

Dynamic VLAN via Microsoft 2012 R2 NPS Server

<https://community.ui.com/questions/Dynamic-VLAN-via-Microsoft-2012-R2-NPS-Server/a869664e-dca4-42d7-a901-525b56df9330>

We currently are using UniFi AP's with controller 5.3.8.2.

Is it possible to have Microsoft 2012 R2 NPS Server assign Dynamic LAN's to clients that connected to the AP's?

Responses (18)

Sort by

Page

1

[redfive](#)

[7 years ago](#)



Take a look [here](#) and [here](#) Cheers, jonatha



0

[C](#)

[CDIMP](#)

[7 years ago](#)



Thank you for the response.

I have been able to configure successfully the RADIUS portion of the setup, but have been unsuccessful in the Dynamic VLAN portion.

The solution in the link was for FreeRADIUS. However, I may be able to utilize the following settings and see where that goes.

Framed-Protocol : PPP

Service-Type : Framed

Termination-Action : RADIUS-Request

Tunnel-Medium-Type : 802

Tunnel-Pvt-Group-ID : (VLAN number, as an octet string)

Tunnel-Type : VLAN

■

0

[redfive](#)

[7 years ago](#)

■

Yes, the solution is for freeradius because the 3d is on freeradius, but the post I linked (first link) should be for windows NPSCheers,jonatha

■

0

[C](#)

[CDIMP](#)

[7 years ago](#)

■

It is for NPS and that is working as expected, but not for Dynamic VLAN.

■

1

B

[bmartindcs](#)

[7 years ago](#)

■

I'm having same issue.

Server 2012R2

Unifi AP-AC-PRO running 3.7.21.5389

Unifi Controller running 5.2.9

I've got Radius working fine with NPS as long as I don't try to use Dynamic VLAN via Radius.

Radius Attributes I add are:

Tunnel-Pvt_Group-ID = <VLAN I WANT>

Tunnel-Type = Virtual LANs (VLAN)

Tunne-Medium-Type = 802

Enabled Radius Assigned VLAN within Unif Controller.

Looking at logs with debug mode on, on the AP, I see that Radius completes, and the AP understand that the client should be getting the correct VLAN as per the following being logged:

```
Jan 15 13:09:05 UBNT user.warn kernel: [ 3262.410000] ieee80211_ioctl_setparam: VLANID32 = <CORRECTVLANHERE>
```

However, client doesn't get DHCP. I statically set the IP on the device and no change. Enabled port mirroring on the switch port that the AP connects to, and wiresharked that traffic, and never see any packets coming from the client computer in question (looked via IP and/or MAC address). Almost seems like the endpoints are put into limbo within the AP after RADIUS handshaking is completed.

Behavior is same regardless if it's an Android phone, or 2 different Windows 10 wireless laptops.

I've also simply tried communicating (ping, etc) between the 2 laptops, with static IP's set, that should be on the same VLAN (and show as such via AP logs handshaking results, like what I listed above), and they can't communicate with eachother.

I've also SSH into the AP, run tcpdump wide open (not restricted to a specific interface) and see zero of the traffic attempting to be generated from either of the laptops.

I'm testing this with only a single SSID for simplicity. I've tried differing VLAN's too, no change. Wired devices do not have any issue, it's only wireless devices behind the AP.

Only thing I've found from others with same behavior is regarding FreeRadius and needing to enable "use_tunneled_reply = yes" to solve the problem, however I don't know how to do that within NPS or if that's even possible.

■

0

C

CDIMP

7 years ago

■

I have tried all kinds of options ad can only get it to work with static VLAN for the SSID.

Does the port and switch that is connected to the AP have the VLAN trucking.

My initial thought is maybe the switch is stripping the tag.

■

0

B

[bmartindcs](#)

[7 years ago](#)

■

The switch is trunked on those VLANs.

The switch isn't stripping the VLAN tags, as I've wiresharked the feed from the AP and see ZERO traffic from the devices once they are assigned vlan via Radius. In addition, besides wiresharking, I've also ran TCPDUMP directly on the wireless access point and also see ZERO traffic from the devices once they are assigned the dynamic vlan via radius.

It's not the switch. It's like the AP puts the devices into some kind of limbo/jail.

If I go back to static VLAN per SSID, it works fine.

■

0

C

[CDIMP](#)

[7 years ago](#)

■

Didn't think it was just wanted to verify.

Your issue is the exact issue I have as well.

Until they fix this issue or give me an official response as to what's going on, I've needed to look at other vendors to expand my wifi network.

The only resolution that I came up with was multiple SSID's with static VLAN and have the switch segregate the traffic. This is only temporary until I replace the AP's with something else that supports dynamic VLAN and I can get actual support outside of Forums.

■

0

G

greid

7 years ago

■

I am in the exact same place. Was hoping to use Ubiquiti to expand.

■

0

K

Kedare

6 years ago

■

I am having exactly the same issue here.

Were you able to find any way to fix it ?

This is what I get on the AP in the logs (Vlan 101)

```
Jan 31 13:17:28 BCN-WAP-2 daemon.info hostapd: ath8: STA 78:4f:43:62:9a:d3 IEEE 802.1X: authenticated - EAP t
```

And the RADIUS Response:

```
Frame 280: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) on interface 0Ethernet II, Src: Microsof_f
```

Thanks

■

0

A

audio-catalyst

6 years ago

■

i have this running without issues on the latest beta controller and latest beta firmware, but it has been running like this since it first came out.

things to verify :

are all vlans trunked to the ap ?

is you ias log actually returning tge vlan value ?

have you removed under networks any ref. networks that have the same vlan tag ?

■

0

K

Kedare

6 years ago

■

VLANs trunked correctly (As other SSID's are using them already)

The IAS logs return the VLAN (can be seen on the packet capture and on the AP's logs too)

The network work fine when I fix the value as fixed vlan (so 2 SSID's with the same VLAN on the same AP, so I don't think this would be the issue?)

■

0

K

Kedare

6 years ago

■

I updated to the beta one also. No changes so far, I have exactly the same behaviour.

■

0

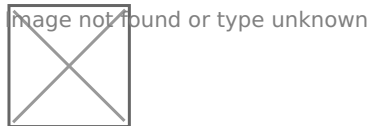
A

[audio-catalyst](#)

[6 years ago](#)

■

these are my working settings on one of the NPS servers :



furthermore, make sure that in your controller, under networks, no networks with vlans that are being given by the NPS excists

■

0

[waterside](#)

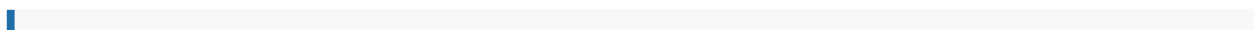
[6 years ago](#)

■

wrote:VLANs trunked correctly (As other SSID's are using them already)

Do you mean you have other SSIDs using the same VLAN as a static assignment? That specifically is documented to be an invaild configuration.

RADIUS-assigned VLANs can not be also statically assigned to SSIDs. This has been in the release notes for a long time:



- You cannot re-use a VLAN ID for dynamic VLAN if it is set as a static value for another SSID on the same AP. So, if I have a SSID set to use VLAN 10, I cannot use VLAN ID 10 for RADIUS controlled VLAN users as those users will not get an IP.

■

0

K

Kedare

6 years ago

■

Looks like this would be the issue, as the same VLAN are still used in the "to be legacy" SSID's

■

0

K

Kedare

6 years ago

■

I confirm that was the issue, removing the legacy SSID and it worked instantly

■

0

langella

6 years ago

■

Sorry for bringing this back but I'm having the same issue and I don't understand why I have to remove the network VLAN with same VLAN ID that NPS is given. If I delete it how am I supposed to configure DHCP?

I'm sure I am missing something here because does not make any sense.. hahahah

Revision #1

Created 5 January 2024 04:52:55 by ColtM

Updated 7 August 2024 23:24:39 by ColtM