ENHANCED PLANT AND SYSTEM MONITORING USING OPEN-STANDARD DATA CHANNELS AND TOOLS

Aran Sadja, Eric Holcomb & Lee Pedlow
Sony Electronics Inc.

***Abstract*—The complexity and scope of present cable networks eclipse its analog predecessor. The demand for unimpaired service availability and network robustness has been elevated as customer acceptance and dependency has grown for new revenue opportunities such as telephony, broadband data services, video-on-demand and extensive channel offerings, all enabled by the digital revolution in cable television. These new services depend upon networks with high fidelity. The barrier separating error-free reception and complete loss of service is often less than a decibel.**

Operators faced with the requirement for improved service, reduced downtime and 24/7 network availability are also facing the need to reduce capital expenditure, truck rolls and personnel costs. Current solutions for extensive network monitoring are both cost prohibitive and have limited scope of information as well as limited observability, often only providing data for a node or trunk and not to each subscriber tap or CPE.

Cable network infrastructures can vary from plant-to-plant, node-to-node and trunk-to-trunk. From mode hopping lasers and noisy amplifiers to ranging cable modems, operators are challenged by a diverse set of issues that may seem impossible to troubleshoot with any one existing technology.

Using only open-standards, Sony was able to create a unique and encompassing system monitoring tool with unlimited expansion capabilities that can in real-time analyze plant data and automatically report any instances where the quality of service is below established thresholds or suspected failures were found.

Index Terms—**Digital Cable Television, Systems Integration, Open Cable, Network Management**

I. INTRODUCTION

This paper presents an overview of technology and tool sets developed by Sony allowing operators to gather extensive metrics on their entire network, including transports and channels, all the way from the head end to each subscriber device. Information is aggregated and presented in a web-based tool providing operations staff at any level information with variable scope at the network, node, tap or device level. The system includes assignable watermarks for warnings and alarms that in turn automatically activates email, text messaging and paging systems. Trend data is obtained at selectable intervals and this data is stored indefinitely for future auditing, QA, analysis or other purposes. Because the granularity of scope is user selectable, quick determination of where a system fault has occurred can more easily be made, allowing deterministic action to be taken before a call center is flooded with customer complaints. It also facilitates reduction of service labor costs and unnecessary truck rolls because problems can be pinpointed. Problems localized to wiring or other problems at a customer premises are determined without having to dispatch representatives on-site. In many cases, these issues, the source of which having been conclusively identified, may then be delegated to customer service agents and handled over the telephone with the subscriber.

All this capability comes without the need to purchase and deploy costly and complex specialized test equipment and the data server is hosted on an inexpensive PC. The information is made available using existing communications within the subscriber device and extensions to standard protocols.

II. OPEN-STANDARD DATA GATHERING

The first hurdle in creating a plant-wide monitoring system is gathering the appropriate data. Unfortunately, a typical digital cable plant may ultimately have equipment from a number of different vendors, each one possibly using their own proprietary remote monitoring system. In such circumstances, a comprehensive monitoring tool would require a lengthy and costly upgrade for each individual system, the difficulty of obtaining an API (Application Programming Interface) from the vendor to communicate with their equipment not withstanding.

Fortunately for MSOs, most manufacturers do not create their own remote data query system and protocols. Instead, they use one of two major open-standard systems**.**

The two most frequently used methods for gathering data are currently the open-standard SNMP (Simple Network Management Protocol) and the open-standard HTTP (Hyper Text Transfer Protocol) using XML (eXstensible Markup Language) or HTML (HyperText Markup Language) both of which are also open-standards.

DOCSIS requires, and CableLabs ensures, that every cable modem is equipped with a simple SNMP agent and responds to a standard set of requests. This provides a uniform interface to the cable modem, regardless of manufacturer.

To our chagrin, the rest of a cable plant is not as simple to monitor. Luckily, SNMP is the prevailing choice for remote diagnostics due to its explicit design as a standardized method of “Network Management”. Any SNMP enabled device found in the headend will respond to SNMP requests, including all network infrastructures (CMTS, routers, etc) and most servers (Linux & Windows based).

Another common remote query method used by equipment manufactures is by performing an HTTP GET request and parsing the response data. The data is returned in either in XML or HTML format, which can easily be parsed and the appropriate data extracted, or the data is returned in HTML, as a diagnostics web page from which the appropriate data can also be parsed and extracted.

In rare cases, the manufacturer may not provide a remote diagnostics interface, in which case a simple network connectivity test can help infer whether the device has crashed, is hung-up or has lost power.

The use of open standards by manufacturers allows headend equipment to be remotely monitoring with a single tool that can then analyze and present the data.

III. Open-Standard Data Storage

An important aspect of a large monitoring system is the ability to gather data over extended periods of time in order to examine trend information and detect possible future failures based on that data. This data needs to be stored in a conveniently accessible fashion. Enter the open-standard database query language, SQL (Structured Query Language).

The use of SQL allows the monitoring tool to communicate, sans modification, with any SQL standard adhering commercial or freeware database, providing the tool with a multitude of options for data storage.

IV. Headend Redefined

The advanced cable systems of today are vastly different from their analog ancestors. Advanced devices and infrastructure that provide digital video, video-on-demand content, and data services are replacing headends once solely populated with simple legacy analog equipment. The replacement equipment provides more than just a system upgrade to digital video services, but as an integral part of a networked multimedia architecture, this equipment is also capable of reporting on the status of the device and on the information flowing through it. This allows today's system operator to monitor the equipment and meet the challenges of managing such an environment with its corresponding expansion of scope and complexity.

V. Headend Equipment

Effective monitoring begins in the headend, ensuring the core systems of the cable operator are functioning as expected and providing early detection of problems. The Sony system uses various communication paths to aggregate headend systems status. All SNMP (Simple Network Management Protocol) and HTTP (Hyper-Text Transfer Protocol) enabled devices can be polled on scheduled intervals for status updates. Information about video/data delivery, device statuses and real-time log files can be stored on a centralized monitoring server thru the use of databases and the Linux syslog service. By monitoring and analyzing the incoming data, based on MSO defined criteria, the system can automatically take scripted response actions and/or alert appropriate personal through pagers, text messaging, email or other means. This allows efficient problem notification and resolution, minimizes downtime, and reduces maintenance costs. This data is also accessible via HTTP through any standard web browser for operators to examine at their convenience from anywhere in the private, or alternatively, in the public Internet.

Video services are protected by monitoring source devices such as satellite receivers, remultiplexers, rate-shaping groomers, modulators and upconverters. On-demand video systems benefit from the ability to monitor items such as server CPU loads, memory usage, as well as application specific metrics maximizing uptime and system availability for these advanced services. It is also prudent to monitor the programming to ensure that the premium channels are encrypted, while the clear channels remain in the clear.

Based upon the operators' settings, the appropriate support staff will be notified when there is an ASI input failure on a modulator, an oversubscription on a transport passing through a grooming device, or excessive CPU load on a cluster of VOD servers. Using MSO defined thresholds, problems can be averted or corrected with early warnings triggered by a known pattern of events leading to system failures. In many cases, problems can be detected by effective application of thresholds before they become service affecting from a subscriber perspective and corrective action taken prior to noticeable impairment being reported through a flood of calls to a call center.

Data services can be protected by monitoring network infrastructure and related provisioning servers. Everything from the core backend routers to edge devices such as the CMTS are monitored and the data displayed in a network centric web interface. Detailed information about the health of the HFC network as it relates to the data services is analyzed and presented as it is gathered via SNMP from a DOCSIS CMTS.

Bandwidth utilization, modems per node, metrics on upstream/downstream interfaces and modem RF power can be stored and analyzed providing real-time analysis or historical trend data for the delivery system. Alerts can be targeted to specific personnel specializing in the type of trouble or equipment reporting the malfunction, streamlining problem resolution.

VI. Customer Premises Redefined

With one-way technologies, determining the quality of signal at the customers' premises required the customer to call in and complain. The operator then faced the challenge of determining whether the issue was confined to the customer's location or if it was an area wide issue, affecting a branch, node or an entire hub. If no other customers complain, it could be assumed that the issue was localized but without further information, it impossible to conclusively determine without a truck-roll. A technician must then be dispatched to the location, costing the operator in both time and human resources, to determine the specific source and location of the problem.

With two-way technology, every customer device can play a role in monitoring the cable plant's health. A cable modem can help ascertain the health of signal and assist in determining the physical location of the customer. Additionally, two-way capable STBs containing DOCSIS modems can provide more than just video and program guide services to the customer. The STB can keep the operator apprised of every aspect of the STB in the customer's house, ranging from the current video PID to the CA security device ID. This enhanced use of two-way communications allows a revolution in the way cable operators monitor their plant, with a seamless logical extension of the plant past the tap to the actual devices in the subscriber's home. Thus, for the first time operators are provided the opportunity to monitor the network through its endpoints, not just the infrastructure.

VII. Cable Modems

The cable modem is the customer's high-speed gateway to the internet. In order to stay online, a cable modem performs a continuous electronic repartee with the CMTS and in the process creates a plethora of useful network information stored on both the cable modem and CMTS and available thru the open SNMP standard.

The DOCSIS spec requires all cable modems to be SNMP capable and that the MIBs (Management Information Base) and OIDs (Object IDentifiers) comply with standardized values. Because of this, every CableLabs certified cable modem responds in a uniform way to a standard SNMP request. This provides the operator with the freedom to choose any (or multiple) cable modem manufacturer(s) and never have to change the method of acquiring data.

The type of data available on the cable modem ranges from simple to obscure. Whether the operator wants to know if a cable modem is online, or a technician is concerned with the number of T3 Timeouts, this information is accessible thru the monitoring tool.

Of the data available, one of the most valuable pieces of information to the operator is the ability to get live reports on signal health, a key element of which is the upstream power as sent by an individual cable modem. When a cable modem has to "shout" to communicate with the CMTS, the monitoring tool can help differentiate whether the issue is indicative of a poor return path due to a problem at the customer's site or a node wide issue.

In some ways, both cable modems and digital STBs are more finicky about signal levels and quality then their analog predecessors. In analog systems, picture quality degraded proportional to the degradation of the incoming signal quality. In contrast, the magic and curse of digital transmission is that it provides perfect, error free picture quality until the signal is degraded to a point and then the complete transmission is lost. In many cases, the transition between perfection and total loss may only be a fraction of a decibel. It is important to maintain proper levels across a plant to provide consistent service and margins. By polling cable modems at regular intervals and following trends in signal levels, it is possible to detect current and even predict future equipment failures on the delivery infrastructure.

Thru SNMP it is also possible to track a customer's cable modem should it make its way to another part of the system. With our system and a network diagram, it is possible to determine with a fair degree of accuracy, where that cable modem is physically located, and from previous polls, where it should have been located, based on the time tick value, the upstream and downstream frequencies and which CMTS interface it is communicating on. When linked to the billing system, the monitoring tool can provide the operator with specific customer information for each cable modem and STB.

The data available on the cable modem can help an operator at any level determine a problem with a single cable modem or with a whole trunk. This information is not only available remotely, but can proactively monitor, alert, and even maintain a cable plant's health.

VIII. TWO-WAY CAPABLE SET-TOP BOXES

The digital STB is seen as the customer interface to the digital television realm, providing the user with a crystal clear image and an electronic program guide. However, with a two-way capable STB implementing the open TCP/IP standard, the box can also become a cable provider's most reliable monitoring tool, irrespective of whether the television is on or off.

Unlike cable modems, there is yet to be a standardized interface for remote diagnostics on digital STBs, but the use of SNMP on a network-attached STB can provide a wealth of information. The Sony STB, which has an integrated DOCSIS cable modem and uses a proprietary MIB set was used in the design of our tool, but a standardized set of MIBs can be created to allow easy integration of any two-way STB onto a monitored cable plant.

Whether the STB has an integrated DOCSIS cable modem or uses an Ethernet connection, the data available from each subscriber's STB is priceless to the operator. For example, thru the Sony system, a region-wide STB software upgrade can be scheduled and the tool can provide an upgrade report as well as schedule subsequent upgrade attempts for failed boxes. If a box repeatedly refuses the upgrade, the tool will alert the operator, whom can then take appropriate action.

Information about the digital video signal is also available on the STB. A digital cable STB is essentially a debug tool embedded in the customers' home. While decoding the video, the box is also monitoring various aspects of the signal and this information is available via SNMP. Mismatched audio & video PIDs can easily be detected by a poll of the system, QAM data, downstream power levels, bit error rates, SNR, mislabeled channel descriptors and any other information specified in the MIB can be monitored. In the event of a customer call, this information can be used to assist the support technician in determining the cause of the problem.

CA (Conditional Access) information is also made available thru remote diagnostics. Theft of service can be addressed through real-time monitoring of CA using the monitoring tool. When tied into the billing system, the monitoring tool can track PPV or VOD purchases, check when the last account report-back occurred, compare service tier to actual viewing, and in the case of a roaming or rogue access cards or devices, an alert can be sent out and the offending card then be deactivated.

Additionally, a cable operator may want to take advantage of the fact that real-time viewing statistics and habits can be gathered from the STB, within the privacy limits allowed by law. A system poll can tell the operator how many STBs are tuned to any particular channel, and stored data can be analyzed and used for marketing purposes.

IX. PRESENTATION, NOTIFICATION & RESPONSE

Collecting data is half of a monitoring system; the final challenge in creating a versatile solution is providing an interface, notification and response system that is accessible, intuitive, customizable, and capable of filtering the massive quantity of data accumulated while monitoring a cable plant.

To make the data available to the widest audience possible it is advantageous to use an existing open-standard protocol that is already ubiquitous, so HTTP or the "web" was a natural solution. The use of HTTP allows worldwide access to the data thru any browser-enabled device, ensuring availability to technicians with a computer, cell phone, PDA, etc. The data presented can be filtered depending on the device and user, optimizing the time needed to diagnose a problem.

One aspect that has proven both attractive and effective for a major cable operator was to provide key field staff inexpensive laptop PCs and cable modems. This allowed these personnel to access the monitoring data in the field from any available cable network tap to evaluate, in real time, the effect of their corrective actions on the aggregate and individual downstream customers. Sometimes data was monitored in this manner even while climbing a pole!

A monitoring system is not effective without alarm and warning notifications. Gathering data for presentation is useful, but requires constant monitoring in order to repair problems as soon as they arise. To be a proactive monitoring system, definable alarms and subsequent notifications are necessary.

All the data is sorted and formatted for presentation; visual contrasts (colors, font, size etc.) are used to delineate sources of information and to indicate warnings and alarms. Additionally, personnel can have a customized view of the data that addresses their specific needs.

For security, the web interface can either be made publicly available, or a user authentication system can be used to protect the pages. Monitoring system administrators have a separate login and can adjust alarm watermarks, data sources, email recipients and other aspects of the tool thru the web.

Gathering data for presentation is useful, but requires constant monitoring in order to repair problems as soon as they arise. To be a proactive monitoring system, our system allows definable alarms and notifications as necessary. The use of the open-standard, SMTP (Simple Mail Transport Protocol) to email notifications allows a multitude of devices to receive the warnings.

Email alerts are fully customizable and can be sent to any number of recipients and different alarms can be sent to only the appropriate personnel. It is also possible to tailor the notifications to the receiving device; a terse version of the alert can be sent to pagers, cell phones and other mobile devices, while a fully detailed message is sent to standard email accounts.

The tool can also be configured to perform automated responses to failures that have definable remedies, e.g. When a device fails, the monitoring tool can switch the system over to a backup device or when a simple power-cycle is the accepted resolution to an issue, the monitoring tool will contact the network-attached power-switch to reset the equipment.

X. CONCLUSION

Cable Headends are complex and dynamic environments that may be difficult and costly for personnel to keep track of, but by incorporating open-standard monitoring solutions, we have created an automated system capable of monitoring an HFC network from headend to customer node.

This comprehensive monitoring solution saves time by freeing personnel from repetitive tasks that can easily be automated. By analyzing data and sending out notifications, repairs can be made before the customers' viewing experience is compromised. This not only saves money by accelerating repair it also keeps the customer satisfied, reducing churn and disconnects.

Monitoring of backend networks in addition to the statistics gathered from advanced 2-way CPEs (Customer Premises Equipment) employing DOCSIS provides metrics on the entire HFC network. When this monitoring end-to-end paradigm is applied to the MSO's network, the 100% uptime required by today's demanding customer can be better realized.

REFERENCES

[1] *Data-Over-Cable Interface Specifications: Radio Frequency Interface Specification* (Cable Labs SP-RFIv1.1-I08-020301:2002)

[2] ANSI X3.135-1992, *Database Language SQL*

[3] ISO/IEC 9075:1992, *Information Technology-Database Language-SQL*

[4] Jonathan B. Postel, *SIMPLE MAIL TRANSFER PROTOCOL*, RFC 821, Information Sciences Institute, University of Southern California

[5] D. Harrington, R. Presuhn , B. Wijnen, *An Architecture for Describing SNMP Management Frameworks*, RFC 2571, The Internet Society (1999)

[6] *Standard Generalized Markup Language* (SGML) ISO 8879[SGML]

Aran Sadja is in Digital Platform of America (DPA) Tel: 858-942-1438 e-mail: Aran.Sadja@am.sony.com.

Eric Holcomb is in Digital Platform of America (DPA) Tel: 858-942-6089 e-mail: Eric.Holcomb@am.sony.com

Lee Pedlow is in Digital Platform of America (DPA) Tel: 858-942-2538 e-mail: Lee.Pedlow@am.sony.com.