SCTE•ISBE CABLE-TEC EXPO® VIRTUAL EXPERIENCE » OCTOBER 12-15 2020

2020 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS®

Smart Data Powers Service Layer Management For Network Operations 2.0

A Technical Paper prepared for SCTE•ISBE by

Dr Vikram Saksena
Cable CTO
NetScout Systems
310 Littleton Road, Westford, MA 01886
978-614-4383
vikram.saksena@netscout.com

Ryan Eccles
Principal Sales Engineer
NetScout Systems

Table of Contents

List of Figures

1. Introduction

Cable operators have embarked on a network transformation journey to evolve their networks from a centrally controlled, purpose-built platform to a distributed, programmable platform. A programmable network fabric drives service agility by allowing operators to create, change, and personalize services on demand, thereby shrinking service delivery intervals significantly. Together with business process automation and new service innovation, operators are well positioned to drive revenue growth and profitability. In this new era of service agility, operators will have to raise the bar on differentiating themselves on superior service quality to retain and grow their customer base amidst a highly dynamic and competitive landscape. In this paper we describe a powerful approach to service layer management utilizing packet data.

As operators evolve to a distributed, service-oriented architecture, the delineation between network and service management becomes more pronounced. Machine data (syslogs, telemetry, flows, session records, etc.) collected from the network elements is better suited for network management as they directly point to problems in the underlying infrastructure. Being vendor specific and fragmented, it is challenging to correlate machine data from various elements in the network to get an accurate view into service layer problems. A better and more direct way to identify service layer problems is to look at packet data, which is vendor independent, universally available, and carries all the contextual and relevant information pertaining to subscribers and the services they consume. Every transaction between subscribers or between a subscriber and an application leaves a footprint on the operator network which can be analyzed for service performance issues as well as security related threats.

Smart Data, which is actionable metadata derived from packets, delivers superior service management capabilities due to its high-definition nature. Smart Data coupled with Smart Analytics enables proactive service assurance, network automation, just-in-time resource management, SLA management and many other use cases at the speed and agility required for Network Operations 2.0. We also describe an actual operator use case for proactive service assurance of Wi-Fi networks.

2. Extracting Service Intelligence with Smart Data

Smart Data is high-definition, actionable intelligence derived from the ultimate source of truth, IP packets. It is contextual metadata that is structured, timely, and relevant. Smart Data gives operators complete visibility with holistic, end-to-end coverage of control and user plane traffic over multiple dimensions of their network, services, and subscribers. It addresses user experience covering all devices, network services, and applications consumed.

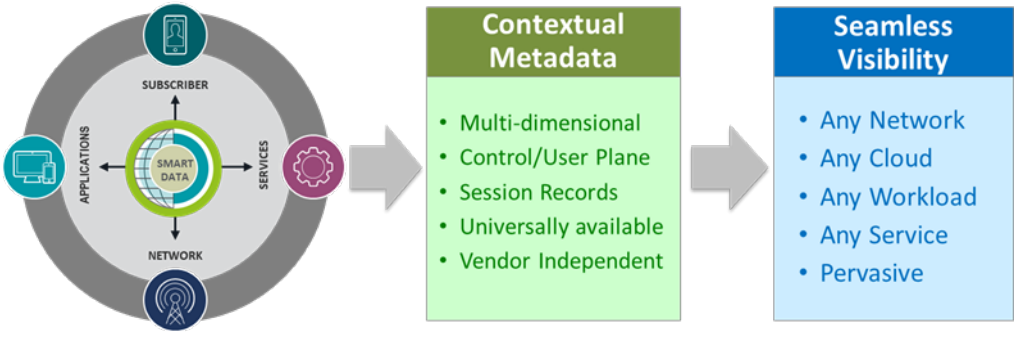

Figure 1 - High Definition Smart Data

Smart Data lowers the cost/complexity barrier of packet-based instrumentation and makes it affordable for pervasive edge to core deployment. Being a software solution it has an optimized, elastic footprint that scales up and down with traffic levels. It offers vendor independence by providing unified metadata with common views and workflows for any service (voice, data, video, IoT), over any network (physical, virtual, fixed or mobile), over any cloud (private or public), and for any workload (virtual-machine or container-based).

3. Addressing Operational Challenges with Smart Analytics

Smart Data is the fuel for Smart Analytics that addresses many operational challenges in current and future networks: providing proactive service assurance, enabling zero-touch automation, reducing churn and improving net promoter score, enabling just-in-time resource management, and advanced threat management for security operations. Having a unified data model that can be leveraged across functional and organization boundaries helps accelerate digital transformation by breaking down the information silos.

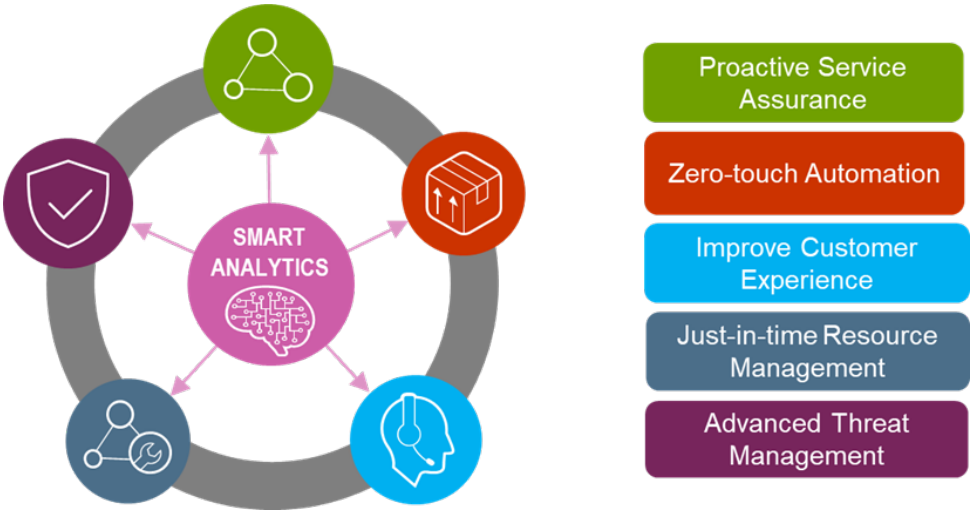

Figure 2 - Smart Analytics

3.1. Proactive Service Assurance

As services become mission-critical, especially for commercial customers, proactive service assurance becomes very important. Smart Data enables service assurance for proactive alerting, rapid problem isolation, and situational analysis. It helps in promoting trouble-free network operation by identifying potential problems before they become service-effecting.

For example, as cable operators deploy mobile services over a combination of Wi-Fi and cellular technologies (4G/5G), the complexity for end to end service assurance increases. Handovers across Wi-Fi and cellular technology domains must be carefully monitored to avoid dropped calls and degraded sessions. From an end user perspective, the service experience must be consistent and disruption-free across both network domains.

3.2. Enable Zero-Touch Automation

One of the benefits of moving to a software-centric network is that corrective actions in the network can be automated with little or no human intervention. In coordination with policy servers and orchestration platforms, service performance triggers based on Smart Data can be used to effect network changes in near real-time. Additional resources can be temporarily increased for virtual machines and containers to deal with traffic spikes in the network by the appropriate use of service performance triggers fed to the policy and orchestration platforms. Such "closed-loop" automation solutions can drastically reduce or eliminate service degradations that could negatively impact user experience.

3.3. Improve Customer Experience

Creating a composite customer experience indicator from Smart Data helps operators better understand their customer experience for the services they consume. Each user is measured for key performance indicators related to accessibility, retainability, and quality of experience for deriving the indicator. With such a customer experience indicator it is possible to visualize the experience for groups of users in different dimensions such as device type, location, service and more. When this indicator falls below the desired levels, network operations can drill down to the details of what caused the degradation. Understanding and rapidly responding to network causes for poor service experience is an important factor in improving customer experience and reducing churn.

3.4. Enable Just-in-time Resource Management

In a hardware-centric network, capacity management required careful planning because hardware had to be ordered and deployed ahead of realized demand. This process created inefficiencies and stranded capital in the network when demand would materialize differently than what was planned for. In a software-centric network, traffic data can be used to scale resources up or down in relatively shorter intervals than what was done before. Analytics based on Smart Data can be used to deploy just-in-time resources as dictated by key service performance indicators. Such a dynamic resource management process allows for more efficient use of capital as capacity deployments can be made to track more closely with the realized traffic demands.

3.5. Early Warning Detection of Advanced Threats

Security threats continue to rise. As networks evolve to a software centric architecture, new attack surfaces are exposed to potential hackers. Hackers have become more sophisticated and continue to develop new attack vectors for exploiting vulnerabilities in open source software and virtualized, cloud-native infrastructures. Smart Data provides deep packet intelligence to identify the potential onslaught of advanced threats which would otherwise escape detection. Sophisticated security analytics algorithms based on Smart Data provide early warning detection of anomalous behavior and alert operators for taking proactive actions to avoid service disruptions.

4. Smart Data Use Cases in Operator WiFi Networks

Wi-Fi networks are now held to a much higher standard than ever before. No longer is best effort wireless service considered acceptable. Additionally, the proliferation of MVNO agreements is further requiring the Wi-Fi service to be especially robust in order to meet subscriber experience requirements. Some of the common challenges that Cable MSOs face in offering carrier-grade Wi-Fi service include:

- Identifying customer login experience problems
- Problem isolation with limited subscriber feedback
- Identifying Wireless Access Gateway problems
- Last mile customer experience telemetry
- Controller stability
- Determination of Wi-Fi performance for operator provided devices versus other devices

This paper will focus on the first three use cases and will demonstrate how the use of Smart Data can help operators become more proactive, isolate the source of problems and reduce service disruptions.

4.1. Instrumentation

Proper instrumentation and Smart Data generation in modern operator Wi-Fi networks requires tapping and monitoring of the links that surround critical application flows that make up the wireless service offering. Figure 3 below shows the common visibility points (indicated by the NetScout logo) in an operator Wi-Fi environment for maximum visibility.

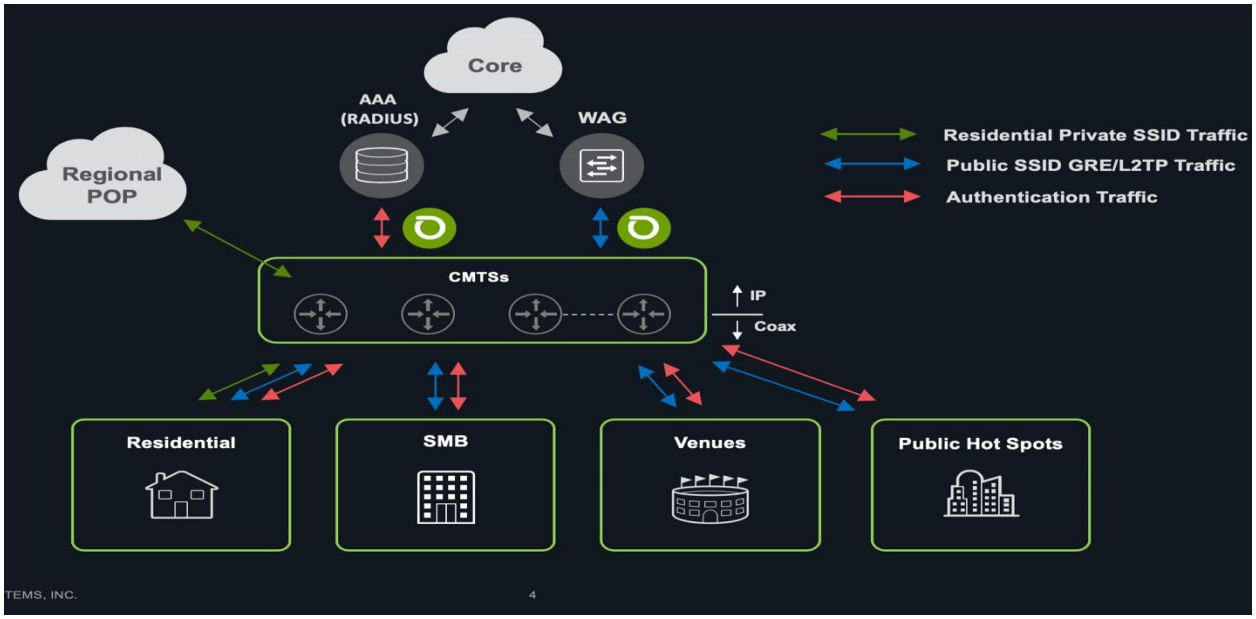

Figure 3 - Wi-Fi Instrumentation Points

4.2. Use Case 1: Slow Customer Login

In many public carrier Wi-Fi environments there is an inherent lack of customer service calls from the subscriber base even during a systemic outage. Subscribers traditionally have grown to view public Wi-Fi as best effort. This is changing rapidly. The ability to use packet-based Smart Data is more important than ever to solving problems quickly and identifying the true subscriber experience. Packet-based metrics are the ultimate source of truth and play a critical role in reducing churn and allowing the operator to become truly proactive.

Figure 4 below illustrates how Smart Data can identify and report on how long it takes for a mobile device to attach and obtain an IP address from the operator Wi-Fi network. The login latency distribution metrics can be dimensioned based on market, region, physical location, AP vendor or even client MAC address.

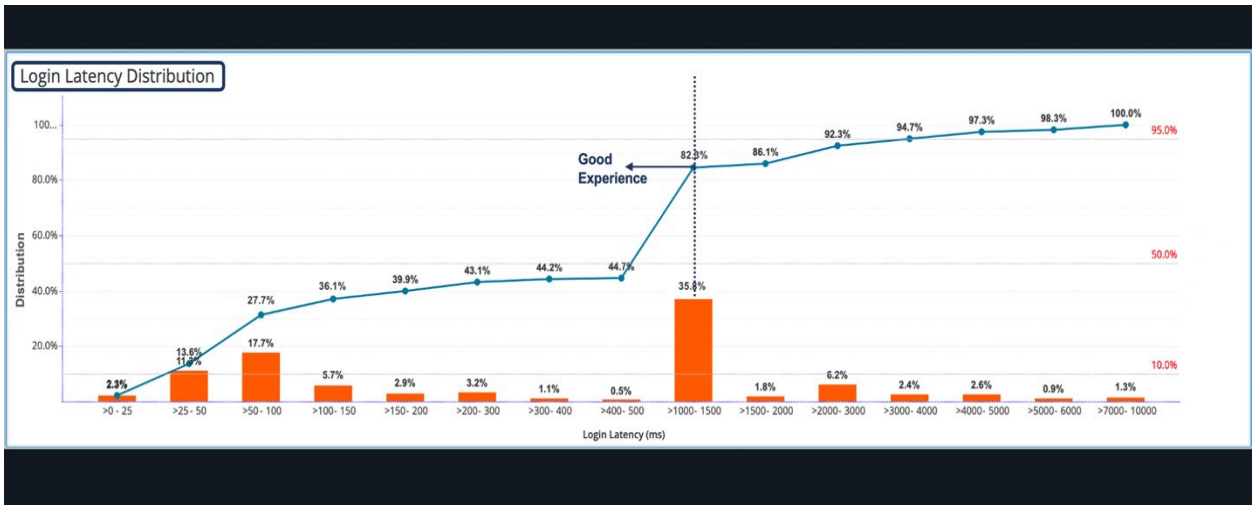

Figure 4 - Login Latency over Time

The figure above illustrates that the majority of devices will get an IP address within the 1 second to 1.5 second range. The ability to trend such data over time and alert on deviations from baseline values is critical to assuring the Wi-Fi service and improving subscriber experience, further illustrating the value of what a Smart Data model can provide in such scenarios.

4.3. Use Case 2: Intermittent Customer Attach Problems

An MSO provider of Wi-Fi service had a low number of problem calls where business subscribers would state that their customers could not connect to their network while waiting for service. The number of calls was not highly significant but was enough to cause the operator to look into whether or not this was a systemic problem.

Using multi-dimensional Smart Data, the operator was able to look back in time at only business vanity SSIDs and trend the portal performance. Figure 5 below shows a 31-day service dashboard view of captive portal transactions for business SSIDs.

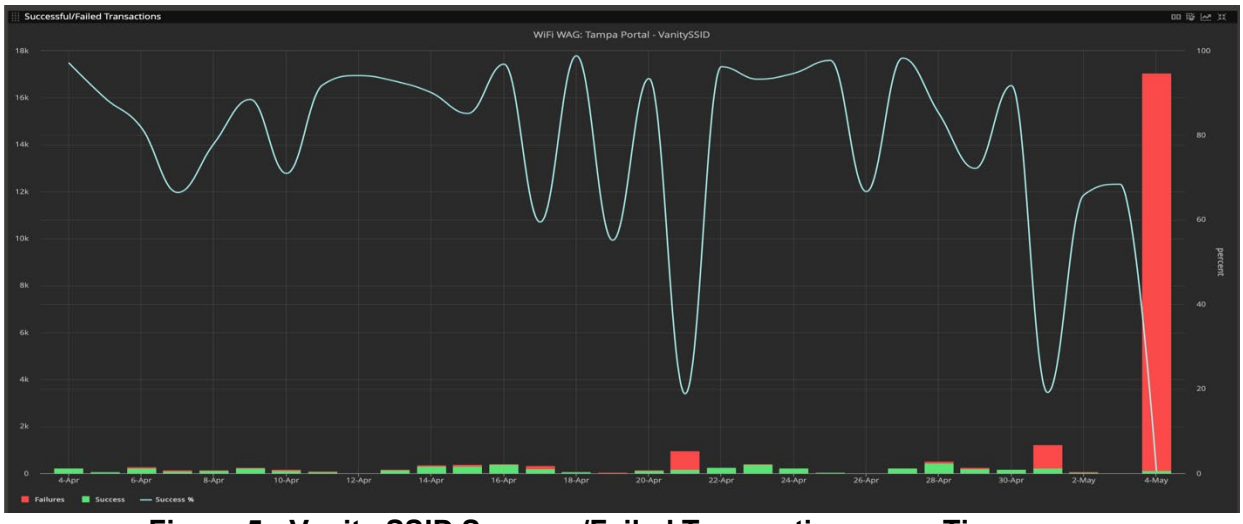

Figure 5 - Vanity SSID Success/Failed Transactions over Time

The operator found that there were periods of low success rates with one being the most severe. Figure 6 below shows a service monitor drill down into Vanity SSID portal transactions for that particular day.

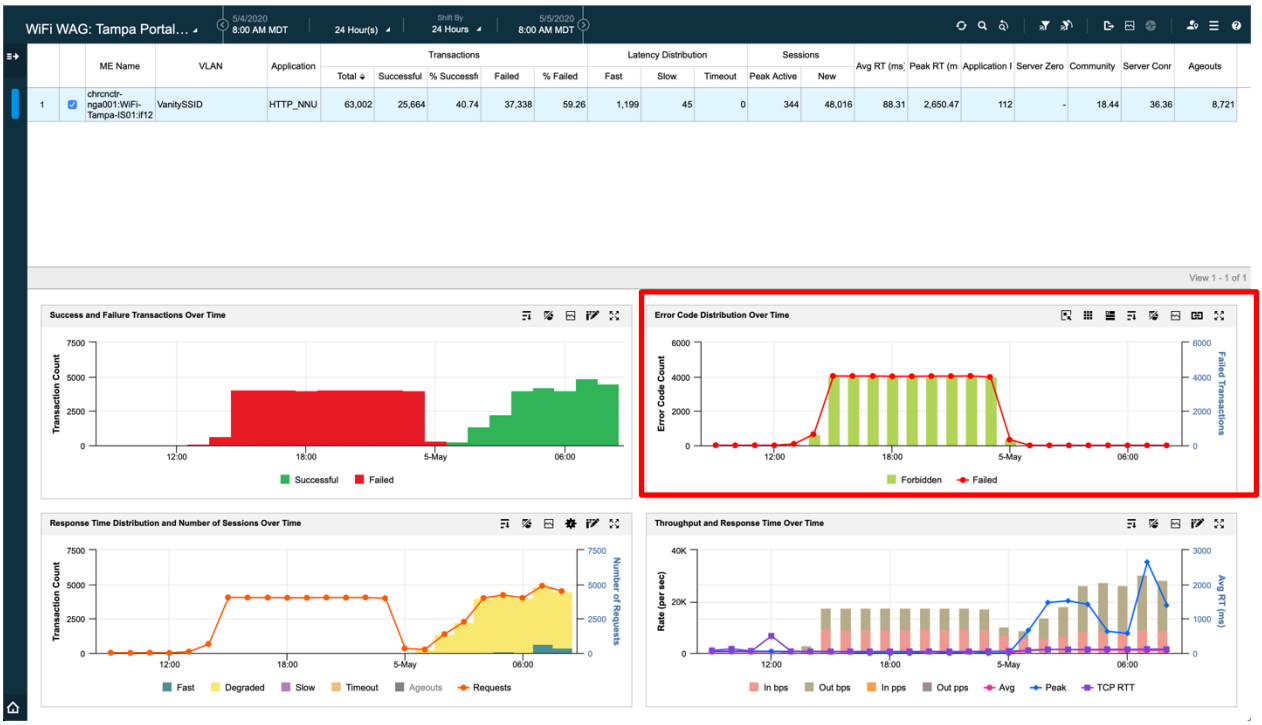

Figure 6 - Vanity SSID Portal Service Monitor

The service monitor shows that during the middle of the day there was a spike in HTTP 403: Forbidden errors. Further drilldown into the packet-based Smart Data showed that the devices that should have been granted access to the Wi-Fi network were not. This data allowed the operator to examine recent provisioning changes that were done incorrectly and put proper measures in place.

4.4. Use Case 3: Decreasing WiFi Network Usage

An MSO offering Wi-Fi service began to detect a downturn in usage over a period of weeks when the opposite was expected. Multiple systems including AAA were checked but nothing explaining the downturn was detected in the data that those systems produced. As a result the MSO turned to packet-based Smart Data to provide a view into individual device behavior.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000			XID	72	Basic Format; Type 1 LLC (Class I LLC); Window Size 0
2	0.076308680	0.0.0.0	255.255.255.255	DHCP	388	DHCP Discover - Transaction ID 0x29bea3d4
3	0.076397520	100.64.250.1	100.64.250.250	DHCP	366	DHCP Offer - Transaction ID 0x29bea3d4
4	0.081758660		'bf	ICMPv6	132	Neighbor Solicitation for
5	0.081763640			ICMPv6	108	Router Solicitation
6	1.054609880			ICMPv6	156	Multicast Listener Report Message v2[Packet size limited during capture]
7	1.171126700	0.0.0.0	255.255.255.255	DHCP	388	DHCP Request - Transaction ID 0x29bea3d4
8	1.171220190	100.64.250.1	100.64.250.250	DHCP	378	DHCP ACK - Transaction ID 0x29bea3d4
9	1.575724530	0.0.0.0	255.255.255.255	DHCP	388	DHCP Discover - Transaction ID 0x29bea3d5
10	1.575811560	100.64.250.1	100.64.250.250	DHCP	366	DHCP Offer - Transaction ID 0x29bea3d5
11	2.064557190	fe80::14a9:b772:673…	ff02::16	ICMPv6	156	Multicast Listener Report Message v2[Packet size limited during capture]

Figure 7 - Packets Showing Incomplete DHCP Exchange

The packets in Figure 7 above revealed that there were devices that were not fully completing the IP acquisition process with the Wireless Access Gateway.

The raw packets were sent to the Wireless Access Gateway vendor and it was identified that there was a bug in their software that would prevent devices from completing the IP acquisition process in specific circumstances. A custom dashboard shown in Figure 8 was then produced to identify the same issue going forward.

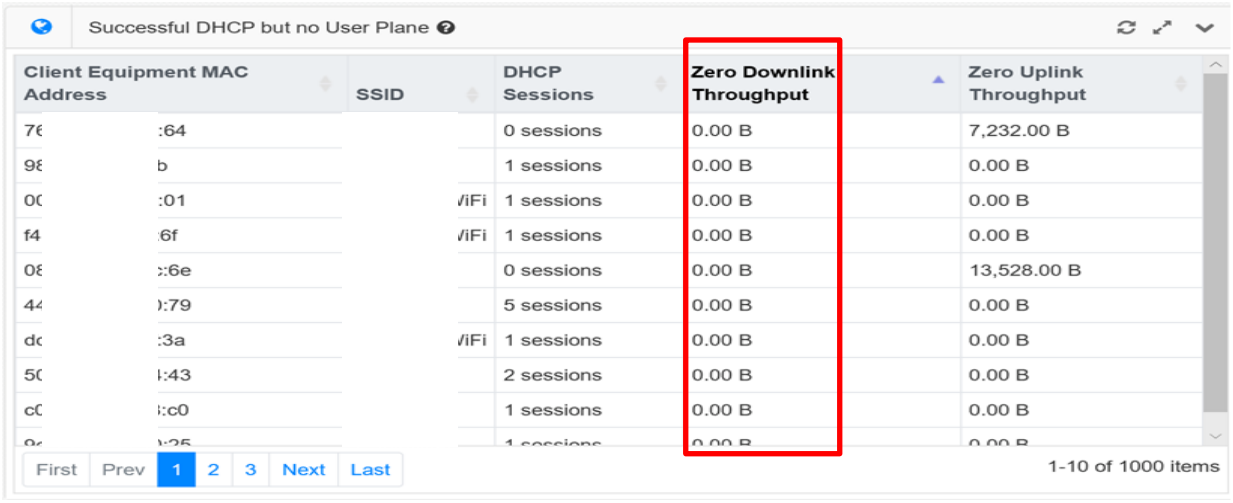

Figure 8 - Custom Smart Data Dashboard

5. Conclusion

Smart Data technology utilizes packet data and generates elastic metadata through pervasive, edge-to-core instrumentation in a distributed operator network. This metadata can be consumed by a variety of upstream applications focused on service operations, network automation, customer experience, SLA management, and security. By leveraging Smart Data technology, the operator teams can proactively monitor, assure and secure all IP services (voice, data, and video) which may run across different domains (physical, virtual, or cloud) and access networks (fixed or wireless) using the same views and workflows. By relying on a common, high definition data platform that provides "visibility without borders", operators can go through their network transformation journey with confidence to innovate while delivering an unparalleled customer experience.

Abbreviations

MVNO	Mobile Virtual Network Operator
MAC	Media Access Control
SSID	Service Set Identifier
HTTP	Hyper Text Transfer Protocol
IoT	Internet of Things
SLA	Service Level Agreement
MSO	Multi System Operator