Implementation and Testing of Cisco IP SLA in Smart Grid Environments

J. Horalek, F. Holik, V. Hurtova
University of Pardubice, Faculty of electrical engineering and informatics Pardubice, Czech Republic
josef.horalek@upce.cz, filip.holik@student.upce.cz

Abstract - Smart grid networks are becoming more and more commonly deployed due to their undisputed benefits. On the other hand, there is a high demand for reliability and functionality of these networks. This paper is analysing usage of the IP SLA for monitoring network state and collecting important information for potential problem detection and solving. The practical part of the paper presents implementation of the IP SLA into the smart grid network environment and its testing. The results from several simulated scenarios with different QoS classes, used within the smart grid networks, are discussed.

I. INTRODUCTION

Securing performance parameters and monitoring of network functionalities are two of the most important tasks of intelligent networks, in order to ensure their effective usage. Most of the backbone and local smart grid networks are using MPLS L3 VPN [1-5] due to its reliability and security. Implementation and testing of this technology in smart grid networks is the main point of this paper. Presented measurement can be used for confirming the SLA and for proactive problem solving of potential issues. The goal of the paper is to prove, if the Cisco proprietary solution for measuring performance parameters is a suitable technology in the industrial environment of smart grid networks built on Cisco devices [6,7]. Two types of measurements were conducted. In the first case, the priority class with g.729a codec, simulating demanding communication of Intelligent Electronic Devices (IEDs); and in the second case, default class simulating standard communication of the same devices.

The paper is further organized as follows: the second section describes the implementation details of the Cisco IP SLA. This implementation is then thoroughly tested in the third section. The paper is concluded in the last section.

II. IMPLEMENTATION OF THE CISCO IP SLA

Cisco Internet Protocol Service Level Agreement (IP SLA) is a proprietary technology introduced by Cisco for effective monitoring of network traffic. It can be used for measuring network performance and performance critical parameters like packet loss, delay, and jitter. IP SLA can therefore detect and prevent problems, which can influence network functionality and performance [8,9]. This is one of the most important tasks in the environment of intelligent energetical networks. Effective monitoring and measurement of the complete network can be done using Cisco RTTMON with management information base (MIB) together with SNMP and IP SLA statistics. IP SLA can also be used for policy-based routing. This type of routing can adjust the direction of packet flows based on actual statistics, and therefore better utilize each link and ensure availability of critical parts of the network.

In order to conduct a measurement, the topology has to contain one Cisco router for packet generation (monitor) and one host, acting as a responder. The responder can be any IED with IP address [10], able to reply to requests (ICMP echo, or HTTP GET). These devices are common in smart grid networks. In the case that the responder is also a Cisco router (in the energetical networks typically a gateway between different areas), IP SLA can be better utilized because a larger number of critical parameters can be measured. The following data collection and presentation is realized with Network Management System (NMS). After successful configuration, the router is collecting results of each operation and save the results in a form of IOS RTTMON statistics. The router is then using SNMP NMS to collect proper information from MIB. From the technology perspective, IP SLA is using a concept displayed in Figure 1. Every operation is defining a type of packet generated by the router, source and destination address, and other values. The configuration also contains time, when each operation should be executed.

A. IP SLA Monitor (Generator)

Tests are defined on the IP SLA monitor. Based on the configured parameters of each test, the IP SLA is generating specific traffic, analysing the results and saving them for a future analysis over CLI or SNMP. The IP SLA monitor can be every Cisco router having IOS with a proper set of functions, depending on the chosen type of test. Processor load on the IP SLA monitor is a critical part for measuring different metrics, especially for recording timestamps. For this reason, a proper methodology has to be used in order not to exceed 30% of the router's CPU utilization. It is therefore recommended to use a dedicated router just for the measurement, so the data traffic would not be influenced and the measurement will get more precise results.

B. IP SLA Responder

IP SLA responder is reacting on tests generated by the IP SLA monitor. The responder creates timestamps with packet received and packet send time and then includes them in the payload. These timestamps will allow the elimination of processing time on the responder from the

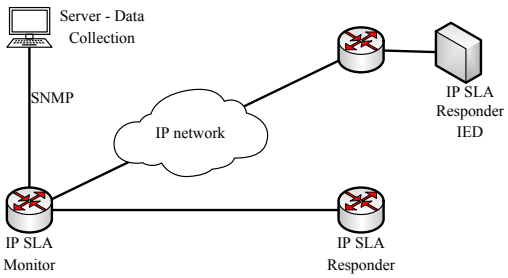

Figure 1. Principles of IP SLA monitoring

final measurement time as shown in Figure 2. As in the case of the monitor, the CPU utilization of the responder should not exceed 30%, so it is important to carefully choose the testing methodology.

$$RTT = T4 - T1 - \Delta \quad (1)$$

where: RTT = Round trip time
T1 = Timestamp 1
T4 = Timestamp 4

C. *Multioperations Scheduler of IP SLA*

Cisco IP SLA allows the use of a multioperations scheduler, which can monitor complex networks containing large number of probes, and is ideal for smart grid networks (containing tens to hundreds of IEDs). This scheduler can be turned on with the "ip sla group" IOS command. The scheduler allows the planning of a sets of IP SLA operations, which allows the monitoring of traffic in a uniformly distributed timeframe. The realization requires the specification of a range (ID) of each probe and the function can then being run at once. This feature helps minimize the CPU utilization and therefore to increase the network scalability. The function is using the following configuration parameters:

- Operation ID numbers – the list of all IP SLA probes and their IDs within a particular group.
- Group operation number – configuration parameter, containing the number of a particular group.
- Schedule period – the amount of time, for which the group of IP SLA operations is planned.
- Ageout – specify for how long the operations actively collecting information are held in a memory.
- Life – the amount of time for operation to actively collect information.
- Frequency – time after which every IP SLA is repeated.
- Start time – a time when the operation will start to collect information.

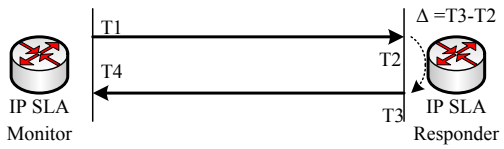

Figure 2. The system timestamps

TABLE I. PARAMETERS OF UDP JITTER TEST

Parameter	SLA-Voice settings	SLA-Normal settings
codec	g.729a	none
packet size	32B	20B+12B
the number of packets	550	100
interval	100 ms	500 ms
frequency	60 s default	60 s default
timeout	5000 ms default	5000 ms default
threshold	5000 ms default	5000 ms default
type of service	184(EF)	0

III. THE TESTING

A. *The Methodology of Testing*

The tests were based on ICMP and UDP implemented in IOS IP SLA. Because most of the smart grid networks are based on MPLS, the UDP jitter operation was selected for testing. This operation is primarily used for diagnosis of real-time application availability, which is essential for smart grid networks. This type of test is also the only one, able to measure with micro-seconds precision, which is important for critical infrastructure. The UDP jitter test is generating sequential information and timestamps for both the sending and the receiving sides. We have chosen two variants of UDP jitter for measuring performance metrics in MPLS L3 VPN infrastructure. These two tests can relevantly simulate proper data flows in smart grid networks. This includes link congestion when collecting data from IED devices and high priority control commands. These tests are:

- UDP jitter with g.729a codec, which is used for measuring in a priority class in a priority traffic (SLA-Voice).
- UDP jitter without a codec, used for measuring in non-prioritized classes (SLA-Normal).

In the case of SLA-Voice variant, data traffic can be separated from control traffic, making the measurement more relevant. In the case of SLA-Normal variant, direct behaviour in the class using a class-default queue can be observed. This corresponds with the process of IED data collection.

Table 1 shows that in the SLA-Voice variant, packets with 32B size will be generated for a 55 seconds with 100 ms intervals between packets and 5 seconds space between each test. This means, that the measurement is taking more than 90% from the complete measurement time length of 60 seconds. This test is not influenced by data flows between end devices like IEDs, but only by the link state. The test will be used only for measurement between substations due to its complexity.

In the SLA-Normal variant, packets with 32B length will be generated for 50 s with 500 ms intervals between

each packet and 10 seconds break between each test. This will ensure, that the measurement will run in more than 80% of the total timeframe of 60 seconds. This test is used for simulation of consumer traffic and parameters in the class-default (with DSCP CS0). This test will be applied in all experiments.

B. Design and Parameters

The measurement was realized on the testing topology depicted in the Figure 3.

Measurement type Provider Edge (PE) - Customer Edge (CE) measured SLA metrics between end stations, CE routers and core PE routers. For this type of measurement, hub and spokes design was chosen. The hub was represented by the IP SLA router (PE router) and spokes were represented by the substation end routers (CE routers). The goal of this measurement was to detect problems with communication technology, which can be rented from an external provider of network connectivity. This measurement can be therefore used for solving connectivity problems (like QoS transparency or packet loss) with the external connectivity provider. In the PE-CE type of measurement, only the SLA-Normal variant was chosen due to the possibility of high CPU utilization on the SLA monitor. This would result in a large increase of identical measurements. Classification of the IPv4 traffic will be conducted based on a DSCP parameter located in the IP header. QoS configuration was done using the same approach as in the case of a service provider – with the minimal setting. As a use case, the consumer would order services and the required speed. In this case, two policy-maps were chosen, with the direction to each substation, and one policy-map of the consumers input (Table 2). One of the policy-maps contains class-default shaping and it is parent for the second policy-map. The second policy-map contains classes for traffic marking.

Traffic coming from a customer will not be remarked at the PE. Traffic in the SLA-Voice class will go through input policing, discarding all the traffic exceeding 50% of the total bandwidth of the interface. This is a standard measure in MPLS networks.

Measurement type Provider Edge (PE) - Provider Edge (PE) measured SLA metrics amongst PE routers in the MPLS network. This type of measurement used full-mesh, where every PE router was connected to all the other PE routers. From the MPLS point of view, the measurement was not realized on the global routing process level. Instead, the dedicated MPLS VPN was created, so tests in each core QoS classes could be defined. This test was aimed at detecting and solving problems within the core infrastructure. QoS in the core

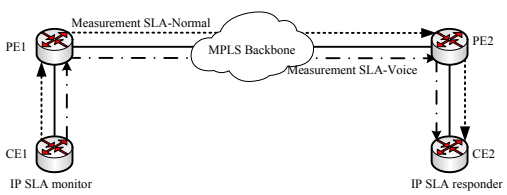

Figure 3. Topology design

TABLE II. CLASS SERVICE FOR CUSTOMERS

Class	DSCP	CoS/EXP	Note
SLA-Voice	CS3, EF	5	Priority class
Critical	CS6	3	Critical traffic, packet loss sensitive
class-default	0	0	Other traffic

infrastructure was similar to PE-CE. The OUT-MPLS policy-map was created and applied on the output interfaces between PE routers. This policy-map contained three classes displayed in the Table 3.

Measurement type Customer Edge (CE) - Customer Edge (CE) was used for measurement of SLA metrics between end points and IEDs. The whole link was therefore monitored – from a single substation, via the whole infrastructure of the provider, to the next substation. This test can be used for the specification of maximum latency, jitter, or packet loss between the central system and a substation. In our case, the router CE1 was used as the monitor and CE2 as the responder. CE1 generated both types of measurements (SLA-Voice and SLA-Normal).

C. Results

Every scenario for diagnosis of Cisco IP SLA behaviour in the environment of smart grid networks on a simulated topology of energetical company, was tested after the configuration. A reference values were collected during the standard traffic. Tables 4 and 5 show parameters gathered from IP SLA probes. Measured data also shows times when the operation was conducted, the number of successful and unsuccessful operations, and the lifetime of the operation. Lastly, the one-way statistics are also available, allowing to analyse information for solving conn connectivity problems of the transport network.

TABLE III. CLASSES OF OPERATIONS FOR BACKBONE TRAFFIC

Class	DSCP	CoS/EXP	Guaranteed bandwidth / exceed action
SLA-Voice	CS3, EF	5	50% (of the total BW) / Packet drop
Critical	CS6	3	Remaining 60% / Can exceed if the capacity is available
class-default	0	0	Remaining 40% / Can exceed if the capacity is available

TABLE IV. SUMMARY TABLE FOR MEASURING SLA-VOICE VARIANT OF NORMAL DATA TRAFFIC

SLA Voice	Measurement PE1-PE2	Measurement CE1-CE2
RTT (avg)	25 ms	35 ms
Latency S->D	7 ms	19 ms
Latency D->S	28 ms	16 ms
Jitter S->D	14 ms	8 ms
Jitter D->S	7 ms	6 ms
Packet loss	0	0
Mean Opinion Score	4,06	4,06
IPCIF	11	11

IPCIF = Calculated Planning Impairment Factor

Results for the scenario: Utilization data lines

The next scenario tested data link usage by an IED. In the high utilization, latency will increase, jitter will fluctuate more, and there can be some packet loss, influencing functionality and effectivity of data centrals. QoS policy with the 5Mbit bandwidth between PE1-CE1 and PE2-CE2 was used for sufficient trustworthiness of the measurement. Data traffic was simulated using pings with the size of 1500 bytes and 0 time limit for the reply. This ensured a link congestion resulting in packet drops in a direction between CE1 and PE1.

Table 6 shows, that in a default class, there is packet loss due to the high traffic load. Unlike in original values, latency and jitter also increased. A direction in which packets are lost can be also detected – in our case it is from CE1 to CE2. Priority class SLA-Voice shows almost no change, proving good conditions of the link without any packet drops in a core or transit infrastructure.

Results for the scenario: Utilization of voice lines

The next tested scenario is focusing on lowering quality of the priority line – the voice in our case. This situation can happen if the communication between IEDs is using more bandwidth than what is assigned to the prioritized traffic. Bandwidth in the test was set to 100Kbit. A typical data flow with G729a codec is using approximately 32Kbit/s. That means, that three parallel transmissions can be realized at once and be fully functional. Simulation was again conducted with a ping tool and packets marked with DSCP EF. Collected data shows, that the priority class became saturated and packets from this class were dropped. The default class transferred practically no traffic, so there were no packets dropped there. The Voice class had a priority over the class-default, resulting in a possibility of delayed packets in the class-default. Despite the possible delay, no packets were dropped in this class.

The results of PE1-PE2 measurement in the SLA-Voice class are present in Table 7 and show increased latency. This however presents only a simulated situation, in the real environment, such traffic should not influence core infrastructure.

The measurement of SLA-Voice between CE1 and CE2 (Table 8.) shows decreased performance parameters for voice technologies and consequent packet loss. Latency rapidly increased to an average of 146 ms, 14 packets were lost, and MOS decreased while IPCIF increased.

On the other hand, SLA-Normal measurement between CE1 and CE2 clearly shows no packet loss. But as already mentioned, the situation where latency in the SLA-Voice priority class will increase, can happen as it happened in our case – to the average of 147 ms.

In both cases it is clear, that the voice traffic was generated from the consumer CE1, because the data drops and latency increased in the direction from the source (CE1) to the destination. This measurement evaluated each state, which can happen on a link. We can then detect in which traffic class is a potential problem and therefore to proactively react.

TABLE V. SLA-NORMAL VARIANT OF NORMAL DATA TRAFFIC

SLA Normal	Measurement PE1-CE1	Measurement CE1-CE2
RTT (avg)	17 ms	41 ms
Latency S->D	10 ms	29 ms
Latency D->S	10 ms	12 ms
Jitter S->D	12 ms	7 ms
Jitter D->S	7 ms	7 ms
Packet loss	0	0

TABLE VI. A COMPARISON OF NORMAL AND LOADED STATE

CE1-CE2	Normal state		Loaded state	
Parameter	**SLA Normal**	**SLA Voice**	**SLA Normal**	**SLA Voice**
RTT (avg)	41 ms	35 ms	211 ms	34 ms
Latency S->D	29 ms	19 ms	165 ms	19 ms
Latency D->S	12 ms	16 ms	45 ms	15 ms
Jitter S->D	7 ms	8 ms	7 ms	13 ms
Jitter D->S	7 ms	6 ms	8 ms	11 ms
Packet loss	0	0	23	0
Packet loss S->D	0	0	23	0
Packet loss D->S	0	0	0	0
MOS	X	4,06	X	4,06
IPCIF	X	11	X	11

TABLE VII. PE1-PE2 COMMUNICATION

PE1-PE2	Normal state	Loaded state
Parameter	**SLA Voice**	**SLA Voice**
RTT (avg)	25 ms	60 ms
Latency S->D	7 ms	28 ms
Latency D->S	28 ms	32 ms
Jitter S->D	14 ms	5 ms
Jitter D->S	7 ms	5 ms
Packet loss	0	0
Packet loss S->D	0	0
Packet loss D->S	0	0
MOS	4,06	4,03
IPCIF	11	12

TABLE VIII. CE1-CE2 COMMUNICATION

CE1-CE2	Normal state			Loaded state
Parameter	**SLA Normal**	**SLA Voice**	**SLA Normal**	**SLA Voice**
RTT (avg)	41ms	35ms	147ms	146ms
Latency S->D	29ms	19ms	101ms	103ms
Latency D->S	12ms	16ms	47ms	44ms
Jitter S->D	7ms	8ms	9	6ms
Jitter D->S	7ms	6ms	9ms	5ms
Packet loss	0	0	0	14
Packet loss S->D	0	0	0	14
Packet loss D->S	0	0	0	0
MOS	X	4,06	X	3,12
IPCIF	X	11	X	20

IV. CONCLUSION

The goal of the paper was to show suitability of Cisco IP SLA implementation in the intelligent environment of smart grid networks. These networks, built on MPLS technology are realizing access into each sub-areas of the smart grid and also providing core data traffic forwarding. Measuring performance characteristics with the IP SLA is important for solution of problems, which can happen in these networks. The conducted measurement scenarios and their results clearly shows, that the IP SLA is a very effective technology for problem solving, while at the same time is providing detailed information about different communication parameters for various data types. This effect was tested during parameter measurement in specific traffic types. It was proven, that the IP SLA is a very complex tool for network monitoring. It allows us to supervise large number of services and traffic commonly used within intelligent networks like smart grid.

ACKNOWLEDGMENT

This work and contribution is supported by the project of the student grant competition of the University of Pardubice, Faculty of Electrical Engineering and Informatics.

REFERENCES

[1] R. Froom, B. Sivasubramanian, and E. Frahim, "Implementing Cisco IP switched networks (SWITCH): foundation learning guide," Indianapolis: Cisco Press, 2010. ISBN 978-1-58705-884-4.

[2] A. Indurkar, A. Patil, and B. Pathak, "Performance failure detection and path computation," in: Proceedings - IEEE International Conference on Information Processing, ICIP, 2015, art. no. 7489357, pp. 90-95.

[3] A. Rayes, and K. Sage, "Integrated management architecture for IP-based networks," in: IEEE Communications Magazine, 2000, pp. 48-53. DOI: 10.1109/35.833556. ISSN 0163-6804

[4] H. Nemati, A. Singhvi, N. Kara, and M. El Barachi, "Adaptive SLA-based elasticity management algorithms for a virtualized IP multimedia subsystem," in: 2014 IEEE Globecom Workshops, GC Wkshps 2014, art. no. 7063377, pp. 7-11.

[5] M. Jiang, J. Byrne, K. Molka, D. Armstrong, K. Djemame, and T. Kirkham, "Cost and risk aware support for Cloud SLAs," in: CLOSER 2013 - Proceedings of the 3rd International Conference on Cloud Computing and Services Science, 2013, pp. 207-212.

[6] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, "Smart Grid Technologies: Communication Technologies and Standards," in: IEEE Transactions on Industrial Informatics. 2011, 7(4), pp. 529-539.

[7] L. Wenpeng D. Sharp, and S. Lancashire, "Smart grid communication network capacity planning for power utilities," in: IEEE PES T&D, 2010 pp. 1-4. DOI: 10.1109/TDC.2010.5484223. ISBN 978-1-4244-6546-0.

[8] F. Holik, J. Horalek, S. Neradova, S. Zitta, and O. Marik, "The deployment of Security Information and Event Management in cloud infrastructure," in: 2015 25th International Conference Radioelektronika (RADIOELEKTRONIKA), 2015, pp. 399-404. DOI: 10.1109/RADIOELEK.2015.7128982. ISBN 978-1-4799-8117-5.

[9] F. Holik, J. Horalek, S. Neradova, S. Zitta, and M. Novak, "Methods of deploying security standards in a business environment," in: 2015 25th International Conference Radioelektronika (RADIOELEKTRONIKA) 2015, pp. 411-414. DOI: 10.1109/RADIOELEK.2015.7128984. ISBN 978-1-4799-8117-5

[10] J. Horalek, J. Matyska, V. Sobeslav, and P. Suba, "Energy efficiency measurements of data center systems," in: 2014 ELEKTRO. pp. 41-45, DOI: 10.1109/ELEKTRO.2014.6847868. ISBN 978-1-4799-3721-9.