ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THBPA05

IT INFRASTRUCTURE TIPS AND TRICKS FOR CONTROL SYSTEM AND PLC

M. Ostoja-Gajewski , National Synchrotron Radiation Center SOLARIS, Krakow, Poland

Abstract

The network infrastructure in Solaris (National Synchrotron Radiation Center, Krakow) carries traffic between around 900 physical devices and dedicated virtual machines running Tango 9 control system. The Machine Protection System based on PLCs is also interconnected by network infrastructure. We performed extensive measurements of traffic flows and analysis of traffic patterns that revealed congestion of aggregated traffic from high-speed acquisition devices. We also applied the flow-based anomaly detection systems that give an interesting low-level view on Tango control system traffic flows. All issues were successfully addressed, thanks to the proper analysis of traffic nature. This paper presents the essential techniques and tools for network traffic patterns analysis, tips and tricks for improvements, and real-time data examples.

INTRODUCTION

This paper is organized in six sections, where each section provides description of one real-life use case. The main goal of this paper is to provide recommendations for improvements of network architecture design.

USE CASE 1: MACHINE PROTECTION SYSTEM - PLC NETWORKS

Machine Protection System (MPS) is dedicated to ensure secure operation of machine elements. It is built on a dedicated PLC system collecting data from sensors (temperature, pressure etc.). When any of the predefined thresholds is reached, the MPS system stops the entire machine by closing valves, switching off power supplies or shutting down klystrons. Most of the equipment is capable of generating interlocks in the case of malfunction. Example: cooling water in klystron is not flowing properly – interlock is generated and MPS system stops the machine.

Figure 1: MPS CPU and IO.

The Solaris MPS is based on Rockwell Automation [1] PLCs . There are 6 CPU modules and hundreds of IO modules (Figure 1) interconnected via computer network. MPS traffic is logically separated into dedicated VLANs. There is a 20ms roundtrip for CPU – IO communication. It means that CPU is pooling for data every 20ms and expecting result from IO. If communication is broken, the MPS system generates “communication interlock”, which in turn triggers immediate shutdown procedure for the machine.

First Approach - Bad Results

There is a natural inclination to minimize cost and design computer networks to handle different sources and types of traffic within shared equipment. The separation of traffic is done in the logical layer, but different sources share the same links infrastructure. The first approach was to aggregate MPS PLC traffic with other sources and utilize shared links and switches infrastructure.

During the building phase, it appeared that there were random occurrences of “lost communication” interlocks which stopped the operation of the entire machine. It could happen once a week or once a month, so it was difficult to catch and correlate the single event that might lead to such a case. But it was evident that some bursty traffic from other sources could increase the latency in PLC traffic to an unacceptable value. Prioritizing PLC traffic also did not help.

Recommendations

In order to address the issue of “lost communication” interlocks, it was decided to build a separate fiber optics infrastructure for PLC traffic only. Most of the network equipment was reused, but the MPS system was provided with dedicated links, with no other traffic sent over the same interfaces. In addition, there were new switches dedicated to handle traffic from beamline MPS systems.

After applying this solution, no further interlocks were observed in the period of more than 2 years of operation.

USE CASE 2: TRAFFIC SEPARATION BASED ON DEVICE TYPE

The computer network for the control system carries traffic for different types of equipment and control system software running in virtualized environment. There are hundreds of ion pump controllers, power supplies, scopes, diagnostic systems, RF systems, timing, and PLC. Also, there are multiple virtual machines running Tango9 control system. All of the network-attached systems produce different patterns of traffic. Figures 2, 3, 4 present examples of traffic from Ion Pump controller, Modulator and Control Room computer.

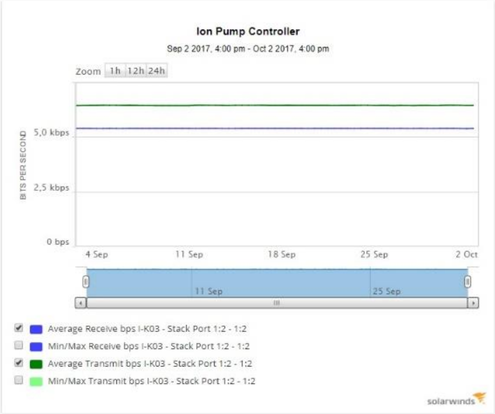


Figure 2: Ion pump controller traffic.

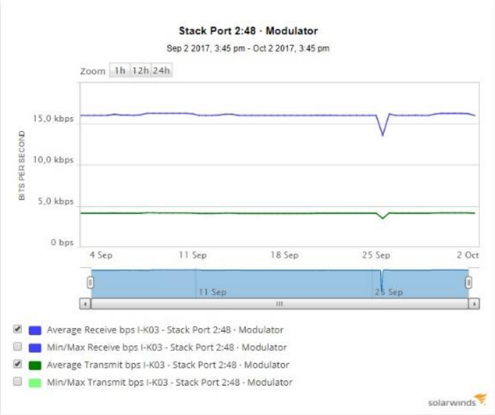


Figure 3: Modulator in section I-K03 traffic.

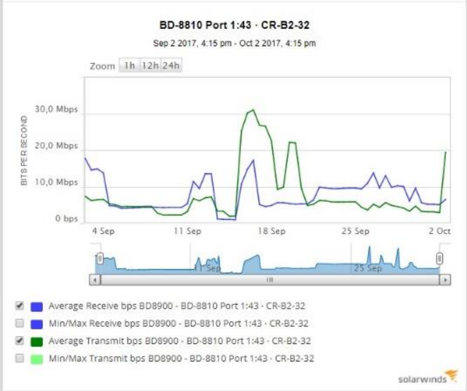


Figure 4: Control Room computer traffic.

Recommendations

Since there are different patterns of traffic depending on the type of equipment, it is recommended to make the logical separation of network by using 802.1q VLANs for each subsystem. It enables controlling the priorities and shaping the bandwidth based on the traffic pattern.

Also, it is recommended to attach the virtual machines with control system to the same VLAN as the controlled subsystem (cf. next use case).

USE CASE 3: COMMUNICATION BETWEEN DEVICES, DEVICE SERVERS AND CONTROL ROOM

In Tango9 [2] control system, all devices are managed by Device Servers. A Device Server is a piece of software that runs on a virtual machine and polls devices for data.

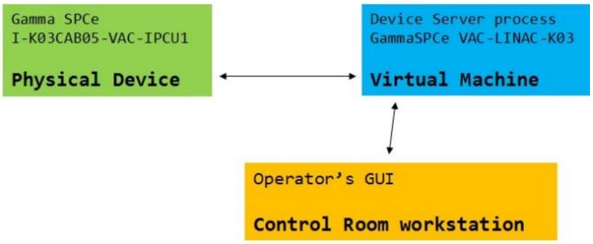
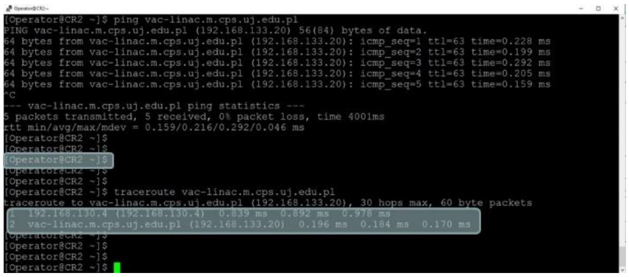


Figure 5: Tango9 communication principles.

Operators in the control room are using GUI applications that communicate with the device server in order to get data and manage devices (see Figure 5). There are two patterns used to receive data: polling and publish/subscribe. It is a crucial that the computer network carrying traffic for the control system should be stable and should provide low-latency capabilities.

Recommendations

In order to provide low latency links, it is recommended to shorten the physical and logical path between control room computers and virtual machines running device servers. Also, the path between virtual machines and devices should be as short as possible.

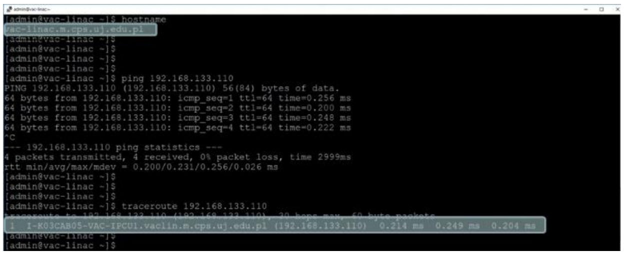


```
[Operator@CR2 ~]$ ping vac-linac.m.cps.uj.edu.pl
PING vac-linac.m.cps.uj.edu.pl (192.168.133.20) 56(84) bytes of data.
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=1 ttl=63 time=0.228 ms
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=2 ttl=63 time=0.199 ms
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=3 ttl=63 time=0.292 ms
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=4 ttl=63 time=0.205 ms
64 bytes from vac-linac.m.cps.uj.edu.pl (192.168.133.20): icmp_seq=5 ttl=63 time=0.159 ms
^C
--- vac-linac.m.cps.uj.edu.pl ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.159/0.216/0.292/0.046 ms
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$ traceroute vac-linac.m.cps.uj.edu.pl
traceroute to vac-linac.m.cps.uj.edu.pl (192.168.133.20), 30 hops max, 60 byte packets
 1  192.168.130.4 (192.168.130.4)  0.839 ms  0.892 ms  0.978 ms
 2  vac-linac.m.cps.uj.edu.pl (192.168.133.20)  0.196 ms  0.184 ms  0.170 ms
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
[Operator@CR2 ~]$
```

Figure 6: Path between the control room computer and the virtual machine running the device server for VAC subsystem.

As shown in Figure 6, the number of 'hops' between the control room computer and the virtual machine is merely "one". It means that the path is very short in terms of routing, giving very low latency.

ISBN: 978-3-95450-193-9 doi:10.18429/JACoW-ICALEPCS2017-THBPA05



```
[admin@vac-linac ~]$ hostname
vac-linac.m.cps.uj.edu.pl
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$ ping 192.168.133.110
PING 192.168.133.110 (192.168.133.110) 56(84) bytes of data.
64 bytes from 192.168.133.110: icmp_seq=1 ttl=64 time=0.256 ms
64 bytes from 192.168.133.110: icmp_seq=2 ttl=64 time=0.200 ms
64 bytes from 192.168.133.110: icmp_seq=3 ttl=64 time=0.248 ms
64 bytes from 192.168.133.110: icmp_seq=4 ttl=64 time=0.222 ms
^C
--- 192.168.133.110 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.200/0.231/0.256/0.026 ms
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$
[admin@vac-linac ~]$ traceroute 192.168.133.110
traceroute to 192.168.133.110 (192.168.133.110), 30 hops max, 60 byte packets
 1  I-K03CAB05-VAC-IPCU1.vaclin.m.cps.uj.edu.pl (192.168.133.110)  0.214 ms  0.249 ms  0.204 ms
[admin@vac-linac ~]$
[admin@vac-linac ~]$
```

Figure 7: Path between the virtual machine and the physical device.

Figure 7 illustrates the concept of the virtual machine running a device server directly attached to the VLAN of the controlled subsystem. There is no routing, but direct switching, so the latency is very small.

The concept of network low latency for the control system is vital for fast response of GUI applications, but also for archiving systems that either poll for data or get notified by a messaging system.

USE CASE 4: DIAGNOSTIC DEVICES - HUGE TRAFIC PRODUCERS

There is a vast number of diagnostic devices used for enhancing smooth operation of the synchrotron machine. Most of these devices produce huge amount of traffic that can easily saturate 1 GBit links.

The perfect example is the Bassler [3] camera with the default settings:

- Resolution: 1280x1024
- Bits per pixel: 12 (in reality: 16bits)
- FPS: no limit (in reality: 40)
- Traffic: ~ 900 MBit/s

During the commissioning of PEEM/XAS beamline, there were 5 cameras (Figure 8) used simultaneously. They were managed either by Pylon application or LimaCCD device server. The total amount of traffic generated by Bassler cameras could not be properly handled by 1Gbit link on the beamline computer.

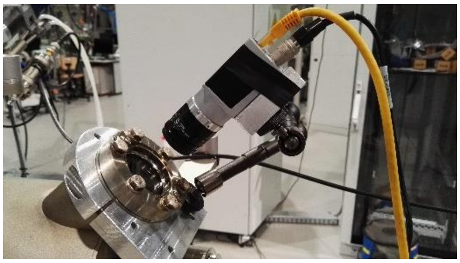


Figure 8: Bassler camera - a huge traffic producer.

Recommendations

It is advised to discuss the resolution of images produced by diagnostic cameras with the beamline or machine operators. It appeared that it was absolutely acceptable for the operators when new settings were applied:

- Resolution: 640x512
- Bits per pixel: 8
- FPS: limit : 25
- Traffic: ~65 MBit/s

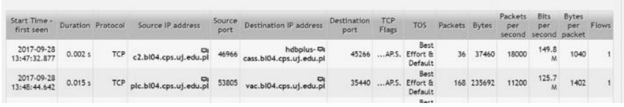
The reduction of the traffic volume was significant and allowed smooth operation of the control system for the beamline.

USE CASE 5: FLOW-BASED TRAFFIC MONITORING

Each communication between two attached devices in a computer network can be regarded as a flow. Flows can vary in duration, size, usage of multiple ports and other aspects. They can be monitored, analysed and classified.

Most of the modern networking devices are capable of producing information about flows and sending it to flow collectors for further analysis. There are couple of variations of flow protocols, depending on manufacturers: NetFlow, IPFIX, sFlow, jFlow.

Tango9 control system produces thousands of flows per second. There are multiple entities communicating with each other: the control room, device servers, physical devices, and archiving systems. Understanding the nature of flows in the control system can help with diagnosis of malfunction of network infrastructure and software layer.



Start Time - first seen	Duration	Protocol	Source IP address	Source port	Destination IP address	Destination port	TCP Flags	TOS	Packets	Bytes	Packets per second	Bits per second	Bytes per packet	Flows
2017-09-28 13:47:32.877	0.002 s	TCP	c2.bl04.cps.uj.edu.pl	46966	hdbplus-cass.bl04.cps.uj.edu.pl	45266	...AP.S.	Best Effort & Default	36	37460	18000	149.8 M	1040	1
2017-09-28 13:48:44.642	0.015 s	TCP	plc.bl04.cps.uj.edu.pl	53805	vac.bl04.cps.uj.edu.pl	35440	...AP.S.	Best Effort & Default	168	235692	11200	125.7 M	1402	1

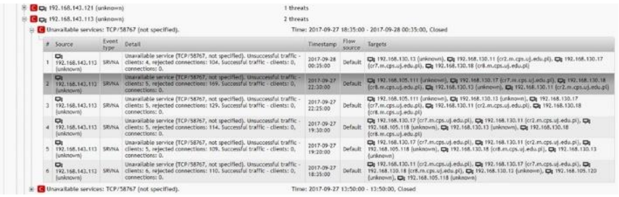
Figure 9: Flow-based analysis.

Figure 9 presents an example of flow between the beamline BL04 control computer and the HDB++ archiving system based on Cassandra database. Also, there is a communication between the PLC device server on a virtual machine and the VAC device server on another virtual machine. The TCP flags are shown as AP.S, which means that communication is established (flags SYN and ACK) and TCP/IP stack is forced to push the data out as soon as possible (flag P).

Recommendations

When looking for unsuccessful connections, one can set filter by TCP flags "S and not A", which means that a packet with a SYN flag was not acknowledged, so the TCP handshake did not succeed.

For the smooth operation of the control system, there is a need to capture and analyse any traffic anomalies that can be produced by malfunctioning devices or software. There is a variety of tools that can be employed to analyse traffic and identify potential anomaly (Figure 10). One of them is Flowmon [4], a tool that brings ability to learn the nature of traffic and to categorize network events by the risk they pose on the infrastructure.



192.168.143.121 (unknown) 1 threats
192.168.143.113 (unknown) 2 threats
Unavailable services: TCP/58767 (not specified). Time: 2017-09-27 18:35:00 - 2017-09-28 00:35:00, Closed

#	Source	Event type	Detail	Timestamp	Flow source	Targets
1	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 4, rejected connections: 104. Successful traffic - clients: 0, connections: 0.	2017-09-28 00:35:00	Default	192.168.130.13 (unknown), 192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.18 (cr8.m.cps.uj.edu.pl)
2	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 5, rejected connections: 169. Successful traffic - clients: 0, connections: 0.	2017-09-27 22:30:00	Default	192.168.105.111 (unknown), 192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.18 (cr8.m.cps.uj.edu.pl), 192.168.130.13 (unknown), 192.168.130.11 (cr2.m.cps.uj.edu.pl)
3	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 5, rejected connections: 129. Successful traffic - clients: 0, connections: 0.	2017-09-27 22:25:00	Default	192.168.105.111 (unknown), 192.168.130.13 (unknown), 192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.130.18 (cr8.m.cps.uj.edu.pl)
4	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 5, rejected connections: 114. Successful traffic - clients: 0, connections: 0.	2017-09-27 19:30:00	Default	192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.105.118 (unknown), 192.168.130.13 (unknown), 192.168.130.18 (cr8.m.cps.uj.edu.pl)
5	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 5, rejected connections: 109. Successful traffic - clients: 0, connections: 0.	2017-09-27 19:20:00	Default	192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.105.118 (unknown), 192.168.130.18 (cr8.m.cps.uj.edu.pl), 192.168.130.13 (unknown)
6	192.168.143.113 (unknown)	SRVNA	Unavailable service (TCP/58767, not specified). Unsuccessful traffic - clients: 6, rejected connections: 110. Successful traffic - clients: 0, connections: 0.	2017-09-27 18:35:00	Default	192.168.130.11 (cr2.m.cps.uj.edu.pl), 192.168.130.17 (cr7.m.cps.uj.edu.pl), 192.168.130.18 (cr8.m.cps.uj.edu.pl), 192.168.130.13 (unknown), 192.168.105.120 (unknown), 192.168.105.118 (unknown)

Unavailable services: TCP/58767 (not specified). Time: 2017-09-27 13:50:00 - 13:50:00, Closed

Figure 10: Example of unsuccessful connections captured by Flowmon.

USE CASE 6 : LOCAL NETWORK DIAGNOSTICS WITH TAP

The network monitoring software provides information on the state of infrastructure elements and particular network interfaces. If there is an issue with a single device attached to a network port (e.g. a huge number of dropped packets), it may be suspected that there is either a physical issue (cabling) or a traffic pattern which can not be handled properly by network equipment.

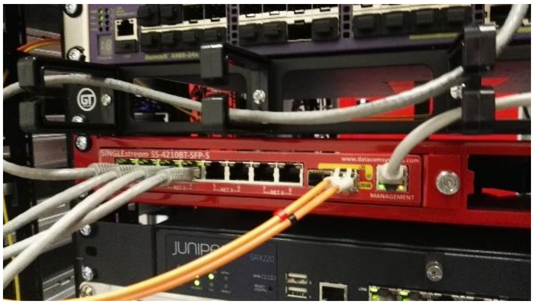


Figure 11: Network TAP [5].

Recommendations

If it is feasible, one can consider using a network TAP (Figure 11) located between the physical device and the network port. TAP is transparent and makes a copy of entire traffic sent between the device and the network port. It includes malformed frames, so it is easier to capture possible issues with cabling (e.g. an unshielded UTP cable interfering with some strong signal sources)

It needs to be noted that the port SPAN or mirroring do not replicate malformed frames, so a network TAP is the only way to capture entire traffic flowing between a device and network equipment.

CONCLUSION

The proper design and implementation of network infrastructure is critical for operation of control systems for Experimental Physics facilities. To achieve stability and predictability of network infrastructure, it is advised to:

- Monitor, analyze and understand network traffic
- Redesign network infrastructure to comply with the existing traffic patterns
- Proactively identify new traffic sources coming with IoT reality

Active monitoring and analysis of traffic patterns can offer a new perspective on how the control system exchanges data. By analysing flows, potential issues generated by software malfunction can be quickly identified.

REFERENCES

[1] Rockwell Automation, Allan Bradley, PLCs, https://www.rockwellautomation.com/
[2] Tango 9 Control System, http://www.tango-controls.org/
[3] Bassler cameras, https://www.baslerweb.com
[4] Flowmon - flow based monitoring system, https://www.flowmon.com
[5] Network TAPs by DatacomSystems, http://www.datacomsystems.com/products/network-taps