QA Cafe

White Paper

qa|CloudShark

Simplifying cloud-managed network troubleshooting with packet captures

A guide for network operators, MSPs, and IT professionals

As more network management moves to the cloud, vendors building cloud-managed network tools have a unique opportunity to provide remote packet capture as part of their platform. Cloud-managed networking systems with built-in packet capture and web-based analysis tools provide wonderful new opportunities for network and security operations, IT pros, and managed service providers.

Learn how to take full advantage of packet capture analysis in cloud-managed networks for your business and your customers.

Cloud-managed networks are becoming the norm

Over the past couple of years, the networking industry has seen an increase in new cloud-managed product offerings. This rapid growth comes from the acceptance and adoption of new cloud technologies among enterprises and small-to-medium enterprises (SMEs) and the dramatic shift to work-from-home environments in the wake of the novel coronavirus pandemic.

These products and services are coming from many industry players, both new and old. Startups with new ideas on how management, analytics, and artificial intelligence (AI) can benefit network operations (particularly around Wi-Fi) are pushing incumbent vendors to develop their own cloud-managed solutions. Many of these startups have been acquired by larger network equipment manufacturers (NEMs), like Cisco Meraki, Cradlepoint, Mist by Juniper, etc. They recognize how interested the market is in these solutions and the speed at which they need to provide them.

Moreover, cloud-managed networks have opened a vast new market for managed service providers (MSPs) and system integrators. MSPs can now offer comprehensive IT solutions by managing, monitoring, and troubleshooting customer networks directly. NEMs can now offer MSP solutions themselves as part of their product offering.

What are cloud-managed networks?

Cloud-managed networks are those networks built using devices that can be managed through a web portal, without the operator having to be on-site. Customers find them easier to manage and deploy and enjoy the flexibility of being in one corner of the world while controlling their networks on the opposite side of the globe.

Access through a remote web portal has several key benefits. Centralized management lets entire IT teams work together with appropriate security, and access controls no matter where they are located. Mass-scale monitoring and analytics are enhanced by the ability to push or pull data from all points in a network. Wi-Fi AP's can all communicate with each other for optimization. Multiple firewalls can be quickly and easily deployed with the same policy, and firmware updates can be deployed across multiple locations with a single click.

These advances allow the people in charge of setting up networks to build and configure more capable and complex environments than ever before. It also means that investigating and troubleshooting application, network, or security issues is a more complex problem.

Benefits of cloud-managed networks

- Standardized experience
- Centralized management
- Monitoring and analytics
- Easy policy deployment
- Firmware/lifecycle management

New cloud-managed troubleshooting capabilities

With more cloud-managed networks being deployed, teams need to look closely at debugging and troubleshooting in these environments. The good news is that most solutions differentiate themselves on the dashboard experience and the data that they provide through their web-portal and API. Many rely on advanced machine learning, artificial intelligence, and other novel techniques for analytics, using computational resources to spot problems and present these findings to users.

The bad news is that relying on logs, dashboards, and other "summarization" tools means that they are interpreting the situation and picking pre-programmed results to present to the user. These results can be unreliable or confusing or miss some important information entirely. What happens in the case of an application error? What about diagnosing a problem with a server you don't have access to? What if the problem actually isn't the network?

Dashboards and consoles are great for monitoring, configuration, and getting quick answers. However, very often, the solutions to complex problems will come from network packet captures.

Packet captures - a necessary challenge

When solving problems in a networked environment, there is no substitute for looking at the packets. In many cases, a packet capture should be one of the first steps in troubleshooting a problem. That first step might indicate that the problem is not the network, point at who is responsible, and immediately free up the network engineer's time to work on issues under their control.

Traditionally, packet capture and debugging were performed by a packet capture tool such as a laptop running Wireshark (where the captures are then stored) or a specialized network tap designed to duplicate packets as they traveled across the network. In certain situations, it was necessary to install capture software directly on the client to determine what it was sending. This was performed by a specialist who was on-site or had the time and budget for travel between sites.

There are several limitations to this when dealing with networks that are cloud-managed and distributed over the globe. It's obviously not practical to always have physical access to cloud-managed network points and defeats the purpose of having a managed network in the first place. Knowing where and when to capture is made more difficult when it's necessary to be present at the network interface and perform a capture in-line.

In today's BYOD and cybersecurity conscious world, it's also impractical to expect specialized software to be installed on most workstations or engineering laptops. Installing capture software may be against company policy entirely, and storing captures locally - when they contain all information traveling over your network - is an insecure way to handle them.

Lastly, there are also some technical difficulties dealing with captures taken in wireless environments. Traffic is encrypted

Troubleshooting with packet captures gives you:

- A complete view of what happened
- Access to actionable details
- Evidence for reporting and remediation

Issues with using packet captures today:

- Cloud-managed networks are distributed
- No good way to capture at the right place and time
- Security policy limits the ability to use native capture software
- Wireless encryption and missing packets

by default and can be bounced around multiple radio channels by smart band-steering AP's. Even without this enabled, it is still difficult to ensure that all the packets have been captured in a wireless environment. Capturing on an access point is the only way to guarantee the analyst is seeing what the network is seeing.

Cloud-managed network providers can provide remote packet capture

Vendors building cloud-managed network tools have a unique opportunity to provide remote packet capture as part of their platform. Since users already have access to their distributed network devices through a unified web-portal, building native packet capture into the devices, controlled through the portal, expands the use case of network devices beyond passing packets or deploying firewalls, making them valuable capture points as well.

Cloud-managed devices with cloud-managed packet captures give users the best of both worlds. It eliminates the need to travel or be on-site for most debugging purposes. Since control of the capture is web-native, there's no need to install specialized client-side software, and IT teams and MSPs can take the end-user out of the workflow of troubleshooting an issue.

Moreover, making network devices into capture points elevates the usefulness of packet captures, making it significantly easier to capture at the right place at the right time, and can even make packet capture a part of the overall intelligence and analytic capabilities of a cloud-managed platform.

Capture analysis tools must also evolve to this new environment

What use are the packets to the network engineer if they still require extra tools to download, install, and view the packets? Just as management has gone from the old terminal connectors of the past to the web-based interfaces of today, so must packet analytics. Captures coming from multiple sources need to be organized, secured, and accessible in a way that makes using them for actionable data - by the entire IT or MSP team - easier.

Cloud-managed networks make it easy to deploy a lot of devices. Packet captures from these must be properly tagged or organized to make them useful to the analyst/engineer. Using a central repository and associating captures with support tickets, location, device type, etc., makes things clearer, safer, and ensures that capture data is never lost. A dedicated capture repository also allows organizations to apply group and user access rules to meet cybersecurity compliance requirements. This also makes it easier to search through large amounts of captured information to narrow down an issue faster.

One often overlooked part of packet analysis is how isolated it has traditionally been. When an engineer works with large files on specialized software installed only on their laptop, it is challenging to share their work and analysis with colleagues and risky if you're

Example: Cradlepoint

Cradlepoint includes remote packet capture on its devices through its NetCloud Service. This lets users treat each Cradlepoint device as a wired or wireless capture point, recording all activity that passes through the device. For wireless captures, the data is decrypted to make analysis possible that couldn't be done by capturing from a host.

Example: Mist AI

Mist by Juniper has made automatic packet capture a feature of their AI capabilities. The Mist Wi-Fi Assurance Service automatically detects and starts capturing packets when an anomaly is detected. With this record, users can rewind in time to see what was going on exactly when the event occurred while eliminating hours or days spent with guesswork or reproducing issues to capture the data.

dealing with sensitive information. If an issue spans departments, the other engineer must often reproduce the same work already done by the first person. Collaborative analysis tools are a novel approach to solving problems that people have assumed is a solo job for too long. The distributed nature of cloud-managed products makes network management a group effort. Troubleshooting and analysis should be too.

Advantages of cloud-managed capture for MSPs

Many MSPs build their business out of deploying cloud-managed networking devices and operating the management system on behalf of their clients. In many cases, the equipment manufacturers themselves build new MSP business units to provide long term value to their customers.

Having native packet capture with collaborative analysis tools makes it significantly easier to operate as an MSP. With no need to deploy capture software to the client, and the ability to collaborate directly with customers on the packet data itself, MSPs can solve issues incredibly quickly without the need to visit a client site or play "back-and-forth" with the end-user to try to troubleshoot a network or application problem.

Cloud-managed networks need cloud-managed capture

As more and more cloud-managed networks emerge, organizations of all sizes look to benefit from them. It is an incredibly flexible and powerful way to deploy networking gear to the world and provide new ways to manage, monitor, and troubleshoot them.

However, we must also not overlook the need to get down to the packets in these networks. Cloud-managed networks must provide cloud-managed packet capture, analysis, and collaboration tools along with their network offering.

Using CloudShark in a cloud-managed environment

Since 2011, CloudShark has provided a powerful, web-based, centralized packet capture analysis and archive tool for network professionals. By integrating with the simple, clean CloudShark API, cloud-managed vendors can bring the full suite of packet analysis capabilities of CloudShark directly to their customers quickly and easily.

Providers like Cisco Meraki, Cradlepoint, and Mist by Juniper all include automatic upload to a CloudShark Enterprise system as part of their service. They have revolutionized the way their users troubleshoot networks. If you want to take advantage of this for your deployment of these products or are interested in integrating your own offering with CloudShark, please contact us!

Example: MSPs deploying Cisco Meraki

Cisco's Meraki cloud-managed networking products are prolific and used by many popular managed service providers who manage wireless networks for enterprises. Cisco Meraki wireless products have native packet capture capabilities, making it easy for MSP customer service to troubleshoot network issues remotely with the detailed information provided.