Alcadis
confidence in connectivity

ICX TECHNOTE

Ruckus ICX configuration – Basic configuration (English translation)

Version:	1.0
Creator:	Herwin de Rijke
Date:	20 November 2019

Index

1 Introduction

This document describes basic configuration when using Ruckus ICX switch.

1.1 Goal

The purpose of this document is to familiarize yourself with several basic steps when configuring a Ruckus ICX switch.

1.2 Target audience

This document is written for technical personnel who want to configure a Ruckus ICX switch and have little experience with it.

1.3 Required knowledge / Requirements

To get the most out of what is described in this document, it is important that you have basic knowledge of the following subjects:

- Basic knowledge IPv4
- Basic knowledge of VLAN's

1.4 Additional documentation

There are many more configuration options and perhaps this configuration does not exactly match your desired application. For this we refer to the various manuals for this product line from the manufacturer such as the Ruckus ICX Switch Quick Start Guide, the Ruckus ICX Security Configuration Guide or the Ruckus Fast Iron Command Reference Guide.

1.5 Supported platforms

This information provided in this technote applies to all models of the Ruckus ICX series

The instructions given in this document are based on firmware version 08.0.70a. We recommend that you upgrade your switch to this version or higher. In other versions as used, certain functions may not be available, or the operation may be different.

2 Basic settings

2.1 CLI Levels

De Command Line Interface is divided into three levels. All levels have their own set of authorizations.

1. User Exec level
   This level is indicated when the "**>**" is displayed at the prompt. In this level information can be displayed and basic tasks such as ping and traceroute can be performed.

2. From User Exec level one level up using the "enable" command will activate the Privileged Exec level. Prompt will change to "#" and more command can be performed. Privileged Exec level can be secured with password.

3. Next level is configurations and can be entered from Privileged Exec level by the "configurations terminal" or "conf t" command. When configuration mode is entered prompt will change to "(config)#". Configuration changes are directly applied to the running configurations. Changed need to be saved using the "write memory" command.

When "exit" is entered current level is left and level lower is entered. When "end" or "Ctrl-z" is entered you will directly get back to the # level. When "quit" is entered user will directly go to the Exec (>) level.

2.2 Saving configuration

All configuration settings that you make are stored in the running configuration by default. If you restart the switch, all these settings will be lost if they are not saved. This has been done deliberately so that you can test a configuration that you have made and only save when it is satisfactory. If the configuration is not correct, you can easily get the old working configuration back by restarting the switch. Using command below you can save the running configuration to start-up configuration.

```
ICX7150-24 Switch(config)#write mem

Flash Memory Write (8192 bytes per dot)
.
Write start-up-config done.
Copy Done.
```

2.3 Factory default

The following privileged EXEC CLI command can be used to delete the entire configuration of the switch:

```
device#erase startup-config
Erase startup-config Done.
dhcp server lease database is also removed
stacking/spx pe flash file is also removed

device#reload
```

2.4 Setting IP address and default gateway

To be able to access the switch at IP level, an IP address must be set. If the traffic of the switch must be routed via an uplink to other subnets or if the switch must be accessible from networks other than those configured on the switch, then a default gateway must also be configured. You can perform this operation by entering the commands below:

```
device#conf t
device(config)#ip address 192.168.168.165/24
device(config)#ip default-gateway 192.168.168.1
device(config)#exit
device#write memory
```

The configured IP address is not bound to a specific VLAN and can be accessed from any VLAN. If you do not want this, you can load the router image and create a virtual routing interface or configure an Out-Of-Band management IP address.

2.5 Configuring switch security

2.5.1 Set Privileged Exec Mode password

By default, the switch is set without user account and every user has access to Privileged Exec mode and therefore all read and write rights to the system. The first step for setting security through passwords is therefore to configure a password for the Privileged Exec level. Because the administrator of the system must have all rights, the password for Privileged Exec mode with all rights is set first.

Privileged Exec level has three levels of authorization:

- 0- Super User level (full read/write access)
- 4- Port Configuration level
- 5- Read Only level

The passwords for these three levels can be configured in the following way:

```
device#config t
device(config)#enable super-user-password [tekst]
device(config)#enable port-config-password [tekst]
device(config)#enable read-only-password [tekst]
device(config)#write mem
```

2.5.2 Creating user account

By default, access via the serial console port is not prompted for a username and password. To be able to do this, a user account can be created in the user table of the switch:

```
device#conf t
device(config)#username [text] password [text]
device(config)#exit
device#write memory
```

2.5.3 Setting Authentication options

After the locally saved user account has been created, the switch must be set to use the local user table to authenticate users when logging in. In addition, it must be specified that when logging in the web GUI the local user table is also used and that authentication for console access is required. In addition, it can be specified that passwords can be changed by all users:

```
device#conf t
device(config)#aaa authentication login default local
device(config)#aaa authentication login default local
device(config)#aaa authentication web-server default local
device(config#enable aaa console
device(config#password-change any
device(config)#exit
device#write memory
```

2.5.4 Install SSL certificate

By default, the switch does not have an SSL certificate, which means that encrypted access to the switch is not possible. To create an SSL certificate use the following syntax:

```
device#conf t
device(config)#crypto-ssl certificate generate
device(config)#exit
device#write memory
```

2.5.5 Enable HTTPS access

To enable access via the HTTPS protocol use the following command:

```
device#conf t
device(config)#web-management https
device(config)#exit
device#write memory
```

2.5.6 Disable HTTP access

To make the switch inaccessible for access via the unencrypted HTTP protocol, use the following command:

```
device#conf t
device(config)#no web-management http
device(config)#exit
device#write memory
```

2.5.7 Disable Telnet server

Since the telnet protocol is not secure, and the telnet sever of the switch is on by default, it is advisable to disable it.

```
device(config)#no telnet server
```

2.5.8 Switch access and security summary

It is of course possible to execute the commands from the previous two paragraphs in one go. For this you can paste the following lines in the Privileged Exec mode CLI prompt (after you have of course entered your own values):

```
config terminal
ip address x.x.x.x y.y.y.y [x.x.x.x = ip adres switch, y.y.y.y is netmasker]
ip default-gateway z.z.z.z [z.z.z.z = ip adres default gateway]
enable super-user-password [tekst]
enable port-config-password [tekst]
enable read-only-password [tekst]
username [tekst] password [tekst]
aaa authentication login default local
aaa authentication login default local
aaa authentication web-server default local
enable aaa console
password-change any
crypto-ssl certificate generate
web-management https
no web-management http
no telnet server
exit
write memory
```