Whitepaper

The Need for Dedicated Scanning

Why a 2-stream, 802.11ac Third Radio Is a Requirement for Enterprise WiFi Today

Abstract

Due to the rise of WiFi as the primary method of network access, enterprises today must deploy some form of persistent channel scanning if they hope to keep their networks reliable and users content. Background scanning, a function by which access radios periodically hop to off-service channels, has been the de facto standard to accomplish this goal. However, high-bandwidth applications like voice and video have made this method of scanning obsolete, while the thought of deploying extra access points strictly for scanning is a costly and untenable solution. The only answer is to deploy a tri-radio access point.

This paper will examine the technical merits and shortcomings of persistent scanning in both "background" and "dedicated" modes. It will explore the specifications by which a tri-radio access point should be engineered, and will explain how a tri-radio is the only option to deliver enterprise with the scanning capabilities needed for performance optimization, WIPS security and enhanced troubleshooting.

Challenges in Enterprise WiFi Today

Today, enterprises increasingly require effective WLAN performance optimization, a strong WIPS (wireless intrusion prevention) security platform and flexible troubleshooting options when investing in WiFi infrastructure. This is driven by a number of factors including compliance requirements, the rising volume of wireless devices on the network (BYOD and IoT in addition to standard-issued devices) and the increasing dependence on WLAN as a primary access method. To accomplish this, enterprises need to deploy persistent channel scanning across their WLAN infrastructure. However, this can be challenging as most enterprise access points to date are dual-radio; in a dual-radio access point, both radios are deployed to provide WiFi access, typically one in the 2.4GHz spectrum and one in the 5GHz spectrum.

Traditionally, enterprises could not rely on these "access" radios to perform the dedicated scanning required to feed into advanced monitoring and security-focused functions like spectrum analysis, wireless intrusion prevention and more. Therefore a solution was proposed to deploy additional access points configured in a "sensor" mode. However, enterprises face the following challenges when accounting for a persistent channel scanning platform in this manner:

- **Increased device cost:** Extra devices are needed to perform persistent channel scanning. This incurs a higher hardware cost both in the upfront investment and ongoing in the form of maintenance.
- **Back-end infrastructure cost:** Additionally, this method requires more back-end infrastructure to support these extra devices. This can result in additional controller licenses (should volume of devices exceed controller capabilities) and other appliances needed to process the higher volumes of data gathered by the dedicated scanning devices.
- **Ethernet port cost:** Extra devices require extra Ethernet drops, thereby adding the cost of POE ports and cabling to the overall solution investment.

These additional costs add up quickly and can be difficult to justify, especially for organizations that utilize funding from public sources (i.e. K-12 school districts applying for E-Rate funding and state and community higher education institutions dependent on state funding); also, this method does not feed into RF and RRM functions at all. An alternative option that has become the de facto standard is to utilize background scanning, wherein "access" radios also perform the duties of persistent channel scanning, albeit in a modified way. But even this method has proved challenging in recent years due to the growth of WLAN usage expressed above. Since this scanning interferes with high bandwidth applications like voice and video, it must be temporarily disabled (when such applications are running) or completely shut off as to not impact users.

This paper explores a third option to achieve persistent channel scanning without the need for additional hardware devices nor the impact on users - a tri-radio access point, wherein two radios act exclusively as "access" radios while the third dedicates its efforts to full-spectrum scanning. This method will be compared to the current standard of background scanning, diving into technical differences and examining the three primary areas of focus where dedicated scanning provides the most benefits.

Technical Overview of Dedicated and Background Scanning

To begin, it is important to understand how access points are deployed and the properties of each scanning method. Access points in an enterprise WLAN have each of their radios tuned to a specific channel in order to provide WiFi connectivity to clients - this is referred in this paper as the "service channel". However, as discussed above, access points also need to scan other WiFi channels, called "off-service channels" in this paper, in order to perform functions related to performance optimization, WIPS and effective troubleshooting. For performance optimization, access points scan off-service channels to evaluate the volume of traffic on them (among other data points) in order to consider on which channel the access point will operate with the smallest amount of interference. For WIPS, access points scan off-service channels regularly as threats can appear on any one of these channels at any given time, including those that are not officially allowed in a specific regulatory domain. For troubleshooting, administrators and support staff need full-spectrum visibility in order to properly identify root cause and remediate.

Off-service channel scanning can be achieved in one of the two ways:

Background scanning describes the technique in which a radio providing WiFi access service scans off-service channels intermittently. As an illustrative example, an access radio, after every ten seconds spent on the service channel to serve WiFi clients, will make a visit to a single off-service channel for 100 milliseconds (see Figure 1). Note that these timings can be variable across vendors and also configurable, but generally are in this same ballpark.

The primary reason why background scanning operates in this manner is that the radio cannot leave the service channel more frequently than once every few seconds, otherwise it will disrupt WiFi client traffic. Also, for the same reason, the scan duration of an off-service channel cannot persist for more than just a few hundred milliseconds.

Dedicated scanning describes the technique in which the radio performing the scan does not provide WiFi access service, but is instead dedicated to channel scanning. This primary operation means the radio is free to travel round robin through all channels, staying for 100 milliseconds on each channel. Depending upon the access point design and mode, one of two scenarios will occur:

- A dual-radio access point dedicated to scanning will use both radios to scan their respective frequencies (2.4GHz and 5GHz) simultaneously
- A single "band-unlocked" radio will alternate back and forth between each frequency, providing visibility into both 2.4GHz and 5GHz

As discussed earlier, a scenario in which an access point is deployed as a dedicated sensor in its own right is typically regarded as an untenable solution for most enterprises. As such the following tables show some important parameters comparing the two most frequently used scanning methods.

Since both methods spend the same amount of time on each respective channel during a scan cycle, and thus pick up the same amount of information per scan, the most effective way to compare the two methods is to see how long it takes to complete one scan cycle. Comparatively speaking, dedicated scanning has a significantly faster scan cycle time. This is owed primarily to the fact that with background scanning, each scan cycle must follow a ten second lull to account for active clients. Understanding scan cycle time is imperative when evaluating the impacts each scanning method has on channel scanning.

Figure 1

Length of Time to Complete One Scan Cycle

	Number of Channels*	Background Scanning	Dedicated Scanning (from a third radio)
2.4GHz Scan	14	2 minutes, 21.6 seconds	1.4 seconds
5GHz Scan	36	6 minutes, 3.6 seconds	3.6 seconds

* Number of channels includes all available channels, even those outside of regulatory domain or available for use (like DFS channels)

WiFi Scanning Math

Scan cycles are calculated by multiplying of the number of channels in a specific frequency by the duration of a single scan - this paper assumes a 100 millisecond scan window, and assumes all channels are scanned independent of regulatory domain (this is best practice) - and then adding them together. For example:

14 channels in 2.4GHz frequency X **100** milliseconds per scan = **1.4** total seconds

36 channels in 5GHz frequency X **100** milliseconds per scan = **3.6** total seconds

Background scanning uses a modified scan duration of 10,100 milliseconds to account for the time spent on the access channel prior to an off-service channel scan (this paper assumes 10 seconds of service before a scan). Also background scanning completes one scan cycle within the timeframe of a 5GHz scan, since both radios scan simultaneously.

Figure 2

Primary Detection Scans and Duration

Detection Scan	Number of Scan Cycles*	Background Scanning	Dedicated Scanning (from a third radio)
Access Point	1	6 minutes, 3.6 seconds	5 seconds
Client Associations	3[§]	18 minutes, 11 seconds	15 seconds
Tx Power Adjustments	10	1 hour, 36 seconds	50 seconds
Data Rate Adjustments	10	1 hour, 36 seconds	50 seconds
Interference	3[§]	18 minutes, 11 seconds	15 seconds

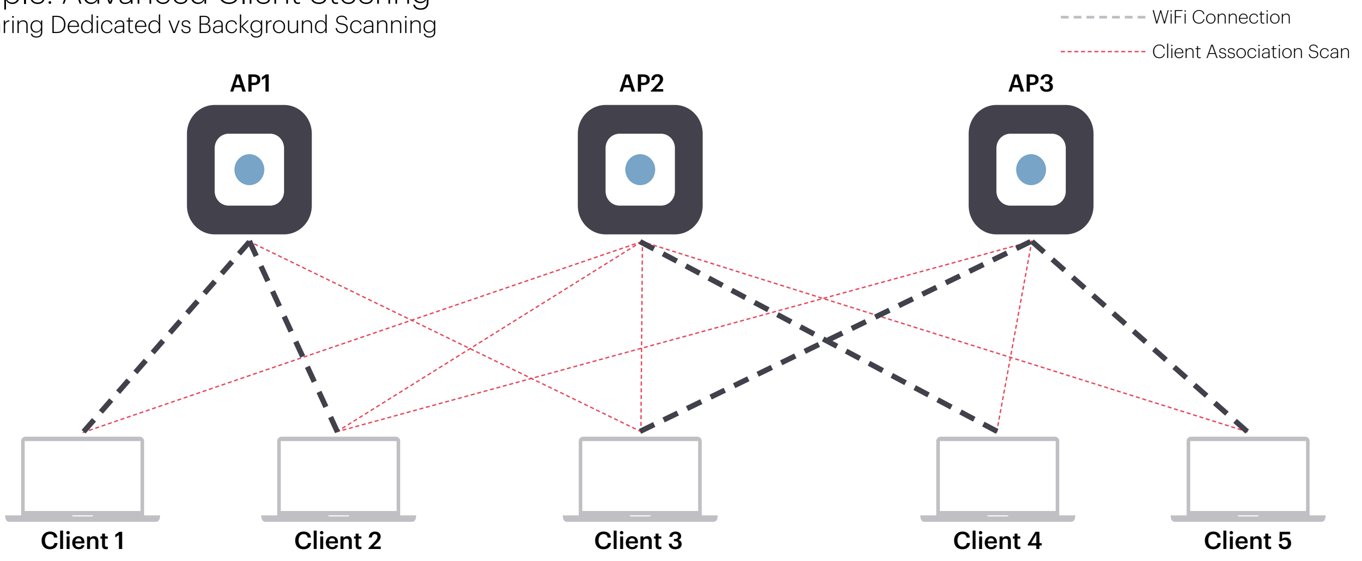
* The Number of Scan Cycles indicates the minimum number needed to collect a viable dataset that can be used by an access point for analysis to make a potential change

[§] This number is an average based on lab testing and real-world observation. As such,access points may require more scan cycles to collect the minimum necessary data needed to properly analyze and act

Figure 2 identifies five primary areas of detection - these represent datasets that access points use to analyze wireless conditions. For example, "Access Point" detection scan data contains data points like the number of available networks per channel, associated clients to respective networks, relative distance of each client as a measure of signal strength (RSSI) and more. Each dataset requires a specific number of scans before enough pertinent information is collected. Therefore, every function an access point performs to optimize performance, enforce security policies or enhance troubleshooting efforts can be assessed based on how much time is needed before taking an action. As the table clearly illustrates, background scanning requires significantly more time to complete a scan cycle.

Example: Advanced Client Steering

Comparing Dedicated vs Background Scanning



Detection Scan	Number of Scan Cycles	Background Scanning	Dedicated Scanning (from a third radio)
Access Point	1	6 minutes, 3.6 seconds	5 seconds
Client Associations	3	18 minutes, 11 seconds	15 seconds

The following example demonstrates why dedicated scanning from a third radio is the only effective way to empower access points to automatically react to environmental disturbances. In the diagram above, three neighboring access points are supporting five wireless clients.

The gray dotted lines connecting each client to an access point represent their direct connection and is emblematic of a common issue in WLAN today - sticky clients. Despite being physically nearby an access point, clients will often “stick” to an access point that is farther away simply because it was the original access point it encountered. The result is poor performance for the sticky client (whose data rate drops considerably with distance) as well as other associated clients (who see a dip in performance as a result of the aggregate data rate dropping).

Load balancing is the answer to this common issue; to perform load balancing an access point first needs to collect access point and client association scan data (represented by the red dotted lines). Collectively this informs the access points that certain clients are connected inefficiently. In a best-case scenario, three scan cycles are required to collect enough information to act.

It is clear that dedicated scanning, which requires at most 15 seconds to complete three scan cycles, will have an almost immediate effect on the troubled clients, correcting their connections and improving performance across the board. Background scanning requires almost 20 minutes before it can act - this considerable amount of time makes this particular action very ineffective; the client must suffer poor performance and, since the clients may have moved positions and disrupted the access point algorithms, new scan cycles are required to recompute. The end result is no corrective action is taken at all.

It is important to reemphasize that because background scanning has a considerable impact on high-bandwidth applications like voice and video, the process of scanning off-service channels can disrupt and negatively impact active voice calls and video streams, even if the user does not break from the access point directly. From an administrator’s perspective, this results in the need to temporarily disable (as when such applications are running) or completely shut off this function all together as to not impact users. This is often touted as a “best practice” for high-usage networks. As a result, these networks receive no scan data at all, completely handicapping every function designed to improve network quality.

Benefits of Tri-radio Access Point

Given the limited visibility and the fact that background scanning is often disabled, a tri-radio access point, in which two radios are designed for access and a third designed for dedicated scanning, provides the only tenable method to perform persistent off-service channel scanning, offering a cost-effective and overall easier to manage solution. This eliminates the cost of extra devices and extra Ethernet drops, and, in the case of Mojo Networks' cloud subscription and C-130 access point, there is no extra back-end cost for WIPS service or WLAN performance optimization features that operate from the scan data of the third radio.

Despite the intrinsic benefits a third radio brings, simply having one is not enough. It is essential that the radio used in this capacity is engineered to a proper specification. There are two primary specifications that should be considered above all - the number of supported spatial streams and the supported 802.11 standard. As such, a 2-stream 802.11ac scanning radio is required to provide high-fidelity visibility into the available RF spectrum, exceeding the capabilities compared to a 1-stream and/or 802.11n scanning radios for following reasons:

1-stream versus 2-stream scanning radio

The spatial stream number on a scanning radio dictates the type of wireless frames that can be heard. A scanning radio with less spatial streams than those used by an active wireless client cannot detect those transmission frames (e.g. a 1-stream scanning radio cannot "hear" frames transmitted by a 2-stream wireless device). Generally speaking, WiFi traffic contains a mix of frames transmitted at different spatial streams, with the bulk of traffic today traveling over either 1 or 2 streams. For this reason, a 2-stream scanning radio can monitor virtually all wireless frames while a 1-stream radio can only see a fraction of them.

802.11ac versus 802.11n

Chronologically, the 802.11ac standard came after 802.11n. The 802.11ac standard, among other aspects, specified a change to the preamble of MAC frames. A common stipulation is that this preamble change (like others) is backward compatible, so an 802.11ac radio can read both 802.11n and 802.11ac frames in the air. However, an 802.11n radio cannot read 802.11ac frames. 802.11ac traffic as a percentage of total wireless traffic is growing by the day, and as a result 802.11n radios become increasingly blind to many wireless frame transmissions. This means an 802.11n scanning radio is severely handicapped when delivering meaningful off-service channel visibility today.

How 2-stream, 802.11ac Dedicated Scanning Radios Impact WLANs

The increased visibility of a 2-stream, 802.11ac scanning radio, measured both in terms of breadth of data and high velocity of data, favorably impacts performance optimization, WIPS security and troubleshooting capabilities. The following section explores each area of focus in details.

Performance Optimization

RRM (Radio Resource Management) is a collection of techniques in which access point radios continuously analyze the RF spectrum to do the following:

- Adjust the operating channel to mitigate co-channel interference
- Adjust the operating power to optimize coverage
- Provide coverage-hole protection by automatically increasing the power when neighboring access points fail
- Ensure clients are evenly load-balanced between available access points, channels, and/or bands
- Ensure clients are connected to the best possible access point (addressing "sticky" or otherwise inefficient client behavior) by steering them to the right access point

To work effectively these techniques require constant visibility into the entire RF spectrum, i.e. all candidate WiFi channels in the 2.4GHz and 5GHz bands. Without this information, RRM functions either shut down completely or, working from incomplete data, make poor decisions that can have even greater negative impact on the network.

The Traditional Approach

Traditionally, most WLAN vendors have relied on background scanning to fuel RRM functions. Increasingly however, enterprises across all verticals are regularly running voice and video applications over WiFi rather than over the wire. Unfortunately this means performance of these applications takes a hit with background scanning; during the time a radio scans an off-service channel, the applications are starved of wireless bandwidth. Even though the scan duration can be as short as 100 milliseconds, this has an impact on quality of service and can even completely disconnect active voice and video streams.

As a result, most WLAN vendors automatically turn off background scanning when the access point detects any voice or video traffic; this is, in fact, considered "best practice" today. This means that access points rarely if ever get the chance to perform off-channel scans and build information about other channels when it supports voice and video applications. This prevents the access point from making correct (or any) RRM decisions when it's needed the most: while attempting to deliver top-quality voice and video.

A Third Radio Means RRM is Always Active

This is where the third radio comes to the rescue, scanning all the channels and providing the necessary spectrum information for critical RRM functions continuously even in the presence of voice and video applications. Furthermore, a dedicated third radio completes a full spectrum sweep across every 2.4GHz and 5GHz channel much faster compared to background scanning. Thus, RRM decisions can be made faster and with better information so the access point can react effectively to changes in the RF environment.

In addition, since 2-stream, 802.11ac scanning radios can read significantly more frames compared to 1-stream and/or 802.11n scanning radios, it can provide higher fidelity information about traffic patterns on the off-service channels. This then facilitates better quality decisions about channel selection and switching for the purposes of performance optimization.

WIPS Security

Behavioral Logic for WIPS

The key to accurate and effective WIPS detection and prevention (i.e. containment) is behavioral logic. Behavioral logic analyzes the connection patterns of wireless devices to identify threats and eliminate false alarms; it goes beyond detecting the mere presence of devices in the wireless space. Like RRM, this comprehensive approach requires constant visibility across the entire RF spectrum, even those channels which are not considered candidate channels in a given regulatory domain. As a result, background scanning is not an acceptable solution due to the following reasons.

1) Detection latency and blind spots

The intermittent scanning of off-service channels creates long intervals of time between successive visits to the same channel. It may also be possible that specific types of activity are not detected during a single visit to the channel and may require multiple visits before it coincides with the activity in question. These factors result in a large detection latency of a particular threat. Even worse, the malicious activity may fall between successive visits to the off-service channel, going completely undetected by intermittent scans resulting in a false negative.

2) Limitations in over-the-air containment

In order to prevent (i.e. contain) many wireless threats, WIPS uses over-the-air prevention techniques. In these techniques, a WIPS radio transmits specially crafted wireless packets (deauthentication packets) to target radios (access point, client, or both) to break their connection. However, once the target radio is disconnected from the threat-posing connection, it usually attempts to reconnect automatically, and hence, needs to be targeted on a continuous basis. This means for effective containment to occur, a radio performing WIPS duties needs to send a steady stream of disconnect messages to keep the target radio out of the threat-posing connection. In background scanning, since WiFi service is the primary function of the radio, its ability to visit off-service channels where threats need to be contained is restricted. This makes over-the-air prevention impracticable or even impossible with background scanning.

3) Real time applications

For real time applications like voice or web conferencing, the brief interruption of service to clients during the periods of background scanning severely impact the application's' performance. As a result, background scanning is typically disabled (either temporarily or permanently) when a radio is supporting real time applications, thereby completely losing the WIPS protection.

"Present" WiFi devices can be detected based on broadcast beacons and probes that they transmit at base rates, but this does not provide much information beyond whether or not a device is active. To properly feed the system so it can use behavioral logic, the scanning radio must to be able to see as many frames as possible (both volume and type) when it visits a specific channel. A 2-stream, 802.11ac radio facilitates this, while a 1-stream, 802.11n radio cannot since it is blind to many frames as described above.

Best-in-industry WIPS engine

Data collection is only as good as the data analysis engine behind it! Powered by over 30 patents and unique Marker Packet™ techniques, the Mojo WIPS engine processes scan data collected by the third radio to automatically classify devices and connections, detect genuine threats and eliminate false alarms, and to perform reliable prevention of threat posing connections without ever disrupting co-existing neighborhood traffic. This is all done without requiring ongoing manual intervention in the form of signature updates and rule exceptions, which results into lower operational overhead and eliminates human error.

Troubleshooting

Improved Packet Capture for Troubleshooting

Advanced troubleshooting for WiFi networks can be challenging, especially when it comes to debugging persistent issues. Beyond standard Level-1 responses to reboot network cards and wireless clients, packet captures are necessary to identify the root cause of deeper WiFi related issues (those affecting the access point, underlying network, or both) and determine the appropriate long-term solution. This can be challenging in its own right for two main reasons:

1. Traditional packet captures initiated from an access point only capture traffic passing between the selected access point and associated clients only. This misses the majority of communication occurring between nearby clients and access points, limiting the amount of available data to analyze
2. To initiate a broader packet capture, "access" radios must change into a "sensor" mode to perform dedicated scanning; this immediately disrupts all associated clients and may not be possible during normal operating hours

In contrast, a 2-stream, 802.11ac third radio provides flexible packet capture capabilities free from the challenges listed above. Not only can it be tuned to any channel across both spectrum (e.g., to troubleshoot neighboring access points operating on different channels than the current access point), but it can do so without disrupting ongoing service to clients on the current access point. In addition, a 2-stream, 802.11ac radio can capture most of the WiFi traffic transmitting to and from nearby access points (as discussed above), providing a fuller picture which enables more effective troubleshooting.

This all results in a clearer picture of the network in a moment of disruption. With more information to analyze, stronger correlations can be seen that have a large impact on the overall health of the network.

State-of-the-Art Hardware Design for Mojo C-130

The Mojo C-130 is an enterprise-grade 4x4 MU-MIMO tri-radio 802.11ac access point with dual concurrent 5GHz and 2.4GHz band radios supporting 802.11a/n/ac Wave 2, 802.11b/g/n, four spatial streams, and data rates of up to 1.8 Gbps and 800 Mbps, respectively. It is the only access point today that contains a third 2x2 MIMO 802.11ac radio for dedicated multi-function scanning.

C-130 features an industry-leading hardware design which includes:

Powerful CPU: A dual core 1400 MHz CPU with separate WiFi offload engine, which will allow intelligent applications such as DPI and analytics while maintaining high WiFi throughput

Latest WiFi Chipset: The latest generation QCA 9994 Wave-2 chipset that supports highest available density of MU-MIMO clients and 160MHz channels at 256 QAM

Optimized Antennas: Carefully designed internal antennas that offer high sustained, consistent throughput, uniform rate-reach and cellular coexistence at carrier grade reliability

Beautiful Industrial Design: A confident design that merges seamlessly and proudly in most environs and delights just as much as the performance and power under the hood

Ergonomic Mounts: T-grid adapters and wall mount designed for quick installation. Ceiling brackets require no tools and can be mounted in seconds, cutting technician time.

Omniscient Security Radio: The only access-point with a dedicated 2x2 802.11ac radio with Rx/Tx sensitivity that maximizes detection of rogue access points and offer automatic over-the-air protection (OAP) without impacting associated clients

Immaculately Packaged Hardware: Electronics under the hood - the printed circuit board, ten separate antennas, heatsinks, connectors, USB, Ethernet and power ports - are packaged with surgical cleanliness.

High Quality Components: High quality components were selected resulting in mean time between failures of 150 years or annualized failure rate of less than 0.7%

Lowest cost: Industry leading hardware offered at the industry's lowest cost for a Wave-2 enterprise access point.

Conclusion

Given the growth and demand of WiFi as a primary medium over which wireless clients of all shapes and sizes use bandwidth-intensive applications for voice, video and data, the necessity for WiFi networks to dynamically adjust their settings to maintain a strong, reliable connection is imperative. The only way to inform access points such that they can make these decisions is through off-channel scanning. When considering the benefits and challenges of scanning as a background function or in a dedicated mode, it is clear that dedicated scanning is the only viable option for enterprises today given the limited capabilities of background scanning.

In fact, an enterprise using voice or video on a regular basis should consider discounting completely any platform that strictly relies on background scanning, given that it will either impair communication beyond usability or, more likely, automatically disable itself while these applications are running. This results in an absence of wireless security monitoring, power and channel selection processes, and spectrum analysis when wireless clients needs it most.

Furthermore, a tri-radio device equipped with a 2-stream, 802.11ac radio is the quintessential choice to achieve the level of dedicated scanning needed, since this expanded specifications increases the depth of visibility, feeding more and better information to access points.

The C-130 has the industry's only 2-stream, 802.11ac third radio dedicated to scanning. It enhances enterprise WLAN across three main areas of focus:

1. Enabling full-time, full-powered WIPS such that the most complete airspace is constantly monitored and active security measures are fed real-time data so threats and inappropriate connections can be automatically disabled
2. Maintaining peak performance by offloading critical scanning functions to a dedicated, "non-access" radio and increasing the fidelity of data captured so RRM and traffic optimization techniques make better and faster decisions
3. Improving troubleshooting efforts through flexible packet capture capabilities that do not disrupt active users and feed more and better data into analysis tools for quicker resolution