What’s with all the [virtual] Ruckus?

September 2019
written by Maciej Zurawski
Senior Network Engineer

This article will probably please those who look for a raincoat or get the shivers when hearing the word “cloud”. This time we will be testing a controller-based WiFi solution.

Since I have already tested 2 new WLAN solutions from Arista and Juniper Networks I thought why not try something we already use in our office. Still, if you don’t have much space in your rack cabinet don’t panic – it will be a virtual controller.

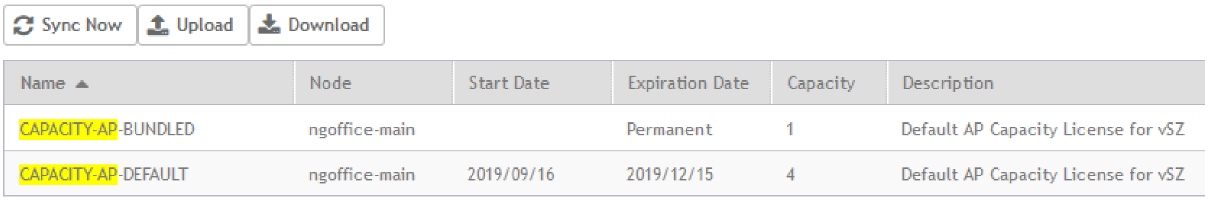
People who think subscription models should remain for venues like Netflix would find something for themselves in Ruckus as well. Many people in the industry are already familiar with the name Ruckus Networks or Ruckus Wireless as they were known before acquisition by the Arris Group. They have an interesting history of who bought them and why, but this is not the subject of this blog post. Because they have been in the market for 15 years, they have a very strong foundation which I would like to verify.

As stated before we already have some Ruckus APs and having in mind that some of our customers are not so eager to move everything to the cloud (including Wireless LAN), I’ve tried Virtual SmartZone (vSZ) which is a NFV-based WLAN controller and looking at the product description “cloud-ready”. But I guess in that case the customer would need to set up a whole cloud infrastructure. Since this solution really differs from those previously tested, it would follow its own path of “test whatever I can think of and have enough time for”.

For the tests version 5.1.2.0.302 was used. Interesting information for all unbelievers (which is the approach I strongly recommend, since everyone makes mistakes) there is a possibility for everyone who already has Ruckus APs to perform such test by themselves since vSZ comes with an embedded RTU license with 1 instance license and 5 AP Capacity license, valid for 90 days from the first setup. Same as before, this article is written from the position of a person not having any previous experience with Ruckus, so this would test how easy it is to manage, configure and find any relevant information in the documentation provided by the vendor. Just to make an important remark, there is a lot of knowledge of Ruckus in our company, it is just me that I never really had anything to do with their products and it seemed a good idea to have me be the child in the fog looking for my own way.

Testing Inventory

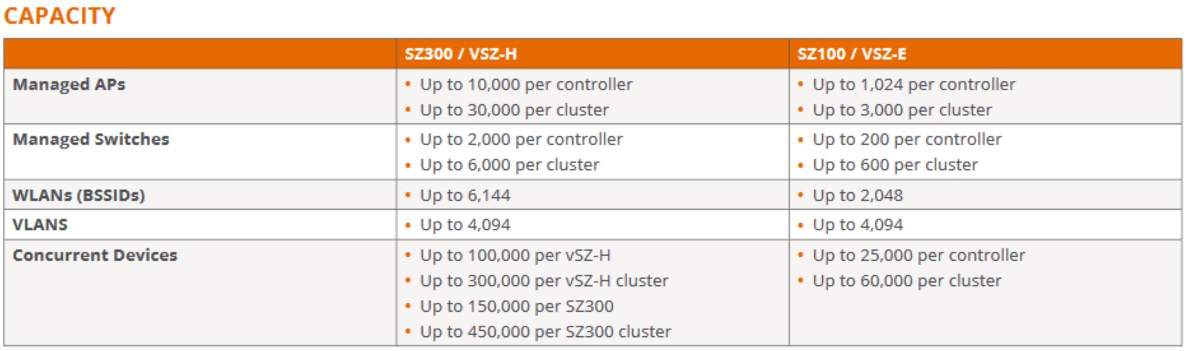
As our company uses Ruckus APs in our office, I didn't have to look long for test devices and just needed to wait for a good opportunity to snatch them. Freshly installed vSZ will come with the license allowing it to manage 5 APs, 4 licenses are temporary and will expire after 90 days the remaining one is permanent.



Name ▲	Node	Start Date	Expiration Date	Capacity	Description
CAPACITY-AP-BUNDLED	ngoffice-main		Permanent	1	Default AP Capacity License for vSZ
CAPACITY-AP-DEFAULT	ngoffice-main	2019/09/16	2019/12/15	4	Default AP Capacity License for vSZ

Having in mind low usage (1 access point) I went for the vSZ-E (Essentials) profile. I first thought that the profile will influence the number of devices in the cluster or the cluster's capability but this is not the case. Both vSZ-E and vSZ-H (High Scale) can be clustered in the 3+1 setup, they differ in the capabilities and in how well they scale. They can be compared to the hardware equivalents:

- SZ100 – vSZ-E
- SZ300 – vSZ-H



CAPACITY

	SZ300 / VSZ-H	SZ100 / VSZ-E
Managed APs	• Up to 10,000 per controller • Up to 30,000 per cluster	• Up to 1,024 per controller • Up to 3,000 per cluster
Managed Switches	• Up to 2,000 per controller • Up to 6,000 per cluster	• Up to 200 per controller • Up to 600 per cluster
WLANs (BSSIDs)	• Up to 6,144	• Up to 2,048
VLANS	• Up to 4,094	• Up to 4,094
Concurrent Devices	• Up to 100,000 per vSZ-H • Up to 300,000 per vSZ-H cluster • Up to 150,000 per SZ300 • Up to 450,000 per SZ300 cluster	• Up to 25,000 per controller • Up to 60,000 per cluster

There are of course more differences then the managed devices count, as I wrote before, they differ in the supported feature set. Supported only on the vSZ-H:

- Geo-Redundant Clustering (failover between clusters)
- Multi-tier Tenancy (RBAC)
- Partner Domain Layer (Tenants separation)

It is important to decide which profile to go with since this influences resource usage and the profile cannot be changed after it is configured, so put some effort into planning. Always consult release notes for the target version to verify requirements. I've got an interesting side note from my colleague, that Ruckus can deny support when assigning higher resources to vSZ, so always try to use exact specs.

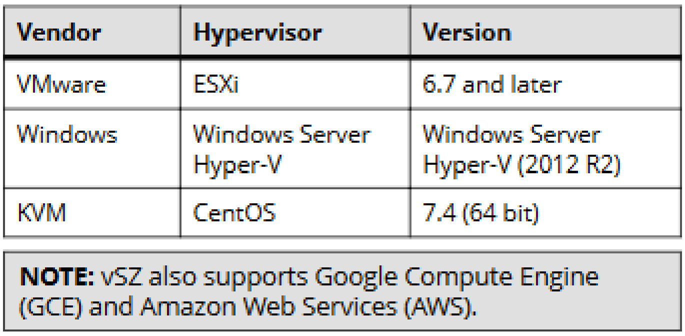
There is one additional appliance that can spark an interest in some people, vSZ-D which decouples data plane, from the control plane which is managed by the vSZ. vSZ-D enables to handle tunneling and encryption of all user data from APs to a specified destination, different from local breakout or location of vSZ, but still being centrally managed by the vSZ. This allows, for example, to manage QoS, security, and roaming centrally. vSZ-D will as well support vTWAG, and since it can run its own DHCP server and perform NAT, it can masquerade users for the upstream network environment. Now, enough about the controller.

Let's look at the AP. The only access point I could snatch was a Ruckus R500. Maybe it is not the newest Ruckus product but it performed well under our requirements. I could test if it would perform well with the newest firmware on vSZ. There is no point in bringing up the specifications of the AP since it cannot be compared with the previously tested models. I looked through the Ruckus portfolio for any AP, which can stand up for a fight with Arista C-130 and Mist AP41, and I think R750 is comparable to these two. Maybe it lacks the extra scanning antenna but background scanning can be done inbound on the "client" antennas. It has some other proprietary features, onboard BLE, and comes with the 2,5Gbps uplink port.

Getting started

Controller initial setup

First, we need to set up a VM for the controller. Since vSZ supports different Hypervisors there is not a problem to find a suitable environment for testing. Everyone should be able to adapt it easily to his own production environment, even if you only run VMs in the cloud. Below is the list of supported hypervisors for the 5.1,2 release:

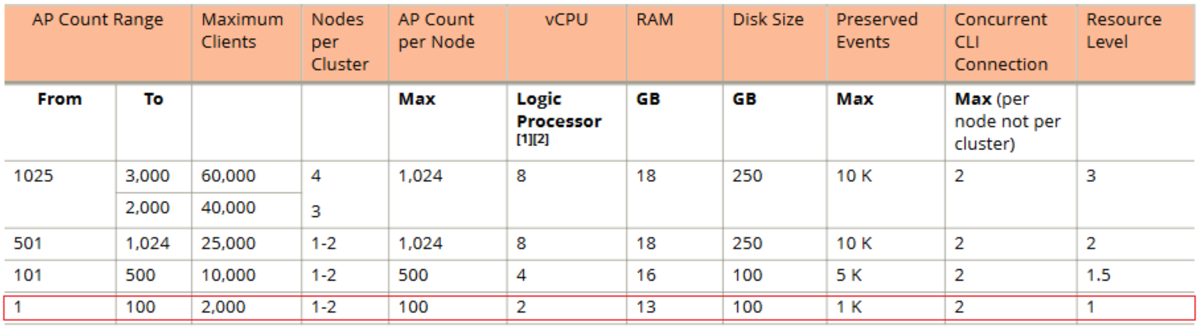


Vendor	Hypervisor	Version
VMware	ESXi	6.7 and later
Windows	Windows Server Hyper-V	Windows Server Hyper-V (2012 R2)
KVM	CentOS	7.4 (64 bit)

NOTE: vSZ also supports Google Compute Engine (GCE) and Amazon Web Services (AWS).

Since I wanted to see if the upgrade procedure is complicated I deliberately used initially version 5.1.0, and then downloaded *.ximg patch to upgrade to 5.1.2. I will stand by that and everyone saying that I just downloaded the wrong version in the first place are wrong. As already mentioned in the controller description it is important to assign proper resources to the VM since we would have currently 1 AP and there are no plans to scale (for production environment we would set up a new controller), I went for the lowest resource usage level. Since there is nothing out of ordinary in the importing VM into hypervisor in case of vSZ I'll skip that part.

TABLE 5 vSZ Essentials required resources



AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	vCPU	RAM	Disk Size	Preserved Events	Concurrent CLI Connection	Resource Level
From	**To**			**Max**	**Logic Processor** [1][2]	**GB**	**GB**	**Max**	**Max** (per node not per cluster)	
1025	3,000	60,000	4	1,024	8	18	250	10 K	2	3
	2,000	40,000	3							
501	1,024	25,000	1-2	1,024	8	18	250	10 K	2	2
101	500	10,000	1-2	500	4	16	100	5 K	2	1.5
1	100	2,000	1-2	100	2	13	100	1 K	2	1

After powering up VM we need to configure the network interface to be able to communicate with the controller. There are 2 options:

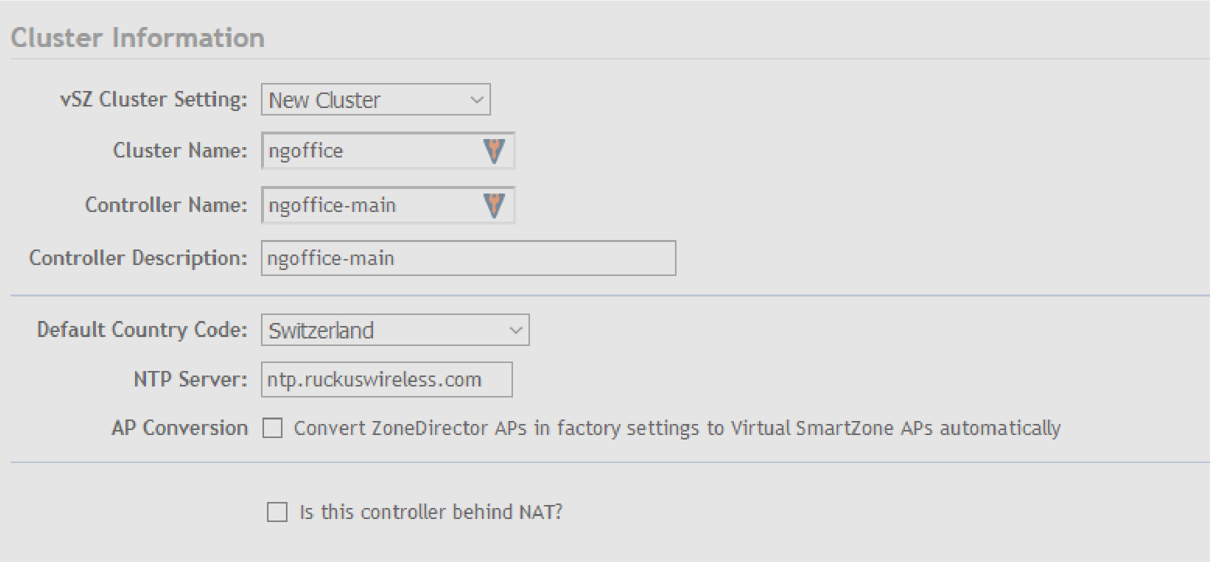
- VM console and going through the setup wizard
- use default network settings and let VM obtain the address from the DHCP server on the management interface … and then go through configuration wizard but on the webGUI.

Since we are hardcore CLI fans, we went with the first option and the process was quite easy to follow:

Network setup

```
################################
#       Welcome to vSZ         #
################################
Last login: Mon Sep 16 08:32:57 2019 from 192.168.182.181
Please wait. CLI initializing...
Welcome to the Ruckus Virtual SmartZone - Essentials Command Line Interface
Version: 5.1.0.0.496
vSZ> en
Password: *****
vSZ# setup
################################################
Start vSZ setup process:
################################################
************************************************
vSZ Profile
************************************************
1. Essentials
2. High Scale
Enter "i" for more information
************************************************
Select vSZ Profile (1/2): 1
WARNING! You cannot change the vSZ profile once you complete setup. Are you
sure
 you want to install the "Essentials" profile? (y/n)[Y] y
Network is not setup
************************************************
IP Version Support
************************************************
1. IPv4 only
2. IPv4 and IPv6
************************************************
Select address type: (1/2) 1
<...truncated...>
```

After configuring the network I could use web interface to finish the initial configuration, which in my case, was creating a new cluster.



Cluster Information

vSZ Cluster Setting: New Cluster

Cluster Name: ngoffice

Controller Name: ngoffice-main

Controller Description: ngoffice-main

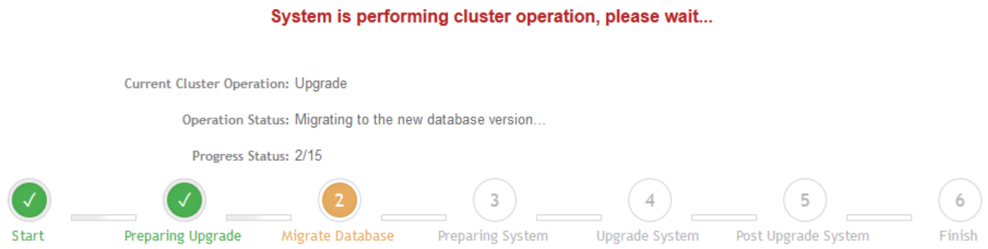
Default Country Code: Switzerland

NTP Server: ntp.ruckuswireless.com

AP Conversion ☐ Convert ZoneDirector APs in factory settings to Virtual SmartZone APs automatically

☐ Is this controller behind NAT?

The last step as mentioned at the beginning was to do an upgrade from 5.1.0.0.496 to 5.1.2.0.302. This as well involved updating the Signature package to the version 1.430.1. And to be fair I just uploaded ximg file, clicked on “proceed” and went away for around 30min, so the upgrade can be done unattended but of course, this is not wise for the production devices since bad things tend to happen and it is better to address them earlier then later. After the initial controller reboot, when new software is uploaded and needs to be reloaded, you would get a status page when the device is back and running, getting an overall status of the installation.



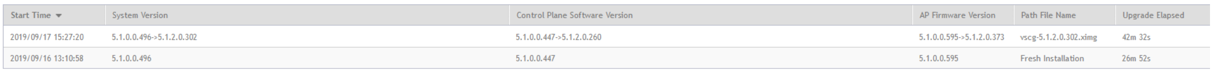
System is performing cluster operation, please wait...

Current Cluster Operation: Upgrade

Operation Status: Migrating to the new database version...

Progress Status: 2/15

My upgrade took around 45min to finish, but this probably would depend on the load of the device, especially database usage.



Start Time ▼	System Version	Control Plane Software Version	AP Firmware Version	Path File Name	Upgrade Elapsed
2019/09/17 15:27:20	5.1.0.0.496->5.1.2.0.302	5.1.0.0.447->5.1.2.0.260	5.1.0.0.595->5.1.2.0.373	vscg-5.1.2.0.302.ximg	42m 32s
2019/09/16 13:10:58	5.1.0.0.496	5.1.0.0.447	5.1.0.0.595	Fresh Installation	26m 52s

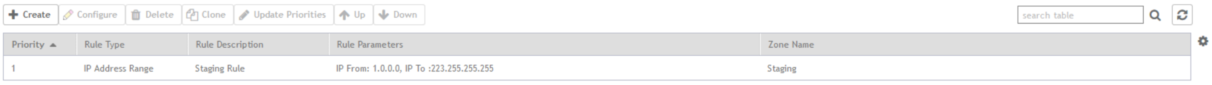
Connecting AP and configuring WLANs

The controller is prepared so I continue with creating new zones. Of course, since 1 AP would not divide well into multiple zones I created 2 and ended up with 3. Zones and groups are like buildings and floors for the Arista, they are used to group devices with the common set of properties and which should share the same configuration and firmware; you can manage multiple devices by assigning templates. So I created 2 new zones, 1 for testing, 1 for staging and was left with the default zone which cannot be removed.

It’s always a good idea to create a staging zone if there is a need to auto-discover new APs which would be provisioned in the future. I need to mention that in some outputs, commands and documentation pages, vSZ is reflected as the SCG (SmartCell Gateway), which as far I was able to find, was the old name for the SZ. Through this article, I will sometimes use these two names interchangeably.

An additional step I always like to do before starting any sort of configuration is to create non-default admin accounts and create user access profiles (if possible). In the vSZ administrators are tied together with the permissions, resources and account security via the user groups. Users can have additional login security enabled, each login request to the WebGUI can be secured with the captcha mechanism and/or 2FA can be enabled, using SMS authentication tokens. If we want to use 2FA, we must already have a service configured on the SMS gateway provider Twilio. I would like to see more options there, like OTP applications.

To prepare I changed the AP rules for controller discovery. I tried to generalize rules based on the AP IP address by assigning it to the Staging zone. And as well disabling the option to automatically approve all join requests from APs. I could enhance it even more with the AP MAC OUI validation which would narrow down which APs can connect to the system. This is not spoof-proof but a nice addition to the auto registration process.



Priority ▲	Rule Type	Rule Description	Rule Parameters	Zone Name
1	IP Address Range	Staging Rule	IP From: 1.0.0.0, IP To :223.255.255.255	Staging

APs can be discovered or added to the vSZ using one of the two methods. Either you configure manually, on the AP, vSZ (SCG) IP and then let it try to establish a connection and request registration or, the preferred approach, configure option 43 on the DHCP which will point all APs to the specific controller already. Of course, it is better to use DHCP for all operational usage. Option 43 is Vendor Specific Info and it has TLV format, for the Ruckus there are two values for the type (T):

- 0x03 for the ZoneDirector (ZD)
- 0x06 for the SmartZone (vSZ)

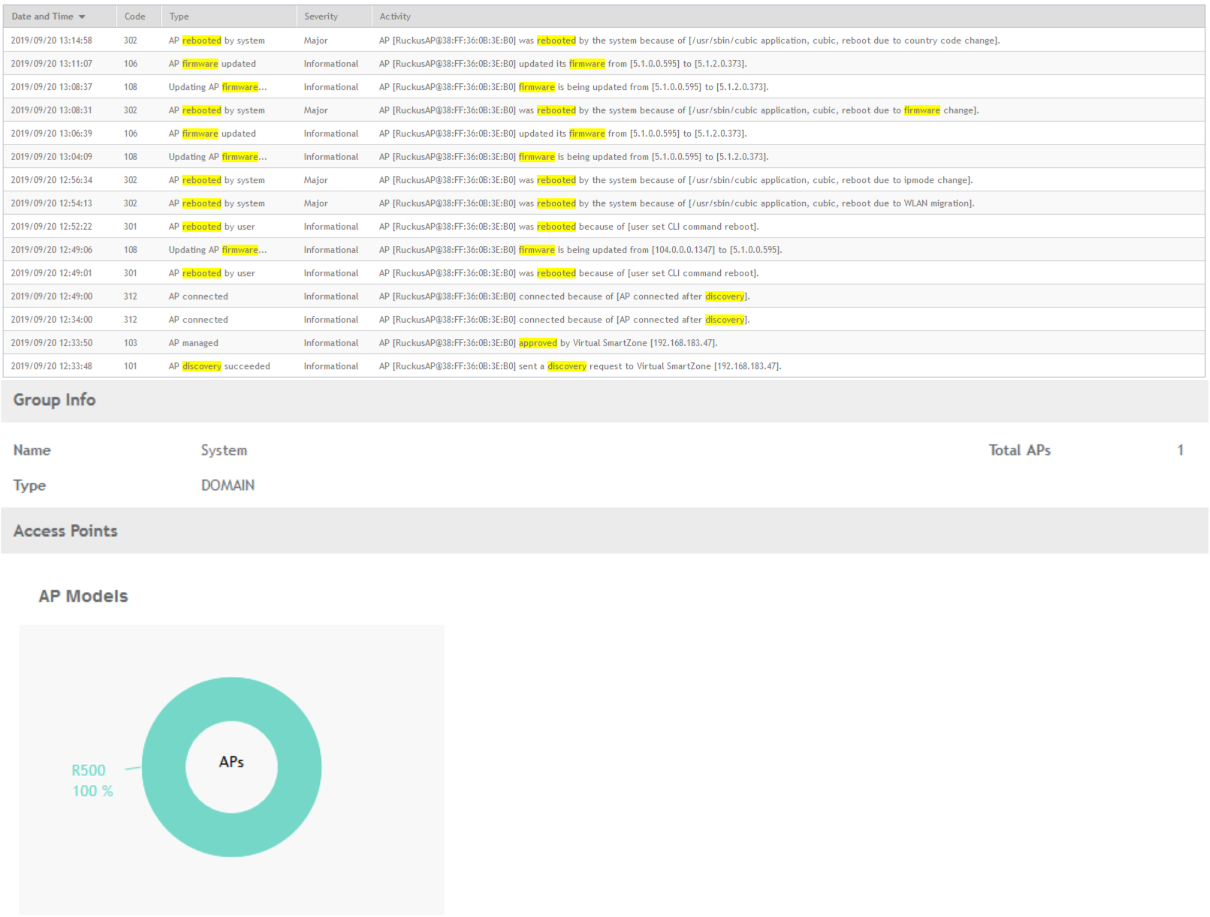
The rest is usual, length of the Value part, and the Value itself which is in most cases IP address of the controller. For the future, I used PERL to quickly generate me option 43, which I configured on the DHCP server serving currently my test AP, but initially, I configured vSZ manually on the AP.

```
perl -e 'my $output; for (split //, $ARGV[0]){$output.=unpack "H*", $_};
print "06".sprintf("%02x", length($ARGV[0])).$output;' 192.168.182.47
060e3139322e3136382e3138322e3437
```

To attach AP manually to the vSZ, you need to obviously log on to the AP CLI and then specify the IP address of the vSZ. I’m not sure if this was necessary, or I just don’t want to wait until the process starts by itself, but I set the state of the SCG service to initialize.

```
setscg ip <vSZ>
setscg init
```

I waited around 30 min for the process to finish. There was actually a lot going on, at least 3 firmware upgrades and several reboots. It is worth noting that when AP is managed by the vSZ it would have different firmware, so it is not easy to switch AP back to the standalone (unleashed).



Date and Time ▾	Code	Type	Severity	Activity
2019/09/20 13:14:58	302	AP rebooted by system	Major	AP [RuckusAP@38:FF:36:0B:3E:B0] was rebooted by the system because of [/usr/sbin/cubic application, cubic, reboot due to country code change].
2019/09/20 13:11:07	106	AP firmware updated	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] updated its firmware from [5.1.0.0.595] to [5.1.2.0.373].
2019/09/20 13:08:37	108	Updating AP firmware...	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] firmware is being updated from [5.1.0.0.595] to [5.1.2.0.373].
2019/09/20 13:08:31	302	AP rebooted by system	Major	AP [RuckusAP@38:FF:36:0B:3E:B0] was rebooted by the system because of [/usr/sbin/cubic application, cubic, reboot due to firmware change].
2019/09/20 13:06:39	106	AP firmware updated	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] updated its firmware from [5.1.0.0.595] to [5.1.2.0.373].
2019/09/20 13:04:09	108	Updating AP firmware...	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] firmware is being updated from [5.1.0.0.595] to [5.1.2.0.373].
2019/09/20 12:56:34	302	AP rebooted by system	Major	AP [RuckusAP@38:FF:36:0B:3E:B0] was rebooted by the system because of [/usr/sbin/cubic application, cubic, reboot due to ipmode change].
2019/09/20 12:54:13	302	AP rebooted by system	Major	AP [RuckusAP@38:FF:36:0B:3E:B0] was rebooted by the system because of [/usr/sbin/cubic application, cubic, reboot due to WLAN migration].
2019/09/20 12:52:22	301	AP rebooted by user	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] was rebooted because of [user set CLI command reboot].
2019/09/20 12:49:06	108	Updating AP firmware...	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] firmware is being updated from [104.0.0.0.1347] to [5.1.0.0.595].
2019/09/20 12:49:01	301	AP rebooted by user	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] was rebooted because of [user set CLI command reboot].
2019/09/20 12:49:00	312	AP connected	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] connected because of [AP connected after discovery].
2019/09/20 12:34:00	312	AP connected	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] connected because of [AP connected after discovery].
2019/09/20 12:33:50	103	AP managed	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] approved by Virtual SmartZone [192.168.183.47].
2019/09/20 12:33:48	101	AP discovery succeeded	Informational	AP [RuckusAP@38:FF:36:0B:3E:B0] sent a discovery request to Virtual SmartZone [192.168.183.47].

Group Info

Name	System	Total APs	1
Type	DOMAIN		

Access Points

AP Models

If there are any problems with the connection you can troubleshoot directly from the AP CLI level.

```
rkscli: get scg
------ SCG Information ------
SCG Service is enabled.
AP is managed by SCG.
State: RUN_STATE
Server List: 192.168.183.47
SSH tunnel connected to 192.168.183.47
Failover List: Not found
Failover Max Retry: 2
DHCP Opt43 Code: 6
Server List from DHCP (Opt43/Opt52): Not found
SCG default URL: RuckusController
SCG config|heartbeat intervals: 30|30
SCG gwloss|serverloss timeouts: 1800|7200
Controller Cert Validation : disable
-----------------------------
rkscli: get version
Ruckus R500 Multimedia Hotzone Wireless AP
Version: 5.1.2.0.373
rkscli: get sshtunnel
SSH tunnel service is enabled
SSH tunnel connected to 192.168.183.47
ToSforSSH tunnel: 0
CipherforSSH tunnel: 128
OK
```

Related Service See how we help businesses with our network engineering services:

Network Engineering We provide engineering services for over the whole lifecycle process. See more

Seeing an AP was a first success as I was not sure the EoL AP would be discovered without a problem on the newest software, but my concerns were unfounded. The next step was to create WLANs and verify traffic. Since my lab did not allow bridging traffic locally on the AP I used the same setup as with other wireless vendors – AP-based DHCP/NAT. In that configuration the AP runs a DHCP server locally and distributes IP addresses to connected clients, then customer traffic is locally NAT translated to the WAN interface IP address.

We need to enable DHCP and NAT service on the APs which is not running by default. There are three modes for doing that:

- on each APs – all access points in the domain will get IP from WAN router and can provide DHCP/NAT service.
- on selected APs – all access points in the domain will get IP from WAN router, but only selected ones will provide DHCP (maximum 2 devices) and NAT gateway (maximum 10 devices). Devices can be selected manually or a selection can be done by the system. I didn't find any configuration knob which would influence which device is selected for a

specific role.

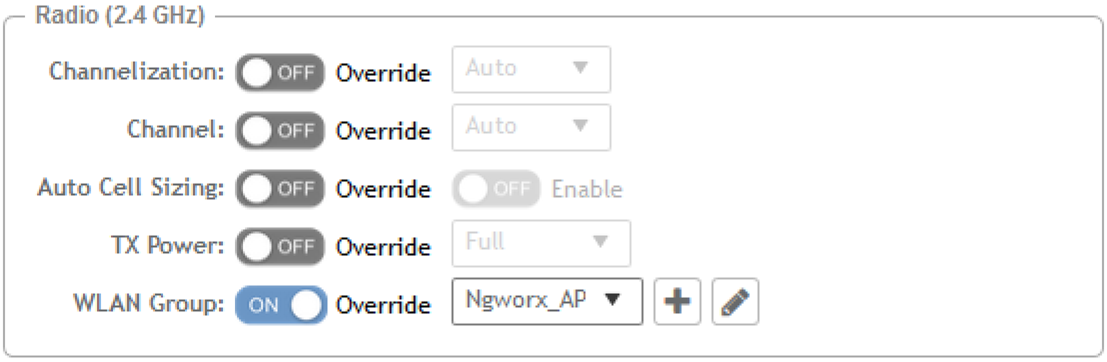
- on hierarchical APs – designated access points (gateway APs) in the domain will get an IP from the WAN router which provides the DHCP and NAT service. All non-designated APs will get an IP address from the gateway device.

The last mode is supported only on devices with more than one Ethernet port since the second port needs to be connected to the bridged network. A well-known mode for local bridging at the AP or sending traffic to the data plane device (GRE tunnel) is still there, I just had to use something more complex since it would be too easy to configure something I already know … and the fact that I could not use other options without redesigning the network.

The configuration is straightforward when admins understand all the modes, then it boils down to selecting a mode for the whole zone, designating DHCP pools (they would be tied together to the WLANs via the access VLAN) and if mode requires that, select APs and assign specific roles.

Proceed with the configuration of networks. Networks are created in the zones as the WLAN groups (WG) which then can be assigned within the zone to the access point groups (AG) to the specific radio band if you need to “override” the default AG. It was not obvious the first time I tried to do that but this could be my bias from previously tested solutions where all the settings were actually in one place, not like here:

- WG are in the “Wireless LANs”
- AG are in the “Access Points”



Radio (2.4 GHz)

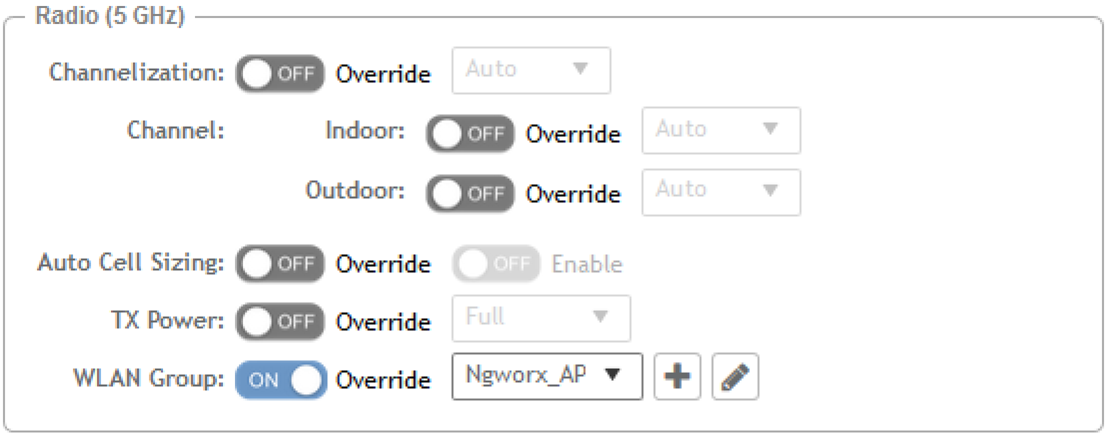
Channelization: OFF Override Auto

Channel: OFF Override Auto

Auto Cell Sizing: OFF Override OFF Enable

TX Power: OFF Override Full

WLAN Group: ON Override Ngworx_AP



Radio (5 GHz)

Channelization: OFF Override Auto

Channel: Indoor: OFF Override Auto

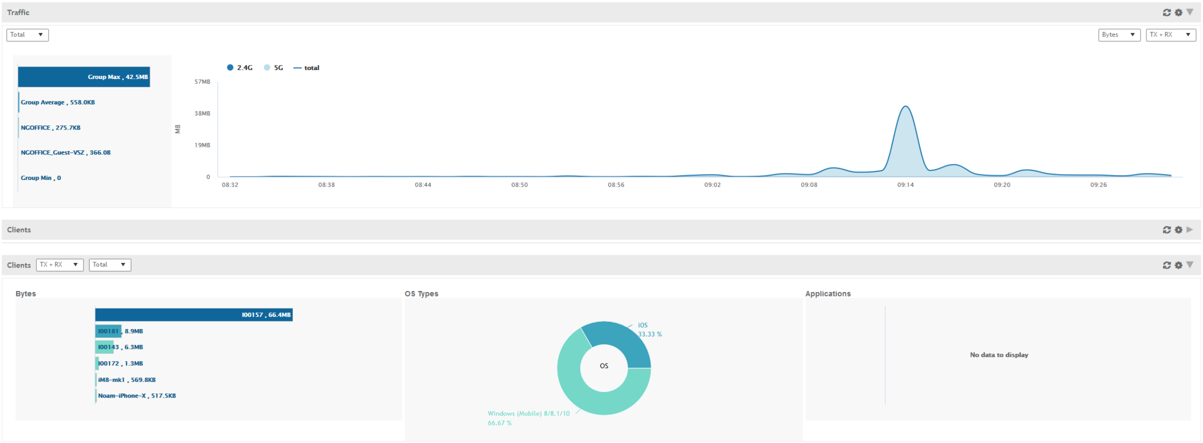
Outdoor: OFF Override Auto

Auto Cell Sizing: OFF Override OFF Enable

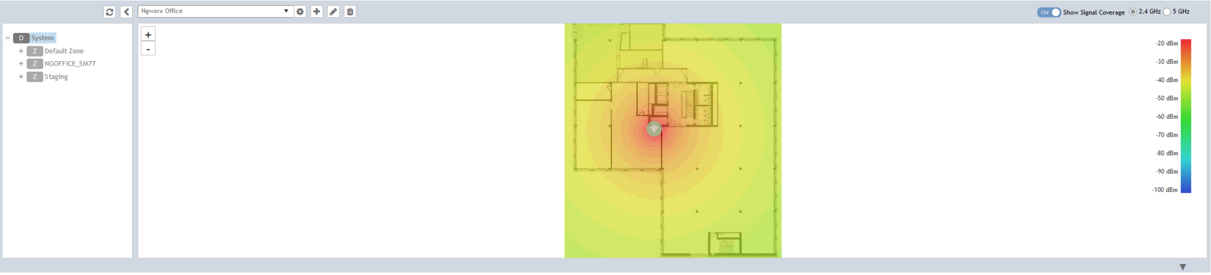
TX Power: OFF Override Full

WLAN Group: ON Override Ngworx_AP

If you want to create a Wireless LAN in a specific zone I advise you to select it before clicking the “create” button. I was surprised when you change zones in the configuration context all the fields are cleared. After everything is configured and a considerable amount of time has gone by we can call it a success. I already saw some devices connected, since I basically honey potted my colleagues into using this “new” network.

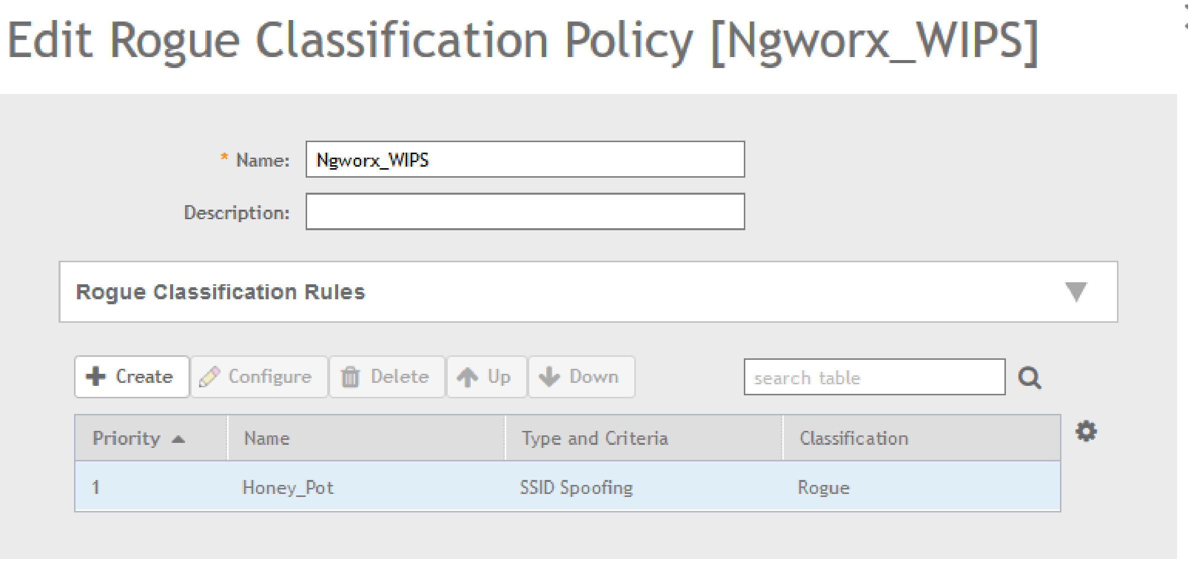


As a final touch, I added floor plan to the zone, so that I can put in there all my APs and have a nice “live” view.



Security

I was not able to find any dedicated radio for the frequency scanning. So, I assume all of it is done in parallel to the customer traffic which can limit network performance, or maybe some APs from the pool can be converted into a security scanner. Still, it is usable and enables the network to auto-heal in cases of interference (auto channel selection) and identifying rogue devices. Maybe the Ruckus solution is not as sophisticated as Arista (Mojo) but it is comparable to deploying Mist (and even have wider range of classification rules). I as well have the impression that it is still actively developed so this is not the last word from Ruckus. ☒ Sadly since I had only one device I did not test that fully but I saw that there are many options for the offending device classification, based on various characteristics.



Edit Rogue Classification Policy [Ngworx_WIPS]

* Name: Ngworx_WIPS

Description:

Rogue Classification Rules

Priority ▲	Name	Type and Criteria	Classification
1	Honey_Pot	SSID Spoofing	Rogue

Rules which we can currently apply for the classification are:

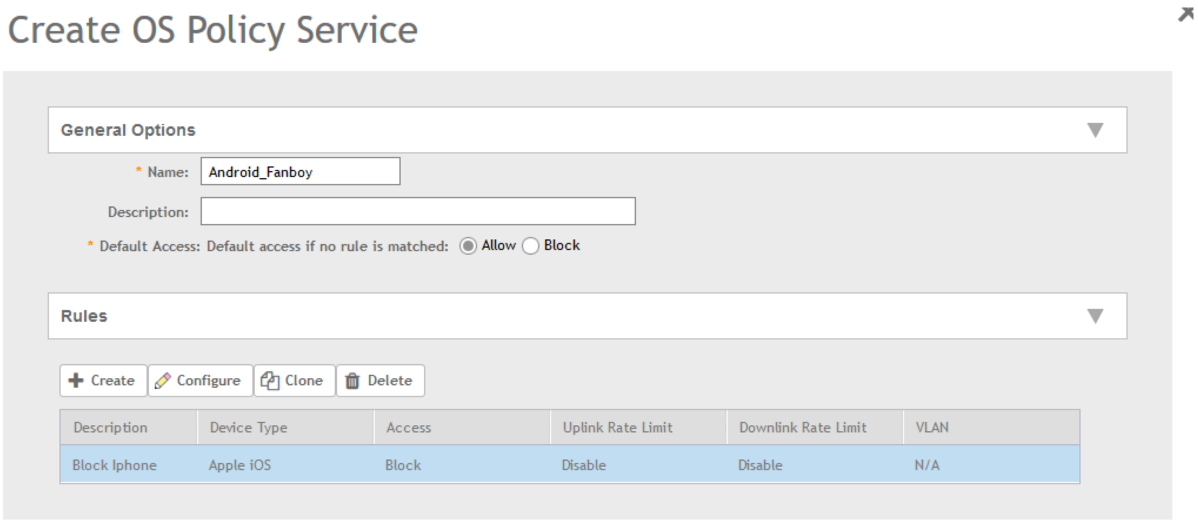
- Ad Hoc – monitoring AP can detect the ad hoc network as rouge
- CTS Abuse – used when the number of CTS frames per second to a specific receiver MAC address exceeds the specific threshold
- RTS Abuse – used when the number of RTS frames per second to a specific receiver MAC

address exceeds the specific threshold

- Deauth Flood – used when the number of de-authentication frames per second exceeds the specific threshold from a specific transmitter
- Disassoc Flood – used when the number of disassociation frames per second exceeds the specific threshold from specific transmitter
- Excessive Power – used when TX power exceeds the specific threshold from specific transmitter
- Low RSSI – used when RSSI (dBm) is below the specified threshold
- MAC OUI – can base APs based on the vendor MAC address
- BSSID Spoofing
- SSID Spoofing
- NULL SSID
- Specific SSD

There is a possibility to assign roles to the users or whole WLANs, which can limit usage or access to certain applications (in case of Ruckus, you can configure your own applications!), limit overall available bandwidth or incorporate URL filtering rules. Users are mapped to the roles via the authentication but to leverage that feature fully you would need central authentication since it would be hard to map users only based on PSK authentication.

One additional feature I'm not sure I saw during the previous testing was the OS Policy which allows admins to deny or allow access to the network based on the OS characteristics of the connecting device.



Create OS Policy Service

General Options

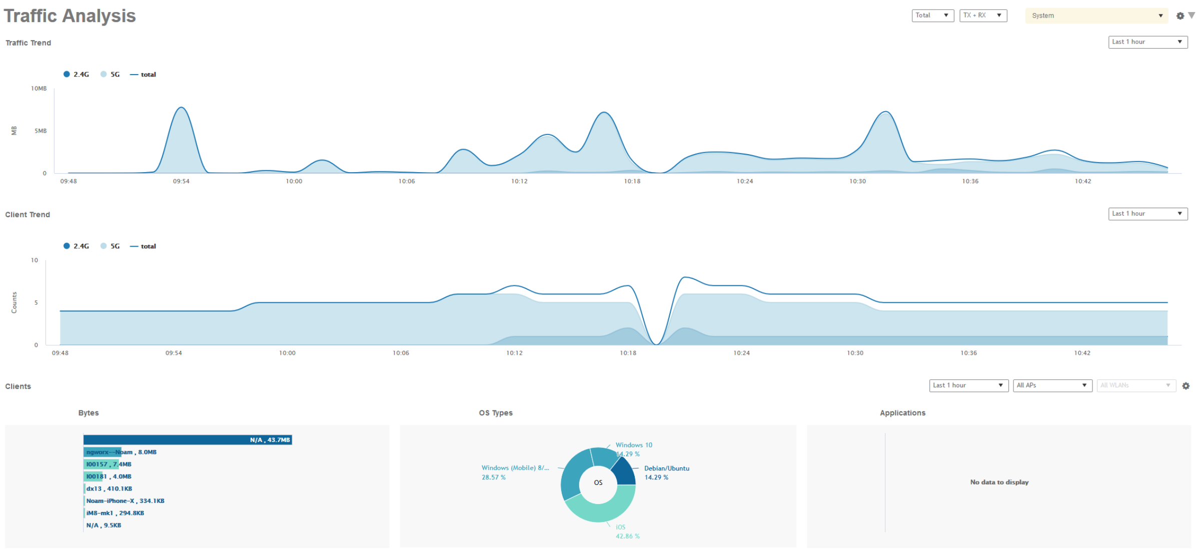
* Name:	Android_Fanboy
Description:	
* Default Access:	Default access if no rule is matched: ● Allow ○ Block

Rules

Description	Device Type	Access	Uplink Rate Limit	Downlink Rate Limit	VLAN
Block Iphone	Apple iOS	Block	Disable	Disable	N/A

Maintenance

As with all previous solutions maintenance mostly takes place from the dashboard.



Traffic Analysis

Total ▼ TX + RX ▼ System ▼

Traffic Trend

Last 1 hour ▼

Client Trend

Last 1 hour ▼

Clients

Last 1 hour ▼ All APs ▼ All WLANs ▼

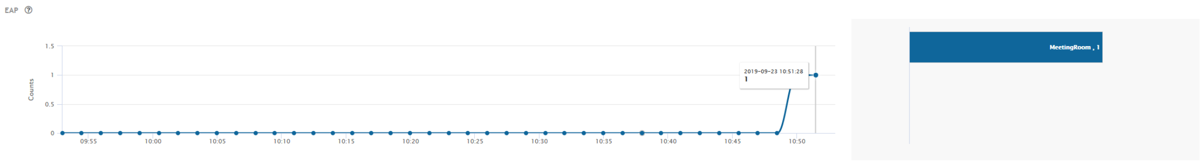
Bytes

OS Types

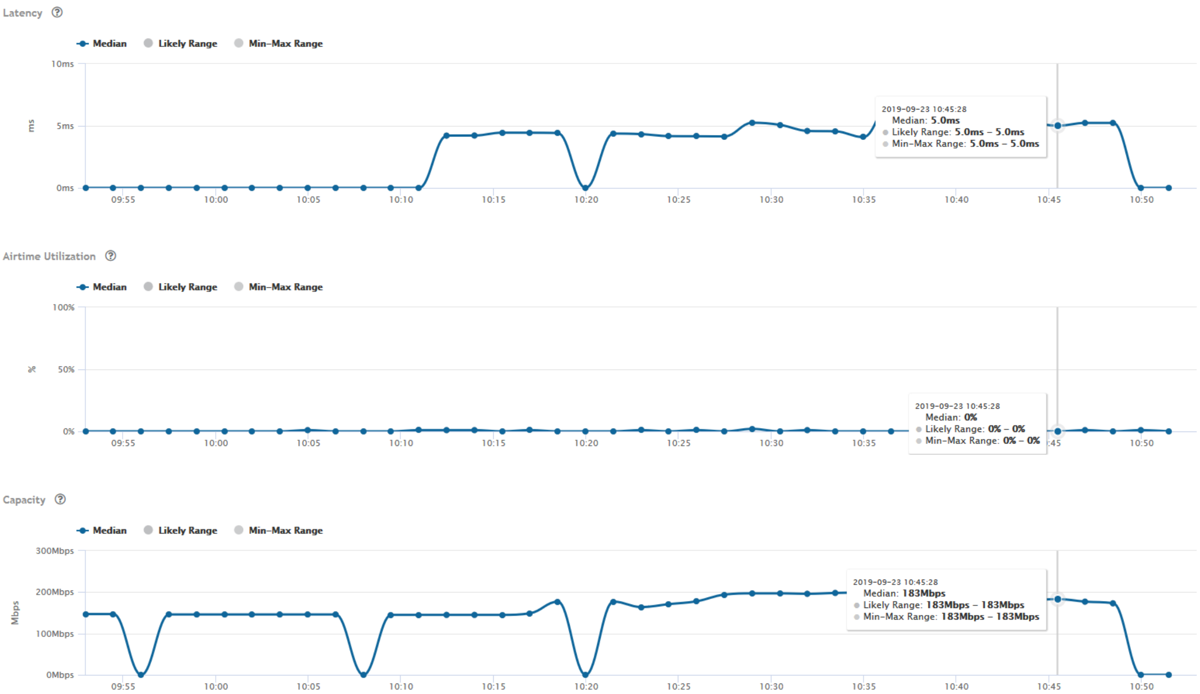
Applications

No data to display

Maybe it is not infused with AI and Machine learning which means that there won’t be pointers to exactly what can be wrong in your network and dynamically chaining KPIs, but still, all information needed is in one place. You can count on the aggregated data statistics and reasons for the most recent connection problems. Maybe it does not fit in with current minimalist standards of the web dashboard designs but to me, it is appealing and most information, which can be found in the other vendor’s solution, can be found on the vSZ dashboard. Maybe, a fine touch would be an option to modify its layout and size.



EAP



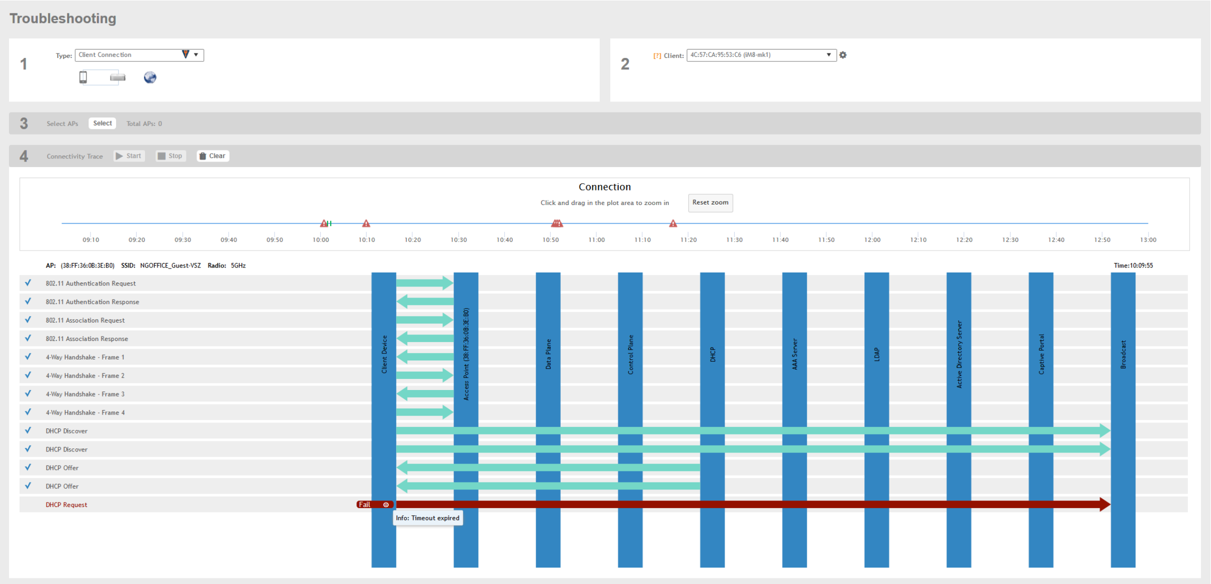
vSZ supports SNMP so you do not have to overhaul your monitoring. The controller should do all the monitoring for you and notifications can be implemented better then SNMP traps/informs, for example API or webhooks. I must mention you can configure SMTP for the events which would breach configured thresholds so SNMP is not the only option for monitoring controller state. In my opinion giving administrators freedom of choice is a plus and this shows Ruckus has experience and didn't have to start from scratch, but can reuse what they have created in their long history (for the industry standard).

Troubleshooting

The last point I want to mention about the vSZ capabilities is the troubleshooting of the client issues. There are multiple places where to look for information in cases of issues:

- in dashboard
- in clients tab
- in WLANs tab
- in access points tab

Maybe one thing I would really like to see would be quickly jump between places. Probably after a while, it gets natural but I was struggling at the beginning since I was used to hyperlinks. I constantly tried to go to the client summary information by clicking client on the table with all clients connected to a specific network. On the other hand, I cannot really say a bad word about the quality of the provided information, I think this is enough at least for initial troubleshooting and to quickly find common problems. You can as well see the historical data and event captures from live connectivity traces.



Troubleshooting

1 Type: Client Connection

2 [?] Client: 4C:57:CA:95:53:C6 (iM8-mk1)

3 Select APs Select Total APs: 0

4 Connectivity Trace ▶ Start ■ Stop Clear

AP: (38:FF:36:0B:3E:B0) SSID: NGOFFICE_Guest-VSZ Radio: 5GHz

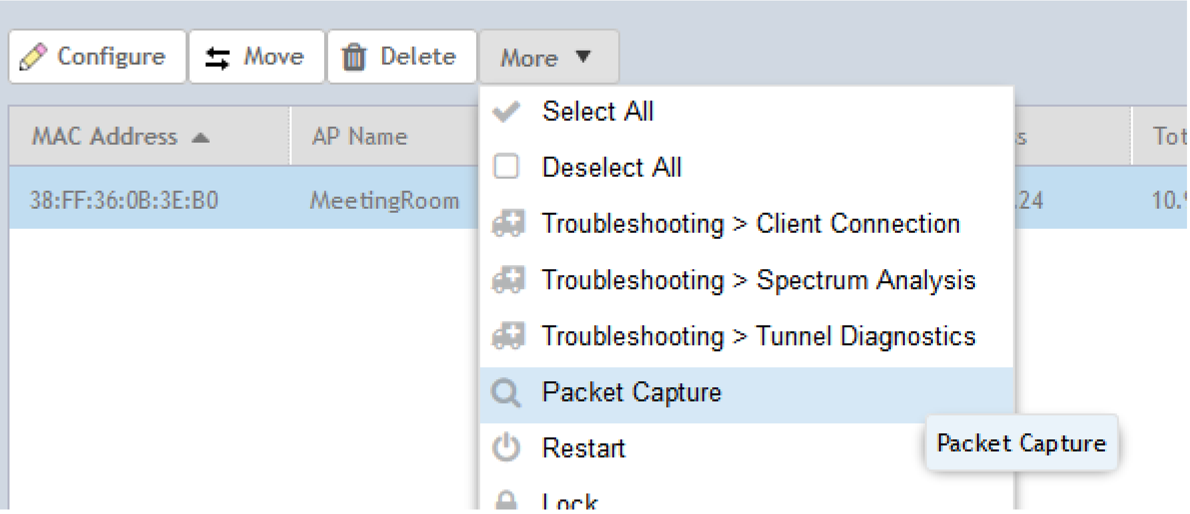
Time:10:09:55

✓ 802.11 Authentication Request
✓ 802.11 Authentication Response
✓ 802.11 Association Request
✓ 802.11 Association Response
✓ 4-Way Handshake - Frame 1
✓ 4-Way Handshake - Frame 2
✓ 4-Way Handshake - Frame 3
✓ 4-Way Handshake - Frame 4
✓ DHCP Discover
✓ DHCP Discover
✓ DHCP Offer
✓ DHCP Offer
DHCP Request

Fail

Info: Timeout expired

Packet captures are a good example of how troubleshooting is scrambled in different places. In the same place we can do client connectivity traces, spectrum analysis, and tunnel diagnostics so I would assume here you can as well initiate a packet capture from a specific AP. But in vSZ this option is in the AP context menu.



Configure
Move
Delete
More ▼
Select All
Deselect All
Troubleshooting > Client Connection
Troubleshooting > Spectrum Analysis
Troubleshooting > Tunnel Diagnostics
Packet Capture
Restart
Lock
Packet Capture

MAC Address ▲	AP Name	s	Tot
38:FF:36:0B:3E:B0	MeetingRoom	.24	10.'

Final thoughts

As with the previous tests I was working a lot with the vendor’s documentation and it was different I would not say worse, don’t get me wrong, but I was already used to previous vendors. I can say, if you worked before a lot with the switching or routing platforms documentation, it is the same flavour. I would be glad to see some online training or care packages for people new to the solution, I was just spoiled by Mist and Mojo, that I could just spend few hours watching or reading all important information in one batch and then just research additional features if needed. I must say I was afraid when I started this test since I had no big experience with the controller based solutions, I was expecting this to be tiresome and I would actually hit a lot of limitations, but it wasn’t so bad. If I had more time and had to work on it on a daily basis, I think we could become a good “virtual” friends with vSZ. So in the end, what everyone was waiting for … bullet point summary!

What I did not like:

- Look and feel of the WebGUI makes an impression it is for more experienced admins
- I actually did not enjoy working with the documentation, it took me a while to adapt (but as I said, I was biased by the previous tests)
- No dedicated scanning radio (or I just was not able to find that)*

What I liked:

- That there is a possibility to manage both switches and AP (Arista is working on a similar approach but it was not ready at the time of the test)
- It is a solid solution with strong foundations
- Decoupled control and data plane
- Ruckus is really implementing constantly new features to not be left behind (they of course as well have own patents, but are aware of the changing market)
- Option to “cloudify” your wireless setup in the public or private cloud, freedom of environments
- Good alternative to the subscription model
- Wide AP portfolio
- Ruckus managed to have all features that competition have (of course implementation varies)

** I saw an option for the “monitoring APs”, I thought that this could mean, that admins can turn some APs to be security or performance monitoring devices, but I was not able to configure it or find more information to clearly define how it works.*

Abbreviations

NFV	Network Function Virtualization
RBAC	Role-Based Access Control
RTU	Right-to-Use license
SCG	SmartCell Gateway
vSZ-D	virtual SmartZone – Data Plane
vSZ-E	virtual SmartZone – Essentials
vSZ-H	virtual SmartZone – High Scale