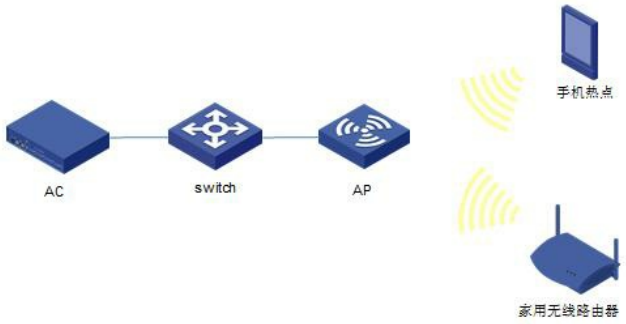
WIDS扫描无线热点干扰典型配置举例

WIDS wlan优化 殷俊 2017-09-28 发表

在公共wifi使用场景中，特别是大型会展、机场候机厅、火车站候车厅、体育馆等场所，wifi信号数量不可控，存在大量wifi信号。如公共场所的多厂家wifi设备部署、商铺办公私设无线路由器、用户私设手机热点等。大量wifi信号的存在导致干扰严重，严重影响用户体验。特别是在无线WLAN网络高密覆盖场景，无线资源更加紧张。

对于这种wifi信号较多的场景，大多数客户是通过在现场通过wifi扫描软件采集现场存在的wifi信号信息，而这些信息可能随着用户实际使用行为动态变化，不可能时时刻刻守在现场扫描。因此，我司无线可以通过WIDS模块让AP对周遭环境进行无线网络扫描，只需远程监控就可采集现场实际存在的wifi信号，评估干扰源。



1.配置WIDS扫描监控

#进入系统视图

<AC> system-view

配置AP的工作模式为Monitor模式，即此时AP仅做监测AP（对非法设备进行检测），不做接入AP。

[AC] wlan ap ap model WA4620i-ACN

[AC-wlan-ap-ap] serial-id 210235A29G007C000022

[AC-wlan-ap-ap] work-mode monitor

[AC-wlan-ap-ap] radio 1

[AC-wlan-ap-ap-radio-1] radio enable

[AC-wlan-ap-ap-radio-1] radio 2

[AC-wlan-ap-ap-radio-2] radio enable

配置规则，添加允许厂商列表的AP的OUI,一般配置为添加我司无线AP的OUI，根据客户具体需求，也可以添加其他设备作为信任的OUI（Organizational Unique Identifier，全球统一标识符），OUI参数被定义为一个固定的16进制数字符串，该列表最多可配置64条。

<AC> system-view

[AC] wlan ids

[AC-wlan-ids] device permit vendor 3891d5

[AC-wlan-ids] device permit vendor 487ada

配置规则，添加允许SSID列表的SSID，为1～32个字符的字符串，区分大小写。最多可配置256条。

[AC-wlan-ids] device permit ssid H3C

2.验证WIDS扫描监控结果

显示检测到的rogue AP信息。

<AC>dis wlan ids detected rogue ap

Total Number of Entries : 111

#AP = number of active APs detecting, Ch = channel number

Detected Rogue AP(s) List

MAC Address Vendor #AP Ch Last Detected SSID

000a-eb89-3fab Shenzhen T... 7 9 2016-09-05/14:45:32 "测试网"

0019-8851-ae34 Wi2Wi, Inc 5 1 2016-09-05/14:45:31 "dmngpro-dee933"

001d-43b0-176c Others 2 6 2016-09-05/14:41:46 "LCP0039"

009a-cd54-7620 Others 5 10 2016-09-05/14:45:27 "zj24hours-2"

00d0-ca00-0962 INTRINSYC ... 2 1 2016-09-05/14:36:59 "Eyesir_00274"

00d0-ca00-09e8 INTRINSYC ... 6 1 2016-09-05/14:45:31 "Eyesir_00276"

04a1-517f-da8a Others 7 44 2016-09-05/14:45:22 "NETGEAR94-5G"

0857-0065-895e Others 6 1 2016-09-05/14:45:31 "TVB_WiFi"

……..

字段	描述
MAC Address	检测到的client端的MAC地址
Vendor	检测到的client端厂商
#AP	检测到该设备的AP数 如果在多个AP上开启了WIDS功能，那么有可能出现多个AP都检测到某一个设备的设备类型
Ch	最后一次检测到该设备的信道
Last Detected Time	最后一次被检测到的时间
SSID	用来标识ESS的SSID

在功能一般用在无线wifi信号较多的高密部署场景，AP在做扫描监控时不建议同时作为无线业务接入，同时运行时对无线接入性能影响较大。一般建议在这类场景单独部署一台AP用来做扫描监控。
在配置WIDS允许列表时，需要提前搜集当前已部署的我司无线设备OUI以及可能涉及到的其他厂商OUI或者mac，配置到允许列表，以防止误扫为rogue ap。