Integrated Network Management Across Multiple Services – Time Warner Cable's Regional Operational Support Systems

SCTE TEC EXPO – June, 2007

Kristopher Kortright, Time Warner Cable
Colin Horton, C-COR
Paula Weaver, C-COR

Contents

ABSTRACT

The cable television network has evolved into the cable telecommunications network, as MSOs deliver multiple services to their subscribers using a blend of their digital network and HFC infrastructure. The current service offerings of high speed data, switched digital video, Voice over IP, video on demand and commercial services now require sophisticated and integrated routines for monitoring, troubleshooting, and resolving service affecting events. In addition, to maintain the level of customer satisfaction required of a telecommunications network, the impact of the service affecting event must be immediately communicated to customer service, dispatch, NOC technicians, operational groups and ultimately the subscriber.

This paper will discuss the concept of an Operational Service Communication Tool (OSCT) which integrates all of an MSO's network monitoring platforms into one "source of truth" and the best practices for proactively monitoring and managing multiple services across the network using that OSCT.

INTRODUCTION

Typical Service Disruption Scenario Today

Today, most MSO's operate multiple independent tools and/or processes for detecting service interruptions. For example, three "no service calls" from the same node often automatically generate a service outage from within the billing system. Because the billing system tracks only the relationship of subscribes to Nodes (or in some cases Trunk Bridgers or Line Extenders) service outages are declared in multiple nodes by this approach even though the actual cause may be a device that feeds all of these nodes. Issues affecting single services or even components of services (voice mail for Voice Over IP) are not easily communicated to the customer service representatives let alone the subscriber with any accuracy, nor can most billing system outage detection processes detect them. As a proactive customer service philosophy, detecting service disruptions based solely on phone calls from unhappy subscribers is a failure.

NOC or other technical personnel oversee network monitoring or element management tools and can determine that a network device has created a service disruption. However, since there is no representation in the billing system of most of the devices monitored by these tools, web sites, flashes or pop-up screens are used to communicate these outages to the customer service representative (CSR). This service disruption communication technique requires action by the CSR (or in the case of flashes a good memory) while they are in the midst of handling high call volumes in the most efficient manner.

These separate service disruption detection processes often have no way of communicating with each other, and so neither is aware of the service disruptions the other has detected. For example, a CMTS card issue might result in field technicians being sent to 4 or 5 nodes before it is realized that the real cause is in the hub and a headend technician is dispatched.

The typical service disruption scenarios described above using the current methods of outage detection (customer calls) could result in several truck rolls; work orders created for Service Technicians to the home if the CSR doesn't realize the customer is part of a "known service interruption" and work orders for Plant Technician to each of the separate nodes. In the middle of the scenario is the Dispatch Centers who must try to coordinate where the actual problem is on each node. In the above scenario the actual problem was in the headend (CMTS) and not at the separate nodes.

MSO's have continuing goals to improve customer service, and add new services/revenue streams, in addition they face increasing competitive pressures. The typical silo based service disruption management process that is in place today is not likely to improve customer service or seamlessly add new services and the associated revenues.

THE OSCT CHALLENGES

Managing multi-service multi-platform MSO systems is a three-fold technical challenge. The first challenge is the isolation of service disruptions to the exact source across all service lines carried over the MSO network. The second challenge is the dissemination of service impacting information to all points in the MSO organization in real-time. The final challenge concerns the integrity and accuracy of the service delivery topology documentation and on subscriber billing data (maintaining data integrity and accuracy is essential for successful solutions to the first two challenges).

These three objectives together frame the technical challenge of MSO network management today. Management of multi-service multi-platform without meeting these challenges can make the MSO blind to service impacting events.

We will first explore each of these challenges to build a framework for the needs of a network monitoring system.

CHALLENGE ONE – ISOLATION OF SERVICE DISRUPTIONS TO THE EXACT SOURCE

The rapidly expanding variety of services and protocols carried over MSO networks increases the complexity and challenge of fault isolation down to specific customer impacts. Therefore the first objective in monitoring multi-service MSO networks is the synthesis of service degradation and outage information together across all service-lines into a single system. From this common source of truth a coherent, definable point of impact can be determined for most customer impacting events.

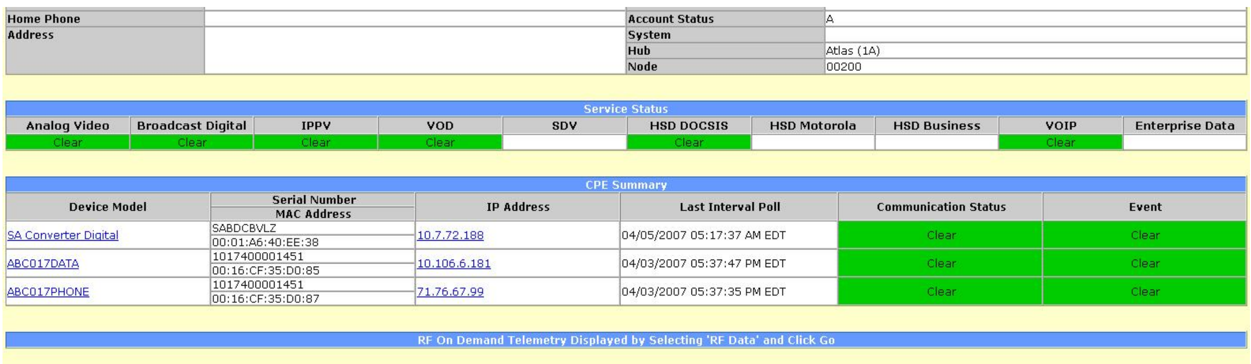
To synthesize service degradation and outage information together, an OSCT must have the following:

1. Sources of Service status at the point of service delivery.
2. Ability to correlate or aggregate individual device service status to points in the service transport topology (in particular, those that are not managed by any other system).
3. Ability to analyze service disruptions on all services in a subscribers home.
4. Data for the correlation process to map individual service statuses to the service transport topology.
5. Knowledge of services and how those services are transported to the subscriber.
6. Monitor managed devices and integrate with other service degradation and outage detection systems.

Today, the subscribers' CPE device is not only critical to the delivery of services to the subscriber but in most cases is also capable of providing information about not only its health, but the health of the transport network feeding it (if data from multiple CPEs is aggregated). A large number of CPE devices are capable of responding to requests for their current on line or off line status (ping) as well as returning telemetry data that indicates the health (RF Receive Levels, TraOSCTit Levels, Error rates, etc.) of the network as they view it. The subscriber's CPEs provide the OSCT their view of network status and health at the point of service delivery in the subscriber's home. Individual CPE statuses can be correlated to generate statistically significant information that can then be used to infer the status of the service transport topology. For service outages, the ping or on/off line status of individual CPEs can be correlated. For service degradations, the telemetry health data can be correlated.

The OSCT's correlation process needs to know the relationship of individual CPEs to the service delivery devices (typically HFC outside plant devices). Billing system data contains information that ties a subscriber and their CPEs to the outside plant device (typically the Node) that is the last active device feeding that subscribers home.

The data from billing can also be used by the OCST to provide an in-home status check of all the CPEs that the subscriber has. The results of a successful on line (Ping) test in a subscriber's home is shown in **Figure 1**. This online test examines the High speed data service, all of the video services delivered by the digital set top box and the Voice Over IP service in this subscriber's home.h



Home Phone		Account Status	A
Address		System	
		Hub	Atlas (1A)
		Node	00200

Service Status

Analog Video	Broadcast Digital	IPPV	VOD	SDV	HSD DOCSIS	HSD Motorola	HSD Business	VOIP	Enterprise Data
Clear	Clear	Clear	Clear		Clear			Clear	

CPE Summary

Device Model	Serial Number / MAC Address	IP Address	Last Interval Poll	Communication Status	Event
SA Converter Digital	SABDCBVLZ 00:01:A6:40:EE:38	10.7.72.188	04/05/2007 05:17:37 AM EDT	Clear	Clear
ABC017DATA	1017400001451 00:16:CF:35:D0:85	10.106.6.181	04/03/2007 05:37:47 PM EDT	Clear	Clear
ABC017PHONE	1017400001451 00:16:CF:35:D0:87	71.76.67.99	04/03/2007 05:37:35 PM EDT	Clear	Clear

RF On Demand Telemetry Displayed by Selecting 'RF Data' and Click Go

Figure 1: Subscriber's Home CPE On Line Test Successful.

Supplying the correlation process data that shows the interconnection of the service transport topology components enables it to automatically determine the root cause of a service disruption. The status of individual CPEs can be related to the last active device feeding them, then that device's parent, and then that device's parent, and so on, thus automatically determining the highest common point in the network that is the cause of a service disruption. The HFC portion of the typical MSO service delivery transport system, which includes Gigabit Ethernet networks, 10/100 Ethernet networks, coaxial cable and passive splitting/combining networks, and Hybrid Fiber Coax (HFC) networks, is shown in **Figure 2**.

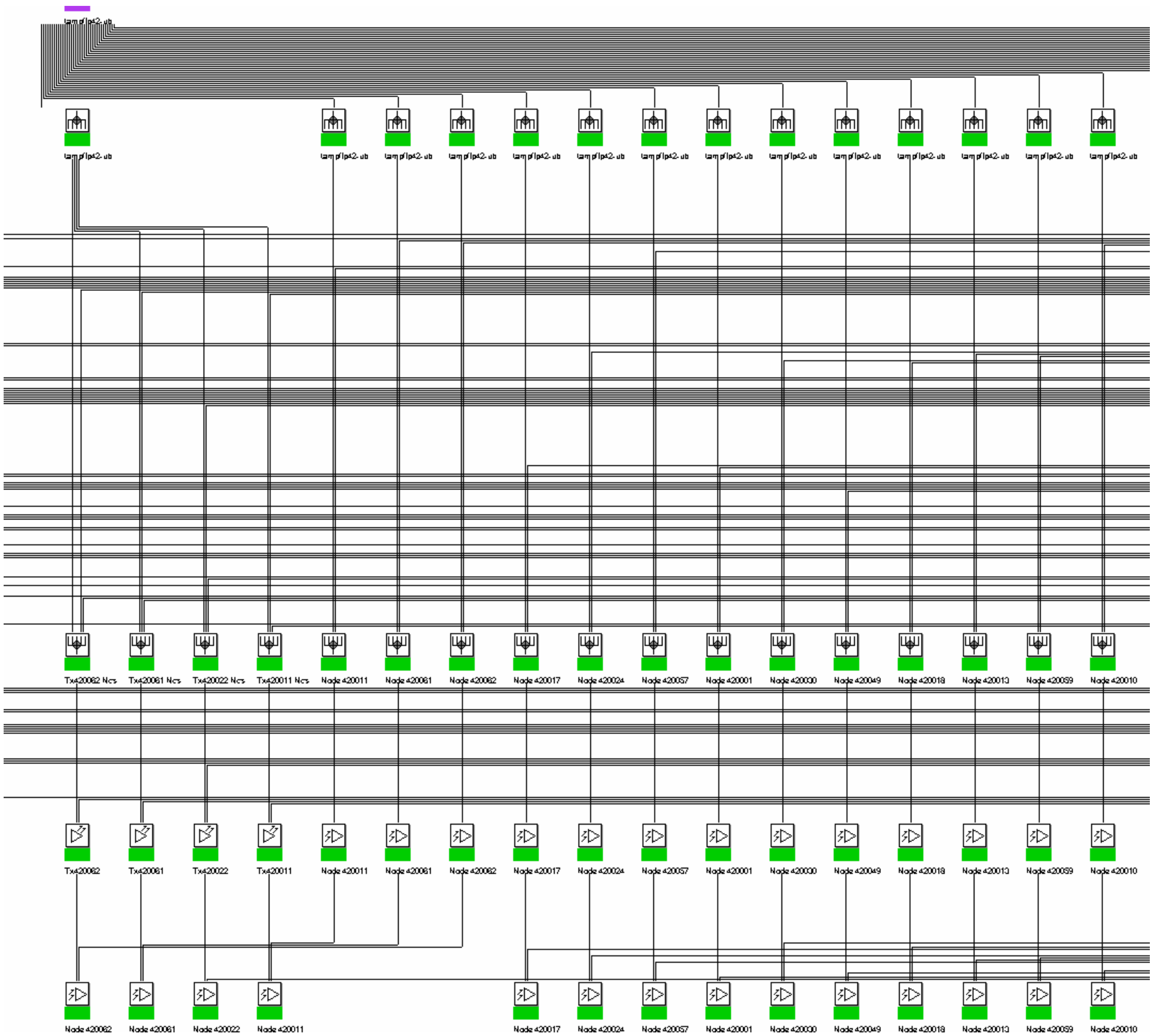


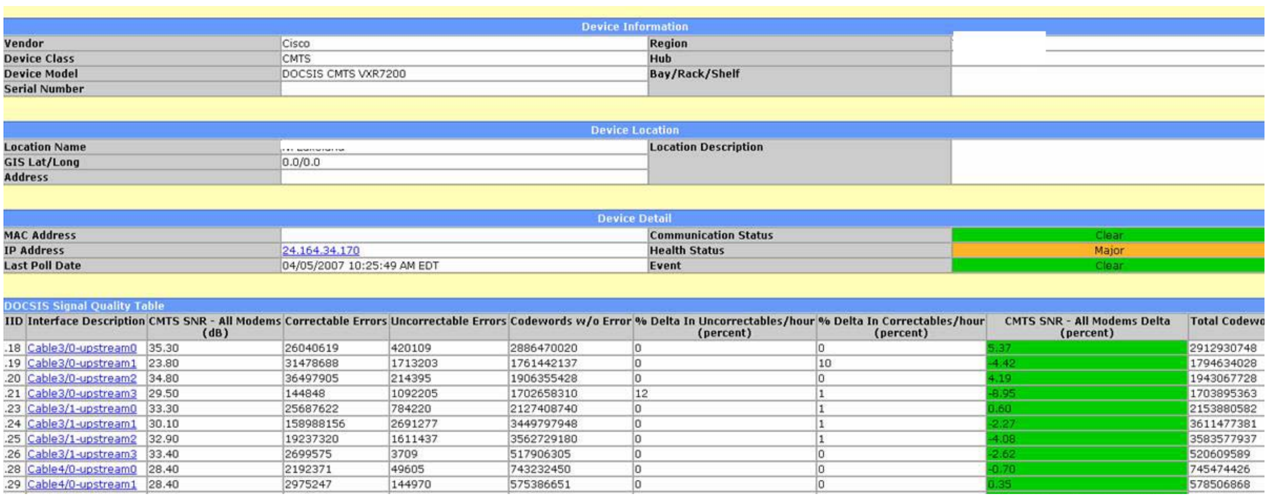
Figure 2: HFC Connectivity Data for a Hub

For the automatic correlation process to work within a hub, the connectivity data must also model how services flow over the physical connections between devices. This way only DOCSIS based CPEs are used to determine the operational status of HFC components that connect the CMTS to the Node. The service flows are defined by the services that the MSO's network supplies:

- Analog video
- Digital Video
- Video On Demand
- High speed data
- Voice over IP

The correlation process can determine the operational status of unmanaged (and often unmanageable devices) especially in the HFC outside and inside plant of a cable network. However, not all service disruptions can be determined from CPEs. In each hub, there are a number of managed devices that can be monitored directly by the OSCT or other management tools. The data from this monitoring can also be used to detect service disruptions.

Devices such as CMTS should be monitored directly by the OSCT to ensure that critical data is available for detecting service disruptions. Where parameters exceed acceptable thresholds, alarms should be generated. A view of CMTS health data that pertains to the reverse path from the HFC plant is shown in **Figure 3**.



Device Information			
Vendor	Cisco	Region	
Device Class	CMTS	Hub	
Device Model	DOCSIS CMTS VXR7200	Bay/Rack/Shelf	
Serial Number			

Device Location			
Location Name	[illegible]	Location Description	
GIS Lat/Long	0.0/0.0		
Address			

Device Detail			
MAC Address		Communication Status	Clear
IP Address	24.164.34.170	Health Status	Major
Last Poll Date	04/05/2007 10:25:49 AM EDT	Event	Clear

DOCSIS Signal Quality Table

IID	Interface Description	CMTS SNR - All Modems (dB)	Correctable Errors	Uncorrectable Errors	Codewords w/o Error	% Delta In Uncorrectables/hour (percent)	% Delta In Correctables/hour (percent)	CMTS SNR - All Modems Delta (percent)	Total Codewo
.18	Cable3/0-upstream0	35.30	26040619	420109	2886470020	0	0	5.37	2912930748
.19	Cable3/0-upstream1	23.80	31478688	1713203	1761442137	0	10	-4.42	1794634028
.20	Cable3/0-upstream2	34.80	36497905	214395	1906355428	0	0	4.19	1943067728
.21	Cable3/0-upstream3	29.50	144848	1092205	1702658310	12	1	-8.95	1703895363
.23	Cable3/1-upstream0	33.30	25687622	784220	2127408740	0	1	0.60	2153880582
.24	Cable3/1-upstream1	30.10	158988156	2691277	3449797948	0	1	-2.27	3611477381
.25	Cable3/1-upstream2	32.90	19237320	1611437	3562729180	0	1	-4.08	3583577937
.26	Cable3/1-upstream3	33.40	2699575	3709	517906305	0	0	-2.62	520609589
.28	Cable4/0-upstream0	28.40	2192371	49605	743232450	0	0	-0.70	745474426
.29	Cable4/0-upstream1	28.40	2975247	144970	575386651	0	0	0.35	578506868

Figure 3: CMTS Health View

The manageable portion of MSO networks are often well managed by existing tools (typically based on SNMP monitoring). These existing tools are specialized and are often heavily utilized by Network Operations Center (NOC) personnel. Because of the valuable service delivery status data that can supplied by these existing systems, their data needs to be integrated into the OCST. For example, an SNMP trap for a large number of modems with high upstream error rates indicates a service disruption for DOCSIS modems and eMTAs.

To integrate this data, the OCST must be able to receive SNMP traps from devices and convert them to an alarm it can understand, or receive alarms from other management tools. To be of value to the OCST, it must be able to integrate these externally generated alarms with its own alarms and be able to relate the source device for these external alarms to devices it knows about in its service delivery network topology data. A diagram showing this external alarm integration is shown in **Figure 4**.

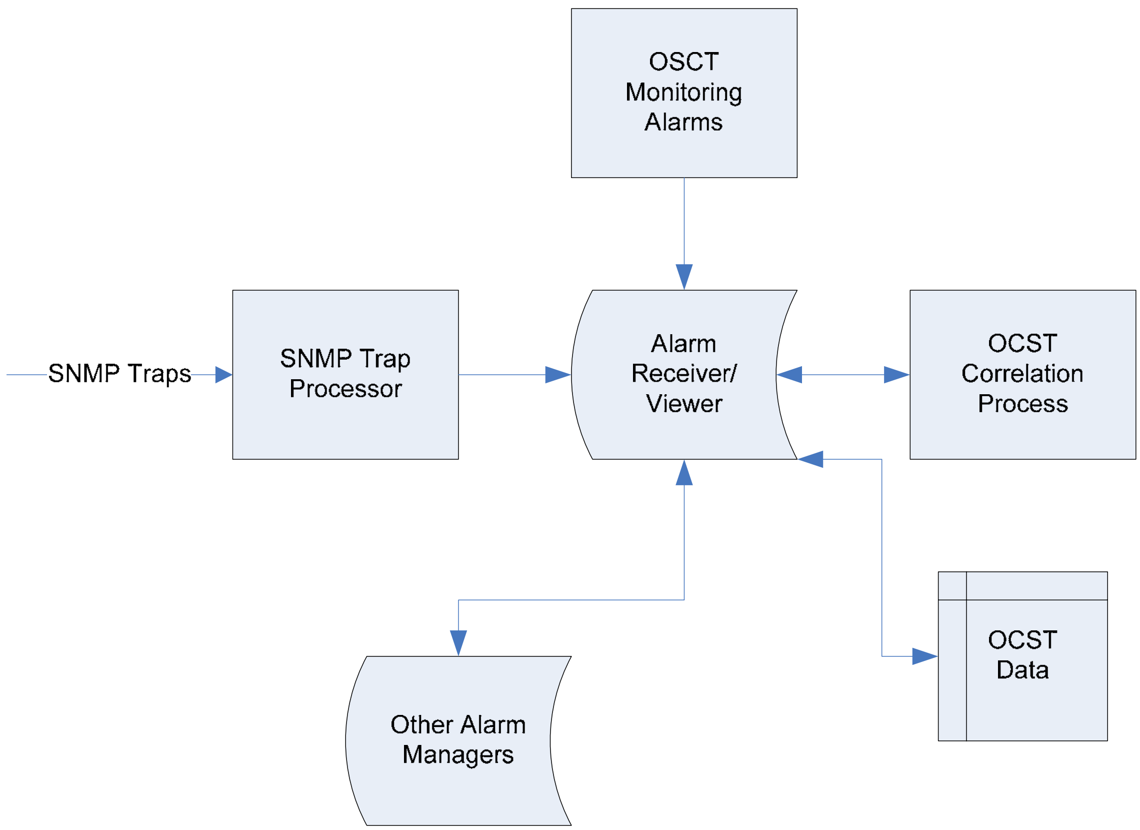


Figure 4: OCST Integration of External and Internal alarms.

Challenge One - Isolation of service disruptions to the exact source, is met by correlating the status of individual CPEs to common points of failure and using telemetry information from managed devices (monitored from within the OSCT or by other managers).

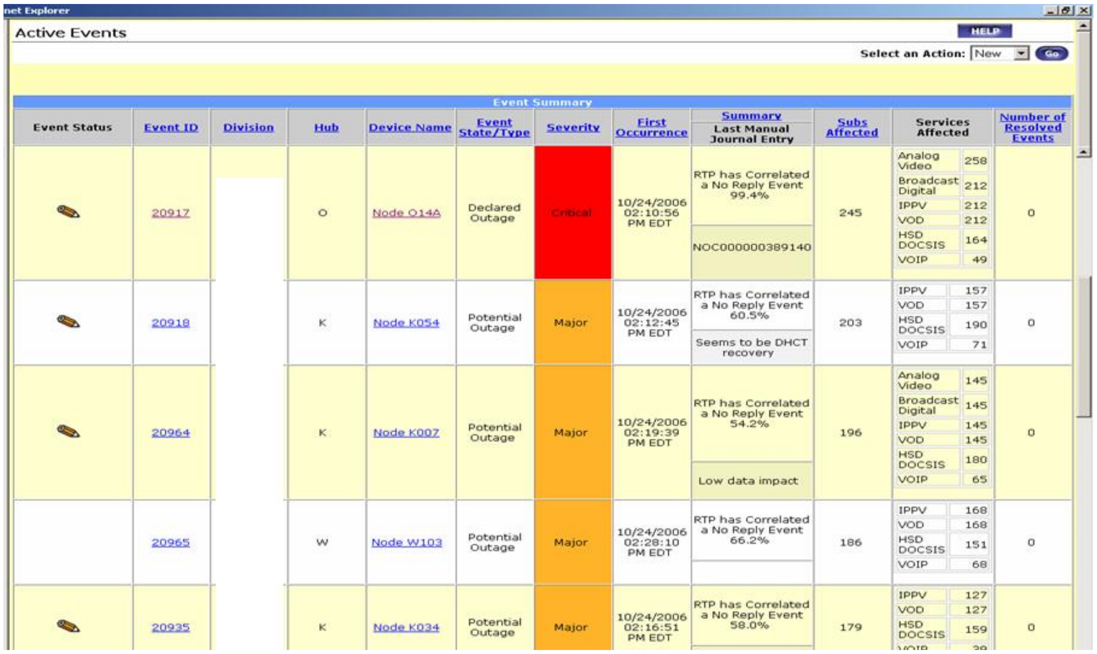
CHALLENGE TWO – DISSEMINATION OF SERVICE IMPACT INFORMATION TO ALL POINTS IN THE MSO

Compounding the fault isolation challenge is the need to communicate subscriber and in-home CPE-level service impacts to all points within the MSO organization in real-time. Communications is typically an under-developed component of most network management platforms, which tend to be focused on engineering and technical audiences. The concept of MSO Operations however is an integrated choreography of NOC, dispatch, field technicians, data center staff and customer service representatives (CSRs) who interact with the subscriber's call. Even the telephony IVR systems that respond when subscribers call are integration points and require real-time knowledge of in-home device and service health.

To disseminate service impact information to all points within the MSO, the OSCT must have the following:

1. Service delivery status information.
2. Means of communicating service delivery status information to all audiences.

The OSCT must take the service disruptions that it has isolated and show the disruption's impact on the subscribers and their services. It must correctly target only those subscribers and only those services that are affected by the service disruption. Note the subscriber's affected information shown in **Figure 5**.



net Explorer

Active Events

HELP

Select an Action: New Go

Event Summary

Event Status	Event ID	Division	Hub	Device Name	Event State/Type	Severity	First Occurrence	Summary / Last Manual Journal Entry	Subs Affected	Services Affected	Number of Resolved Events
	20917		O	Node O14A	Declared Outage	Critical	10/24/2006 02:10:56 PM EDT	RTP has Correlated a No Reply Event 99.4% NOC000000389140	245	Analog Video 258 Broadcast Digital 212 IPPV 212 VOD 212 HSD DOCSIS 164 VOIP 49	0
	20918		K	Node K054	Potential Outage	Major	10/24/2006 02:12:45 PM EDT	RTP has Correlated a No Reply Event 60.5% Seems to be DHCT recovery	203	IPPV 157 VOD 157 HSD DOCSIS 190 VOIP 71	0
	20964		K	Node K007	Potential Outage	Major	10/24/2006 02:19:39 PM EDT	RTP has Correlated a No Reply Event 54.2% Low data impact	196	Analog Video 145 Broadcast Digital 145 IPPV 145 VOD 145 HSD DOCSIS 180 VOIP 65	0
	20965		W	Node W103	Potential Outage	Major	10/24/2006 02:28:10 PM EDT	RTP has Correlated a No Reply Event 66.2%	186	IPPV 168 VOD 168 HSD DOCSIS 151 VOIP 68	0
	20935		K	Node K034	Potential Outage	Major	10/24/2006 02:16:51 PM EDT	RTP has Correlated a No Reply Event 58.0%	179	IPPV 127 VOD 127 HSD DOCSIS 159	0

Figure 5: Service Disruptions Display

The audience consists of the following:

- Management
- NOC
- Dispatch
- Technical Service Representative and Service Technicians
- Customer Service Representatives
- Subscribers

Each audience requires different presentations of the information on service disruptions.

Management should be supplied with data on service disruption history that allows them to measure the total system up time, reaction times before service disruptions are managed, time to restore service disruptions and devices that repeatedly are the source of service disruptions on a region by region or division by division basis.

The NOC is the central place where all service status information is to be reviewed and acted upon, so the NOC needs to see views of all alarms that might affect the delivery of services, such a view is shown in **Figure 6**. The NOC also needs to be able to view the service interruptions that have been detected as shown in **Figure 5**.

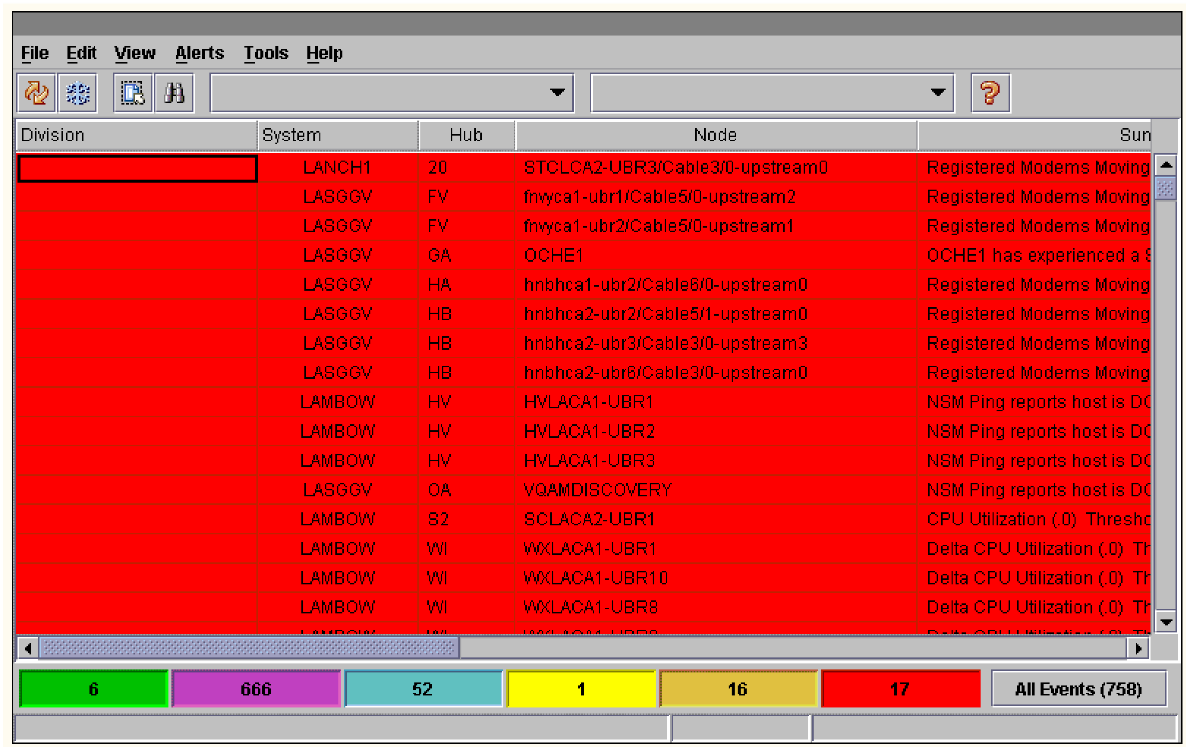
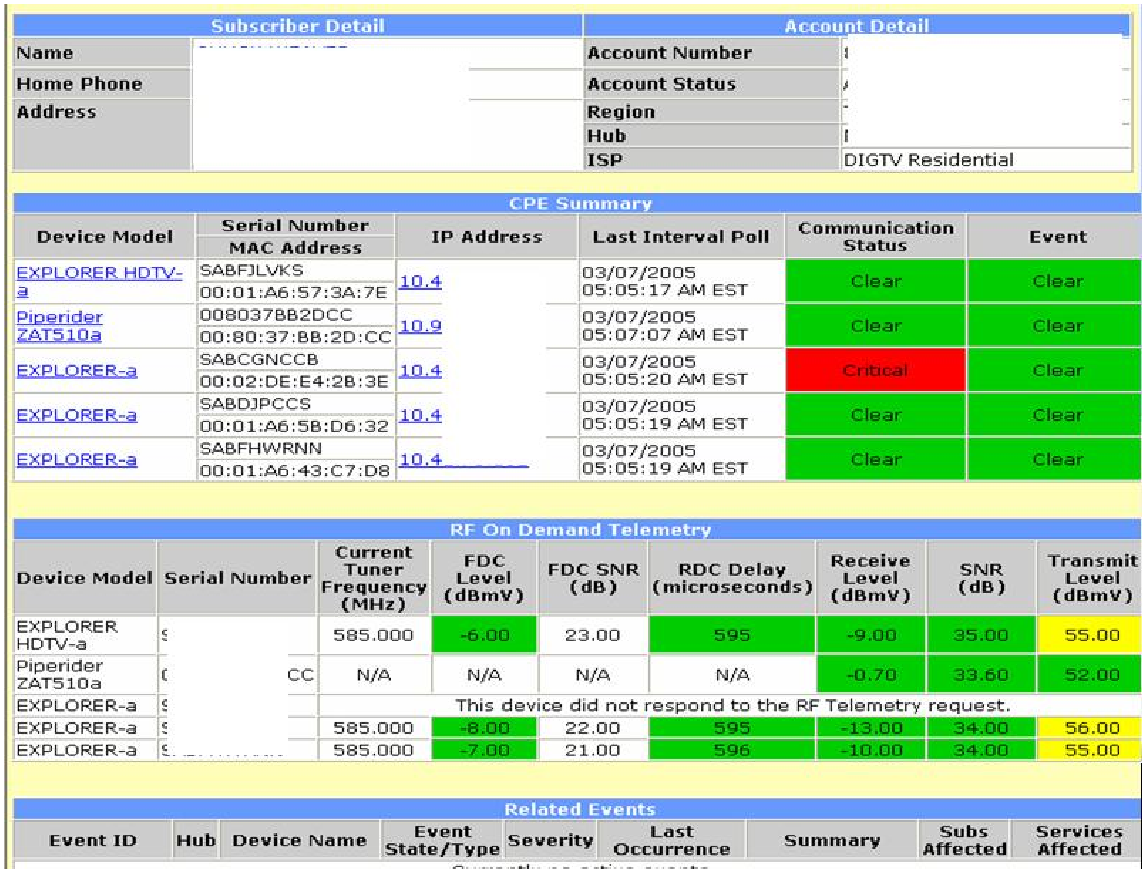


Figure 6: Alarms View for NOC

The dispatch function must be fed information that allows them to dispatch the fix agent to the cause of the service disruption. This information should include the physical location information for the cause of the service disruption, including street address and latitude and longitude.

When a subscriber calls with a service issue and their call is escalated to a Technical Service Representative (TSR), the TSR should be able to view the status and health of the subscribers CPEs. In addition, the TSR should be able to view historical health data to detect intermittent performance issues.

The results of an RF telemetry request of both a DOCSIS modem and a digital set top box are shown in **Figure 7**.



Subscriber Detail		Account Detail	
Name		Account Number	
Home Phone		Account Status	
Address		Region	
		Hub	
		ISP	DIGTV Residential

CPE Summary

Device Model	Serial Number / MAC Address	IP Address	Last Interval Poll	Communication Status	Event
EXPLORER HDTV-a	SABFJLVKS 00:01:A6:57:3A:7E	10.4	03/07/2005 05:05:17 AM EST	Clear	Clear
Piperider ZAT510a	008037BB2DCC 00:80:37:BB:2D:CC	10.9	03/07/2005 05:07:07 AM EST	Clear	Clear
EXPLORER-a	SABCGNCCB 00:02:DE:E4:2B:3E	10.4	03/07/2005 05:05:20 AM EST	Critical	Clear
EXPLORER-a	SABDJPCCS 00:01:A6:5B:D6:32	10.4	03/07/2005 05:05:19 AM EST	Clear	Clear
EXPLORER-a	SABFHWRNN 00:01:A6:43:C7:D8	10.4	03/07/2005 05:05:19 AM EST	Clear	Clear

RF On Demand Telemetry

Device Model	Serial Number	Current Tuner Frequency (MHz)	FDC Level (dBmV)	FDC SNR (dB)	RDC Delay (microseconds)	Receive Level (dBmV)	SNR (dB)	Transmit Level (dBmV)
EXPLORER HDTV-a	S	585.000	-6.00	23.00	595	-9.00	35.00	55.00
Piperider ZAT510a	C CC	N/A	N/A	N/A	N/A	-0.70	33.60	52.00
EXPLORER-a	S	This device did not respond to the RF Telemetry request.						
EXPLORER-a	S	585.000	-8.00	22.00	595	-13.00	34.00	56.00
EXPLORER-a	S	585.000	-7.00	21.00	596	-10.00	34.00	55.00

Related Events

Event ID	Hub	Device Name	Event State/Type	Severity	Last Occurrence	Summary	Subs Affected	Services Affected

Figure 7: TSR View of Subscriber's CPE Health Parameters for all Services

The TSR should then be able to view detailed health data on individual CPEs as shown in **Figure 8** and a history of a CPEs health as shown in **Figure 9**.

Subscriber Detail		Account Detail	
Name		Account Number	
Home Phone		Account Status	
Address		Region	
		Hub	
		ISP	DIGTV Residential

CPE Detail			
Vendor	Scientific Atlanta	IP Address	
Device Class	Set-top Box	MAC Address	00:01:A6:5B:D6:32
Device Model	EXPLORER-a	Communication Status	Clear
Serial Number	SABDJPCCS	Health Status	Minor
Event	Clear	Last Polled	10:53:24 AM EST

Network Detail				
Forward Transmitter	Reverse Receiver	Node	Power Supply	Last Active Device
Tx41011	Node 0055 Rev Rx	Node 0055		Node 0055
Clear	Clear	Clear		Clear

Telemetry Data	
Name	Value
DHCT Status	Ready
BFS Status	Ready
PPV State	n/a
User to Network configuration	Ready
FDC Level {SDiag} (dBmV)	-8.00
FDC SNR {SDiag} (dB)	24.00
Current Tuner Frequency {SDiag} (MHz)	585.000
Tuner Level {SDiag} (dBmV)	-13.00
Tuner SNR {SDiag} (dB)	33.00
Transmit Level {SDiag} (dBmV)	56.00
RDC Delay {SDiag} (microseconds)	595
Transmitted Errors	0
Booted Time	Sat Jan 1:16:36 AM EST (0x41E8B544)
DAVIC Status	Connected
EMM	95
Attempt Date	Never
IPPV last attempt EID	0x0
Success Date	Never
IPPV last success EID	0x0
PowerKey Status	Ready
PTV OS Rev	6:32 PM PST; v3.3.3s5 (1002)
SAM Load Status	Ready QPSK
SI Status	Ready
IPG Load Status	Ready QPSK

Figure 8: TSR view of Detailed CPE Health Data

CH
82
EXI

From: February 28
To: March 7

Poll Date / Graph	Current Tuner Frequency ☐	Tuner Level ☐	Tuner SNR ☑	FDC Level ☐	RDC Transmit Level ☑
03/07/2005 05:05:19 AM EST	585.000	-12.00	32.00	-8.00	55.00
03/06/2005 11:05:18 PM EST	201.000			-8.00	55.00
03/06/2005 05:05:21 PM EST	585.000	-14.00	33.00	-8.00	55.00
03/06/2005 11:05:19 AM EST	585.000	-12.00	33.00	-7.00	50.00
03/06/2005 05:05:20 AM EST	585.000	-11.00	28.00	-11.00	59.00
03/05/2005 11:05:22 PM EST	201.000			-6.00	53.00
03/05/2005 05:05:20 PM EST	213.000			-8.00	54.00
03/05/2005	213.000			-10.00	59.00

Figure 9: TSR View of CPE Health History

The service Technician is scheduled to complete a work order that was scheduled based on the TSR's analysis. The Service Technician prior to their visit to the subscriber's home should view the results of the TSR's analysis.

The customer service representative must be presented with simple red light/green light status information so that they can quickly communicate the subscribers' service status. Based on the information they are supplied, the CSR needs to determine if there is a system level service disruption such as shown in **Figure 10**, or if there is an individual home problem

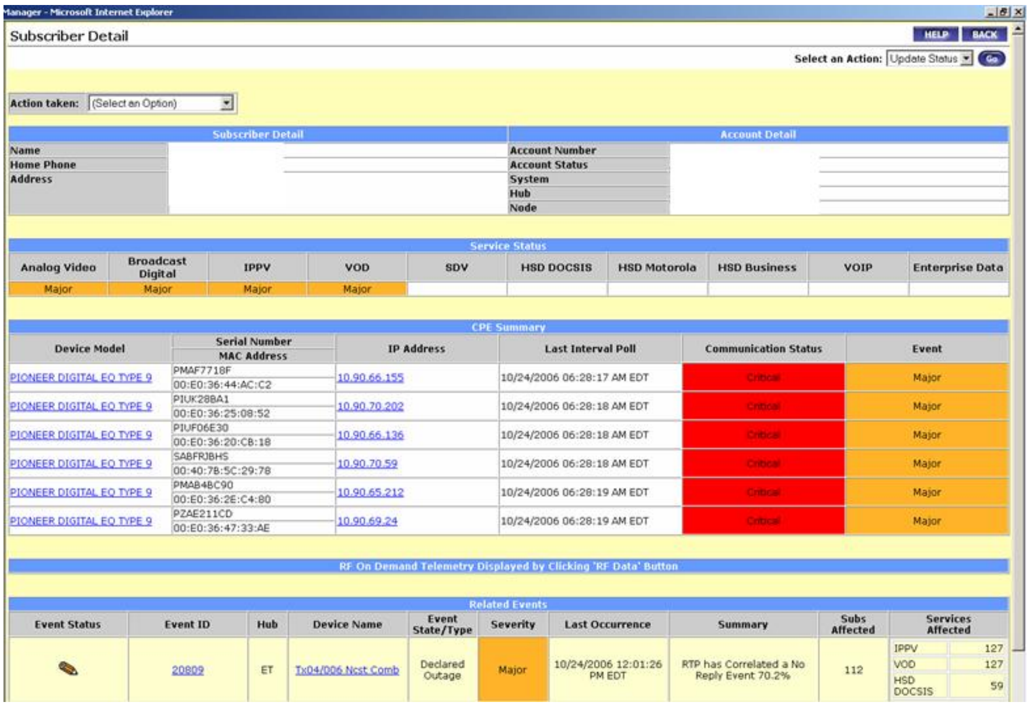


Figure 10: Subscriber's Service Disruption Information

When a subscriber calls about a service disruption, they can be routed to an Interactive Voice Response (IVR) that will automatically handle their call. An OSCT should have an interface that will allow an IVR system to query an individual subscriber's status, respond to the subscriber with their status and eliminate the need for the subscriber to talk to a CSR.

The translation of service disruptions into their impact on subscribers and services requires subscriber data that is resident in the billing system. When the subscriber information is integrated with the service delivery topology, the impact of a service disruption can be determined and communicated to all audiences. The communications objective is achieved by modeling the OSCT user views and reports around the MSO organization, which specific functionality for CSR's, dispatchers, field technicians, NOC operators and plant engineering. When the NOC declares or creates service disruptions, dispatchers and CSRs become instantly aware of them and all subscribers affected by the disruption are so marked in the OSCT. When subscribers call to report trouble, the CSR is empowered with real-time information from the NOC and Dispatch as well as real-time CPE polling of devices in the home.

Engineering views and controls drive the change management events, which are visible to NOC, dispatch and CSR views so that maintenance can be identified as well. Service disruptions correlated to an amplifier, trunk bridger, node or hub and head-end devices allows dispatchers and field personnel to troubleshoot devices that are at or close to the point of impact.

CHALLENGE THREE – MAINTAINING DATA ACCURACY IN SERVICE DELIVERY TOPOLOGY DATA AND SUBSCRIBER DATA

The key to this challenge is that the OSCT must be integrated with sources of data that it depends on and must report data discrepancies so that they can be corrected.

The data required to provide the information on subscribers and their CPEs comes from billing, the OSCT must have the ability to import data from the billing system on a batch or ideally real time basis.

For service delivery topology, the OSCT must have a simple means of loading data either via spreadsheets, or from an external source of data. Typically MSO's have their outside plant data documented in a GIS system as shown in **Figure 101**. The OSCT should be capable of importing service delivery topology information from a GIS source of data. This direct import capability ensures that the information on service delivery topology is accurate and up to date.

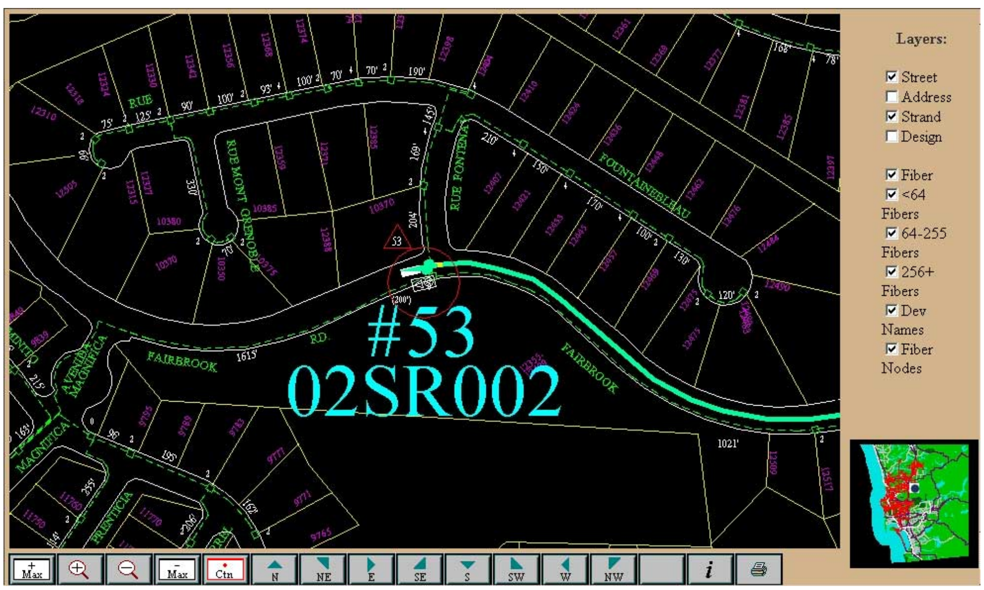


Figure 101: GIS Data for Outside Plant

The OSCT must have the means to detect data errors in the billing or service delivery information and be able to communicate those errors. The MSO must have a change management process in place that updates all billing and service delivery information in the OSCT.

FRAMEWORKS AND STANDARDS

After first exploring the challenges in a complete network monitoring solution today, we now will explore some of the common standards and approaches to network monitoring…

Today, the Information Technology Infrastructure Library (ITIL) and the enhanced Telecom Operations Map (eTOM) provide excellent frameworks for organizing and creating processes that drive network management for the MSO. None of these industry standards define in precise terms how fault isolation is to be achieved in the cable television environment. This task is left to the MSO and its tool vendors and is highly dependant on both the MSO's choice of vendor equipment and their EMS capabilities as well as on the network management platform underpinning the MSO.

Many standards exist for network management communication such as SNMP, Syslog, XML and TL1, but none of them alone provides the whole answer. Most are of no use for the HFC plant. Furthermore no standards exist for how MSO management systems should communicate with one another at a data level when service disruptions affect operations of other client companies, such as voice circuits used to carry VoIP traffic to Telcos or when backhauling video traffic from one region to another. This "Boundary Awareness" concept of identifying and sharing points of impact between companies and between regions and OS systems within an MSO define today's fault isolation challenge.

The OSCT should integrate communication from multiple network management protocols (SNMP, Syslog, XML and TL1) and support data interfaces that allow communications between management systems. Best practices should be developed around the OSCT approach and philosophy of an integrated approach to managing the multi-service multi-network CATV systems in use today and in the future.

CONCLUSION

The challenges of creating and operating an Operations Service Communication Tool have been presented along with what is necessary to successfully deploy and operate such a tool to increase customer service and enhance revenue. In the future, there are opportunities to evolve the OSCT to support new services and/or service delivery platforms such as DOCSIS Set Top Gateways (DSGs), when more opportunities will exist to integrate and detect service disruptions and communicate them throughout the MSO's organization.