XXIV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E
TRANSMISSÃO DE ENERGIA ELÉTRICA

22 a 25 de outubro de 2017
Curitiba - PR

CB/GPC/08

GRUPO – V

GRUPO DE ESTUDO DE PROTEÇÃO, MEDIÇÃO, CONTROLE E AUTOMAÇÃO EM SISTEMA DE POTENCIA-GPC

UTILIZAÇÃO DO PROTOCOLO SNMP EM REDES DE PROTEÇÃO E CONTROLE PARA GESTÃO DO PROTOCOLO RSTP

ALEXANDRE FERNANDES ONÇA (*)
SIEMENS

RESUMO

Segundo a norma IEC-62439, que aborda a resiliência das redes em caso de falhas, o tempo de recomposição da rede deve ser inferior ao tempo de tolerância de degradação do sistema de automação. Em se tratando de redes de proteção e controle de subestações de energia que utilizam protocolo IEC61850, tempos distintos são considerados dependendo do tipo de mensagem a ser trocada. Entre os variados tipos de mensagens, temos como exemplo os telegramas GOOSE que operam com tempos na ordem de milissegundos dependendo da aplicação.

Visando garantir a disponibilidade da rede e buscando a melhor solução em termos de custo x benefício, o protocolo o RSTP tornou-se o mais utilizado em sistema de automações de subestações. Uma vez que o protocolo RSTP requer que todos os equipamentos na rede estejam devidamente configurados para que haja convergência e alta disponibilidade, torna-se útil a utilização de uma ferramenta que realize a gestão das configurações dos equipamentos e também consiga rastrear possíveis falhas na rede de diversas naturezas. Como alternativa simples e eficiente, podemos utilizar o protocolo SNMP para fazer a gestão de switches, roteadores, impressoras, computadores e, em particular, relés de proteção.

Este artigo mostrará a solução desenvolvida sobre a plataforma do Microsoft Excel, onde a aplicação coleta via SNMP dados de todos os IEDs (Intelligent Electronic Device) relacionados e compara os resultados a fim de verificar as possíveis falhas de parametrização ou detectar problemas de hardware como portas e fibras ópticas defeituosas. Mostrará também que é possível obter números de série, versões de firmwares ou qualquer outra informação disponibilizada pelo fabricante.

PALAVRAS-CHAVE

RSTP, SNMP, IEC61850

1.0 - INTRODUÇÃO

As duas principais motivações da norma IEC 61850 são prover a interoperabilidade de IEDs em Sistemas de Automação de Subestações e acompanhar rapidamente as mudanças tecnologicas de comunicação. Sendo assim, o padrão Ethernet foi escolhido por ser amplamente aceito e utilizado comercialmente e cujos esforços se concentrariam em seu aprimoramento, não no desenvolvimento de algo completamente novo.

Em se tratando de redes de proteção e controle em IEC61850, telegramas Ethernet do tipo “GOOSE”, por exemplo, tornaram-se extremamente úteis na substituição de cabos de cobre convencionais em aplicações como mudança de seletividade lógicas ou desligamento de equipamentos primários.

(*) Rua Gerson Benedito de Assis, n° 281 – CEP 13213-000 Jundiaí, SP – Brasil.
Tel: (+55 11) 97460-5467 – Email: alexandre.onca@siemens.com

Tais funcionalidades requererem uma rede seguramente disponível, mas o padrão Ethernet não foi inicialmente concebido para operar em missões críticas. Logo, tornou-se desafiante para os responsáveis técnicos a implementação de soluções complementares, que viabilizassem a redundância e/ou recomposições da rede em caso de falhas.

No entanto, na primeira edição da norma IEC 61850 essas soluções não foram especificadas. Buscando-se, então, auxilio na norma IEC-62439 (que aborda a resiliência das redes em caso de falhas) e considerou-se como premissa que o tempo de recomposição da rede deve ser inferior ao tempo de tolerância de degradação do sistema de automação.

A norma IEC 61850 considera tempos distintos dependendo do tipo de mensagem a ser trocada. Entre os variados tipos de mensagens, temos como exemplo mensagens do tipo 1A “TRIP” que demandam tempos na ordem de milissegundos para execução.

2.0 - PROTOCOLOS DE GERENCIAMENTO DE REDE

2.1 Spanning Tree Protocol (STP)

2.1.1 Histórico e Motivações

O STP é um protocolo nativo da Camada dois do modelo OSI, operado por bridges e switches. A primeira versão foi criada em 1985 [1] por Radia Perlman e incorporado pelo padrão IEEE 802.1D em 1990 [2]. O principal objetivo do protocolo é a conexão de diferentes LANs (Local Area Network), de modo único ou redundante e por equipamentos auto-configuráveis, de maneira que a conectividade possa ser preservada em caso de falhas ou de novas conexões anexadas [2].

O tráfego da camada 2 pode ser divido em mensagens de tipo:

- Unicast: somente um destino
- Multicast: diversos destinos e/ou grupos.
- Broadcast: para todos os equipamentos na rede.

Quando algum segmento de uma rede LAN é conectado de maneira redundante, um telegrama do tipo broadcast (que depois de recebido pelo switch é retransmitido para todas as suas portas, exceto para porta de chegada) pode circular infinitamente (Switching Loops). Na figura abaixo, temos um exemplo deste caso, quando o switch A envia um pacote ao switch B, que envia para o switch C e que retorna novamente para o switch A.

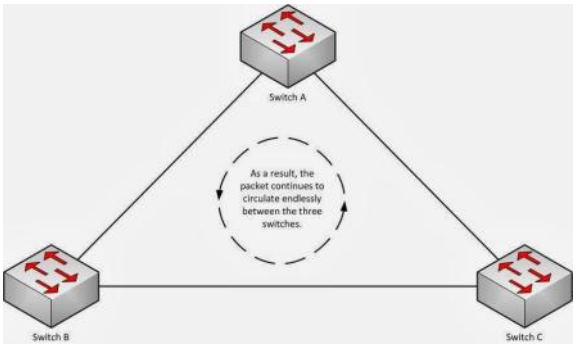

FIGURA 1- Exemplo de Switching Loop [3]

Este processo de retransmissão circular multiplica os telegramas broadcast a cada ciclo, podendo consumir toda banda de rede disponível (Broadcast Storm) e indisponibilizar a rede em poucos segundos.

2.1.2 Breve descritivo de funcionamento do protocolo STP

Analisar a topologia dos switches existentes na rede e desligar conexões que possam ocasionar “loopings” na rede é parte do algoritmo do protocolo STP. O principio de funcionamento baseia-se na ideia de eleger, entre os equipamentos do mesmo domínio, o elemento central “Root”. Este decidirá quais caminhos serão desligados logicamente, a fim de simplificar topologias de rede em árvores.

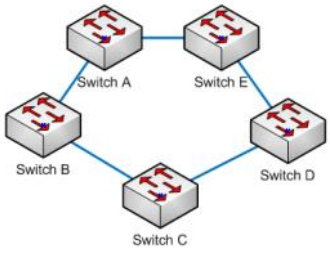

FIGURA 2 - Topologia original

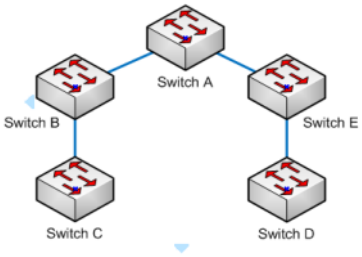

FIGURA 3 - Topologia simplificada

A eleição para decisão do root é realizada através da troca de BPDUs (Bridge Protocol Data Unit) entre os switches. BPDUs são telegramas multicast de camada 2 que compartilham informações, cujo conteúdo envolve parâmetros do protocolo, na busca da convergência (estabilidade) através dos seguintes passos [4]:

- Permitir aos switches enviarem PBDUs entre eles, propagando sua identidade e os custos de caminho.
- Eleger um switch central (Root) entre os todos, utilizando o critério de menor valor de Bridge Priority, seguido pelo menor valor de MAC Address.
- Permitir aos switches calcular a direção e o custo do caminho mais curto para o Root, baseando-se nas BPDUs recebidas dos outros switches mais próximos do Root. Os valores de custo do caminho são inversamente proporcionais à banda de rede do segmento em questão.
- Caminhos com os mais baixos custos serão mantidos. Os demais serão logicamente desligados, evitando-se assim os indesejados “loopings” de telegramas.

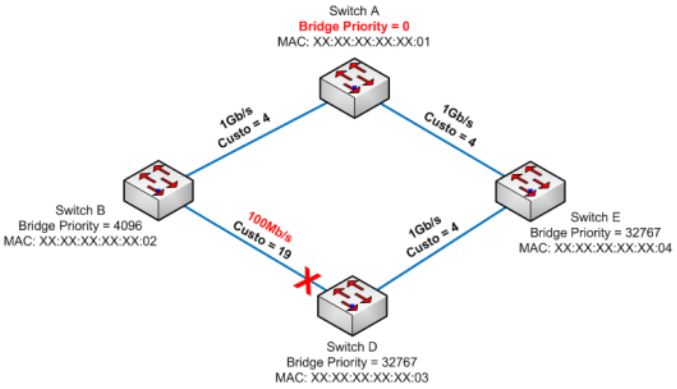

FIGURA 4 - Convergência da rede

Conforme ilustrado na figura 4, o switch A foi eleito o Root da rede por possuir o menor valor de **Bridge Priority (0)** e todos os custos de caminho serão calculados a partir do mesmo. Nota-se que entre o switch B e C, temos a largura de banda menor que as demais (100Mb/s), com valor de custo maior (19). Portanto, este caminho deve ser logicamente desligado, evitando a circulação de telegramas.

2.2 Rapid Spanning Tree Protocol (RSTP)

2.2.1 Melhorias em relação ao protocolo STP

O STP foi o primeiro padrão a ser publicado que provou ser um método confiável para fornecer redundância enquanto elimina loopings. Entretanto, originalmente não foi projetado para ser rápido o suficiente e suprir os requerimentos de disponibilidade das redes de automação de subestações, pois pode demorar mais de 30 segundos para convergir e estabilizar a rede.

Em 2001, foi introduzido o novo protocolo RSTP junto ao padrão 802.1w (futuramente incorporado e aprimorado ao 802.1D em 2004) [5]. O princípio de funcionamento assemelha-se ao antigo STP, porém algumas mudanças em seu algoritmo trouxeram rápida convergência da rede após mudanças de topologia. Dentre as melhorias, podemos citar:

- Registrar caminhos alternativos para o Root. Quando algum link falha, rotas pré-calculadas são automaticamente ativadas e comunicadas aos switches vizinhos.
- Novo procedimento chamado “proposing-agreeing”, onde o switch não precisa aguardar nenhum temporizador para mudar o estado de alguma porta. Ele comunica ao vizinho o novo caminho alternativo e este consecutivamente ao próximo, realizando uma “onda” de “handshakings” até alcançar o final da rede.

- Edge ports: portas dos switchs onde são conectados hosts como computadores e impressoras, permitindo que a porta opere imediatamente sem a necessidade de verificar por loopings. Esta melhoria evita que sejam perdidos pacotes DHCP quando a porta tornar-se ativa.

O protocolo foi desenvolvido para que a convergência da rede seja alcançada mesmo com os valores padrões. Entretanto, visando melhorar o desempenho na convergência, podemos realizar alguns ajustes finos nos seguintes parâmetros:

- Bridge Priority: decrementando este valor é possível forçar a eleição do root da rede para o switch desejado.
- Hello Time: Ajusta o tempo entre a transmissão de BPDUs. Este valor pode ser alterado somente no root da rede.
- Max Age Time: Ajusta a "idade" máxima da BPDU recebida. Representa o tempo máximo de chegada entre as BPDUs e deve ser configurado caso seja necessário compatibilizar a rede com equipamentos que operem em versões anteriores como o STP.
- Forward Delay: Ajusta qual o tempo que o switch aguarda para alterar os estados das portas de "listening" para "learning" e de "learning" para "forwarding". Deve ser configurado caso seja necessário compatibilizar a rede com equipamentos que operem em versões anteriores como o STP.

2.3 Simple Network Management Protocol (SNMP)

2.3.1 Histórico e Motivações

O protocolo SNMP foi criado na década de 80 [7] pelo Internet Engineering Task Force (IETF) para realizar a gerência remota de equipamentos de rede como modems, switchs, roteadores, impressoras, etc. A primeira versão (SNMPv1) foi oficialmente publicada na RFC 1057, a segunda versão (SNMPv2) em 1996 na RFC 1901 e a última versão (SNMPv3) em 1999 na RFC 2571.

A principal motivação para o desenvolvimento do protocolo foi a necessidade de uma ferramenta para monitoramento e gestão de equipamentos de rede, uma vez que a quantidade de ativos aumentava substancialmente. Além de prover dados para diagnósticos, o protocolo permitiria ainda analisar os recursos atuais e fornecer dados para futuras expansões.

2.3.2 Princípio de funcionamento

O funcionamento do SNMP é baseado em dois dispositivos: o Agente e o Gerente. A relação entre ambos é do tipo Cliente-Servidor, onde Gerente (Cliente) deve ser capaz de realizar leitura de valores (GET) para monitorar o dispositivo desejado, assim como escrever (SET) na possibilidade de efetuar alterações de valores. O Agente (Servidor) responde as solicitações e também pode notificar de maneira espontânea (TRAP) o Gerente no caso de exceções [6].

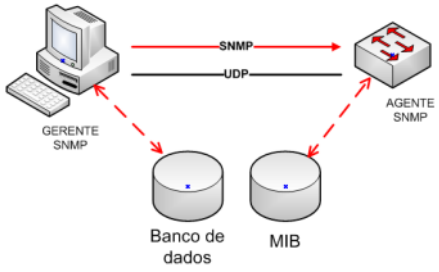

FIGURA 5 - Gerente e Agente SNMP

Cada informação a ser monitorada no Agente é chamada de objeto e possui um endereço único, chamado de OID (Object Identifier), introduzindo-se o conceito de "Objeto gerenciado":

"*Um objeto gerenciado é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados, e as estruturas de dados resultantes são os objetos gerenciados. [8]*"

Na prática, OIDs são organizados de maneira hierárquica e podem ser padronizados ou privados. Na figura abaixo, temos como exemplo o grupo de objetos do protocolo STP/RSTP padronizados:

MIB Object	Type	Access	Syntax	Object Identifier
dot1dStp	GROUP	1.3.6.1.2.1.17.2 iso(1). org(3). dod(6). internet(1). mgmt(2). mib-2(1). dot1dBridge(17). dot1dStp(2)		
dot1dStpProtocolSpecification	SCALAR	read-only	INTEGER	1.3.6.1.2.1.17.2.1.0
dot1dStpPriority	SCALAR	read-write	Integer32 (0..65535)	1.3.6.1.2.1.17.2.2.0
dot1dStpTimeSinceTopologyChange	SCALAR	read-only	TimeTicks	1.3.6.1.2.1.17.2.3.0
dot1dStpTopChanges	SCALAR	read-only	Counter32	1.3.6.1.2.1.17.2.4.0
dot1dStpDesignatedRoot	SCALAR	read-only	BridgeId	1.3.6.1.2.1.17.2.5.0
dot1dStpRootCost	SCALAR	read-only	Integer32	1.3.6.1.2.1.17.2.6.0
dot1dStpRootPort	SCALAR	read-only	Integer32	1.3.6.1.2.1.17.2.7.0
dot1dStpMaxAge	SCALAR	read-only	Timeout	1.3.6.1.2.1.17.2.8.0
dot1dStpHelloTime	SCALAR	read-only	Timeout	1.3.6.1.2.1.17.2.9.0
dot1dStpHoldTime	SCALAR	read-only	Integer32	1.3.6.1.2.1.17.2.10.0
dot1dStpForwardDelay	SCALAR	read-only	Timeout	1.3.6.1.2.1.17.2.11.0
dot1dStpBridgeMaxAge	SCALAR	read-write	Timeout (600..4000)	1.3.6.1.2.1.17.2.12.0
dot1dStpBridgeHelloTime	SCALAR	read-write	Timeout (100..1000)	1.3.6.1.2.1.17.2.13.0
dot1dStpBridgeForwardDelay	SCALAR	read-write	Timeout (400..3000)	1.3.6.1.2.1.17.2.14.0

FIGURA 6 - Conjunto de objetos SNMP (OIDs)

Dessa forma, o conjunto dos objetos gerenciados que procura consolidar todas as informações necessárias para a gerência da rede chama-se “MIB” (Management Information Base). Ao buscar objetos em determinados Agentes, deve-se pesquisar preferencialmente quais as MIBs fornecidas pelo mesmo. Vide figura 7 abaixo:

Standard	MIB Name	Title
RFC 2012	TCP-MIB	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013	UDP-MIB	Management Information Base for the UDP using SMIv2
RFC 1659	RS-232-MIB	Definitions of Managed Objects for RS-232-like Hardware Devices
RFC 2863	IF-MIB	The Interface Group MIB
RFC 2819	RMON-MIB	Remote Network Monitoring management Information Base

FIGURA 7 – Exemplo de MIBs disponíveis para um equipamento

Entretnato, não é pré-requisito colecionar as MIBs dos equipamentos para estabelecer conexão entre dois equipamentos, pois o Gerente solicita ao Agente somente o endereço de OID do(s) objetos solicitados.

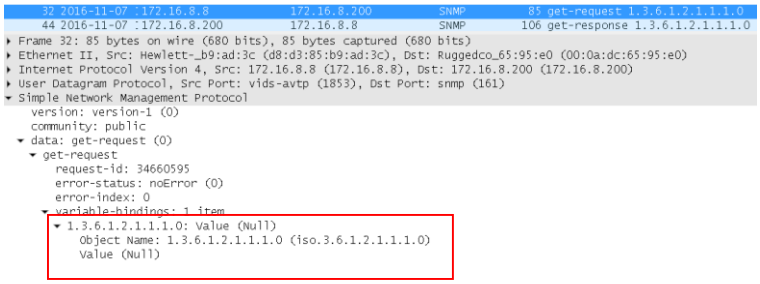

FIGURA 8 - Gerente solicitando objeto ao Agente

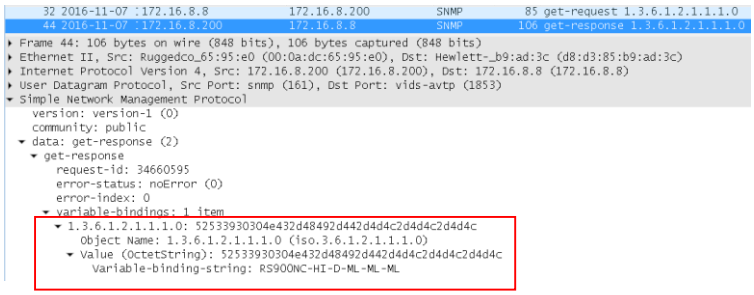

FIGURA 9 - Agente respondendo à solicitação do Gerente

No exemplo das figuras 8 e 9, podemos ver com a trama de telegramas que o Gerente solicita informação do OID “1.3.6.1.2.1.1.1” ao Agente. Para saber do que se refere este objeto, deve-se consultar a MIB correspondente para “traduzir” o endereço em: 1 (iso). 3 (org). 6 (dod). 1 (internet). 2 (mgmt). 1 (**mib-2**). 1 (system). 1 (sysDescr). A descrição para este objeto segundo a **RFC 1213-MIB-2** seria:

"A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters. [9]"

2.3.3 SNMP aplicado em relatórios de ativos e na investigação de problemas de redes

A motivação principal da utilização do protocolo SNMP em sistemas de Automação de Subestações é o gerenciamento dos ativos como switches, relés de proteção, estações de engenharia, etc. Entretanto, pode ser muito útil na coleta de informações que sejam relevantes para indicar a fonte de problemas de instabilidade. Nos exemplos das tabelas abaixo, utilizaremos objetos de MIBs padronizadas e privadas.

Tabela 1 - Identificação de Bridge Priority dos Switches

	.1.3.6.1.2.1.1.3.0	.1.3.6.1.2.1.1.5.0	.1.3.6.1.2.1.17.2.2.0	.1.3.6.1.2.1.17.2.8.0	.1.3.6.1.2.1.17.2.11.0	.1.3.6.1.2.1.17.2.3.0	.1.3.6.1.2.1.17.2.4.0	.1.3.6.1.2.1.17.2.5.0
Status	System up time	Switch Name	Bridge Priority	Configurated Max Age Time	Forward Delay	Time since last topology change	Topology changes	Root ID
Online	468 days, 23:30:44.56	SWT-1A-U17	16384	4000	2100	09:23,1	19279	00 00 00 0A DC 49 4C A0
Online	77 days, 0:59:20.97	SWT-1A-SA4	16384	4000	2100	10:03,1	4687	00 00 00 0A DC 49 4C A0
Online	38 days, 23:43:42.20	SWT-1A-U29	16384	40	21	10:43,1	37586	00 00 00 0A DC 49 4C A0
Online	119 days, 5:03:39.22	SWT-1A-EOL6	16384	40	21	11:23,4	41436	00 00 00 0A DC 49 4C A0
Online	296 days, 4:57:47.23	SWT-1A-U41	16384	40	21	12:04,0	52069	00 00 00 0A DC 49 4C A0
Online	177 days, 0:53:45.55	SWT-1A-LT5	16384	40	21	00:21,1	3278	00 00 00 0A DC 49 4C A0
Online	427 days, 2:48:42.93	SWT-2B-CFE	8192	40	21	00:20,5	50807	00 00 00 0A DC 49 4C A0
Online	293 days, 22:28:22.01	SWT-1B-CCJ	8192	40	21	01:01,1	52918	00 00 00 0A DC 49 4C A0
Online	190 days, 18:42:42.86	SWT-2A-CFE	8192	40	21	00:02,9	27963	00 00 00 0A DC 49 4C A0
Online	293 days, 22:06:01.52	SWT-1B-COU	4096	40	21	00:14,8	64332	00 00 00 0A DC 49 4C A0
Online	293 days, 22:25:20.79	SWT-1A-CCJ	8192	40	21	00:25,0	40071	00 00 00 0A DC 49 4C A0
Online	293 days, 22:04:42.21	SWT-1A-COU	0	0	0	01:05,2	42703	00 00 00 0A DC 49 4C A0

Na tabela 1, podemos verificar se o parâmetro **"Bridge Priority"** dos switches foi ajustado corretamente. Lembrando-se que o protocolo RSTP possui uma limitação de até 40 saltos contados a partir do root até o último elemento da rede. Uma incorreta escolha do elemento root pode levar um determinado elemento a ultrapassar este número máximo permitido ou ainda eleger um elemento inadequado para a função, como um relé de proteção. Pela coluna **"Root ID"** é possível certificar-se de que todos os switches estão considerando o mesmo elemento root.

Podemos relacionar também as colunas **"Topology Changes"** e **"Time since last topology changes",** que representam quantas vezes o switch modificou sua topologia de rede e em qual intervalo de tempo. O sistema em estado de operação não deve realizar mudanças de topologia de maneira aleatória, mas deve-se levar em consideração que caso o sistema esteja em fase de testes, mudanças de topologia são comuns de ocorrerem.

Tabela 2 - Informações adicionais dos Switches

	.1.3.6.1.2.1.1.3.0	.1.3.6.1.2.1.1.5.0	.1.3.6.1.4.1.15004.4.2.3.2.0	.1.3.6.1.4.1.15004.4.2.3.3.0	.1.3.6.1.4.1.15004.4.2.2.6.0	.1.3.6.1.4.1.15004.4.2.3.1.0
Status	System up time	Switch Name	Boot Version	Main Version	CPU usage Percent	Serial Number
Online	468 days, 23:30:44.56	SWT-1A-U17	v2.20.0 (Nov 22 2012 14:19)	v3.12.2 (Aug 27 2013 12:39)	15	900-0711-46564
Online	77 days, 0:59:20.97	SWT-1A-SA4	v2.20.0 (Nov 22 2012 14:19)	v3.12.2 (Aug 27 2013 12:39)	17	900-0810-30609
Online	38 days, 23:43:42.20	SWT-1A-U29	v2.20.0 (Nov 22 2012 14:19)	v3.12.1 (Dec 20 2012 09:17)	24	900-0712-61175
Online	119 days, 5:03:39.22	SWT-1A-EOL6	v2.20.0 (Nov 22 2012 14:19)	v3.12.1 (Dec 20 2012 09:17)	17	900-0712-61174
Online	296 days, 4:57:47.23	SWT-1A-U41	v2.20.0 (Nov 22 2012 14:19)	v3.12.2 (Aug 27 2013 12:39)	18	900-0712-61185
Online	177 days, 0:53:45.55	SWT-1A-LT5	v2.20.0 (Nov 22 2012 14:19)	v3.12.2 (Aug 27 2013 12:39)	15	900-0712-61179
Online	427 days, 2:48:42.93	SWT-2B-CFE	v2.20.0 (Nov 22 2012 14:19)	v3.12.1 (Dec 20 2012 09:17)	29	R21-0810-31603
Online	293 days, 22:28:22.01	SWT-1B-CCJ	v2.20.0 (Nov 22 2012 14:19)	v3.12.1 (Dec 20 2012 09:17)	30	R21-0810-31605
Online	190 days, 18:42:42.86	SWT-2A-CFE	v2.20.0 (Nov 22 2012 14:19)	v3.12.1 (Dec 20 2012 09:17)	23	R21-0810-31608
Online	293 days, 22:06:01.52	SWT-1B-COU	v2.20.0 (Nov 22 2012 14:19)	v3.12.1 (Dec 20 2012 09:17)	24	R21-0310-27232
Online	293 days, 22:25:20.79	SWT-1A-CCJ	v2.20.0 (Nov 22 2012 14:19)	v3.12.1 (Dec 20 2012 09:17)	34	R21-0810-31610
Online	293 days, 22:04:42.21	SWT-1A-COU	v2.20.0 (Nov 22 2012 14:19)	v3.12.1 (Dec 20 2012 09:17)	30	R21-0310-27233

Na tabela 2, é possível coletar demais informações relevantes para elaborar lista de ativos de rede, como versões de firmware e números de série, úteis para futuras intervenções técnicas no sistema e/ou solicitações de suporte técnico com o fabricante. Note também o uso de CPU representado pela coluna **"CPU usage Percent"**, onde se confirma que os equipamentos estão com carga de processamento na CPU em padrões aceitáveis.

Tabela 3 - Informações obtidas em relés de proteção

.1.3.6.1.2.1.1.5.0	.1.3.6.1.2.1.1.1.0	.1.3.6.1.2.1.17.2.2.0	.1.3.6.1.2.1.17.2.3.0	.1.3.6.1.2.1.17.2.4.0
IED NAME	EN100 VERSION	Bridge Priority	Time since last topology change	Topology changes
EN100_O UPATEX41/SIP098EFD814A	SIPROTEC4 EN100_O V04.22.01_01 Ed1	32768	02:41,0	241595
EN100_O UPATEX39/SIP098EFEDFBC	SIPROTEC4 EN100_O V04.22.01_01 Ed1	32768	00:12,0	249769
EN100_O UPP1T09/SIP098EFE9F4F	SIPROTEC4 EN100_O V04.22.01_01 Ed1	32768	01:02,0	272503
EN100_O PABG2T09/SIP098EFEAF73	SIPROTEC4 EN100_O V04.22.01_01 Ed1	32768	01:54,0	291202
EN100_O UPATEX35/SIP098EFEDFBF	SIPROTEC4 EN100_O V04.22.01_01 Ed1	32768	00:02,0	317779
EN100_O UPATEX33/SIP098EFE92B2	SIPROTEC4 EN100_O V04.22.01_01 Ed1	32768	00:29,0	320214
EN100_O PABG2T10/SIP098EFE9EC4	SIPROTEC4 EN100_O V04.22.01_01 Ed1	32768	00:55,0	382921
EN100_O UPATEX36/SIP098EFD8127	SIPROTEC4 EN100_O V04.08.04_01	-2013265911	00:00,8	417761

Na tabela 3, aplicando-se a análise de mudanças de topologia **(Topology changes),** classifica-se a coluna correspondente por ordem numérica e consequentemente o último da lista será o elemento com maior número de mudança. Verifica-se que há possibilidade da instabilidade ser ocasionada por uma incompatibilidade de firmware **(EN100 Version),** já que o elemento encontra-se com versão diferente dos demais. Verifica-se também que a instabilidade pode ser ocasionada pelo valor de “Bridge Priority” informado pelo equipamento, que está muito além do esperado.

Tabela 4 - Informação sobre elementos ethernet vizinhos

.1.3.6.1.4.1.22638.1.1.22.0	.1.3.6.1.4.1.22638.1.1.23.0	.1.3.6.1.4.1.22638.1.1.25.0	.1.3.6.1.4.1.22638.1.1.26.0	1.3.6.1.2.1.2.2.1.6.2	.1.3.6.1.4.1.22638.1.3.4.9.0	.1.3.6.1.4.1.22638.1.3.4.10.0
Link Channel 1 (Channel Status)	**Link Channel 2 (Channel Status)**	**Link Level 1 (under 2464 = abnormal)**	**Link Level 2 (under 2464 = abnormal)**	**MAC Address do elemento**	**RSTP Neighbour Port A**	**RSTP Neighbour Port B**
0	1	0	2464	00 09 8E FE 2B 82	00 00 00 00 00 00	00 09 8E FE 26 0F
0	1	0	2464	00 09 8E FE D4 E4	00 00 00 00 00 00	00 09 8E FE D4 5C
1	1	2464	2464	00 09 8E FE D5 81	00 09 8E FE D5 8C	00 0A DC 49 51 A7
1	1	2464	2464	00 09 8E FE 22 51	00 09 8E FD 81 47	00 09 8E FD 81 4A
1	1	1744	2464	00 09 8E FE 26 5A	00 0A DC 49 1F 07	00 09 8E FE 24 AA
1	1	2464	2464	00 09 8E FD 35 91	00 09 8E FD 81 28	00 09 8E FD 81 4B
1	1	2464	2464	00 09 8E FE 22 50	00 09 8E FE 26 A4	00 09 8E FE 2D 8F

Os modelos de Relé de proteção utilizados no estudo fornecem o MAC Address dos elementos adjacentes conectados as suas portas Ethernet através das colunas “RSTP Neighbour Port A” e “RSTP Neighbour Port B. Esses objetos podem fornecer dados para a elaboração de uma representação gráfica da rede, mostrando a conexão dos equipamentos de maneira dinâmica após uma mudança de topologia.

Entrando em detalhes na coluna “RSTP Neighbour Port A”, identificamos endereço de MAC Address inválido (00 00 00 00 00 00). Este valor é justificado com ajuda da coluna “Link Channel 1” = 0 indicando que a porta Ethernet está eletricamente desligada, comprometendo o desempenho da convergência da rede.

Outro objeto que pode indicar eminência de falhas é o “Link Level”, onde é mensurado o nível óptico da porta Ethernet do equipamento. Note que, de acordo com a especificação do fabricante, valores inferiores a 2464 podem representar falhas no meio físico (fibras ópticas mal conectorizadas, fusões defeituosas). Na tabela 4 podemos observar que um dos equipamentos está indicando valor igual a “1744” e provavelmente está causando instabilidades ao redor do seu trecho.

Tabela 5 - Goose Mismatch de relés de proteção

.1.3.6.1.2.1.1.5.0	.1.3.6.1.2.1.1.1.0	.1.3.6.1.4.1.22638.1.2.1.0	.1.3.6.1.4.1.22638.1.2.2.0
IED NAME	**EN100 VERSION**	**Goose Match**	**Goose Mismatch**
EN100_O UPAG13/SIP098EFD7CDE	SIPROTEC4 EN100_O V04.22.01_01 Ed1	0	0
EN100_O UPAG06/SIP098EFD3579	SIPROTEC4 EN100_O V04.22.01_01 Ed1	0	0
EN100_O PPBG1T06/SIP098EFE299C	SIPROTEC4 EN100_O V04.22.01_01 Ed1	0	0
EN100_O UPAG22/SIP098EFD352F	SIPROTEC4 EN100_O V04.22.01_01 Ed1	0	0
EN100_O UPPTEX19/SIP098EFEDFD4	SIPROTEC4 EN100_O V04.22.01_01 Ed1	0	0
EN100_O PALT3/SIP098EFED605	SIPROTEC4 EN100_O V04.22.01_01 Ed1	7168316	7186362
EN100_O UPPTEX14/SIP098EFD33C4	SIPROTEC4 EN100_O V04.22.01_01 Ed1	0	0

De acordo com a tabela 5, o fabricante do relé de proteção também fornece como informação complementar o número de falhas de telegrama GOOSE do equipamento. Esta informação é de extrema importância para o funcionamento do sistema, uma vez que a falha na transmissão/recebimento desse tipo de telegrama pode comprometer funções vitais, como desligamento de equipamentos primários das subestações de energia.

3.0 - CONCLUSÃO

Concluiu-se então que o protocolo RSTP pode ser o mais indicado em termos de custo x benefício para o gerenciamento da rede, prova de que se tornou o mais utilizado em sistema de automações de subestações no Brasil.

Por mais que a norma IEC 61850 permita a criação de Logical Nodes específicos para uma possível supervisão/gestão do RSTP (lembrando-se que não há Logical Nodes nativos relativos a este tema), muitas horas de engenharia seriam necessárias para parametrizar essas informações nos relés de proteção.

O protocolo SNMP, hoje com quase 30 anos, é bastante conhecido pelos administradores de redes e está se popularizando entre engenheiros de automação de subestações de energia ao passo que o padrão Ethernet está se tornando essencial na comunicação dos equipamentos. A parametrização do protocolo é simples e não demanda excessivos esforços de engenharia para configurá-lo e testá-lo no sistema.

A aplicação desenvolvida teve como motivação principal a necessidade de comparar todos os valores dos objetos SNMP em forma de planilha, onde os resultados poderiam ser cruzados para facilitar global da rede. Existem diversas aplicações gratuitas disponíveis no mercado, mas nem todas emitem relatórios que corroboram para uma análise eficiente das redes Ethernet e seus respectivos ativos. Lembrando que grande parte das IHMs (Interface Homem Maquina) fornece suporte ao protocolo SNMP e que muitas informações úteis poderiam integrar as telas de arquitetura do sistema para garantir o fornecimento de dados mais apurados aos mantenedores.

Há também uma tendência que a gerência da rede de processos seja integrada a infraestrutura corporativa da empresa. Levando-se em consideração a segurança cibernética nesse cenário, equipamentos como Roteadores e Firewalls estarão mais presentes em soluções de Automação de Subestações e consequentemente informações detalhadas das redes, assim como a verificação das configurações de segurança serão de máxima importância.

4.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) Perlman, Radia, “An Algorithm For Distributed Computation Of A Spanning Tree In An Extended Lan”, 1985, Https://Www.It.Uu.Se/Edu/Course/Homepage/Datakom/Ht06/Slides/Sta-Perlman.Pdf

(2) “The Evolution Of The Internet: The Spanning Tree Protocol, A Major Achievement In Internet Routing”, Http://Www.Ipwatchdog.Com/2016/02/04/Spanning-Tree-Protocol-Internet-Routing/Id=65051/

(3) “*Jncia Lesson 6 -- Spanning Tree, Rapid Spanning Tree And Multiple Spanning Tree”,* Http://Aknetworkgeek.Blogspot.Com.Br/2013/11/Jncia-Lesson-6-Spanning-Tree-Rapid.Html

(4) “*Performance Of The Rapid Spanning Tree Protocol In Ring Network Topology”,* White Paper 2007, Https://W3.Siemens.Com/Mcms/Industrial-Communication/En/Rugged-Communication/Documents/Rstp-In-Ring-Network-Topology-En.Pdf

(5) “802.1dtm Ieee Standard For Local And Metropolitan Area Networks Media Access Control (Mac) Bridges”, Página Iii, 2004.

(6) Fraga Contessa, Diego, Rafael Polina, Everton, “Gerenciamento De Equipamentos Usando O Protocolo Snmp”,

(7) Zanella, Beethovem, Alves Jr, Nilton, “*Protocolo De Gerenciamento Snmp”*

(8) “O Que É Uma Mib”, Http://Penta.Ufrgs.Br/Gr952/Trab1/2conceit.Html

*(9) “*Management Information Base For Network Management Of Tcp/Ip-Based Internets: Mib-Ii” (Rfc 1213), 1991

5.0 - DADOS BIOGRÁFICOS

Alexandre Fernandes Onça
Nascimento: 17/11/1982
Cidade: São Paulo / Sp
Formação Acadêmica: Engenharia Elétrica – Ênfase Em Automação E Controle, Usjt – São Paulo/Sp (2002-2007)
Experiência Profissional: Engenheiro De Desenvolvimento De Sistemas Pleno Na Siemens Ltda Desde 2007, Atuando Em Parametrização E Comissionamento De Sistemas De Automação E Controle De Subestações.
Com Certificações Internacionais De Produtos Como Unidades De Automação E Ihms, Tornou-Se Especialista Em Protocolos De Comunicação Utilizados Na Área De Energia Como Iec 61850, Iec 60870-5-101/104, Dnp3 E Modbus.