

验证Wi-Fi吞吐量：测试和监控指南

目录

[简介](#)

[情景](#)

[定义最大预期吞吐量](#)

[建立基准体验](#)

[寻找体验的偏差](#)

[查找问题证据（被动测试）](#)

[1. Cisco Catalyst Center上的客户端保证控制面板](#)

[2. Cisco Catalyst Center上的网络保证控制面板和设备360](#)

[3.人工智能分析](#)

[主动测试基础设施](#)

[排除吞吐量问题](#)

简介

本文档介绍如何监控大型Wi-Fi网络中的吞吐量问题并对其进行故障排除。

情景

在Wi-Fi网络中，没有太多类型的最终用户察觉到了问题。

报告问题的范围可以是：

- 客户端无法连接；
- 客户端突然断开或；
- 用户设备上的应用的感知速度并不令人满意。

在这些简单的症状背后，可能有数百种问题，其中大多数甚至都不涉及实际的Wi-Fi网络，如DNS问题、互联网连接问题等。

管理服务器（如Cisco Catalyst Center）可帮助管理员解决特定问题，本文不会详细介绍可通过Catalyst Center轻松查看和修复的许多类型的日常问题。相反，本文档重点介绍最终用户提供的网络速度较慢的比较模糊的反馈。

如何测试？如何验证整个网络的实际吞吐量？如何将速度与速度相关的问题分类成可操作的项目以改善整体最终用户体验？

这些都是本文档试图回答的问题。

定义最大预期吞吐量

每个网络的第一个问题是：实际可行的潜在最大速度是多少？

由于Wi-Fi是共享介质，因此所体验的速度直接取决于同一信道上同时使用Wi-Fi的客户端和设备的数量。因此，实际可达到的最大速度问题直接意味着在安静的隔离位置有一个客户端设备和单个接入点，而在此位置没有人使用同一Wi-Fi信道。在这些情况下，确定最大速度的因素可归结为：

- 使用的Wi-Fi协议(Wi-Fi 5、Wi-Fi 6、...)
- 客户端和接入点的硬件功能（天线数、空间流数、接入点的以太网连接等）
- 配置（通道宽度，...）

了解这些因素后，您便可以估计出在实验室条件下实际吞吐量可以达到的最大值。

为了快速了解情况，您需要检查客户端报告连接到接入点的数据速率。此数据速率并非您在测试中可以证明的实际吞吐量。这是因为Wi-Fi是半双工介质，具有一些管理开销（需要确认帧，需要传输信标），并且帧之间的静音时间较短，因此能够更好地接收和解码。这意味着，发送数据时，数据会以记录的数据速率发送，但数据并不总是发送。管理和控制帧以低得多的数据速率发送，以确保接收。估计可以考虑达到实际吞吐量测试中使用的数据速率的65%至70%。例如，如果您的客户端报告已连接且正在以866Mbps的速度发送数据，则实际测试必须报告传输速度约为600Mbps。

如果您知道正在使用的配置参数以及涉及的设备的硬件功能，您还可以计算出必须达到的最大数据速率（因此通过使用本节中记录的百分比计算得出的吞吐量）。

如果报告的数据速率与您希望达到的速率不匹配，可以通过配置开始故障排除过程，并验证各种参数以了解差距所在的位置。

一个示例：如果您拥有接入点型号C9120在5Ghz频段以20Mhz信道宽度进行广播和典型的2空间流Wi-Fi 6客户端，则可以计算在非常干净的RF（射频）环境中，使用单个客户端在单个文件传输中可能实现160至200Mbps的速率。

有关吞吐量测试和验证的详细信息记录如下

：<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/212892-802-11ac-wireless-throughput-testing-and.html>。

建立基准体验

了解在典型情况下您的场所可能会出现什么情况非常重要。通常情况下，技术人员在部署开始前会先访问空站点，进行速度测试并记录预期数量。

然后员工或客户进来，网站变得繁忙，实际体验也大不相同。

部署启动后，一个聪明的想法是派遣技术人员测量每个领域的实际体验，并记录网络在平均正常运行时的样子。

这包括网络在令人满意的水平运行时每个无线电设备的平均客户端数量，以及通过速度测试获得的平均吞吐量。

寻找体验的偏差

在运行网络时，可以轻松监控重大警报或突然关闭的设备。本文档重点介绍难点：如何发现仍在运行但提供欠佳最终用户体验的无线网络。

查找问题证据 (被动测试)

您已经亲自测试了您的网络；您知道它运行良好，并且您正在监控管理系统和仪表板。没有任何故障报告：您可以退后一步，放松一下。还是你能？

如果你等待那些抱怨体验不佳的最终用户的回应，你可能会为时已晚。当最终用户投诉时，问题已经持续了很长时间，您只会听到少数用户的声音，而他们发出的声音足够让您听到。

无数用户已经感到沮丧，对您或您的帮助台只字未提，但却给您的网络留下不好的名声。

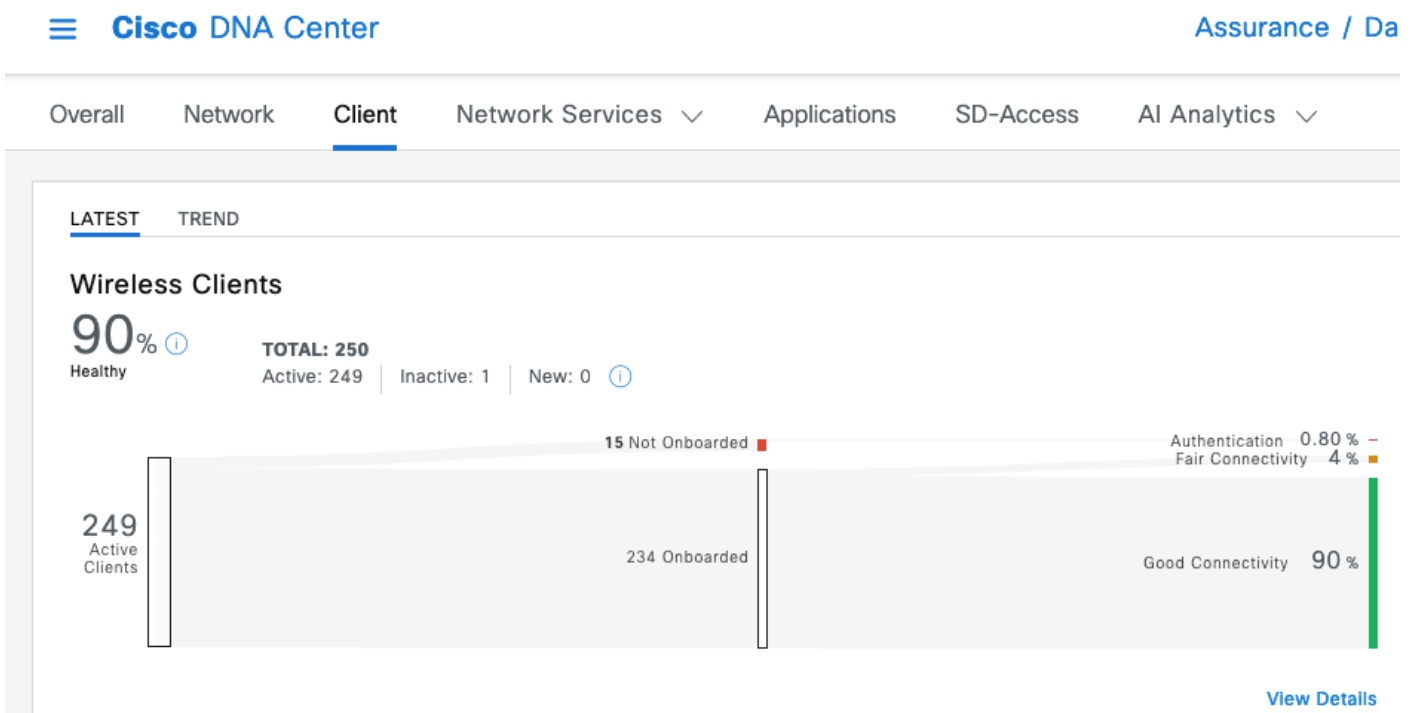
所以，问题是：你怎么能一出现不良的经验就立刻发现它们？

1. Cisco Catalyst Center上的客户端保证控制面板

在Cisco Catalyst Center保证控制面板中，您有一个客户端运行状况的整体图表。

始终有一些客户端由于有人输入错误的密钥而无法连接，或者设备位于覆盖范围的最边缘，因此不要希望能够接触到100%的健康客户端，但要熟悉在您的环境中健康客户端的比例有多高。

一般而言，处于90年代范围是个好消息。



只需快速扫一眼，您就能看到不健康的客户所发生的情况：

- 它们距离AP (无线接入点) 是否很远？
- 是身份验证问题吗？

在此图中，您可以很容易地看到每个类别的比率。

在相同的想法范围内，您可以滚动到该页面的底部并进行过滤，以显示报告为运行状况较差的客户端设备。然后，您可以尝试找出是否存在任何模式：

- 它们可能都在2.4Ghz频段上连接（在许多情况下，这会带来较差的体验）；
- 它们可能都以较低的信号强度被报告；
- 它们可能物理上都在同一个区域。

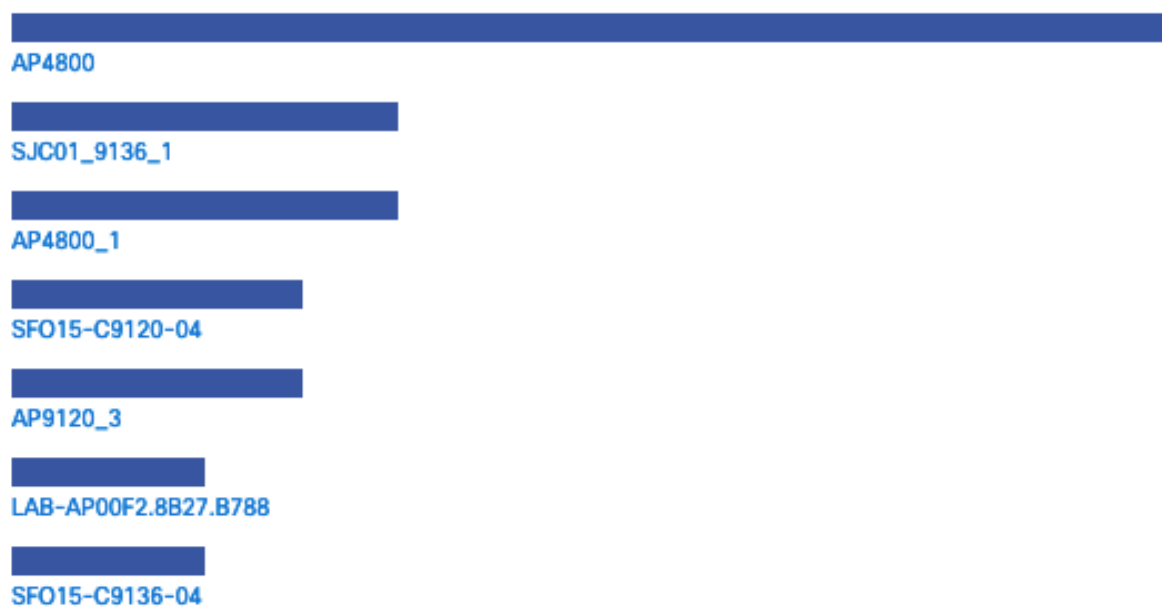
TYPE	Wireless	Wired	OVERALL HEALTH	All	Poor	Fair	Good	Inactive	No Data	
DATA	Onboarding Time >= 10s	Association >= 5s	DHCP >= 5s	Authentication >= 5s	RSSI <= -72 dBm	SNR <= 9 dB				
Identifier	IPv4 Address	Device Type	Health	Tracked	Usage	AP Name	Band	RSSI	Location	Last Seen
Gordon.Thomson-iPad	10.30.100.41	Apple-iPad	2	--	45.67 kB	AP4800	2.4 GHz	-73 dBm	Global/North America/USA/California/San Jose/SJC01/Fir-SJC1-1	Feb 28, 3:13 PM
Shaggy-PC	10.30.100.19	Linux-Workstation	3	--	14.32 kB	AP4800	2.4 GHz	-68 dBm	Global/North America/USA/California/San Jose/SJC01/Fir-SJC1-1	Feb 28, 3:13 PM
SAMSUNG-SM-G930V	10.33.248.101	Unclassified	2	--	12.34 kB	SCJ01_9136_4	6 GHz	-76 dBm	Global/North America/USA/California/San Jose/SJC01/Fir-SJC1-1	Feb 28, 3:13 PM
William.Roy-iPad	10.30.100.49	Apple-iPad	2	--	43.52 kB	AP9120_3	5 GHz	-73 dBm	Global/North America/USA/California/San Jose/SJC01/Fir-SJC1-1	Feb 28, 3:13 PM
Luther.Knight	10.30.100.50	Apple-iPhone	2	--	21.34 kB	SCJ01_9136_2	5 GHz	-72 dBm	Global/North America/USA/California/San Jose/SJC01/Fir-SJC1-1	Feb 28, 3:13 PM
Mia.Smith	10.30.100.51	Apple-iPhone	2	--	12.43 kB	SFO15-C9136-03	5 GHz	-72 dBm	Global/North America/USA/California/San Francisco/SFO15/Fir-SFO15-1	Feb 28, 3:13 PM
Aaliya.Khan	10.30.100.52	Apple-iPhone	3	--	23.14 kB	AP4800_1	5 GHz	-72 dBm	Global/North America/USA/California/San Jose/SJC01/Fir-SJC1-1	Feb 28, 3:13 PM
Liam-PC	10.30.100.59	Linux-Workstation	3	--	21.39 kB	SFO15-C9120-03	5 GHz	-68 dBm	Global/North America/USA/California/San Francisco/SFO15/Fir-SFO15-1	Feb 28, 3:13 PM
Emily-PC	10.30.100.60	Linux-Workstation	3	--	5.43 kB	SCJ01_9136_8	5 GHz	-68 dBm	Global/North America/USA/California/San Jose/SJC01/Fir-SJC1-1	Feb 28, 3:13 PM
SAMSUNG-SM-G930V	10.33.248.121	Android	2	--	15.23 kB	SFO15-C9124-01	5 GHz	-76 dBm	Global/North America/USA/California/San Francisco/SFO15/Fir-SFO15-1	Feb 28, 3:13 PM

2. Cisco Catalyst Center上的网络保证控制面板和设备360

要发现特定潜在问题区域，一个特别好的指标是访问Cisco Catalyst Center的“网络保证”页面。您有一个构件按客户端计数显示排名靠前的接入点：

Top N APs by Client Count

LATEST TREND



[View Details](#)

如果网络中的顶级接入点连接了40个客户端，则表明您状态良好。这意味着所有其他AP（无线接入点）的客户端计数都更低。

另一方面，如果您发现排名靠前的AP具有异常多的客户端，您可以推测该客户端的体验特别差（除非大多数客户端处于睡眠状态且不在网络中活动）。

然后，您可以转到“每个AP”调查，在该调查中，您可以放大此构件中报告的特定顶部AP，以了解其当前运行状况。

查看客户端计数的另一种方法是转到Catalyst Center的Network Hierarchy页面中的映射。进入楼层视图页面后，点击“查看选项”(View Options)，然后在“接入点”(Access Points)部分将显示更改为“关联”(Assoc)。Clients”，用于显示每个AP的客户端计数：

Map

Show Grid



Map Opacity %

51



0

100

Heatmap Type

Operational RSSI



RSSI Cut Off (dBm)

-74



-60

-90

Heatmap Opacity %

54



0

100

Heatmap Color Scheme

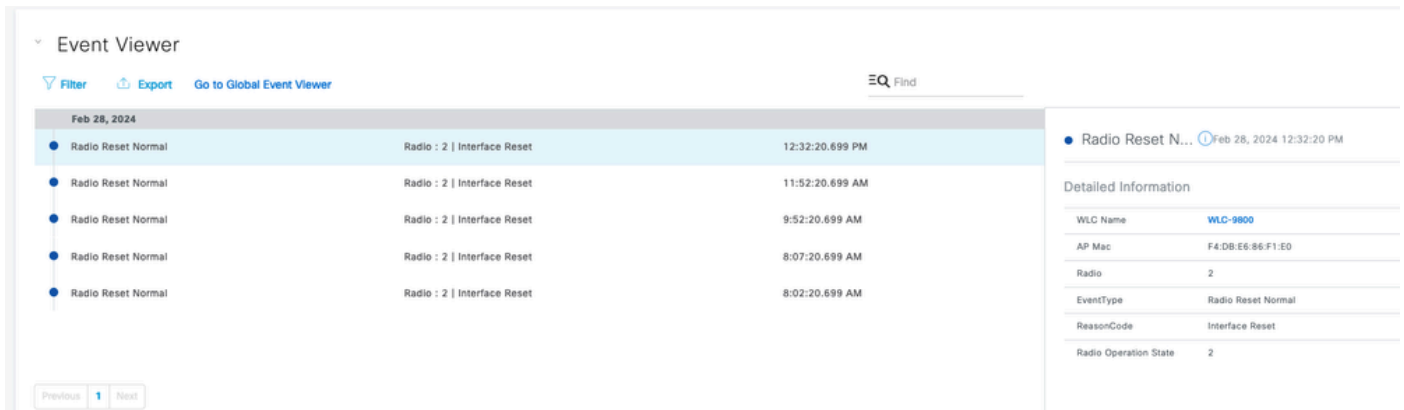
Legacy Natural

Access Points (23)



Display Label

算法设置为运行过于频繁且导致信道频繁更改，从而影响连接的客户端，或者无线电由于各种问题或干扰而不断重置其自身。



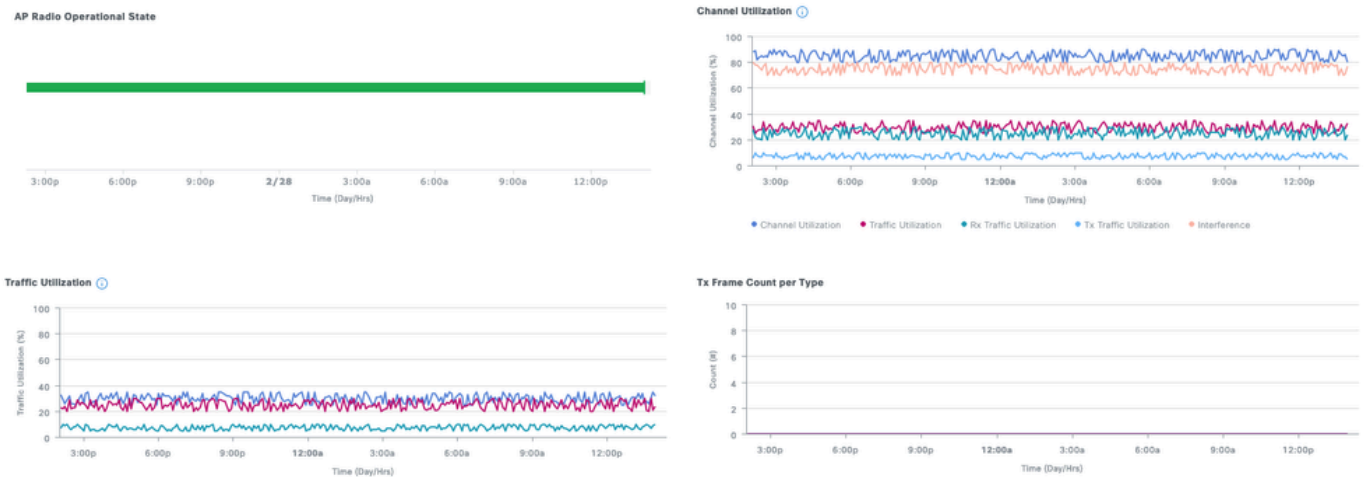
在设备360页面的末尾，您可以将视图设置为“RF”，选择特定无线电，并且您拥有有趣的信息，以便评估问题的根源。

拥有大量客户端并不一定是个问题：这完全取决于它们的活跃程度。

有时，即使有少数客户端，AP也可能忙得不可开交，提供不佳的体验。实际指示器是信道利用率。

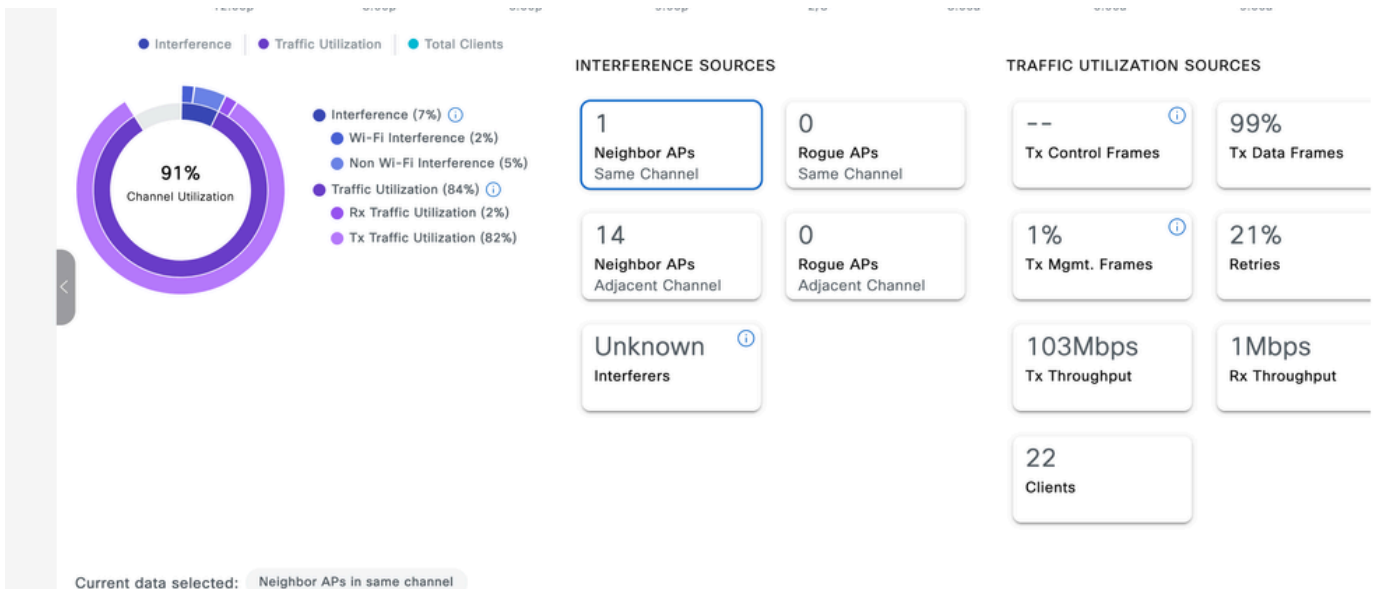
当信道利用率接近100%（甚至从70%开始）时，客户端开始大量争用介质访问、体验延迟和冲突。

这些图形可供您比较总信道利用率和其中负责的AP部分。



例如，如果信道利用率为80%，则意味着有80%的时间是“某人”通过信道进行传输。如果AP显示40%的Rx利用率和40%的Tx利用率，您知道只有此AP负责保持信道繁忙（即没有其他AP在传输），并且它在接收和传输之间很好地平衡。如果AP结合的Rx和Tx使用率与信道使用率相距甚远，则意味着另一个AP（非法或受管）正在使用同一信道并导致同一信道干扰。

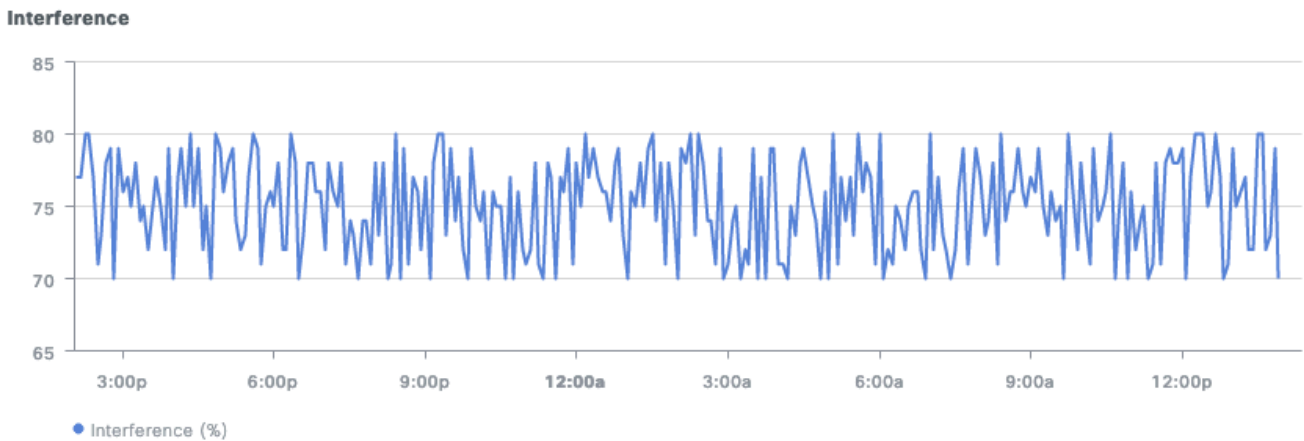
此屏幕截图显示了信道非常繁忙的AP(91%):



该图显示，只有7%的利用率是由其他AP和非WiFi源导致的，而且AP在82%的时间内忙于传输，只有2%的时间处于接收状态。

客户端数量和总吞吐量表明一个或多个客户端可能正在下载大型文件。

干扰图允许您确定信道是否因Wi-Fi传输或实际干扰（非Wi-Fi）而保持忙碌：



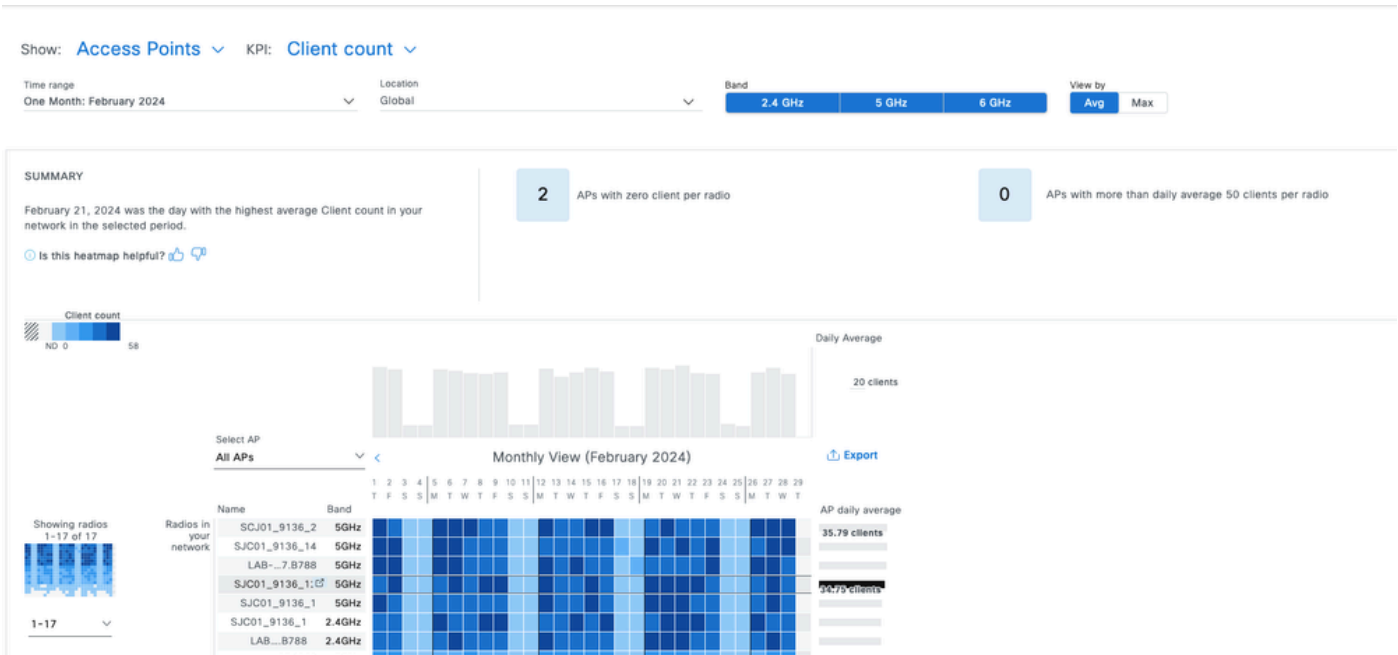
根据经验法则，您需要照顾客户端计数和信道利用率最高的AP。然后，您需要评估此负载是否合理，以及它是否为该区域的最终用户带来不良体验。

3.人工智能分析

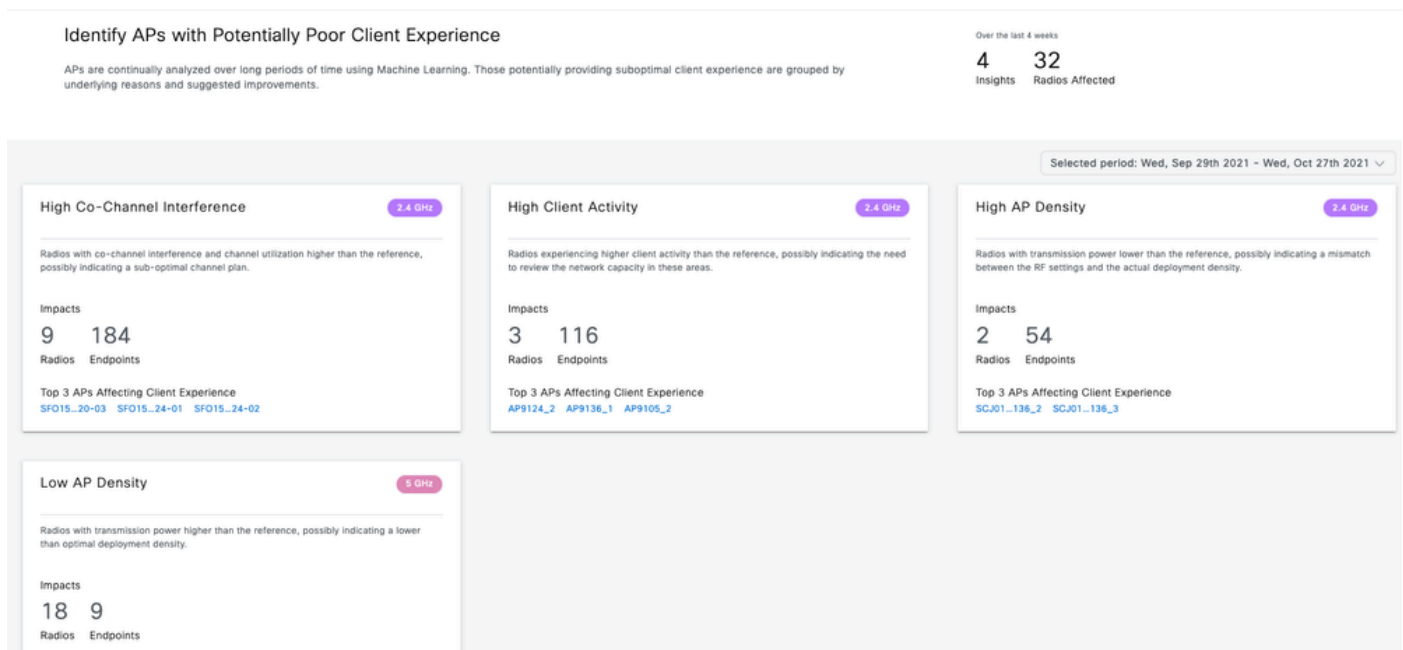
AI分析为您提供更智能的监控。监控不再基于固定阈值，而是根据基线使用情况进行调整。

网络热图提供客户端计数的发展过程，以找出一周内客户端计数最高的AP。您还可以轻松发现始终未连接客户端的AP：相反的问题也是一个问题。

这些AP可能存在物理问题（安装问题、天线问题等），或者如果无线电被冻结（并且该AP重新启动后修复），则可能存在软件问题。



Trends and Insights页面为您提供定期显示高信道利用率或客户端活动的AP列表，以便您可以轻松交叉检查这是否与最繁忙的区域相匹配，或者是否存在异常情况：



主动测试基础设施

当用户报告某个特定领域的体验不佳时，您希望积极测试该体验以确认他们的反馈。典型测试与实际客户端流量有很大差异，了解这一点很重要。

用户通常会尝试使用他们喜爱的应用程序，如果能够运行，他们就会很高兴。他们很少传输大文件。他们最喜爱的应用程序可能有不同的行为：

- **按需视频**：这可以消耗任意数量的带宽（这取决于视频是720p还是4K）。
 - 它非常容忍抖动，因为它会提前缓冲几秒或几分钟视频。该模式看上去像一个在短暂时间内进行的大文件传输，然后在视频从缓冲区播放期间保持静默，直到下次预加载为止

- 语音呼叫：这仅占用极少的带宽，但对延迟和抖动极为敏感。
 - 这有可能使用QoS（服务质量）标记，因此会面临不同于尽力而为流量的（按优先顺序）体验。
- 数据：社交媒体应用以突发方式下载数据。
 - 具体数量取决于内容以及用户滚动的速度。

典型的吞吐量测试应用程序会最大化协议以达到尽可能高的传输速度：它会尝试预订介质并发送尽可能多的数据帧。这并不是与实际应用（文件传输除外）相同的使用类型，这些应用本质上是非常繁忙的。

测试真实的应用程序会模仿用户行为，但无法得到要比较的实际指标和数字。只有网络畅通或不畅时，您才会感受到主观感受。

在吞吐量测试方面，许多网站很受欢迎，在测试客户端和互联网之间的整个带宽时，它们提供了很好的最终用户体验情况。但是，如果您要单独验证您的无线网络与Internet连接、路由和防火墙问题，建议使用专用的吞吐量测试工具，如Iperf：<https://community.cisco.com/t5/wireless-mobility-knowledge-base/iperf-test-for-measuring-the-throughput-speed-of-a-wlan-client/ta-p/3142047>。

此工具允许在客户端和网络中放置的服务器之间进行特定测试。这样，您就可以将服务器移动到网络中的特定位置，并测试长网段上的吞吐量，以验证每个部分。首先将Iperf服务器放置在与AP相同的交换机上，在本地交换或支持矩阵的无线情况下，将无线客户端放置在AP上；在中心交换情况下，将Iperf服务器放置在与WLC（无线LAN控制器）相同的交换机上（如果可能，将放置在客户端VLAN中）。

如果您使用锚点WLC，则必须将Iperf服务器与锚点WLC放在同一交换机上，因为它是流量终止的位置。有时候，创建非锚定WLAN（无线LAN）比较有趣，看看锚定本身和非锚定WLAN是否会导致吞吐量可能下降。

使用多个客户端同时进行吞吐量测试实际上没有意义。在吞吐量测试期间，希望该单台客户端使用全部可用信道通话时间。因此，如果两个客户端同时执行吞吐量测试，它们各自将结果至少分为一半。如果使用更多客户端，冲突开始以数字形式出现，结果不再具有代表性。

有多种第三方工具可自动执行网络测试。请注意，当您在一个区域测试吞吐量时，您实际上是在测试期间使用所有通话时间，因此过于频繁地测试网络是不明智的，因为这对其他客户端具有破坏性。

排除吞吐量问题

确定吞吐量问题时，可以考虑以下几个因素来隔离问题：

- 如果在开始测试之前RF环境已经繁忙，请隔离。信道利用率越高（不在测试范围内），吞吐量测试结果就越低。如果发现信道利用率问题，请检查其他AP是否存在于同一信道的相同区域中，并重新考虑RF设计。缩小信道宽度、消除欺诈、使用具有更集中覆盖范围的不同天线都是不错的选择。添加更多AP并非总是最佳选择。
- 获取吞吐量测试的Over-The-Air捕获结果，并查看802.11层是否存在大量数据重试（以占有数据帧的百分比表示）。重试次数较多意味着RF环境可能是问题。还要检查使用的数据速率、使用的可能不是最优的协议或空间流的数量。在空中捕捉中，大型数据传输的性质非常特殊

，您会看到数十个数据帧具有相同的源和目标，并且彼此之间的增量时间非常短，随后是块ACK。如果传输的特征是在每个数据帧之后有一个常规ACK，或者存在大量请求发送/允许发送请求，则可以轻松解释低吞吐量。

- 验证WLAN上的所有安全类型是否都存在吞吐量问题。有时，客户端和AP之间的特定安全不兼容会导致吞吐量降低。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。