某局点WX3510H-F MAC认证无线终端频繁下线的经验案例

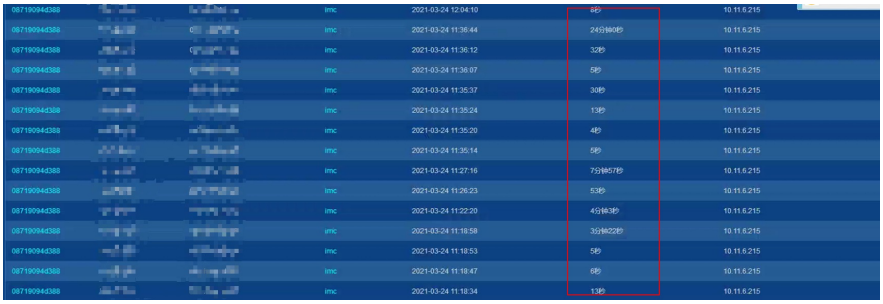
wlan安全 张腾 2021-03-30 发表

组网及说明

无线控制器对接IMC做MAC地址认证

问题描述

IMC上看到同一用户频繁上下线，导致业务无法正常使用



过程分析

1、核对设备以及IMC侧配置没问题

2、采集设备侧debug信息发现大量用户存在短时间内认证次数达到IMC设置的阈值而导致认证失败的现象

*Mar 24 11:06:44:451 2021 HFEPC-AC-WX3510 RADIUS/7/PACKET:

User-Name="34de1a7911e8"

User-Password=******

Service-Type=Call-Check

Framed-Protocol=PPP

NAS-Identifier="HFEPC-AC-WX3510"

NAS-Port=16779316

NAS-Port-Type=Wireless-802.11

NAS-Port-

Calling-Station-

Called-Station-

H3c-Nas-Startup-Timestamp=1601632549

Acct-Session-

H3c-User-Vlan-Id=2100

H3c-Ip-Host-Addr="0.0.0.0 34:de:1a:79:11:e8"

NAS-IP-Address=10.11.72.230

H3c-Product-

*Mar 24 11:06:44:452 2021 HFEPC-AC-WX3510 RADIUS/7/PACKET:

01 b1 01 15 75 9d 54 b4 d2 6c 5c b8 79 5a 93 ff //**设备发送code 1认证请求报文**

45 5d 55 24 01 0e 33 34 64 65 31 61 37 39 31 31

65 38 02 12 2f 91 f1 10 e4 be 10 92 62 58 b6 20

90 96 51 4d 06 06 00 00 00 0a 07 06 00 00 00 01

20 11 48 46 45 50 43 2d 41 43 2d 57 58 33 35 31

30 05 06 01 00 08 34 3d 06 00 00 00 13 57 12 30

31 30 30 30 30 30 30 30 30 30 30 32 31 30 30 1f

13 33 34 2d 44 45 2d 31 41 2d 37 39 2d 31 31 2d

45 38 1e 19 39 43 2d 45 38 2d 39 35 2d 39 46 2d

33 32 2d 45 30 3a 68 66 65 70 63 1a 0c 00 00 63

a2 3b 06 5f 76 f9 25 2c 28 30 30 30 30 30 30 30

34 32 30 32 31 30 33 32 34 31 31 30 36 34 34 30

31 34 36 64 37 63 38 30 38 31 30 30 34 30 34 1a

0c 00 00 63 a2 85 06 00 00 08 34 1a 21 00 00 63

a2 3c 1b 30 2e 30 2e 30 2e 30 20 33 34 3a 64 65

*Mar 24 11:06:44:453 2021 HFEPC-AC-WX3510 RADIUS/7/PACKET:

3a 31 61 3a 37 39 3a 31 31 3a 65 38 04 06 0a 0b

48 e6 1a 13 00 00 63 a2 ff 0d 48 33 43 20 57 58

33 35 31 30 48

*Mar 24 11:06:44:453 2021 HFEPC-AC-WX3510 RADIUS/7/PACKET:

Reply-Message="E63620: The request is dropped by UAM because of 21 consecutive authentication failures. Please try again 1 minutes later." 由于短时间内认证次数达到IMC设置的阈值，所以IMC回复code3认证失败的报文

*Mar 24 11:06:44:454 2021 HFEPC-AC-WX3510 RADIUS/7/PACKET:

03 b1 00 90 b2 fb 0b fb 58 94 ee 92 66 ce 43 f0 //**IMC回复code3认证拒绝报文**

8e e8 94 2c 12 7c 45 36 33 36 32 30 3a 20 54 68

65 20 72 65 71 75 65 73 74 20 69 73 20 64 72 6f

70 70 65 64 20 62 79 20 55 41 4d 20 62 65 63 61

75 73 65 20 6f 66 20 32 31 20 63 6f 6e 73 65 63

75 74 69 76 65 20 61 75 74 68 65 6e 74 69 63 61

74 69 6f 6e 20 66 61 69 6c 75 72 65 73 2e 20 50

6c 65 61 73 65 20 74 72 79 20 61 67 61 69 6e 20

31 20 6d 69 6e 75 74 65 73 20 6c 61 74 65 72 2e

3、MAC地址认证和802.1X认证都是准入认证，在终端漫游后都需要重新认证，因此怀疑终端频繁漫游导致频繁认证，在AC上查看某一终端的漫游轨迹，发现确实存在频繁漫游的现象

display wlan mobility roam-track mac-address 0871-9094-d388

Total entries: 54

Current entries: 54

BSSID Created at Online time AC IP address RID AP name

9ce8-959f-4c10 2021-03-24 12:19:59 00h 08m 48s 127.0.0.1 2 y1f03
307b-acd5-6670 2021-03-24 12:17:32 00h 02m 27s 127.0.0.1 2 y2f05
9ce8-959f-4c10 2021-03-24 12:14:30 00h 03m 02s 127.0.0.1 2 y1f03
307b-acd5-6b70 2021-03-24 12:13:31 00h 01m 00s 127.0.0.1 2 y2f05
9ce8-959f-89d0 2021-03-24 12:12:56 00h 00m 35s 127.0.0.1 2 y3f03
9ce8-959f-4c10 2021-03-24 11:54:38 00h 18m 17s 127.0.0.1 2 y1f03
9ce8-9592-6670 2021-03-24 11:54:24 00h 00m 15s 127.0.0.1 2 y2f04
9ce8-9592-6680 2021-03-24 11:54:18 00h 00m 04s 127.0.0.1 3 y2f04
9ce8-959f-32f0 2021-03-24 11:54:13 00h 00m 05s 127.0.0.1 2 y3f07
9ce8-959f-6170 2021-03-24 11:54:02 00h 00m 10s 127.0.0.1 2 y4f08
9ce8-959e-d510 2021-03-24 11:53:46 00h 00m 17s 127.0.0.1 2 y4f02
9ce8-959f-6170 2021-03-24 11:53:34 00h 00m 12s 127.0.0.1 2 y4f08
88df-9e1f-8690 2021-03-24 11:53:25 00h 00m 08s 127.0.0.1 2 y4f01
9ce8-9592-6680 2021-03-24 11:53:20 00h 00m 05s 127.0.0.1 3 y2f04
9ce8-9592-6b10 2021-03-24 11:53:12 00h 00m 08s 127.0.0.1 1 y6f03
9ce8-9592-6b20 2021-03-24 11:53:07 00h 00m 05s 127.0.0.1 2 y6f03
dcda-8005-3b60 2021-03-24 11:52:58 00h 00m 09s 127.0.0.1 1 y1f06
88df-9e93-d290 2021-03-24 11:25:32 00h 27m 26s 127.0.0.1 3 y2f02
dcda-8005-3b60 2021-03-24 11:25:00 00h 00m 32s 127.0.0.1 1 y1f06
9ce8-9592-6b30 2021-03-24 11:24:55 00h 00m 05s 127.0.0.1 3 y6f03
9ce8-959f-6410 2021-03-24 11:24:25 00h 00m 30s 127.0.0.1 2 y3f02
9ce8-959f-8570 2021-03-24 11:24:13 00h 00m 12s 127.0.0.1 2 y3f04
9ce8-959f-8560 2021-03-24 11:24:09 00h 00m 05s 127.0.0.1 1 y3f04
9ce8-959f-5f30 2021-03-24 11:24:02 00h 00m 06s 127.0.0.1 2 y4f09
9ce8-959f-4c10 2021-03-24 11:16:04 00h 07m 58s 127.0.0.1 2 y1f03
9ce8-9592-6660 2021-03-24 11:15:12 00h 00m 53s 127.0.0.1 1 y2f04
307b-acd5-6670 2021-03-24 11:11:09 00h 04m 02s 127.0.0.1 2 y2f05
9ce8-959f-4c10 2021-03-24 11:07:47 00h 03m 23s 127.0.0.1 2 y1f03
307b-acd5-38c0 2021-03-24 11:07:42 00h 00m 05s 127.0.0.1 1 y1f05
9ce8-959f-69b0 2021-03-24 11:07:36 00h 00m 05s 127.0.0.1 2 y3f09
88df-9e93-a200 2021-03-24 11:07:23 00h 00m 14s 127.0.0.1 3 y2f03
88df-9e93-d290 2021-03-24 11:07:14 00h 00m 08s 127.0.0.1 3 y2f02
88df-9e93-d270 2021-03-24 11:07:09 00h 00m 06s 127.0.0.1 1 y2f02
88df-9e1f-8690 2021-03-24 11:06:57 00h 00m 11s 127.0.0.1 2 y4f01
dcda-8005-3b70 2021-03-24 10:58:40 00h 08m 17s 127.0.0.1 2 y1f06
88df-9e93-d290 2021-03-24 10:55:39 00h 03m 01s 127.0.0.1 3 y2f02
9ce8-959f-89d0 2021-03-24 10:52:49 00h 00m 10s 127.0.0.1 2 y3f03
9ce8-9592-6660 2021-03-24 10:52:36 00h 00m 13s 127.0.0.1 1 y2f04
9ce8-959f-4c00 2021-03-24 10:52:31 00h 00m 05s 127.0.0.1 1 y1f03
307b-acd5-6670 2021-03-24 10:50:16 00h 02m 15s 127.0.0.1 2 y2f05
9ce8-959f-4c10 2021-03-24 10:49:32 00h 00m 44s 127.0.0.1 2 y1f03
9ce8-959f-5f30 2021-03-24 10:48:24 00h 01m 07s 127.0.0.1 2 y4f09
9ce8-959e-d4d0 2021-03-24 10:48:14 00h 00m 10s 127.0.0.1 2 y4f03
9ce8-959f-6410 2021-03-24 10:47:53 00h 00m 22s 127.0.0.1 2 y3f02
dcda-8005-3b70 2021-03-24 10:43:37 00h 04m 15s 127.0.0.1 2 y1f06
9ce8-959f-4c10 2021-03-24 10:39:16 00h 02m 40s 127.0.0.1 2 y1f03
9ce8-959f-4c00 2021-03-24 10:38:51 00h 00m 26s 127.0.0.1 1 y1f03
9ce8-959f-4c00 2021-03-24 10:38:49 00h 00m 01s 127.0.0.1 1 y1f03
9ce8-959f-4c00 2021-03-24 10:37:37 00h 00m 51s 127.0.0.1 1 y1f03
9ce8-959f-4c00 2021-03-24 10:37:35 00h 00m 02s 127.0.0.1 1 y1f03
9ce8-959f-4c00 2021-03-24 10:35:58 00h 00m 18s 127.0.0.1 1 y1f03
9ce8-959f-4c00 2021-03-24 10:33:21 00h 02m 34s 127.0.0.1 1 y1f03
307b-acd5-6660 2021-03-24 10:33:15 00h 00m 06s 127.0.0.1 1 y2f05
9ce8-959f-4c00 2021-03-24 10:33:01 00h 00m 14s 127.0.0.1 1 y1f03

解决方法

优化每个AP射频口发射功率，尽量保证AP间信号不重叠，2.解决终端频繁漫游的问题，MAC认证终端频繁下线的问题迎刃而解。