Alcadis
confidence in connectivity

ICX TECHNOTE

Ruckus ICX configuratie – Basisinstellingen

Versie:	1.0
Auteur:	Herwin de Rijke / Willem Fieggen
Datum:	20 april 2018

Inhoud

1 Inleiding

In dit document worden een aantal basisinstellingen voor een Ruckus ICX switch beschreven.

1.1 Doelstelling

De doelstelling van dit document is het bekend maken met een aantal basis stappen bij het configureren van een Ruckus ICX switch.

1.2 Beoogd publiek

Dit document is geschreven voor technisch personeel die een Ruckus ICX switch willen configureren en hier nog weinig ervaring mee hebben.

1.3 Voorkennis/Benodigdheden

Om optimaal te kunnen profiteren van wat er in dit document beschreven staat is het van belang dat u basiskennis heeft van de volgende onderwerpen:

- Basiskennis van IPv4
- Basiskennis van VLAN's

1.4 Verdere documentatie

Er zijn nog veel meer configuratie opties en wellicht dat deze configuratie niet precies aansluit bij de door u gewenste toepassing. Hiervoor verwijzen wij graag naar de diverse manuals voor deze productlijn van de fabrikant zoals de Ruckus ICX Switch Quick Start Guide, de Ruckus ICX Security Configuration Guide of de Ruckus FastIron Command Reference Guide.

1.5 Ondersteunde platformen

De informatie in deze Technote is toepasbaar op alle modellen in de Ruckus ICX serie.

De instructies die in dit document gegeven worden zijn op basis van firmware versie Version 08.0.70a. Wij raden aan om uw switch te upgraden naar deze versie of hoger. Mogelijk zijn in andere versies als gebruikte versies bepaalde functies niet beschikbaar of is de werking anders.

2 Basis instellingen

2.1 CLI Levels

De Command Line Interface is in drie verschillende levels onderverdeeld. Ieder level heeft zijn eigen bevoegdheden. We onderscheiden de volgende levels:

1. User Exec level
   Dit level wordt weergeven door de groter dan teken (>) prompt. In dit level kan informatie weergegeven worden en kunnen basistaken als ping en traceroute uitgevoerd worden.

2. Vanuit User Exec level kan een level omhoog gegaan worden naar Privileged Exec level door het `enable` commando uit te voeren. De prompt verandert hierdoor in het hash teken (#). In dit level kunnen veel meer commando's uitgevoerd worden, inclusief die van het User Exec level. Het Privileged Exec level kan met een wachtwoord beveiligd worden.

3. Het volgende level is configuration (of config) en wordt vanuit het Privileged Exec level bereikt door het CLI commando `configuration terminal` (of `conf t`) uit te voeren. Na het uitvoeren van dit commando verandert de prompt in `(config)#`. Configuratie veranderingen die hier doorgevoerd worden, zijn direct toegepast op de running configuratie (in het RAM actieve configuratie). Om deze configuratie veranderingen in de startup-config op te slaan zodat deze na een reboot bewaard blijven dient het `write memory` commando uitgevoerd te worden. Het configuration level bevat sub-levels voor individuele of groepen poorten, VLANs, routing protocollen en andere onderwerpen.

Met het `exit` commando verlaat u het huidige niveau en gaat u een niveau lager. Door `end` of Ctrl Z in te voeren gaat u direct naar het # niveau. Door het `quit` commando uit te voeren gaat u direct naar het User Exec (>) level.

2.2 Configuratie opslaan

Alle configuratie instellingen die u maakt worden standaard opgeslagen in de running configuratie. Als u de switch herstart zullen al deze instellingen verloren gaan indien ze niet zijn opgeslagen. Dit is bewust gedaan zodat u een gemaakte configuratie kunt testen en pas opslaat zodra deze naar wens is. Mocht de configuratie toch niet juist zijn dan kunt u eenvoudig de oude werkende configuratie terug krijgen door de switch te herstarten.

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

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

2.3 Factory default

Het volgende privileged EXEC CLI commando kan gebruikt worden om de gehele configuratie van de switch te wissen:

```
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 IP adres en default gateway instellen

Om de switch op IP niveau te kunnen benaderen dient een IP adres ingesteld te worden. Mocht het verkeer van de switch via een uplink naar andere subnetten gerouteerd moeten worden of als de switch vanaf andere dan op de switch geconfigureerde netwerken benadert moet kunnen worden dan dient er ook een default gateway geconfigureerd te worden.

```
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
```

Het geconfigureerde IP adres is niet aan een bepaald VLAN gebonden en is vanaf ieder VLAN benaderbaar. Mocht u dit niet willen dan kunt u het router image laden en een virtueel routing-interface aanmaken of een Out-Of-Band management IP adres configureren.

2.5 Switch beveiliging configureren

2.5.1 Instellen wachtwoord voor Privileged Exec Mode

Standaard is de switch zonder gebruikersaccount ingesteld en heeft iedere gebruiker toegang tot Privileged Exec mode en dus alle lees en schrijfrechten tot het systeem. De eerste stap voor het instellen van beveiliging door middel van wachtwoorden is dan ook het configureren van een wachtwoord voor Privileged Exec level.
Omdat de beheerder van het systeem alle rechten moet hebben, wordt het wachtwoord voor Privileged Exec mode met alle rechten als eerst ingesteld.

Privileged Exec level heeft drie autorisatie niveaus:

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

De wachtwoorden voor deze drie niveaus kunnen op de volgende manier geconfigureerd worden:

```
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 Gebruikersaccount aanmaken

Standaard wordt er voor toegang via de seriële console poort niet om een gebruikersnaam en wachtwoord gevraagd. Om dit wel te kunnen doen, kan er in de user tabel van de switch een gebruikersaccount worden aangemaakt:

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

2.5.3 Authenticatie opties instellen

Nadat het lokaal opgeslagen gebruikersaccount is aangemaakt dient ingesteld te worden dat de switch de lokale user tabel gebruikt om gebruikers te authenticeren bij het inloggen. Daarnaast moet worden aangegeven dat bij het inloggen van de web GUI ook de lokale user tabel wordt gebruikt en dat authenticatie voor console toegang vereist is. Daaranaast kan aangeven worden dat wachtwoorden door alle gebruikers verandert mogen worden:

```
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 SSL certificaat installeren

Standaard beschikt de switch niet over een SSL certificaat waardoor verseutelde toegang tot de switch niet mogelijk is. Om een SSL certificaat aan te maken gebruikt u de volgende syntax:

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

2.5.5 HTTPS toegang aanzetten

Om toegang via het HTTPS protocol mogelijk te maken gebruikt u het volgende commando:

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

2.5.6 HTTP toegang uitzetten

Om de switch ontoegankelijk te maken voor toegang via het onversleutelde HTTP protocol gebruikt u het volgende commando:

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

2.5.7 Telnet server uitzetten

Aangezien het telnet protocol niet beveiligd is, en de telnet sever van de switch standaard aan staat, is het raadzaam deze uit te zetten

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

2.5.8 Samenvatting switch toegang en beveiliging

Uiteraard is het mogelijk de commando's uit de vorige twee paragrafen in één keer uit te voeren. Hiertoe kunt u de volgende regels in de Privileged Exec mode CLI prompt plakken (nadat u natuurlijk uw eigen waarden ingevuld heeft):

```
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
```