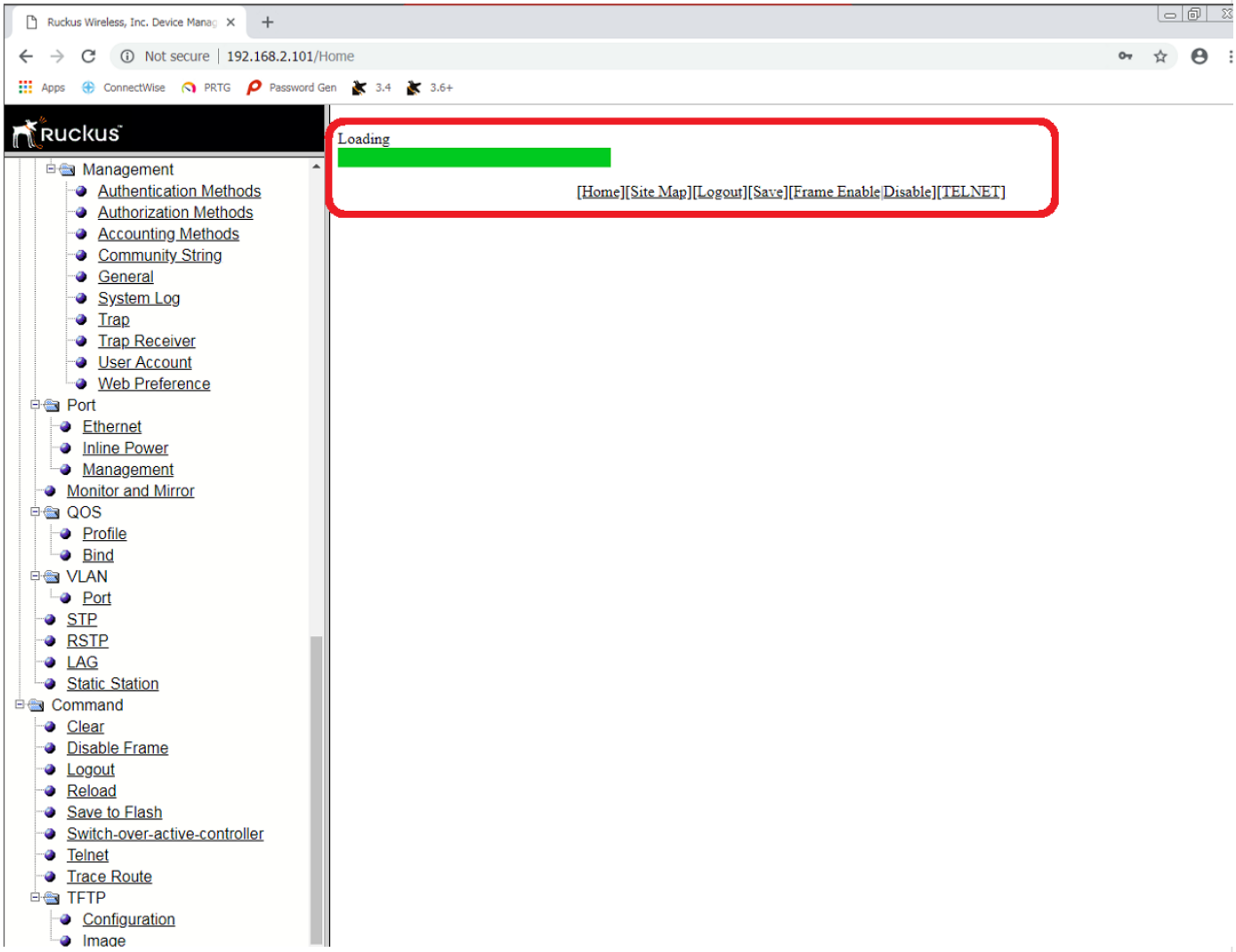
SPS - Switch

SPR - Router

Do not use the ufi.bin files, only use the .bin file types when uploading.

Step 6) On the web interface of the switch click 'Copy from Server'. If successful, the device should start the upgrading process.



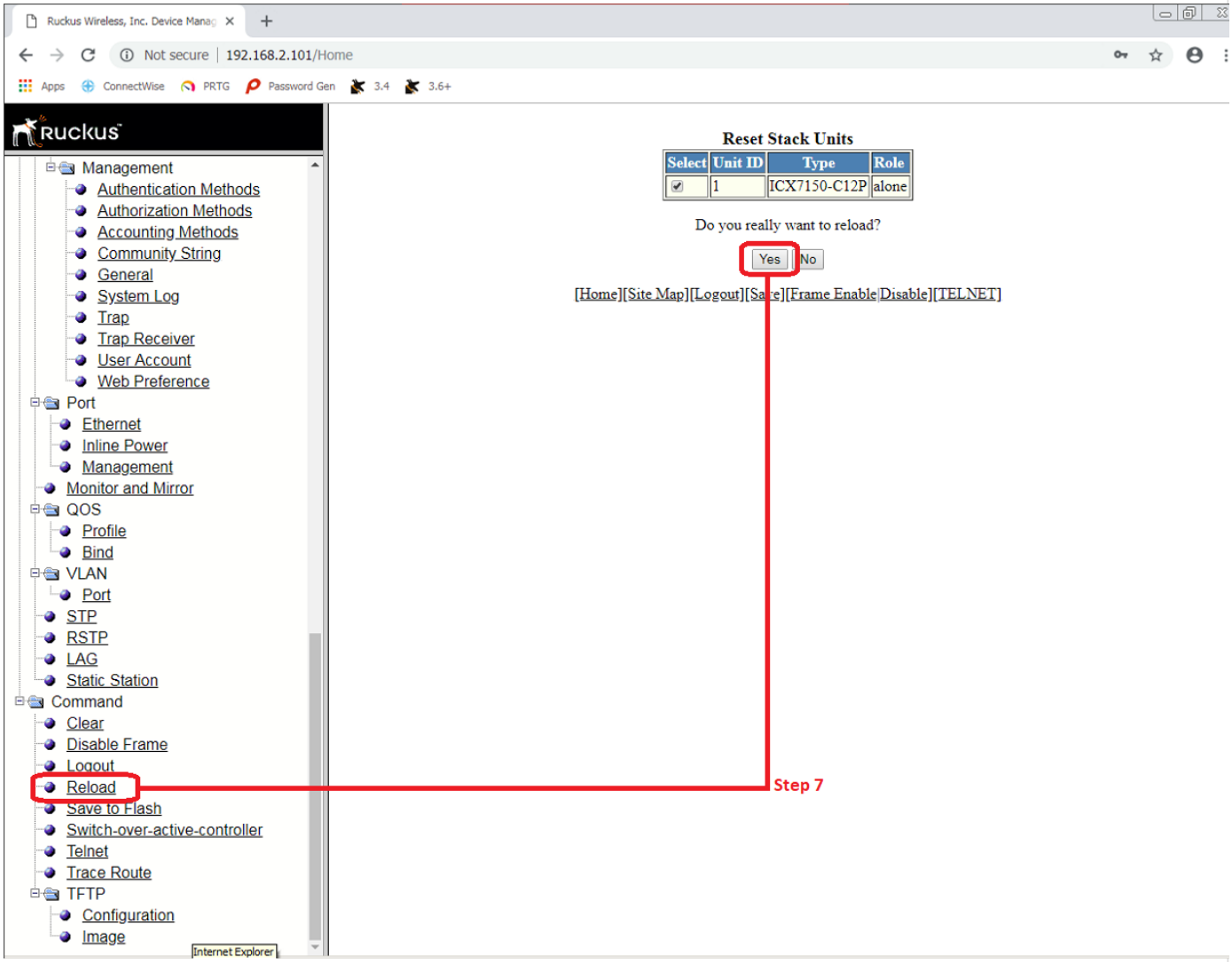


The GUI will then display a red processing bar, wait until this is complete.

You may refer back to the serial connection to monitor progress, it will take a couple of minutes to write the new firmware and restart.

Step 7) Reboot the device. On the web interface browse to: Command > Reload

Confirm with 'Yes' to reboot. Alternatively, perform a hard (physical) reboot.



Step 8) Confirm firmware is upgraded by logging back in after the reboot.

- CLI command: show version

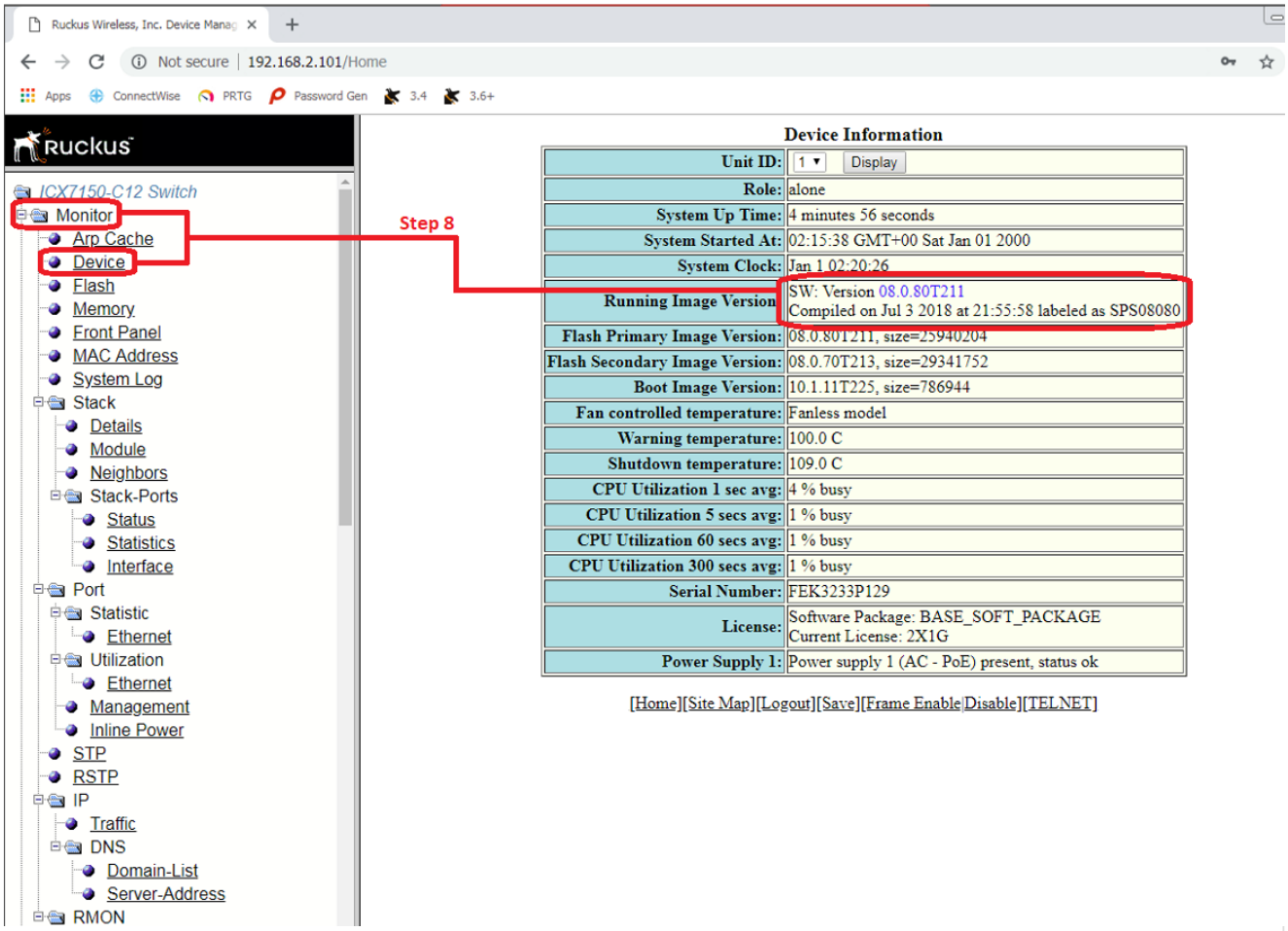
```
ICX7150-C12 Switch>show version
  Copyright (c) 2017 Ruckus Wireless, Inc. All rights reserved.
    UNIT 1: compiled on Jul  3 2018 at 21:55:58 labeled as SPS08080
      (25940204 bytes) from Primary SPS08080.bin
        SW: Version 08.0.80T211
      Compressed Boot-Monitor Image size = 786944, Version:10.1.11T225 (mnz10111)
       Compiled on Wed Dec 13 11:13:34 2017

  HW: Stackable ICX7150-C12-POE
==========================================================================
====
UNIT 1: SL 1: ICX7150-C12-2X1G POE 12-port Management Module
      Serial  #:FEK3233P129
      Software Package: BASE_SOFT_PACKAGE
      Current License: 2X1G
      P-ASIC  0: type B160, rev 11  Chip BCM56160_B0
==========================================================================
====
UNIT 1: SL 2: ICX7150-2X1GC 2-port 2G Module
==========================================================================
====
UNIT 1: SL 3: ICX7150-2X10GF 2-port 20G Module
==========================================================================
====
 1000 MHz ARM processor ARMv7 88 MHz bus
 8192 KB boot flash memory
 2048 MB code flash memory
 1024 MB DRAM
STACKID 1  system uptime is 58 second(s)
The system started at 02:15:38 GMT+00 Sat Jan 01 2000

The system : started=warm start   reloaded=by "reload"

==========================================================================
====
==========       WARNING: Boot-monitor version mismatch!!!      ==========
==========   Please use "show boot-monitor" command for details ==========
==========================================================================
====
```

- Web interface: Monitor> Device


Ruckus Wireless, Inc. Device Manag
Not secure | 192.168.2.101/Home
Apps
ConnectWise
PRTG
Password Gen
3.4
3.6+
Ruckus
ICX7150-C12 Switch
Monitor
Arp Cache
Device
Flash
Memory
Front Panel
MAC Address
System Log
Stack
Details
Module
Neighbors
Stack-Ports
Status
Statistics
Interface
Port
Statistic
Ethernet
Utilization
Ethernet
Management
Inline Power
STP
RSTP
IP
Traffic
DNS
Domain-List
Server-Address
RMON
Step 8
Device Information
Unit ID: 1 Display
Role: alone
System Up Time: 4 minutes 56 seconds
System Started At: 02:15:38 GMT+00 Sat Jan 01 2000
System Clock: Jan 1 02:20:26
Running Image Version: SW: Version 08.0.80T211
Compiled on Jul 3 2018 at 21:55:58 labeled as SPS08080
Flash Primary Image Version: 08.0.80T211, size=25940204
Flash Secondary Image Version: 08.0.70T213, size=29341752
Boot Image Version: 10.1.11T225, size=786944
Fan controlled temperature: Fanless model
Warning temperature: 100.0 C
Shutdown temperature: 109.0 C
CPU Utilization 1 sec avg: 4 % busy
CPU Utilization 5 secs avg: 1 % busy
CPU Utilization 60 secs avg: 1 % busy
CPU Utilization 300 secs avg: 1 % busy
Serial Number: FEK3233P129
License: Software Package: BASE_SOFT_PACKAGE
Current License: 2X1G
Power Supply 1: Power supply 1 (AC - PoE) present, status ok
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

Clouding an ICX Switch

Introduction

SmartZone management and monitoring of ICX switches. The initial release (v.08.0.80) is the first step toward a full-featured wired/wireless integration plan and focuses on monitoring, status, usage visibility, and some basic management, including configuration backups and firmware management.

Method

To direct an ICX switch to the cloud there are a few parameters that **must** be met;

- SZ Firmware (must be v.5 minimum)
- ICX Firmware (must be v.08.0.80 minimum)

Once the following has been met, check the connection to the cloud controller by pinging the necessary IP, for example;

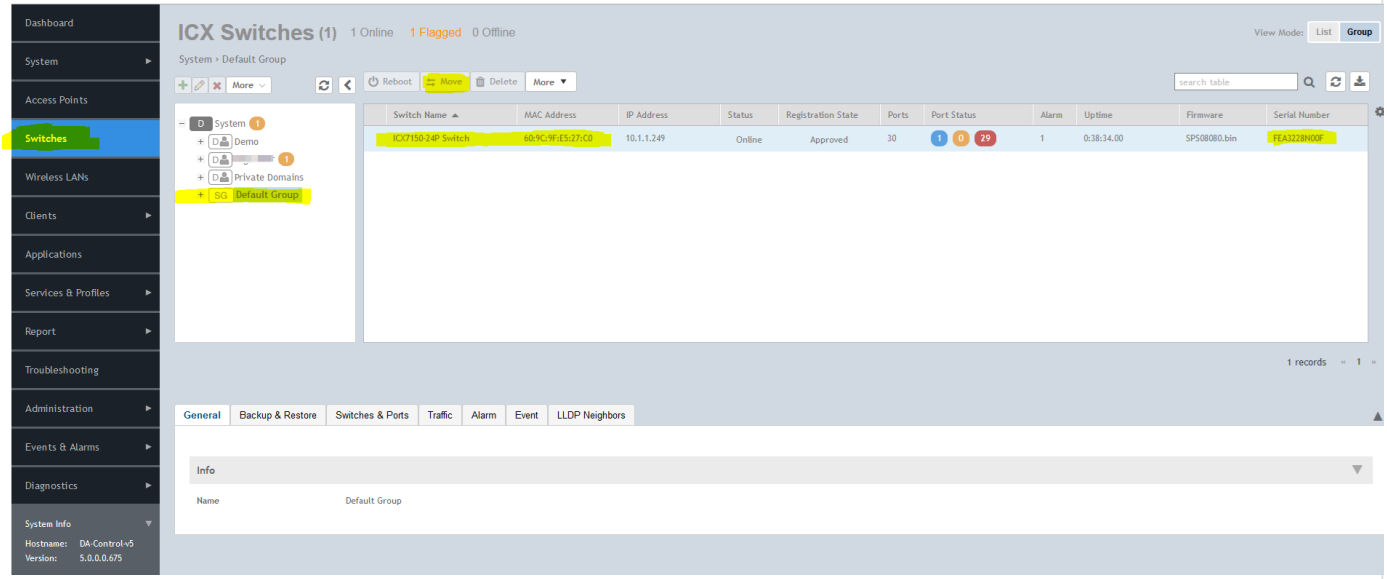
```
SSH@ICX7150-24P Switch>ping xxx.xxx.xxx.xxx
Sending 1, 16-byte ICMP Echo to xxx.xxx.xxx.xxx, timeout 5000 msec, TTL 64
Type Control-c to abort
Reply from xxx.xxx.xxx.xxx   : bytes=16 time=13ms TTL=53
Success rate is 100 percent (1/1), round-trip min/avg/max=13/13/13 ms.
SSH@ICX7150-24P Switch>
```

Should you not be able to ping the controller you must check the following; L2/L3 network, firewall(s), etc.

Point the Switch toward the cloud with the following command(s) your IP may vary depending on the vSZ you are directing your switch to;

```
SSH@ICX7150-24P Switch>en
No password has been assigned yet...
SSH@ICX7150-24P Switch#conf t
SSH@ICX7150-24P Switch(config)#sz active-list xxx.xxx.xxx.xxx
Version 08.0.92 onwards use the command below.
SSH@ICX7150-24P Switch(config)#management active-list xxx.xxx.xxx.xxx
SSH@ICX7150-24P Switch(config)#
```

Log in to the SZ and go to: Switches > Default Group (Staging Zone), highlight the device, and move to the required switch group. The switch will appear in the group as **offline** until approved. check the MAC address to ensure you have the correct switch.



Highlight the correct switch and then click move to relocate the switch to the correct zone as required.

Recovering Software Image

Introduction

This section explains how to recover ICX devices from image installation failure or deleted or corrupted flash images.

Method

IMPORTANT

Text marked in **Red** is a variable command and may differ from your configuration.

- Connect a console cable from the ICX switches console port to your PC/laptop.
- Connect an Ethernet cable from the management port (the port located under the console port on the ICX switch) to the PC/laptop which will need to host a TFTP server. boot up your ICX switch while continuing to press 'B'. The device will be in boot mode for recovery.
- Set the TFTP server IP address that hosts a valid ICX software image using the setenv serverip command.
  ICX 7450-48> setenv serverip **192.168.88.1**

- Set the IP address, gateway IP address, and netmask for the ICX switch (management port), and save the configuration using the setenv ipaddr, setenv gatewayip, setenv netmask, and saveenv commands.
  ICX 7450-48> setenv ipaddr **192.168.88.2**
  ICX 7450-48> setenv gatewayip **192.168.88.254**
  ICX 7450-48> setenv netmask **255.255.255.0**
  ICX 7450-48> saveenv

  Note: The IP address and the gateway IP address set for the device management port should be for the same subnet as the TFTP server NIC.
- Enter the printenv command to verify the IP addresses that you configured for the device and the TFTP server.
  ICX 7450-48> printenv
  baudrate=9600
  ipaddr=192.168.88.2
  gatewayip=192.168.88.254
  netmask=255.255.255.0

serverip=192.168.88.1
uboot=brocade/ICX7450/bootcode/spz10115
Version:10.1.06T215 (May 15 2015 - 11:28:23)

- Test the connectivity to the TFTP server from the device using the ping command to ensure a working connection.
  ICX 7450-48> ping **192.168.88.1**
  ethPortNo = 0
  Using egiga0 device
  host 192.168.88.1 is alive

- Provide the file name of the image that you want to copy from the TFTP server using the setenv image_name command.
  ICX 7450-48> setenv image_name **SPR08090.bin**

- Update the flash using the update_primary or update_secondary command as appropriate.
  ICX 7450-48> update_primary

- Set the file name of the boot image which was copied from the tftp server.
  > setenv uboot **SPR08090.bin**

- Update the uboot file.
  ICX 7450-48> update_uboot

- Load the image from the primary or secondary flash using the boot_primary or boot_secondary command as appropriate.
  ICX 7450-48> boot_primary

- *Optional/Recommended:* Providing the switch boots correctly you may now want to ensure both primary and secondary banks are hosting valid and working software images. To do this you can use the method above (steps 8-11 on the opposite bank that you previously flashed) or refer to the following article(s):
- Upgrading ICX Firmware via USB
- Upgrading ICX Firmware via TFTP

Recovering from a Lost Password

Introduction

If a password has been configured for the device but the password has been lost, you can regain Super User access to the device using the following procedure.

Method

Recovery from a lost password requires direct access to the serial port and a system reboot.

1. Start a CLI session over the serial interface to the Ruckus ICX device.
2. Reboot the device.
3. While the system is booting, before the initial system prompt appears, enter b to enter the boot monitor mode. (you may need to tap 'b' much like when you are trying to enter a BIOS with F2 or Delete)
4. Enter **no password** (You cannot abbreviate this command.)
5. Enter **boot** This command causes the device to bypass the system password check.
6. After the console prompt reappears, assign a new password.

ICX Spanning Tree Commands

Introduction

Best practice switch port configuration for trunk and access ports.

Method

Apply the below config line at EXEC level globally.

system-max spanning-tree 253

Apply the below configs on a port/interface level as per switch port mode.

Trunk Port
spanning-tree 802-1w admin-pt2pt-mac

Access Port
spanning-tree 802-1w admin-edge-port

RSTP for PtP Link(s) Configuration Guide

Introduction

The client would like to use RSTP on ICX switches for automatic failover of a primary and secondary wireless PtP link.

Requirements

2x ICX switch, 1x primary wireless bridge, 1x secondary wireless bridge

Method

Enable RSTP on ICX switches. By default, each port-based VLAN on the device has its own spanning tree. To enable 802.1w Draft 3 in a port-based VLAN, enter commands such as the following.

device(config)# vlan 1

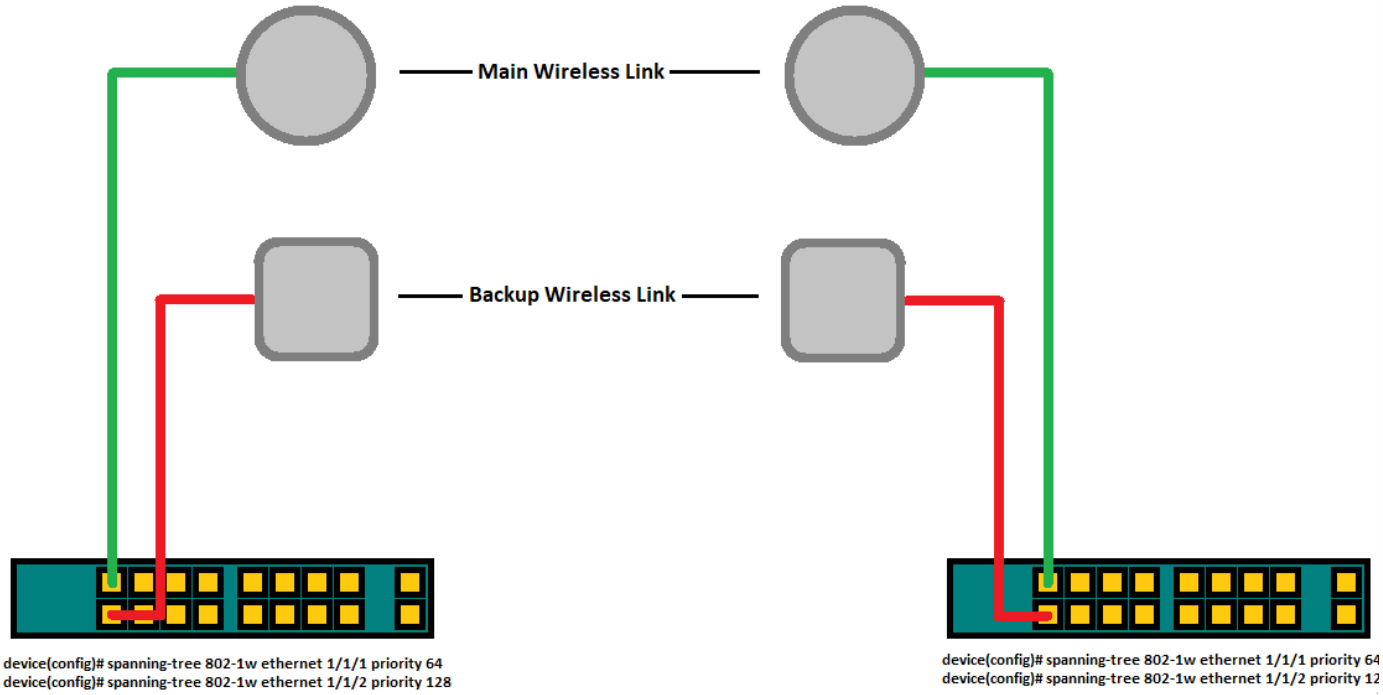
device(config-vlan-1)# spanning-tree rstp

Note

STP must be enabled before you can enable 802.1w Draft 3.

- STP is disabled by default on Ruckus Layer 3 Switches.
- STP is enabled by default on Ruckus Layer 2 Switches.

Once complete run the following command on the switch ports where the primary radios are terminated (on both switches):



device(config)# spanning-tree 802-1w ethernet 1/1/x priority 64

By default all ports have a priority of 128* so if you give a priority of 64 that port will be preferred to be Forwarding on RSTP.

With this setup both primary ports will be functioning in a *forwarding* state. Dynamically, one of the backup ports will also be running in a *forwarding* state while the opposite end will be running in a *discarding* state to prevent a loop. Should the main wireless link disconnect or one of the heads power down, both backup ports will resume a *forwarding* state.



Ports roles can have one of the following states:

- Forwarding - 802.1W is allowing the port to send and receive all packets.
- Discarding - 802.1W has blocked data traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is forwarding. When a port is in this state, the port does not transmit or receive data frames, but the port does continue to receive RST BPDUs. This state corresponds to the listening and blocking states of 802.1D.
- Learning - 802.1W is allowing MAC entries to be added to the filtering database but does not permit forwarding of data frames. The device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.

- Disabled - The port is not participating in 802.1W. This can occur when the port is disconnected or 802.1W is administratively disabled on the port.

Link reference: (http://docs.ruckuswireless.com/fastiron/08.0.80/fastiron-08080-l2guide/GUID-65F3A36C-6A87-4752-9CBD-5C7E7CB505F9.html)

How to Configure RSTP (802.1w) and Implement Spanning Tree Best Practices on ICX Switches

Hello everyone,

Today, I'd like to delve into configuring Rapid Spanning Tree Protocol (RSTP) on ICX switches and share some best practices. By default, ICX switches operate using the standard 802.1d Spanning Tree Protocol (STP) on a per-VLAN basis. However, for faster network convergence, it's advantageous to switch to RSTP (802.1w). I'll guide you through general configuration steps and highlight some key practices that serve as a solid foundation for many network setups. While these configurations might not fit every scenario perfectly, they're a great starting point.

Enabling RSTP on VLANs

First, we'll enable RSTP on your desired VLANs. You can configure multiple VLANs simultaneously or handle them individually. Here's how to enable RSTP on VLANs 10, 20, and 30:

Copy code

```
ICX# configure terminal
ICX(config)# vlan 10 20 30
ICX(config-mvlan-10*30)# spanning-tree 802-1w
```

Setting the Root Bridge Priority

Next, it's essential to set the root bridge priority. If you don't specify a priority, the switch uses the default value of 32768. To ensure your switch becomes the root bridge, assign it a lower priority number. Setting the priority to zero guarantees that this switch will be the root:

Copy code

```
ICX(config-mvlan-10*30)# spanning-tree 802-1w priority 0
```

Your configuration should now resemble:

Copy code

```
vlan 10 by port
 tagged ethernet 1/1/1 to 1/1/48 ethernet 1/2/1 to 1/2/8
 spanning-tree 802-1w
 spanning-tree 802-1w priority 0
!
vlan 20 by port
 tagged ethernet 1/1/1 to 1/1/48 ethernet 1/2/1 to 1/2/8
 spanning-tree 802-1w
 spanning-tree 802-1w priority 0
!
vlan 30 by port
 tagged ethernet 1/1/1 to 1/1/48 ethernet 1/2/1 to 1/2/8
 spanning-tree 802-1w
 spanning-tree 802-1w priority 0
```

Optimizing Switch-to-Switch Links

For optimal convergence times, define switch-to-switch connections as point-to-point links. Assuming ports 1/2/1 through 1/2/8 are your inter-switch links, configure them like this:

Copy code

```
ICX# configure terminal
ICX(config)# interface ethernet 1/2/1 to 1/2/8
ICX(config-if-1/2/1-1/2/8)# spanning-tree 802-1w admin-pt2pt-mac
```

This updates your configuration to include:

Copy code

```
interface ethernet 1/2/1
 port-name Switch-to-Switch Connection
```

```
spanning-tree 802-1w admin-pt2pt-mac
```

Configuring Edge Ports

For ports connected to end devices (edge ports), define them as operational edge ports to expedite the transition to the forwarding state. If ports 1/1/1 through 1/1/48 are your edge ports, use the following commands:

Copy code

```
ICX# configure terminal
ICX(config)# interface ethernet 1/1/1 to 1/1/48
ICX(config-if-1/1/1-1/1/48)# spanning-tree 802-1w admin-edge-port
```

You can also enable STP BPDU Guard on these ports to protect against accidental loops by shutting down the port if a BPDU is received:

Copy code

```
ICX(config-if-1/1/1-1/1/48)# stp-bpdu-guard
```

This results in:

Copy code

```
interface ethernet 1/1/1
port-name Client Port
spanning-tree 802-1w admin-edge-port
stp-bpdu-guard
```

Monitoring RSTP Status

To view RSTP information, use the following commands:

Copy code

```
ICX# show 802-1w
ICX# show 802-1w detail
```

Note: If you're using the standard 802.1d STP, the commands are `show spanning-tree` and `show spanning-tree detail`. For Multiple Spanning Tree Protocol (MSTP), use `show mstp` and `show mstp detail`.

For a comprehensive list of configuration options and further details, refer to the **FastIron Layer 2 Switching Configuration Guide**.