SIMPLE NETWORK MANAGEMENT PROTOCOL CO-EXISTENCE WITH HYDROCARBON PROCESS AUTOMATION COMMUNICATION REAL-TIME NETWORK

Soloman Almadi, School of Information Systems, Computing & Mathematics, Brunel University, UK,
Almadism @aramco.com

Ramzi El-Haddadeh, Brunel Business School, Brunel University, UK,
Ramzi.El-Haddadeh@brunel.ac.uk

Masaud Jahromi, College of Engineering, Ahlia University, Bahrain
mjahromi@ahliauniversity.edu.bh

Abstract

Hydrocarbon Process Automation Applications (HPAA) utilizes Real-time network connecting process instrumentations, controllers, and real-time logic control applications. Conventional practice is to dedicate a real-time network for process automation applications and prevent other applications from utilizing the same infrastructure. An important application that can help optimize, improve network performance, and provide rapid response time in network diagnostics and mitigation is Simple Network Management Protocol (SNMP). This paper addresses the co-existence of SNMP traffic with real-time applications. The impacts of activating this protocol with the real-time HPAA utilizing high speed Ethernet network design will be examined. Empirical data for an implemented Hydrocarbon process automation system will be used to illustrate the interdependency of application performance, traffic mix, and potential areas of improvements. The outcomes of this effort demonstrate the co-existence of SNMP with HPPA, given special considerations (i.e., bandwidth, number of applications, etc.).

Keywords: SNMP, Hydrocarbon Process Automation Applications (HPAA), Real-time Network, Controllers.

1 INTRODUCTION

In early Hydrocarbon Process Automation Applications (HPAA), network nodes presented simple interfaces and interconnected with limited low speed network backbone, utilizing proprietary solutions and protocols. The complexity and functionality of these nodes have been increasing and supporting multiple arrays of functions. Wilbanks (1996) discussed intelligent nodes (i.e., microprocessor-based communication enabled devices) as extensively used in the lower layers of the process automation instrumentation and control in the manufacturing field and being extended into hydrocarbon upstream and downstream fields.

Boyer (2004) provided an overview of the new developed systems which include a multitude of operational functionality that span massive performance data acquisitions, control, embedded command, peer to peer communication, and Human-Machine Interfaces. As a result of network nodes and intelligent steady evolution and standardization, the amount of information that must be exchanged over the network has also increased for configuration and operational purposes. Ethernet based interfaces for the intelligent nodes and Ethernet high-speed network nodes provided a

homogenous platform that is operable with different systems, and enabled massive performance and profiling data access for the end user.

As described by Case, Fedor, Schoffstall, and Davin (1990), the most common mechanism for keeping tabs on Ethernet based network health is SNMP. A monitoring program (agent) is embedded within each device, and that gathers information on its network activity. The collected information is in the form of messages called Protocol Data Units (PDU) and is stored in a database called a Management Information Base (MIB). Centralized server, network management station(s), with a monitoring application are used by the administrator (or an automated or scheduled process) for polling all or some of the network nodes, requesting information that was collected.

Case, Fedor, Schoffstall, and Davin (1990) outlined different SNMP capabilities. SNMP can also be used by the network administrator to reconfigure specific devices and automatically notify the network management station if certain predefined conditions, or events, occur. These alerts are called traps.

SNMP is a highly complex protocol that can be difficult to implement. Also, SNMP is not very efficient. It relays unnecessary information, such as the version number, which is included in every message and other overhead packets. Hence, it increases network bandwidth utilization as discussed by Schdnwdlder, Prast, Harvan, Schipperst, and & Van de Meent (2007).

Previous work on assessing SNMP impacts was focused on communication networks for public and enterprise users. Papagiannaki, Cruz, and Diot (2003) addressed the Sprint IP backbone network focusing on the characterization of traffic congestion by analyzing link utilization at various times. The study was able to identify traffic bursts, their duration, and drivers. Packet or byte loss was not illustrated in this study.

Mochalski, Micheel, and Donnelly (2002) investigated the packet loss as it relates to delay across network components (router, firewall, switches) where the primary focus is packet loss during delay. Hall, Pratt, Leslie, and Moore (2003) assessed and analyzed packet loss on web traffic and its download time. They were able to ascertain a direct relationship between packet loss and web page download time. The study is focused on SNMP co-existence for process automation network and on analyzing packet error, utilization, and application performance by using several set up scenarios. This includes varying the traffic load, network alarm flooding, and focusing on the weakest link in the network topology.

This paper is organized as follows: a background on process automation networks is presented in section 2. Followed by a case study on system network connectivity is provided in section 3, Network Performance Analysis Method in section 4, and test cases in Section 5. Results and Analysis are in Section 6. Conclusion, with possible future work, is outlined in Section 7.

2 PROCESS AUTOMATION NETWORKS

The current process control network is based on layered architecture connecting process instrument, control layer, and Process Operational & Engineering layer. Schickhuber & McCarthy (1997) outlined the different key layers of the existing process automation network, figure 1. The first layer is the instrumentation which is directly engaged in process of sensing and transmitting process performance data and managing process settings. Different types of instrumentation in this layer are connected via a low speed data networks (i.e., foundation filed bus, Modbus, etc.). The low speed network carries cyclic or event driven messages from and to the instrumentation. This network connects to the second layer, which is the Control Layer; where another special dedicated network is used to connect the different controllers.

The controller layer network is a high speed network to connect different controllers to each other and to a high speed server; Operational and Engineering Layer. The final layer is a standard based Ethernet network used to support the Operational and Engineering layer. High-speed servers,

engineering workstations, and databases are connected to this network to provide automated and manual intervention as well as interface with Enterprise Resource Planning (ERP) databases for management and optimization.

With a networked environment, process decisions and control functions can be distributed among controllers and risk areas. Shah and Spada (2005), some of key challenges of existing networking is the need for having a special network for each layer based on different specifications, protocols, and operational requirements. In addition, the instrumentation layer and controller layer are becoming more intelligent. Significant data is being collected and executed by these two layers.

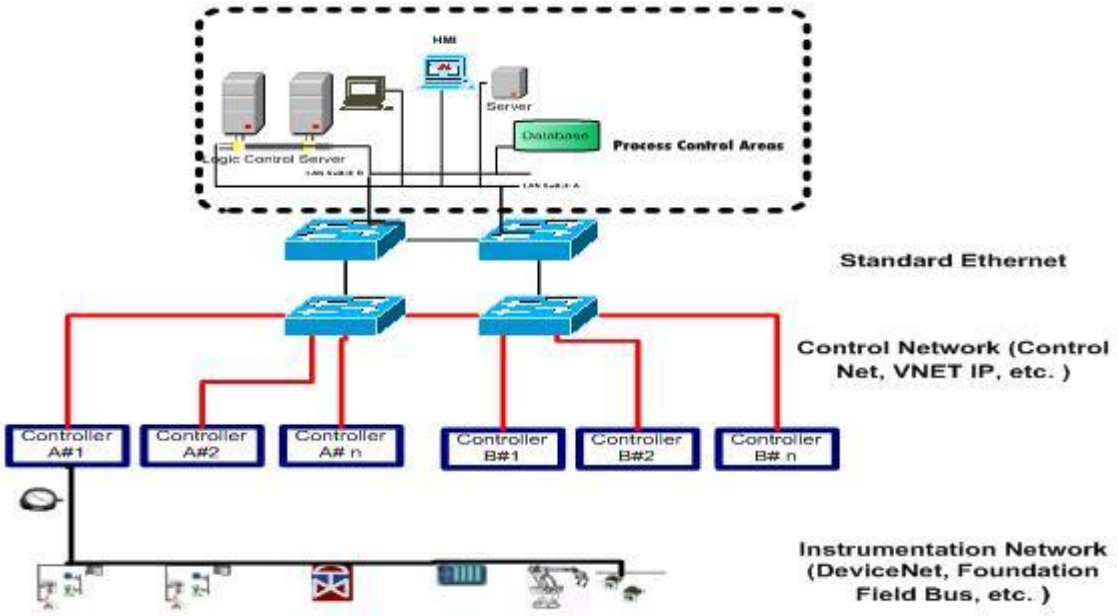


Figure 1. Existing Process Control Network- Separate/Layered

Major shifts in business environments (for example: business to business, security, etc.) and advancement in technology have resulted in Ethernet being the most widespread communication technology in electronic data processing systems. Further, vendors and standard bodies have invested extensive resources to ensure Ethernet can keep up with the continued "quality of service" demanded by end users and their applications. Hence, IP over Ethernet has become the standard protocol that offers a wide range of data transmission rates over different mediums (e.g., copper, optical fiber, and/or "wireless").

This technology is now extending its usability in support of industrial automations. Along with the advantages of standardized communication, that leads to an open system interface and lower operational cost. Ethernet leads to a seamless infrastructure that stretches, with the help of network filters and secures access, from the office to the machine or sensor. Most of today's process automation system implementations are based on a proprietary system, network solutions, and vendor-specific architectures. This includes hardware, software, protocols and, for some, the physical network infrastructure.

The conventional high speed network solution for existing process automation systems is typically designed and implemented to support all of the controllers, sensors, and subsystem traffic requirements. The common practice is limited to process automation traffic (i.e., alarm events, controller interlocking program events, and control device programs events, etc…) a is the sole user for the network. This strict networking rule is set forth to ensure zero (0%) packet error, zero (0%) packet discarded, and minimum delays during anticipated packet peak load. Hence, support type applications such as maintenance, asset management, large file transfers, etc., are not permitted to run concurrently with the process automation applications, on the same network.

Robinson, B. & Liberatore, V. (2004) [6] experimented cross traffic impact on real time traffic for Proportional Integrator Controller (PI) loop and he concluded that bursty cross traffic has adverse effect on the stability of the distributed process control even when the average utilization is low. The experiment was confined to an Ethernet network setup based on 10Mbps and 100Mbps. In addition, this effort did not consider combining other real-time traffic, for example, voice to identify relationship impacts between the distributed process automation traffic and other real time support applications (Simple Network Management Protocol (SNMP)). The stringent requirements for ensuring a zero (0%) packet error, zero (0%) packet discarded, and minimum delays along with running other process automation applications, SNMP, could now be mitigate with the introduction of Giga-bit in the process automation environments.

The benefits of a real-time Giga-bit network can be further maximized when used in a wide area network. Multiple operational plants can be managed from a common command and control center or different control centers that are geographically dispersed; providing back up support for each other when needed. As a result, a distributed autonomous command and control center is formed. This concept can be extensively and effectively used in managing local plant process automation (i.e., within the factory or plant operation field) for different plants apart from each other. This concept is not applied in petrochemical and hydrocarbon (oil and gas) producing operating environments. These different industries typically have a stand alone, local real-time network with dedicated controllers to manage a designated process. These networks are typically connected to the information resource planning and management systems located within the operating facility and are seldom connected to each other (Cabezas, Selga and Samitier, 1999, Kalapatapu, 2003, Hausmann, 2003, Brunner, 2005)

3 CASE STUDY SYSTEM NETWORK CONNECTIVITY

The network is composed of primary and backup switches running concurrently. The switches are based on Cisco Giga-bit Ethernet technology. The network is used to connect process controllers, Human Machine Interfaces, and field instruments. Digital performance data is collected by the field instruments and sent to the process automation controllers. The controllers evaluate the collected data and based on an embedded logic control loop, decisions are either made and executed back to the instrument or sent to the master control station for further automated analysis and decision tree making. The outcomes are sent back to the impacted controllers and instruments. Traffic monitoring system is based on SNMP utilizing Cisco Works as defined in Cisco (1992-2008).

The process automation network topology that was tested is based on fully redundant Giga-bit Ethernet network; star/tree architecture. Several branches (domains) utilizing Layer 2 Giga-bit Ethernet switches are connected to one redundant Layer 3 switch. Each domain (branch) has several switches with a maximum of nine (9), but in reality can be more than 9 switches as this is governed by the process control type, coverage area, and number of controllers served by each domain (Figure 2). The Giga-bit Ethernet network is configured based on best effort (i.e., QoS features were not activated). The network is exclusively dedicated to HPAA applications. Hence, there is no Web, FTP, or multimedia traffic. The bandwidth utilization, CPU utilization, and packet error rate are key indicators used to assess the impacts of running live SNMP traffic within a process automation

network. The target is to keep the Giga-bit Ethernet Network at 50% utilizations (500Mbps overhead capacity) to absorb traffic bursts.

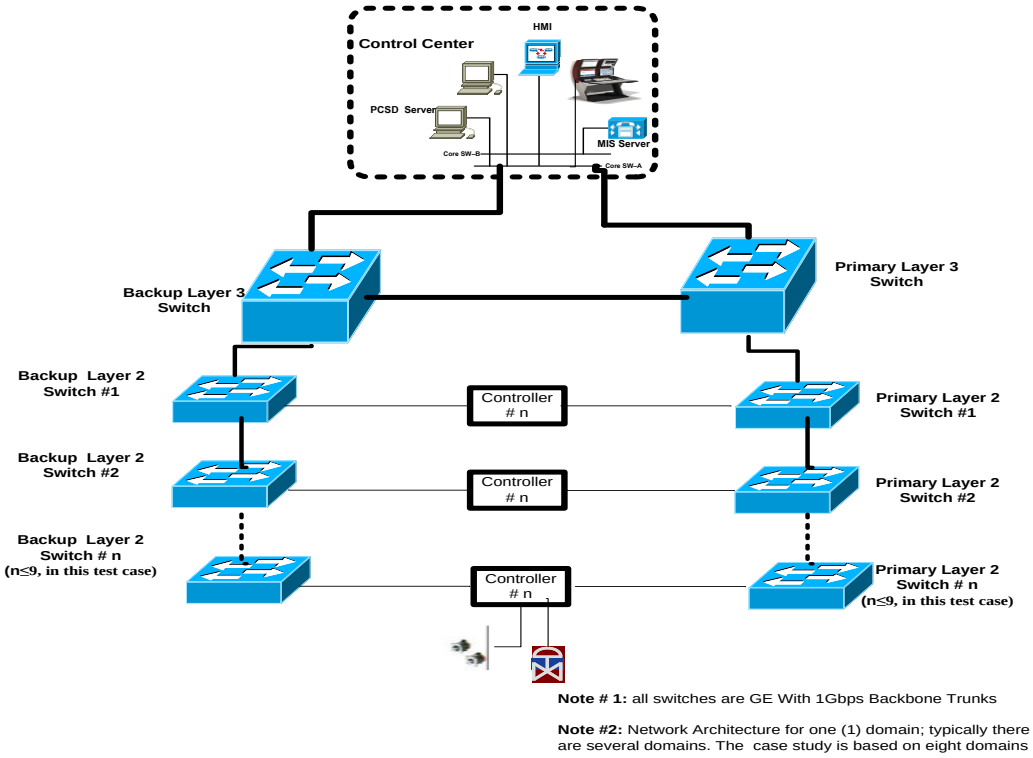


Figure 2. Network Architecture for One (1) Domain.

Components	Instrumentation Input/output	Controllers	Ethernet switches	Router	No of Domains	Maximum Link Speed	Access Port Speed
Total Number	10,000	65	40 Layer-2	2 Layer 3	8	1Gbps	100/10 Mbps

Table 1. Traffic Source Profile

4 CASE STUDY SYSTEM NETWORK CONNECTIVITY

SNMP agent is used to collect performance data (packet loss, utilization, etc.) from the Layer 2 switches and the Layer 3 switch. Collected SNMP data is sent to a master station and in this case SNMP is based on Cisco Works. IPref Traffic generator tool, as defined in IPerf (2008), was used to inject traffic (TCP and UDP) at key points in the network topology. The tool is based on a client-server environment and has the ability to generate a traffic load and measure performance concurrently.

SNMP maximum message size is 1,500 bytes with a minimum of 484 bytes. Schdnwdlder, Prast, Harvan, Schipperst, and & Van de Meent (2007) discussed how to perform large-scale SNMP traffic measurements and traces to develop a better understanding of how SNMP is used in production networks. The research illustrates SNMP traces that include GetBulk requests containing larger

response messages. Although most, if not all, GetBulk response sizes could be observed, no response message was larger than roughly 1400 bytes. This implies no fragmentation and confirms a minor SNMP traffic load was added to the production network. SNMP's request and response polling cycle directly govern the traffic addition. Poll cycle of 30 seconds is adequate for acquiring performance data in most implementations. In our study case, the polling cycle is a bit more granular: every 5 seconds.

The traffic collection methodology in our study case is based on SNMP agents running in all the different switches (Layer 2 and Layer 3). We decided to monitor the largest domain (nine Layer 2 switches daisy chained to a Layer 3 switch). The first Layer 2 switch connected to the Layer 3 switch has the aggregate traffic of all the subtending switches sending traffic to the Layer 3 switch, where the Controller Host Server is connected. The Layer 3 switch is connected to all the different domains. Hence, monitoring this switch provides performance data on each domain's trunk connected to the Layer 3 switch, and overall switch performance.

5 TEST CASES AND RESULTS

Several systematic test cases were conducted to illustrate impacts on the process automation network while SNMP agents are on a predetermined network performance; polling cycle of 5 seconds. The primary focus during all of these different test cases is to monitor the densest domain as mentioned in section 3 (i.e., 9 Layer 2 switches daisy chained to the Layer 3 switch). The busiest switch is anticipated to be the Layer 3 switch connecting all the domains to the Controller Host Server. Trunk utilization, CPU, packet discarded and packet errors were the key indicators for overall performance of the process automation network and SNMP. In addition, HPAA performance, including delay and accessibility to the instrumentation and controllers, comprised the second set of data validating the impacts.

5.1 Steady State Operation Test Case

The first test case was based on process automation network running in a steady state operation and SNMP is active. All different instrumentations, controllers and host servers were collecting data, validating their integrity; running logic loops and decisions are made back to other upstream and or downstream controller to regulate the actual process.

The very first step was to activate SNMP traffic and assess the status of the overall network during the HPAA steady state operation (Figure 3). This figure depicts the actual bandwidth utilization vs. time for the Layer 3 Giga-bit Ethernet trunk connecting the densest domain. The utilization peaked at 1% (10 Mbps) most of the time. This low utilization validates the fact SNMP traffic has negligible additional traffic load impacts during steady state operation. To confirm this, both the Layer 3 and Layer 2 switches in question were investigated further by analyzing the performance of their CPU and memory utilization. It was found that both switches had a modest CPU and memory utilization, less than 50%. In addition, there was no packet error. Figure 4 depicts these outcomes.

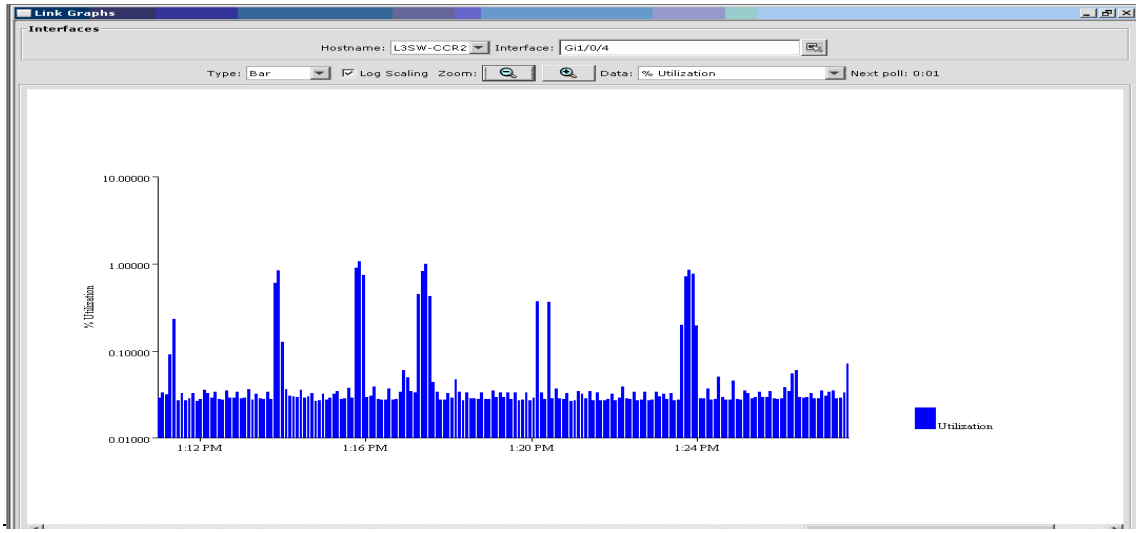
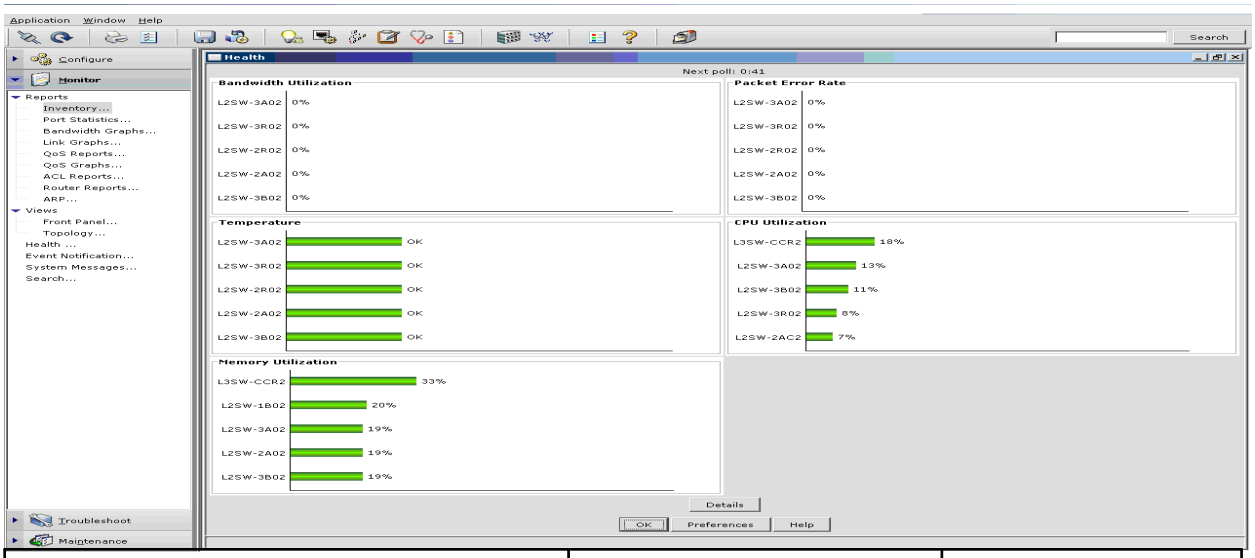


Figure 3. *Layer 3 Bandwidth Utilization — SNMP and Process Automation Steady State Operation*



Switch	Memory Utilization	CPU Utilization
Layer 3 (Backbone)	33%	18%
Layer 2 (Access)	20%	13%

Figure 4. *Memory; CPU Utilization, Packet Errors — SNMP and Process Automation in Steady State Operation*

5.2 Steady State Operation Test Case with Alarm Flooding

The second test case is based on process automation network running in a steady state operation, SNMP is active (i.e., test case 1) and invoking massive alarms by a sudden multi-controller failure. While it is not possible to have all the controller failed at the same time point, the composite impacts of the massive alarms, normal traffic load, and SNMP application was depicted in Figure 5. The test

outcome shows bandwidth has peaked from 10Mbps to 12Mbps (1% to 1.2% bandwidth utilization). The peak traffic was momentary and then subsides to the normal traffic load of 10Mbps (1%). It was also noted that most of the additional traffic load was unicast and broadcast due to the nature of alarms flooding of the HPAA application, as displayed in figure 6. This test case also confirms packet error rate was zero and there were no discarded packets.

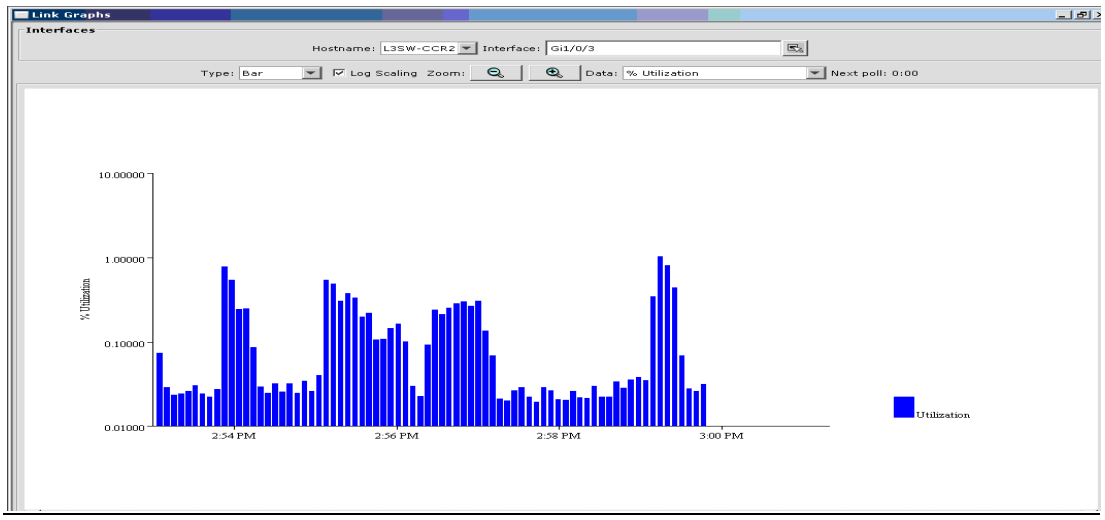


Figure 5. Massive Alarm Flooding — 1.2% Peak Utilization

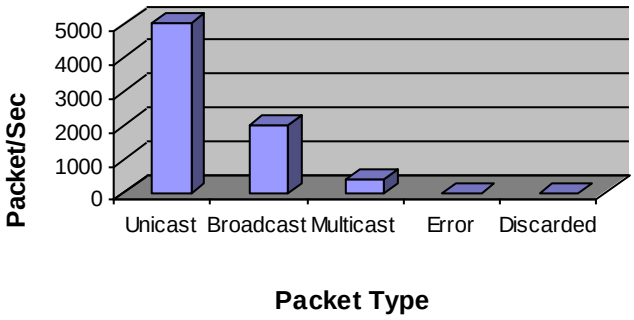


Figure 6. Packet Type: Packet Transmission by Service Type

5.3 Superimpose Steady State Operation with Traffic Injector Test Case

The third test case is based on process automation network running in a steady state operation, SNMP is active (i.e., test case 1) and utilizing traffic generator tool, as defined in IPerf (2008). This traffic generator tool is used to inject traffic (TCP and UDP) traffic at selected points in the network topology. The tool is based on client server environment so multi-client (traffic injection source) can be utilized to send traffic to a server connected to the densest domain.

A total of three different clients running at 100 Mbps were used concurrently to generate a total of 300Mbps (Figure 7). The maximum trunk bandwidth utilization was 32% (320 Mbps) as shown in

Figure 8. Also, there were zero packet errors for both the process application traffic and SNMP application as show in (Figure 9).

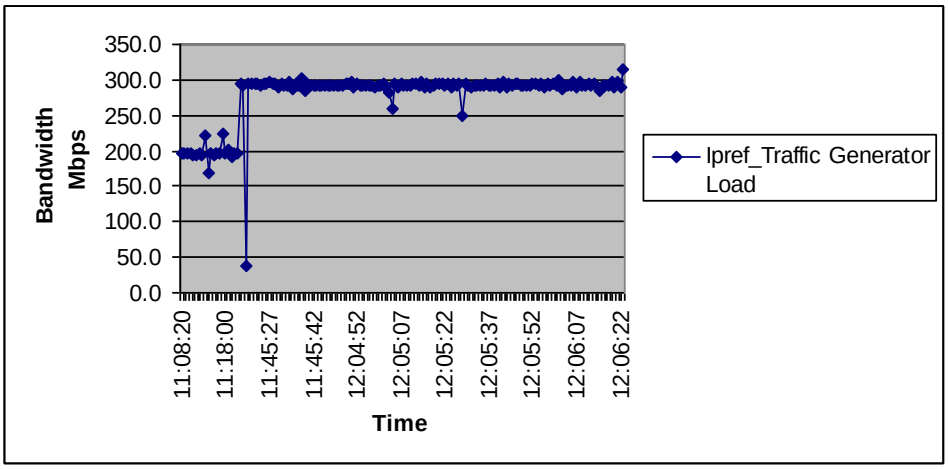


Figure 7. Traffic Injector IPref-300Mbps

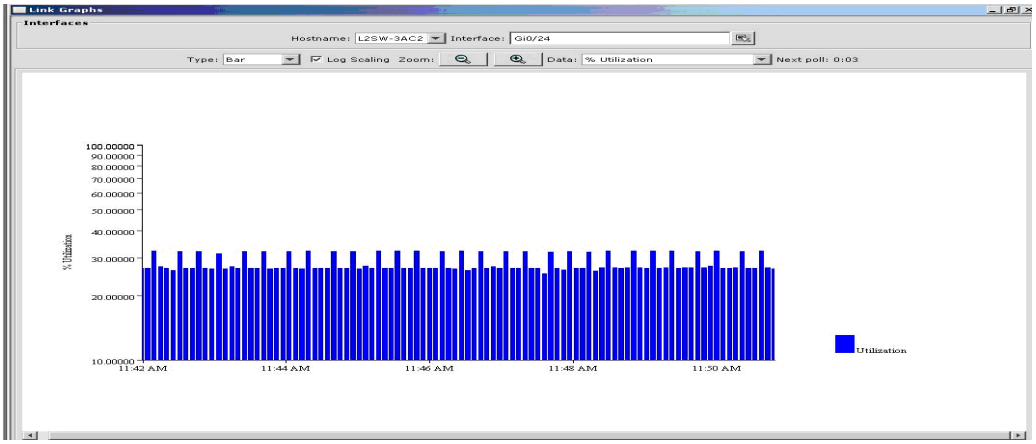


Figure 8. Layer 3 Switch, 32% Utilization (320Mbps)

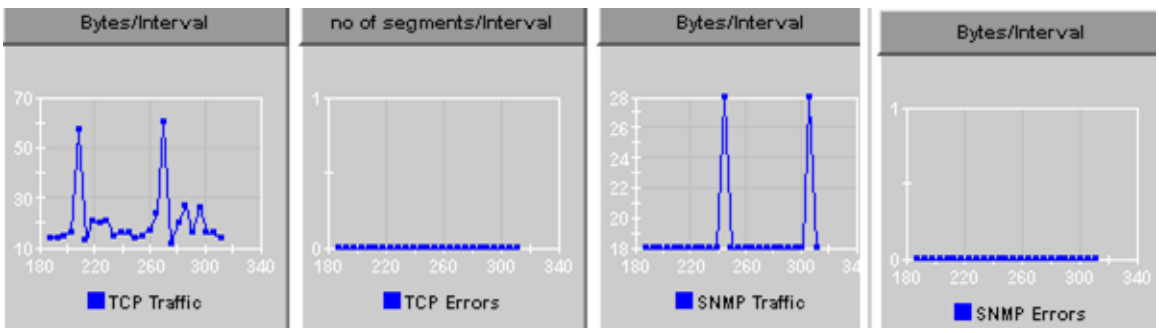


Figure 9. Zero Packet Error during Stress test

6 DISCUSSION

The three different test cases outlined in section 5 clearly show that SNMP application has minimal traffic load on the overall network. In steady state, with massive alarms, and using traffic injector, the overall performance of HPAA was not impacted. Packet error rates and discarded packets for both SNMP and HPAA were zero in all test cases. Hence, digital control (on/off) and continuous control can be supported on test network infrastructure without risking the process operation.

The test network environment Gbps backbone gives an indication that Fast Ethernet (100Mbps) would have run at 10 to 12 % peak. Hence, one may deduce that even a Fast Ethernet network can support the co-existence of SNMP traffic with HPAA. This could provide even more realistic conclusions specifically when Quality of Service and a complete full duplex trunking are imbedded in such a Fast Ethernet network. This outcome lessens the overly conservative approach of utilizing a proprietary Ethernet solution, adopted in most of the existing implementations for oil and gas plants, and also reduces the actual need for higher speed Ethernet switching and bandwidth trunking requirements.

Due to lab test environment limitations, the test cases did not include actual commands from the master stations, for the digital synthesis (on/off) and control of real-time traffic. By addressing the controller-to-controller traffic, the case study evaluation lent itself to the initial purpose of confirming the co-existence of SNMP traffic with HPAA application.

7 CONCLUSION AND FUTURE WORK

SNMP provides significant performance data for process automation, network diagnostics, and problem mitigation. SNMP traffic can co-exist with Ethernet-based HPAA supporting real-time oil and gas upstream (Oil Wells, Digital Field) and downstream (Gas and Oil Process Separation). The minimum network speed is Giga-bit Ethernet, to ensure available overhead capacity for traffic bursts. The case study demonstrated increasing the traffic load by 30 times (10 to 300 Mbps) resulted in zero packet error and in utilization below the targeted 50%.

Additional network enhancements such as dedicated VLAN and Layer 2 QoS activation should safe guard HPAA traffic from SNMP during traffic bursts. Work is in progress to develop the optimal network architecture for a converged IP-based network in support of HPAA. This paper's outcomes are being used as a basis in researching and completing the intended objectives.

REFERENCES

Boyer, S. (2004) SCADA: Supervisory Control and Data Acquisition, 3rd edn. ISA.

Brunner, C., (2005) 'IEC 61850 Process Connection', 15th PSCC, Liege, PP. 22-26

Cabezas, R., Selga, J., & Samitier, C., (1999) 'A new Generation of Packet Switch Designed for the Integration of Operational Services', CIGE Symposium, PP. 1-8

Case, J., Fedor, M., Schoffstall, M., & Davin, J. IETF, (1990), Simple Network Management Protocol (SNMP), 7 October 2008, http://www.ietf.org/rfc/rfc1157.txt

Cisco, (1992-2008), CiscoWorks LAN Management Solution (LMS), 11 December 2008, http://www.cisco.com/en/US/products/sw/cscowork/ps2425/index.html

Hall, J., Pratt, I., Leslie, I., & Moore, A., (2003) 'The Effect of Early Packet Loss on Web Page Download Times', Passive and Active Measurement Workshop, PP. 1-12

Hausmann, A., (2003) 'SCADA and Telecom Systems for Oman Gas Company', Oil Gas European Magazine, PP. 93-96

Iperf, (2008), The National Laboratory for Applied Network Research (NLANR Project, 15 March 2008, http://iperf.sourceforge.net/

Kalapatapu, R., (2003) 'What Users Need When They Select, Design, Implement a SCADA System', InTech ISA, PP. 1-6

Mochalski, K., Micheel, J., & Donnelly, S., (2002) 'Packet Delay and Loss at the Auckland Internet Access Path', Passive and Active Measurement Workshop, PP. 46-55

Papagiannaki, K., Cruz, R., & Diot, C., (2003) 'Network Performance Monitoring at Small Time Scales', Internet Measurement Conference, PP. 1-7

Robinson, B., & Liberatore, V., (2004) 'On the Impact of Bursty Cross-Traffic on Distributed Real-Time Process Control', IEEE International Workshop on Factory Communication Systems, PP. 147-152

Schdnwdlder, J., Prast, A., Harvan, M., Schipperst, J., & Van de Meent, R (2007) 'SNMP Traffic Analysis: Approaches, Tools, and First Results', Integrated Network Management 10th IFIP/IEEE International Symposiu, PP. 323-332

Schickhuber, G., & McCarthy, O., (1997) 'Distributed Fieldbus and Control Network Systems', Computing & Control Engineering Journal, PP. 21-32

Shah, H., & Spada, S., (2005) 'New Generation of Motion Control Networks Fills the Gaps', ARC Advisory Group, PP. 4-22

Wilbanks, W., (1996) '50 years of progress in measuring and controlling industrial processes', IEEE Control Systems Magazine, PP. 62, 64-66.