The Shift from Element Monitoring to Packet Monitoring to Service Monitoring

Ian Wheelock, Principal System Architect, ARRIS
Hari Nair, Sr. Staff Architect, ARRIS

Contents

Introduction

DOCSIS networks have always had good instrumentation for cable plant monitoring. The cable modems in the plant also function as probes for the network providing the operator good visibility into physical plant conditions. However as DOCSIS networks become the ubiquitous access network over which a wide variety of media and communications are delivered, and subscriber expectations of quality of service have been raised, operators have wanted to expand their understanding of network conditions from physical metrics to the quality of service delivered to customers.

In this paper, we describe a method to expand the role of DOCSIS Customer Premises Equipment (CPE) from physical and packet- level monitoring probes to aiding in service monitoring. We describe the considerations in the choice of active probes, the network, and service impact considerations from performing these tests.

Existing Element Monitoring

Current DOCSIS CPE provides a number of different measures that can be routinely sampled to develop an overall picture of how well the physical cable plant is operating. At a minimum, signal strength and downstream SNR values can be collected by the CPE, while upstream signal strength can be collected by the CMTS. Recording the actual downstream and upstream channels in use by the CPE allows for a network-wide view of physical cable plant performance to be accumulated over time. Maintaining time-based records of plant performance helps with identifying trends associated with plant health.

Metrics relating to received and transmitted packet and octet counts can also be sampled. Such sampling may be performed by a management system that collects details from either some or all of the CPEs and CMTS systems deployed in the cable plant. Combining the collected metrics with metadata associated with the CPE (such as traffic tier) and CMTS information (such as upstream and downstream channels) allows the management system to provide useful statistics as to the overall data health of the DOCSIS network.

Extensions like IPDR on the CMTS enable management systems to get access to accurate byte counts for individual CPEs with granularity down to the DOCSIS service flow level. These byte counts can be used to determine overall usage levels of each individual subscriber, helping with limiting excessive usage or feeding into billing systems for MB level billing.

The accumulated data metrics can also help with capacity planning. The constant 24-hour a day monitoring of the data performance of the network on an upstream and downstream basis (or on a more logical notion of DOCSIS 3.0 downstream or upstream service group (DS-SG or US-SG)) provides the actual data use versus the capacity of the network. Network management systems perform analysis of these figures and present information to the operator identifying problem areas of their network that are running above acceptable performance thresholds. Such analysis allows service providers to plan for capacity expansion of their networks in order to keep up with the data demand from their subscribers.

VoIP related monitoring is also provided by some management systems based on information available from deployed DOCSIS MTA devices and CMTS platforms. Such management systems help with the complete VoIP lifecycle management, from initial network analysis and optimization to ongoing fault, performance, and capacity planning. Mean Opinion Score (MOS) data collected from MTAs is used in the analysis of the service.

Utilizing all these different types of monitoring provides service providers reliable and useful information as to the performance of their network. The metrics are provided to the operators through suites of analysis and graphical tools. Some management systems tie these basic metrics together and generate summary 'performance at a glance' metrics, arranging the most likely problem areas in optimum ways for the provider to act upon.

Even with all this data collection and analysis, the only real customer "service" that is being actively monitored is VOIP. Data bandwidth levels are monitored, but only really tell a small part of the customer experience. With so many services being delivered either by the operator (basic web serving, QAM based video service, walled garden IPTV service, Wi-Fi service, etc.) or 3rd parties across the operator network (basic web serving, OTT video, gaming, storage backup, etc.), getting visibility into how well these services are performing from a subscriber viewpoint is critical to reduce churn and optimize the network.

Advanced Network Probes

Some systems do exist in the market to cover areas such as QAM based monitoring and IP service monitoring. These systems typically require a physical 'probe' unit to be deployed either in the operator's network (in the case of end-to-end MPEG video monitoring) or by technicians into a subscriber's home location.

MPEG video monitoring probes in the operator network are deployed and maintained as part of the overall video monitoring setup. They are in constant use providing real-time status information as to the quality of delivered video streams and associated metadata (SI, PSIP, etc.). Multiple probes deployed in series provide operators with visibility in to how well the MPEG video streams are operating before they hit the final EQAM devices for transport over the HFC plant. Such monitoring enables faster troubleshooting in the event of a video outage, ruling the network in or out as the source of the outage.

Probes can also be used by technicians to troubleshoot issues occurring during installation or, alternatively, can be deployed into a subscriber premises after problems post-installation have been reported. Providing the probe for remote troubleshooting is more cost-effective than having a technician on site for hours or days attempting to observe a subscriber issue and then attempt to fix it.

New classes of probes are going beyond the basic analysis of MPEG video, and are now beginning to analyze the performance of IP, in particular IP video delivery. They are typically deployed as "man in the middle" probes, being able to observe all IP traffic of interest delivered to and coming from a subscriber network on a real-time basis. Monitoring traffic using this technique assists in determining the performance of such traffic, for example monitoring and reporting the bit rate associated with an adaptive bit rate (ABR) IP video stream being played by a subscriber device.

Deploying physical probes into subscriber premises attracts additional CapEx (probe cost) and OpEx (deployment) costs. These costs seem to be justified in terms of the results associated with using them (e.g. dealing with customer issues efficiently and keeping happy customers).

Now, imagine having the ability to enable equivalent probe functionality in the entire subscriber footprint of the service provider network without having to order a new piece of physical equipment or arrange a truck roll to deploy it.

Measuring Network Performance

The FCC has been operating a program known as "Measuring Broadband America[i]" for the last number of years. The program was developed out of a recommendation by the National Broadband Plan (NBP) to improve the availability of information for consumers about their broadband service.

The goal of the program is to identify the nationwide performance of residential wireline broadband service in the United States. The program has concentrated on examining service offerings from the 13 largest wireline broadband providers using automated, direct measurements of broadband performance delivered to the homes of thousands of volunteers. Volunteers are provided with measurement devices known in the study as "Whiteboxes" that are configured to run custom software from SamKnows (a UK based company retained under contract by the FCC to assist in the program). The most recent report by the FCC contained measurements from over 6,700 Whiteboxes deployed across the footprint of the 13 selected broadband providers.

The Whitebox software runs a collection of periodic tests that aim to collect data representative of typical services in use by subscribers. Technical details of the 2013 report are available online[ii], but a summary is presented here.

The tests run by the Whitebox platform include download/upload speed, web browsing, UDP latency and packet loss, video streaming, voice over IP, DNS resolution and failures, ICMP latency and packet loss, latency under load, availability and consumption. The tests were conducted by the Whitebox devices to remote test nodes operating outside of the broadband providers' networks. Test nodes were also deployed within the networks of the broadband providers and results were collected to those nodes, but were not included in the final results of the most recent (Feb 2013) report.

The February 2013 report, as in previous reports, emphasizes two metrics that are of particular relevance to consumers: ***speed*** and ***latency***. The report highlights the results of the following tests of broadband speed and latency:

- Sustained download speed
- Sustained upload speed
- Burst download speed
- Burst upload speed
- UDP latency

The FCC program has become an important indicator of wireline broadband performance. A number of large cable service providers actively participate in the study. The use of Whiteboxes in the network to conduct packet based testing and the acceptance of the results by the providers and wider broadband community indicates

that active subscriber side measurement testing is extremely valuable and is considered representative of user experiences.

Creating a DOCSIS CPE Probe

Based on the brief technical description provided by the FCC on the operation of the Whitebox device, it is clear that the actual measurements themselves are not overly complex. Deploying the same functionality (along with some of the DNS related tests) within existing DOCSIS CPE devices is well within the processing power of these devices.

Existing DOCSIS CPEs have considerable processing capabilities, allowing additional software to be developed to run in the home, such as fully featured routing, voice over IP call handling, configuration web page, etc. Some CPEs already have some basic troubleshooting options for assisting in technician installs, as well as for running local tests remotely from the NOC.

New and future DOCSIS CPEs are being developed using extremely capable SOC (system on chip) processors. The SOCs are incorporating large numbers of functions that formerly resided in external integrated circuits on the CPE motherboard (such as Ethernet switches, MoCA interfaces, voice processing functions, etc.). In addition to the extra functionality, the SOCs are getting much more processing power than before.

This processing power is being targeted at new functions like 'gateways' that provide a one-stop shop for all home networking needs, or as 'application servers' that provide new software services for the home (that would otherwise run on a dedicated PC in the home).

Some of this same processing capability can be utilized to provide monitoring functions in the CPE similar to those available in custom probes. Being able to download a firmware update with probe-like functionality to deployed CPE devices enables the entire network to participate in packet and service monitoring.

Packet Monitoring

Based on the earlier descriptions of network probes and the FCC Measuring Broadband America program, the industry seems to have accepted the use of probes for troubleshooting hard-to-diagnose network issues, and for determining subscriber related latency and speed measurements.

Using modified DOCSIS CPE probes to perform these FCC-style tests provides the option to have visibility of performance across the entire DOCSIS network footprint. Running these tests and reporting real-time results can help identify real issues occurring before a customer call center is inundated with support calls.

Control Platform

Specialized control platforms are required to manage such large numbers of available probes in the network. Coordinating subsets of probes to run tests across the network requires advance knowledge of probe presence within the topology. In addition to running the tests, the actual results of the tests must be collected and stored. The stored results are then analyzed to provide refined performance results to the operator in real-time. Analysis rules must be defined to limit the total information supplied to what can be used.

Overall performance data from every node in the network can be modeled. In the case of parts of the network reporting poor performance, the control platform must be able to integrate with other management systems that are already performing element monitoring (for plant monitoring and data counts). The combination of the packet monitoring and existing element monitoring provides a powerful tool for troubleshooting issues in the network. Not only can the probes be used for periodic performance monitoring of the entire plant, they can also be brought to bear on issues identified by other management systems. Running actual traffic tests through problem areas of the plant can help diagnose issues.

The control platform needs to understand the location of test nodes that the probes rely on to conduct their tests. The FCC report relied on results from Whitebox to off-net test nodes. In the case of monitoring the DOCSIS network, on-net test nodes can be used by the probes as well as off-net test nodes.

As the DOCSIS CPE probe is a software modified cable modem, activating this software has the potential of enabling probes at every point of the network. This is an extremely powerful benefit, but one that has to be managed carefully. Running performance tests on every modem in a network segment at the same time will completely saturate the data network. Careful probe selection across the network topology and scheduling of test runs, performed by the control plane platform, is required to minimize the overhead of traffic testing to the overall network. At a minimum, selecting single probes on every DS-SG/US-SG would likely give sufficient coverage across the network. The speed tests could be organized to run periodically, say once an hour, but those

tests can generate large bursts of traffic. In an effort to get more visibility per hour of collected results, more probes may be required per DS-SG/US-SG. Some other tests, such as UDP latency, can run for much longer periods but only generate minute amounts of data. Scheduling tests to run across every hour while minimizing the impact on the network is crucial to getting realistic performance monitoring metrics.

Internal Network Monitoring

In most cases, the on-net test nodes used by probes will be located relatively close to the CMTS the probes are associated with. However, it is also possible to consider using on-net test nodes throughout the data network to provide additional network visibility. Having probes communicate across internal boundaries in the provider's network allows traffic routing performance to be monitored. Tracking the results of probe tests to these remote on-net test nodes can provide an indicator as to how stable the routing of the network is. Marked changes in latency or speed performance across these results can point to network equipment outages, incorrect route updates, DNS issues, or other subtle networking issues.

Service Monitoring

Deploying DOCSIS CPE probes and using the limited set of FCC tests outlined earlier (along with DNS related tests) brings a new dimension to determining the performance of the network. Like existing element monitoring, results of the tests can also be retained and used for trend analysis to understand if changes to the network are resulting in realistic performance benefits for users.

The limited tests are concentrated in specific areas, though. They are focused on speed and latency and do not directly consider the performance of services, such as IP video or VoIP. The FCC-deployed Whitebox does include the ability to run additional tests more focused on these areas.

With the introduction of more powerful SOCs as outlined earlier, the newly released latest generation DOCSIS CPE platforms and gateways are much more capable of running software to mimic services such as IP Video streaming or testing VoIP services. As well as acting as service clients, these devices can also be modified to perform "man in the middle" analyses, monitoring service specific flows directed to connected home devices. Monitoring the actual TCP connections allows for bandwidth, delay, packet loss, and other performance indicators to be identified in the home in a similar fashion to how some existing network probes operate.

These new platforms also provide Wi-Fi and MoCA networking services to the home. Using the same "man in the middle" monitoring, it is possible to distinguish between the different network interfaces in use and provide targeted network measurements. Such measurements can be very useful, for example, in helping to determine degraded home Wi-Fi performance.

Some of these platforms are hybrid devices, providing both MPEG QAM video tuners alongside DOCSIS tuners. Such platforms can be adapted to provide the typical QAM MPEG video analysis provided by standalone probes available today. Running the full set of ETSI TR101290 fault detection is doable within the processing power of the new SOC platforms. Spectrum analysis features within the DOCSIS platforms can also be combined with the fault detection to provide a complete QAM monitoring solution. As devices such as these are deployed within the DOCSIS network, they can start to act as "canaries," performing QAM/MPEG video analysis on behalf of existing STBs in the network that are only capable of playing back video.

Conclusion

The existing network management platforms in use today rely heavily on element monitoring of CPE and CMTS devices. The information provided helps with capacity planning and troubleshooting network problems. The broadband industry seems to accept the use of distributed probes to collect detailed performance data for their networks. Extending the DOCSIS CPE device with basic network test functionality effectively makes it a probe. Coupling these probe devices with new back-office software to coordinate the probes across the DOCSIS network brings visibility to how the overall network is functioning. Comparing all parts of the network together helps identify where the network is running at peak performance, or where problems exist. Integrating the probe results/analysis with existing element monitoring helps to develop a bigger picture of how the network is running. Extending the probe capability in newer SOC platforms brings even more visibility into service monitoring. New hybrid devices bring the capability of QAM/MPEG video analysis enabling real end-to-end video monitoring wherever such platforms are deployed in the network. Being able to collect performance results of how well services are being delivered over different home network interfaces helps determine subscriber quality of service and quality of experience.

---

i http://www.fcc.gov/measuring-broadband-america

ii http://data.fcc.gov/download/measuring-broadband-america/2013/Technical-Appendix-feb-2013.pdf