UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ – UTFPR
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA – DAELN

RENAN WILLY FERNANDES

ESTUDO DE CASO: ANÁLISE DE TRÁFEGO EM REDES DE COMUNICAÇÃO DE SUBESTAÇÕES COM FOCO NOS PROTOCOLOS DA NORMA IEC-61850

CURITIBA
2015

ESTUDO DE CASO: ANÁLISE DE TRÁFEGO EM REDES DE COMUNICAÇÃO DE SUBESTAÇÕES COM FOCO NOS PROTOCOLOS DA NORMA IEC-61850

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR
Orientador: Prof. MSc. Fabiano Scriptore de Carvalho

CURITIBA

2015

RESUMO

FERNANDES, Renan W. **Estudo de Caso: Análise de Tráfego de Rede de Comunicação de Subestações com Foco nos Protocolos da Norma IEC-61850**. 2015. 62 f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

A presente monografia aborda um estudo de caso relacionado à análise do tráfego em redes de comunicação em subestações implementadas de acordo com a norma IEC-61850. Apresenta alguns resultados e define o estado de funcionamento das redes analisadas, bem como define o comportamento das redes em situações consideradas normais. O projeto tem início utilizando o método bibliográfico, seguido de coleta de dados em campo, inserção dos dados coletados em planilhas e finalmente obtenção de informações para análise. Este trabalho busca ter o conhecimento do funcionamento na prática de redes baseadas na norma IEC-61850 e encontrar possíveis falhas de configuração de rede e dos dispositivos a ela conectados.

Palavras-chave: IEC-61850, Análise de Tráfego, Redes de Comunicação, Automação de Subestações.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

1.1. TEMA

Desde o inicio da utilização comercial da energia elétrica, com as primeiras unidades geradoras feitas por Thomas A. Edison em 1882, o desenvolvimento tecnológico nas áreas de geração, transmissão e distribuição de energia elétrica nunca cessou. Em nossa sociedade a energia elétrica se estabeleceu como um dos pilares que sustentam o desenvolvimento de um país, bem como corporações e plantas industriais. Neste contexto algumas empresas deste ramo, que se preocuparam em desenvolver e dominar novas tecnologias tornaram-se grandes corporações multinacionais e hoje promovem uma corrida tecnológica na busca de retorno financeiro.

Nas diversas áreas que envolvem projetos relacionados à utilização da energia elétrica, a área mais dinâmica é a automação de subestações, pois tem sido diretamente afetada pelo desenvolvimento da eletrônica no decorrer dos anos. O controle remoto de subestações via rede telefônica já era possível nos anos 1930, mas com capacidade para poucos pontos de indicação e comando. Em meados dos anos 1960 a comunicação digital tornou viáveis sistemas de aquisição de dados automáticos com medições e comandos de mais pontos e com menor atraso (Mackiewicz, 2004). Mas até os anos de 1970 a tecnologia de controle de subestações era baseada em equipamentos eletromecânicos. A partir da década de 1980, com a consolidação da tecnologia eletrônica, o controle de subestações começa a adotar equipamentos eletrônicos para aquisição de dados e envio a um centro de controle remoto (Pereira, 2007). Com isto inicia-se também o desenvolvimento de redes de comunicação com diversos protocolos. Ainda no inicio da década de 1980 houve um grande aumento na quantidade e tamanho das redes de comunicação, e, desta forma, empresas desenvolvedoras de tecnologia sentiram o problema causado pela grande diversidade de redes e protocolos disponíveis.

Em 1984 a International Organization for Standardization (ISO) apresentou o modelo descritivo de redes de comunicação, conhecido como Open System Interconnection (OSI). Esta foi uma ferramenta importante para fabricantes no desenvolvimento de tecnologias de comunicação com maior compatibilidade e interoperabilidade (Siemens, 2013). Mas como ainda havia a necessidade do desenvolvimento de um protocolo que atendesse às necessidades de uma subestação ainda foi necessário o esforço no desenvolvimento de outro padrão. Em 2002 foi publicada a norma IEC-61850, mas os esforços no desenvolvimento desta norma iniciaram no final da década de 1980. Algumas das motivações desta norma são:

- Garantir uma padronização na comunicação entre dispositivos eletrônicos de diferentes fabricantes,
- Definir um sistema que seja a prova de desenvolvimentos tecnológicos,
- Garantir que o sistema como um todo opere de maneira uniforme,
- Identificar funções dentro de uma subestação e, baseado em suas necessidades, definir corretamente os requerimentos de comunicação,
- Definir modelamento que possibilite troca de informações através de uma rede de comunicação.

A norma IEC-61850 adotou o padrão Ethernet (ISO/IEC-8802/3) como meio de ligação entre dispositivos eletrônicos de subestações (IEC, 2003). Desta forma os conceitos oriundos de redes ethernet chegaram aos sistemas de proteção e automação de subestações herdando, assim, os benefícios de uma tecnologia consolidada e moderna (SCHWEITZER ENGINEERING LABORATORIES, 2010). Com isto os sistemas de automação de subestações agregaram mais possibilidades de serviços com uso de protocolos como TCP e UDP; obtiveram um ganho na confiabilidade no sistema de comunicação; diminuíram os custos de implementação (Mackiewicz, 2004).

Assim, como os sistemas de automação de subestações agregaram os benefícios das redes Ethernet, também abriram possibilidade para os possíveis problemas decorrentes destas redes. Agora tornou-se imprescindível garantir a correta configuração das LAN's (Local Area Network) observando requisitos como: configuração de VLAN's, priorização de pacotes, configuração de protocolos spanning tree, verificação do comportamento da rede com mensagens broadcast e multicast, verificação de possíveis sobrecargas na rede.

1.2. OBJETIVOS

1.1.1 Objetivo Geral

Diagnosticar o estado de redes baseadas na norma IEC-61850 através de captura de pacotes e análise dos dados obtidos.

1.1.2 Objetivos Específicos

1) Descrever o funcionamento dos protocolos e requisitos de configuração de uma rede baseada na norma IEC-61850.
2) Definir de quais dispositivos da rede serão feitas capturas através do espelhamento da porta do switch e efetuar captura de pacotes com uso de software sniffer (Wireshark).
3) Montar tabelas Excel com os dados obtidos através das capturas realizadas, como taxa de bits por segundo, tamanho médio de pacotes, taxa de utilização da rede por protocolo, comportamento de comunicação de cada tipo de dispositivo. Diagnosticar estado das redes.

1.3. JUSTIFICATIVA

A publicação da norma IEC-61850 tem permitido um avanço tecnológico considerável, ao normatizar e introduzir na automação de subestações uma rede tão consolidada e versátil como são as redes ethernet. Com isto o leque de possibilidades de serviços que poderiam ser executados pelos diversos dispositivos instalados em

uma rede elétrica, aumentou muito e hoje dispositivos que antes se restringiam a apenas proteger os circuitos nos quais estavam inseridos (de forma mecânica), hoje fornecem uma grande quantidade de variáveis online, acesso remoto, diagnósticos, etc., além de cumprir com seu objetivo básico de proteger o circuito de forma mais eficiente. A aplicação da norma já produziu, e tem produzido redes elétricas mais inteligentes, e foi um passo importante na direção das Smart Grids.

Entretanto, junto com o avanço, a tecnologia trouxe para as redes de automação de subestações a possibilidade de problemas inerentes a redes ethernet.

A motivação deste trabalho é originada de problemas vivenciados em subestações elétricas de plantas industriais que afetaram o processo da mesma, como, por exemplo, falha de sinalização de disjuntores, falha de comando remoto em disjuntores, falha de automatismo em painéis, etc. Como tais problemas tiveram forte suspeita de problemas de rede, julgou-se necessária uma verificação detalhada do estado das redes de automação das subestações da planta industrial. Na figura a seguir pode-se ver uma topologia simplificada da rede da referida planta industrial.

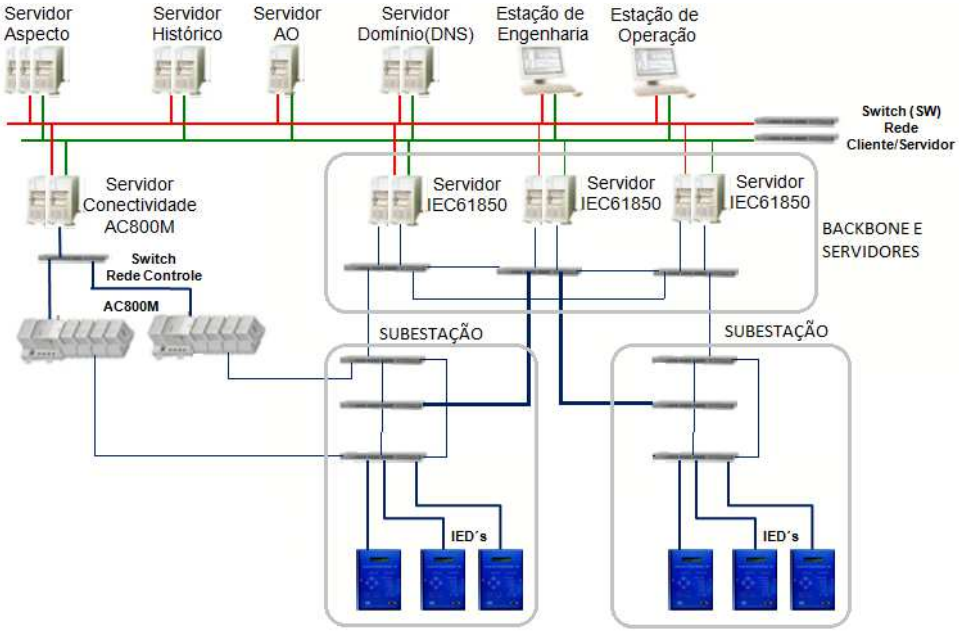


Figura 1- topologia simplificada da rede IEC 61850

Fonte: O Autor

Embora a norma IEC-61850, nos seus capítulos 4 e 10 preveja testes documentados de conformidade e desempenho da rede de automação por parte de fabricantes, comissionadores e integradores de sistema, o referido sistema não possui nenhum teste de desempenho documentado nem relatos de que foi aprovado em testes relativo a rede ethernet. Além disso, é necessária a criação de uma Linha de Base para cada LAN, pois, segundo a Cisco (2015), “Um administrador de rede precisa medir o desempenho inicial e a disponibilidade de dispositivos de rede e links críticos para poder determinar a diferença entre comportamento anormal e desempenho correto da rede [...]”. Com isto faz-se necessária a realização deste trabalho, de forma a documentar o estado de funcionamento das redes de automação das subestações das referidas plantas industriais.

1.4. METODOLOGIA

A pesquisa realizada apresenta como metodologia a ser utilizada a classificação de Estudo de Caso, descritiva com abordagem quantitativa.

Para Beuren (2009) “a pesquisa descritiva preocupa-se em observar fatos, registrá-los analisá-los, classificá-los e interpretá-los, e o pesquisador não interfere neles.” Complementa ainda que, a pesquisa descritiva tem por objetivo esclarecer determinadas características e fenômenos inerentes a ela divergindo-se assim de uma pesquisa explicativa que segundo Beuren (2009) “[...] tem por objetivo aprofundar o conhecimento da realidade, procurando a razão, o porquê das coisas [...]”.

Uma abordagem quantitativa emprega a complexidade de instrumentos estatísticos desde o início, coleta, até o tratamento dos dados. Contudo Beuren (2009) menciona que “Esse procedimento não é tão profundo na busca do conhecimento da realidade dos fenômenos, uma vez que se preocupa com o comportamento geral dos acontecimentos”, mas destaca que é de extrema importância visto que esse tipo de pesquisa visa garantir precisão nos resultados evitando distorções de analise e interpretações (BEUREN, 2009)

A pesquisa do tipo estudo de caso “[...] caracteriza-se principalmente pelo estudo concentrado de um único caso” (BEUREN, 2009). Destaca ainda que esse tipo de estudo é preferível á pesquisadores que buscam aprofundar seus conhecimentos em determinado assunto específico.

Por isso, a presente pesquisa se enquadrará nos aspectos descritos anteriormente.

2. REFERENCIAIS TEÓRICOS

Neste capítulo pretende-se abordar alguns conceitos necessários ao entendimento do funcionamento de redes ethernet locais bem como para o desenvolvimento do trabalho.

2.1 MODELO DE REFERENCIA OSI

As primeiras redes de computadores não possuíam interoperabilidade entre equipamentos de fabricantes diferentes, por exemplo, uma empresa que adotasse a solução IBM para sua rede de computadores não poderia usar equipamentos DEC (*Digital Equipment Corp*. Atualmente HP). Como se pode imaginar, por muitas vezes esta situação fez com que a tecnologia, ao invés de trazer soluções e facilidades trouxe mais problemas e dificuldades para seus usuários. Este foi o cenário criado através da implantação de redes que se utilizavam exclusivamente de protocolos de comunicação proprietário (protocolo fechado)

No inicio da década de 80 a ISO (International *Organization for Standardization*) juntamente com diversos fabricantes iniciou esforços para elaboração de um padrão abrangente para concepção de protocolos abertos de comunicação de rede, ou seja, foi um passo importante para criação de protocolos de comunicação interoperáveis independentemente do fabricante do equipamento. Em 1984 a ISO apresentou a norma ISO 7498 – *Open Systems Interconection*, mais popularmente conhecida como modelo OSI. O modelo OSI é apenas uma referencia, e, portanto, não há a obrigatoriedade de fabricantes seguirem este modelo, mas sob pena de não serem interoperáveis com outros equipamentos. Este modelo estabelece uma organização hierárquica baseada em sete camadas, onde cada camada é responsável por um processo requerido na comunicação de dados sendo o nome (função) de cada camada: Física, Enlace, Rede, Transporte, Sessão, Apresentação, Aplicação. Nesta respectiva ordem conforme figura 2. (Filippeti, 2009).

Segundo Tanenbaum (2003), os princípios aplicados para se chegar às sete camadas, de forma resumida, são:

> “1. Uma camada deve ser criada onde houver necessidade de outro grau de abstração.
> 2. Cada camada deve executar uma função bem definida.
> 3. A função de cada camada deve ser escolhida tendo em vista a definição de protocolos padronizados internacionalmente.
> 4. Os limites de camadas devem ser escolhidos para minimizar o fluxo de informações pelas interfaces.
> 5. O numero de camadas deve ser grande o bastante para que funções distintas não precisem ser desnecessariamente colocadas na mesma camada e pequeno o suficiente para que a arquitetura não se torne difícil de controlar.”

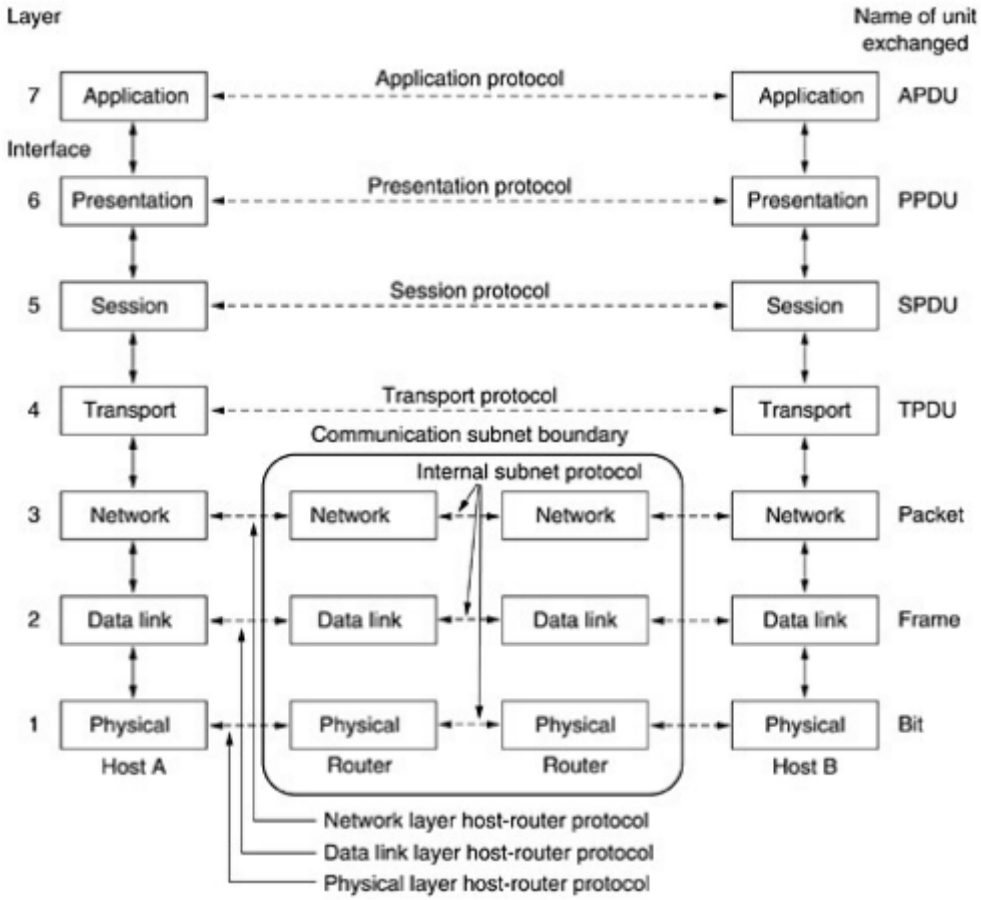


Figura 2- Modelo de comunicação de dados baseado na arquitetura OSI.

Fonte: Tanenbaum, 2003

A seguir, na figura 3, apresenta-se uma tabela que apresenta de forma resumida as sete camadas do modelo OSI com suas funções.

Camada	Descrição	
Aplicação	**Application Layer** - Provê a interface com o usuário	
Apresentação	**Presentation Layer** - Trata da semântica, compressão e descopressão, criptografia e tradução dos dados	
Sessão	**Session Layer** - Gerencia o"diálogo" entre as portas lógicas e mantém a separação dos dados de diferentes aplicações	**Nome da PDU**
Transporte	**Transport Layer** - Provê a comunicação confiável (ou não) e executa checagem de erros antes da retransmissão dos segmentos.	Segmento/ Segment
Rede	**Network Layer** - define e gerencia o endereçamento lógico da rede (ex.IP)	Pacote/ Packet/ Datagram
Enlace	**Data-link Layer** - Acomoda os pacotes em "quadros" através do processo de encapsulamento. Detecta erros, porém, não os corrige.	Quadro/ Frame
Física	**Physical Layer** - Responsável pela movimentação dos bits estre as pontas e pela definição das interfaces, especificações elétricas e de	"bits"

Figura 3- Descrição das camadas do modelo OSI.

Fonte: Filippetti, 2009

2.2 ETHERNET

Segundo a Cisco, a Ethernet é atualmente a tecnologia predominante nas redes locais (LAN). A Ethernet opera na camada de enlace de dados e de endereçamento, enquadramento e acesso ao meio nos padrões de camada física. Em outras palavras, a Ethernet define os protocolos da camada 2 e as tecnologias da camada 1.

Os padrões que definem as tecnologias e protocolos empregados nas redes Ethernet são a IEEE 802.2 e IEEE 802.3. Na figura 4 pode-se verificar um esquema de como se relacionam os padrões IEEE aplicados a redes Ethernet.

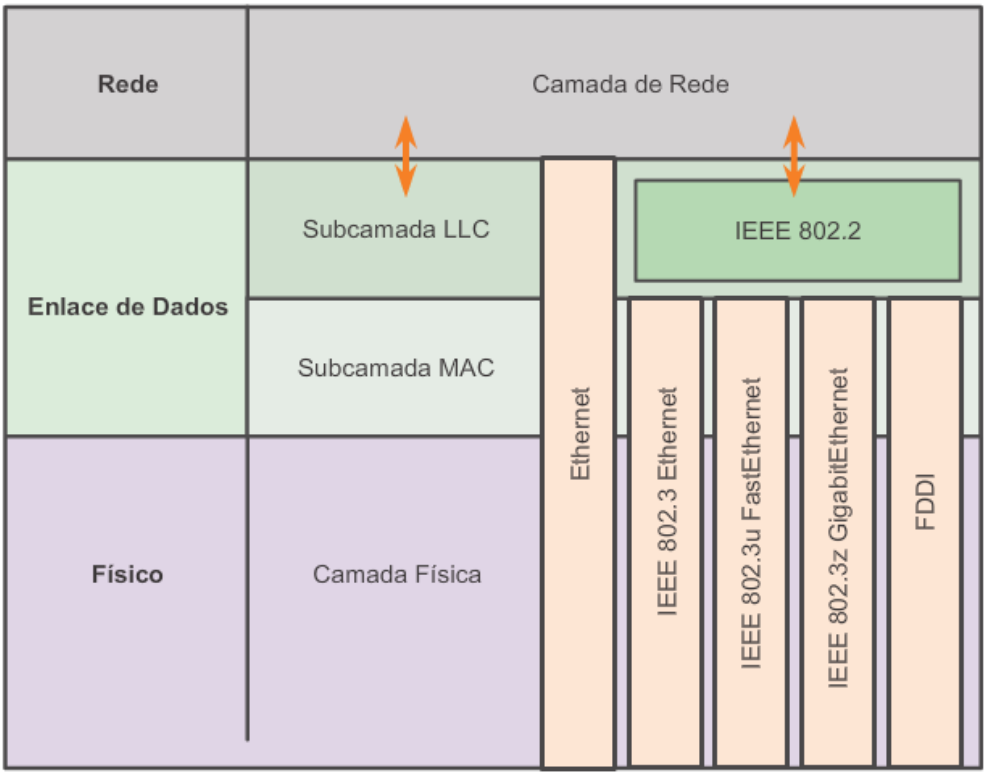


Figura 4- Esquema de inter-relacionamento entre padrões referentes a rede Ethernet.
Fonte: Cisco 5.0

2.2.1 Camada Fisica

Referente a camada física, as redes Ethernet usam uma técnica de acesso ao meio chamada de CSMA/CD (*Carrier Sense Multiple Access with Collision Detect*). Nesta técnica, os dispositivos

monitoram o meio físico de forma a detectar um sinal de transmissão de dados. O dispositivo só inicia a transmissão de dados quando não há sinais de dados no meio físico, indicando que o meio está livre. Se um sinal for detectado, os dispositivos entendem que outro dispositivo já esta utilizando o meio físico para transmissão de dados, assim, os dispositivos que detectaram o sinal aguardam um tempo aleatório para retornarem ao processo de inicio de comunicação pela rede. Esta técnica visa evitar colisões de sinais no meio físico, o que tornaria indecifrável os dados contidos nos sinais elétricos. Mas mesmo assim ainda pode haver colisões quando dois dispositivos iniciam uma comunicação ao mesmo tempo. Neste caso a técnica do CSMA/CD permite que os dispositivos detectem a colisão, interrompam a comunicação e aguardem um tempo aleatório para retomarem a comunicação que tentaram fazer anteriormente (Cisco CCNA 5.0).

Os sinais elétricos que trafegam pelo(s) par(es) de fios dos cabos de uma rede ethernet são codificados através de uma técnica de codificação chamada Manchester. Esta codificação permitiu aos dispositivos receptores determinarem exatamente o inicio e o fim de cada bit, sem fazer referencia a um *clock* externo. Na codificação Manchester, cada período de bits é dividido em dois intervalos iguais. Um bit 1 binário é enviado quando o nível de tensão é definido como alto durante o primeiro intervalo e baixo no segundo intervalo. Um bit 0 (zero) binário é exatamente o oposto (figura 5). Esse esquema garante que cada período de bit terá uma transição na parte intermediária, tornando fácil para o receptor sincronizar-se com o receptor.

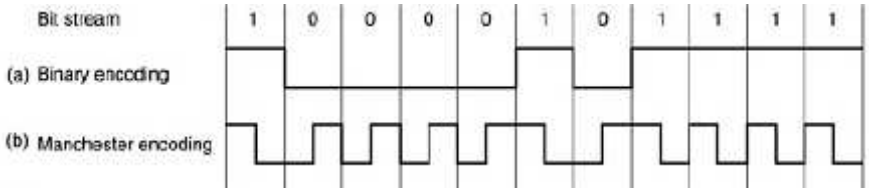


Figura 5- Codificação Manchester

Fonte: Tanenbaum, 2003

Ainda referente aos aspectos da camada física da rede ethernet, é importante observar os conceitos de "*half-duplex*" e "*full-duplex*". A rede Ethernet *half-duplex* utiliza apenas um par de cabos com sinal fluindo em ambas as direções, isto significa que colisões podem ocorrer. Desta forma, em modo *half-duplex*, a rede atinge uma eficiência de no máximo 60%, mas quanto maior a rede menor será a eficiência neste modo. Assim não se pode transmitir a velocidades superiores a 10Mbps. A rede Ethernet *full-duplex* utiliza dois pares de cabos, um para transmissão e outro para recepção de dados. Desta forma não há colisões de dados e a recepção e transmissão podem ocorrer simultaneamente. Neste modo, as velocidades podem alcançar até 100Mbps em ambas direções (Filippetti).

Vale ressaltar que além das normas IEEE (*Institute of Electrical and Eletronics Engineers*) referentes à Ethernet, existem outros órgãos que normatizaram diversos outros componentes utilizados nas redes Ethernet e formas de implementação como por exemplo:

- ISO (*International Organization for Standardtization*):
    - ISO 8877: adotou os conectores RJ (RJ-11 e RJ-45).
    - ISO 11801: padrão de cabeamento de rede semelhante a EIA/TIA 568.
- EIA/TIA (Associação de Indústrias de Telecomunicações/ Associação de Indústrias Eletrônicas):
    - TIA-568-C: Padrões de cabeamento de telecomunicações.
    - TIA-569-B: Padrões de encaminhamento e espaços para telecomunicações em edifícios comerciais.
    - TIA-568-C: Codificação por cores de fibra óptica.
    - TIA-942: Padrão para Infraestrutura de telecomunicações para *data centers*.
- ANSI (Instituto Nacional de Padronização Americano):
    - 568-C: Pinagens RJ-45. Desenvolvido em conjunto com EIA/TIA.

2.2.2 Camada de Enlace de dados

Como pode ser visto na figura 4 (seção 2.2), a camada de enlace de dados é dividida em duas subcamadas: LLC (*Logical Link Control*) e MAC (Controle de Acesso ao Meio).

A subcamada LLC define processos de *software* que fornecem serviços aos protocolos de camada de rede. Conforme a figura 6, ela introduz a informação no quadro que identifica qual protocolo de camada de rede está sendo usado para o quadro. Essas informações permitem que vários protocolos de camada 3, como IPv4 e IPv6, usem a mesma interface e o mesmo meio físico de rede. O LLC é um protocolo padronizado pela norma IEEE 802.2, e, segundo Tanenbaum (2003), tem como objetivo ocultar diferenças entre diversos tipos de rede da série de normas IEEE 802, fornecendo um único formato e uma única interface com a camada de rede.

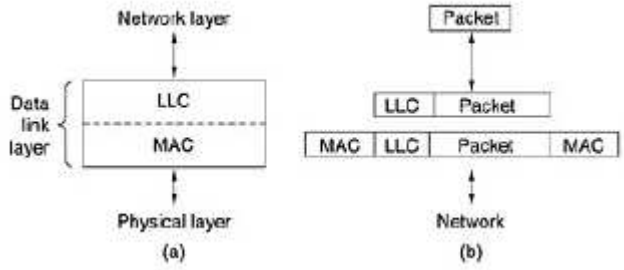


Figura 6- Cabeçalho LLC
Fonte: Tanenbaum, 2003

A subcamada MAC define os processos de acesso ao meio físico realizado pelo *hardware*. Ela fornece o endereçamento do dispositivo na rede Ethernet e delimita os dados de acordo com as exigências do sinal físico e do tipo de protocolo da camada de enlace de dados que esta sendo usado. Desta forma o cabeçalho MAC possui (figura 7):

-Preâmbulo - é uma sequencia de 8 bits na forma de 10101010. O preâmbulo serve para sicronizar o *clock* do transmissor e receptor.

-Endereço de origem e destino – Identificam os endereços dos dispositivos conectados no meio físico, sendo que cada endereço possui 48 bits.

-Tipo – Indica o serviço de camada superior contido no quadro e possui 2 *bytes*.

-Dados ou *payload* – é pacote de camada superior (camada de rede) que deve ser transportado pelo meio físico. Este campo possui de 46 a 1500 *bytes*.

-Sequencia de verificação de quadro (FCS) – um valor usado para verificar se o quadro está danificado.

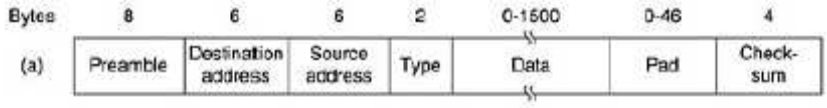


Figura 7- Cabeçalho ethernet

Fonte: Tanenbaum, 2003

Do cabeçalho ethernet é importante destacar alguns detalhes dos campos de endereços. Os endereços MAC, compostos por seis octetos (1 octeto contém 8 bits), normalmente são representados na forma hexadecimal, desta forma são necessários dois algarismos hexadecimais para representar um octeto, por exemplo, 00-07-E9-42-AC-28. Em uma rede ethernet cada dispositivo deve ter seu endereço MAC, e cada endereço deve ser único. Este endereço único e exclusivo de cada dispositivo chamamos de endereço *unicast.*

Dentre os endereços MAC, o endereço de destino FF-FF-FF-FF-FF-FF identifica um pacote *broadcast* (este é um endereço reservado para esta funcionalidade). Um pacote *broadcast* é recebido e processado por todos os dispositivos que estão na mesma rede. Alguns protocolos utilizam esta funcionalidade para executar seus serviços.

Existem também os endereços chamados *multicast*, que permitem que um dispositivo de origem envie um pacote a um grupo de dispositivos. Este endereço aparecerá no cabeçalho ethernet no campo endereço de destino. O endereço *multicast* é um valor especial que começa com 01-00-5E.

2.3 SWITCHES

Switches são dispositivos de rede que têm a função de encaminhar pacotes ethernet baseado nas informações do cabeçalho ethernet do pacote, por isso o *switch* é classificado como um dispositivo de rede de camada 2, isto também significa dizer que o *switch* não precisa processar endereços de camada 3 (como, por exemplo, IP).

Para o seu funcionamento o *switch* faz uma tabela MAC que relaciona suas portas à endereços MAC *unicast* dos diversos dispositivos que estão ligados à uma de suas portas (interfaces). Quando um dispositivo inicia uma transmissão e uma interface do switch recebe um *frame* o *switch* armazena o endereço de *hardware* (MAC *address*) do dispositivo transmissor em sua tabela MAC, registrando a interface à qual esse dispositivo está conectado. Em um primeiro momento, o switch não tem outra opção a não ser “inundar” a rede como esse *frame*, uma vez que ele não possui em sua tabela MAC o registro da localização do dispositivo destinatário. Este tipo de mensagem é um exemplo de uma mensagem *broadcast*. Se um determinado dispositivo responder a essa mensagem de *broadcast*, o *switch* irá capturar o endereço de *hardware* desse dispositivo e registrá-lo em sua tabela MAC, associando o endereço MAC desse dispositivo à porta que recebeu o *frame*. Neste exemplo o *switch* teria dois endereços em sua tabela MAC, podendo assim estabelecer uma conexão ponto a ponto entre os dois dispositivos. Isto significa também que os *frames* pertencentes a essa transmissão serão encaminhados apenas aos dois dispositivos participantes. Nenhuma outra porta de *switch* irá receber os *frames*, a não ser as duas portas mapeadas. No caso dos dispositivos não se comunicarem com o *switch* novamente por um determinado período de tempo, este irá apagar os endereços de sua tabela MAC, mantendo-a assim a mais atualizada possível (Filippetti, 2009).

O modo de funcionamento dos switches os tornam capazes de fornecer a cada uma de suas interfaces a velocidade nominal da interface (seja 10Mbps, 100Mbps ou 1Gbps), já que os switches

eliminaram as colisões de rede. O processo de encaminhamento dos *switches* também é considerado rápido, pois trabalha apenas com o cabeçalho da camada 2, sem necessitar processar os cabeçalhos de camadas superiores, como é o caso dos roteadores, por exemplo, que usam endereços de camada 3 e 4 para executar seus processos.

2.4 SPANNING TREE PROTOCOL

Alguns casos em que há a necessidade de aumentar a confiabilidade e disponibilidade de redes Ethernet, existe a possibilidade de criar caminhos alternativos para encaminhamento dos dados de rede, bem como o estabelecimentos de enlaces redundantes com uma rede local. A figura 8 exemplifica uma topologia de rede com caminho alternativo de transmissão de dados. Entretanto com uma rede local interligada com *switches*, o estabelecimento de caminhos alternativos e redundâncias de *enlaces* podem provocar efeitos indesejados como lentidão da rede e até mesmo indisponibilidade total.

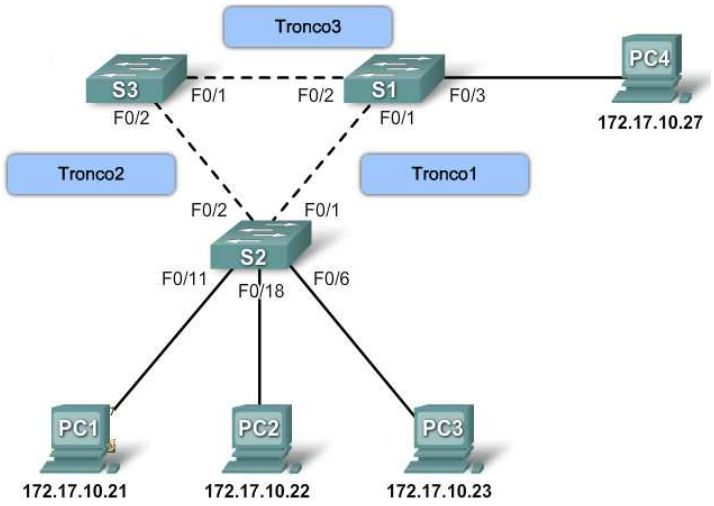


Figura 8- Topologia de rede com redundancia de caminhos

Fonte: Cisco, CCNA 5.0

Como foi visto anteriormente, quando um dispositivo encaminha uma mensagem broadcast na rede, o *switch* encaminha esta mensagem para todas as suas interfaces conectadas na rede (exceto a interface por onde a mensagem chegou ao *switch*). Se o dispositivo que estiver conectado a uma interface de *switch* for outro *switch*, também irá encaminhar a mensagem *broadcast* para todas as outras

interfaces. Desta forma, numa topologia como a apresentada na figura 8, a mensagem *broadcast* ficaria circulando entre os *switches* indefinidamente. Este fenômeno é chamado de *loop*. Quando outro *broadcast* for enviado, este também ficaria circulando entre os *switches*, ou seja, todos os *broadcasts* enviados a estes *switches* ficariam “aprisionados” no *loop*, isto pode causar o fenômeno conhecido como “*broadcast storm*”, e isto causa sobrecarga de processamento em todos os *switches* envolvidos no *loop*, reduzindo a velocidade e desempenho do *switch*, além disso todos os dispositivos da rede receberão continuamente as mensagens *broadcast*, ou seja perderão capacidade de processamento e largura de banda de rede.

Para permitir que uma rede trabalhe com enlaces redundantes, é necessário que o *switch* desabilite um dos enlaces redundantes e utilize somente um enlace para transmissão de dados, e na ocorrência de uma falha deste enlace, ele deve ser capaz de encaminhar os dados pelo outro enlace que estava desabilitado. Para isto foi criado o protocolo *Spanning Tree* (STP), originalmente pela extinta DEC (*Digital Equipament Corporation*). Posteriormente o IEEE homologou sua própria versão do protocolo, denominada IEEE 802.1d.

Portanto a função principal do STP é monitorar a rede constantemente identificando os enlaces ativos e certificando que *loops* de rede não ocorram, de forma a fazer com que haja apenas um caminho lógico para os dados fluírem pela rede.

O algoritmo do STP faz com que os *switches* troquem pacotes conhecidos como BPDU (*Bridge Protocol Data Unit*). A primeira função das trocas de BPDU’s entre os *switches* é a eleição de *root-bridge* (switch-raiz). Esta eleição ocorre através de uma variável conhecida como BID (*Bridge* ID), o switch com o numero BID mais baixo torna-se automaticamente o *root-bridge*. Este switch será a referência para o STP estabelecer o caminho lógico na rede. Após a determinação do *switch* raiz, o STP calcula o melhor caminho para o *switch* raiz, enquanto o cálculo é feito, todas as portas ficam no estado de bloqueio, impedindo a transmissão de dados. O algoritmo do STP utiliza os valores de custo de caminho e de porta para determinar

quais interfaces permanecerão bloqueadas. O custo de caminho é calculado utilizando os valores de custo de porta (figura 9) associado com a velocidade de cada porta de switch por um determinado caminho. Se houver dois caminhos para o *switch* alcançar o *switch* raiz ele escolherá o caminho de menor custo.

Velocidade de link	Custo (Especificação de IEEE Revisada)
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

Figura 9- custo de porta segundo a IEEE

Fonte: Cisco CCNS 4.0

Quando o STP determinar os caminhos disponíveis, ele irá configurar as interfaces dos *switches* de alguma dessas formas:

- Porta Raiz – As portas de *switch* mais próximas do *switch* raiz;
- Porta Designada – Todas as portas não-raiz que ainda podem encaminhar o trafego na rede;
- Porta Não-designada – Todas as portas cofiguradas em um estado de bloqueio para impedir *loops*.

O STP é determinado logo após a inicialização de um switch. Se uma porta migrar do estado de bloqueio diretamente para o estado de encaminhamento, a interface poderia criar um loop temporário até que o STP atualizasse o switch de todas as informações da rede. Por esta razão, o STP introduz cinco estados de porta:

- Bloqueio – A porta é uma porta não-designada e não participa do encaminhamento de quadros. Ela recebe quadros BPDU para determinar o local e a ID de raiz do *root bridge* bem como o estado final de cada porta;
- Escuta – Neste momento a interface não só recebe quadros de BPDU como também transmite seus próprios quadros

BPDU e informa os switches adjacentes de que a porta do switch esta se preparando para participar da topologia ativa;

- Aprendizagem – A porta começa a preencher sua tabela MAC;
- Encaminhamento – A porta é considerada parte da topologia ativa e encaminha dados;
- Desabilitado – A porta não participa do STP e não encaminha quadros. Isto acontece quando a porta é desabilitada administrativamente.

Se houver uma mudança de topologia após a convergência da rede o STP irá detectar esta mudança através da mudança do estado de uma porta que torna-se inativa ou quando uma interface do *switch* faz a transição para o estado de encaminhamento e houver uma interface designada. Quando uma mudança é detectada, o *switch* notifica o *switch* raiz do STP. O *switch* raiz por sua vez transmite as informações em *broadcast* por toda a rede.

Como foi dito o STP necessita de um tempo de convergência para permitir o encaminhamento de dados, este tempo é devido a alguns temporizadores que o STP utiliza para seu funcionamento .Em 1982 foi introduzido RSTP (*Rapid Spanning Tree Protocol*). O protocolo foi normatizado pela IEEE 802.1w. A maioria dos parâmetros permaneceu inalterada. O RSTP adianta o novo calculo do STP quando a topologia de rede de camada 2 é alterada. O RSTP pode obter uma convergência muito mais rápida em uma rede corretamente configurada, às vezes em menos de cem milésimos de segundos. O RSTP redefine o tipo de portas e seus estados. Se uma porta for configurada como uma porta alternativa ou de backup, ela pode mudar imediatamente para um estado de encaminhamento sem esperar que rede seja convergida (Cisco CCNA 4.0).

2.5 VLAN

Como foi visto anteriormente, o *switch* comuta pacotes através de endereços MAC, assim o fluxo de dados através de um *switch*

poderia ocorrer entre qualquer dispositivo ligado à sua rede; e *frames* com endereço de *broadcast* ou *multicast* que chegam ao switch são propagados para todas as suas portas. Muitas vezes estes efeitos não são desejados. Muitas vezes é necessário que o tráfego de dados entre alguns dispositivos da rede seja isolado de outros tipos de tráfego, mas no mesmo *switch*. Também muitas vezes é necessário limitar a propagação de *frames broadcasts* para que não haja sobrecarga na rede local.

A solução para estes casos são as VLANs (*Virtual Local Area Network*). Como o nome já sugere, as VLANs são redes locais virtuais, implementadas através de uma única infraestrutura física de uma rede local. Ou seja, um *switch* que suporta VLANs pode abrigar diversas redes locais isoladas dentro de si. Desta forma cada interface do *switch* faz parte de uma VLAN previamente criada no *switch*. As portas agrupadas na mesma VLAN podem trafegar dados entre si, mas não trafegam dados para outras portas agrupadas em VLAN diferente.

Neste contexto, iremos nos deparar com interfaces do switch na configuração *trunk* (tronco). A porta *trunk* é usada para interligar *switches* ou interligar *switch* a um roteador. Ela pertence a todas as VLANs, assim, pode encaminhar dados a todas as VLANs e todas as VLANs podem encaminhar dados por ela, para assim os dados chegarem a outro switch (também na porta *trunk*) ou a um roteador. Mas nesta situação existe um problema: como um *switch* saberá a que VLAN pertence um determinado quadro que esta chegando a sua interface?

O IEEE definiu um formato de quadro estendido através da norma 802.1Q. Este quadro consiste no quadro padrão ethernet com um rótulo (*tag*) de VLAN de quatro *bytes* no cabeçalho. Este rótulo identifica o numero da VLAN no quadro ethernet. O rótulo é adicionado ao quadro pelo *switch* no lado de envio do tronco de VLAN, analisado, e removido pelo *switch* no lado de recebimento do tronco (Kurose, 2010). O rótulo é composto pelo campo ID de protocolo de VLAN, que sempre tem o valor 0x8100 (2 *bytes*). O segundo campo de 2 *bytes* contém três subcampos. O principal é o identificador de VLAN, que

ocupa os 12 *bits* menos significativos. O campo de três *bits* chamado Prioridade torna possível distinguir o tráfego de tempo real permanente do tráfego real provisório e do tráfego não relacionado ao tempo, a fim de fornecer melhor qualidade de serviço em redes ethernet e não tem nenhuma relação com VLANs. Há também o campo CFI (*Canonical Format Indicator*), que também não tem relação com VLANs e está fora do escopo deste trabalho. Na figura 10 é ilustrado como o rótulo da IEEE 802.1Q foi inserido no cabeçalho ethernet da norma 802.3.

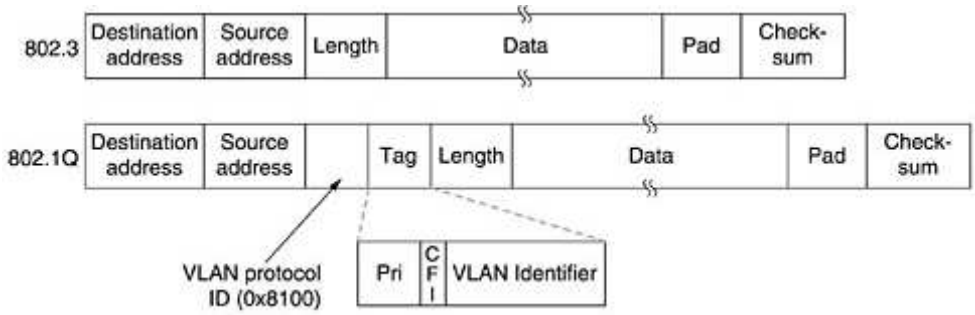


Figura 10- Os formatos de quadros ethernet 802.3 e 802.1Q

Fonte: Tanembaum, 2003

2.6 NORMA IEC-61850

A norma do *International Electrotechinacal Commission* (IEC) 61850 foi elaborada com a função normatizar todos os processos envolvidos em um sistema de redes de comunicação de subestações elétricas.

Subestações são componentes chaves de um sistema de energia elétrica, pois facilitam a transmissão e distribuição elétrica de forma eficiente. Elas desempenham uma função vital ao sistema monitorando e controlando o fluxo de energia e provê interconexões entre geradores, transmissores, distribuidores e consumidores finais. Desta forma, sistemas de automação de subestação permitem que o controle e monitoração em tempo real seja possível além de melhorar a disponibilidade, eficiência, confiabilidade e segurança ao sistema elétrico.

Os sistemas de automação de subestações sempre acompanharam o desenvolvimento da eletrônica. Por muito tempo os

relés eletromecânicos (dispositivo de proteção da rede elétrica) e medidores analógicos dominaram a automação de subestações. Com a evolução da eletrônica os relés e medidores passaram a ser eletrônicos e, finalmente, de serem capaz de interagir com outros dispositivos através de algum protocolo de comunicação. Na década de 70 foi criado o protocolo serial Modbus, onde já era possível a troca de diversas informações entre dispositivos através de um rede de comunicação, mas possuía muitas limitações relacionado à velocidade, o fato de não permitir mensagens espontâneas para sinalizar eventos, e também pelo fato de permitir estampa de tempo nos quadros. Após o Modbus, ainda foram criados outros protocolos como o Profibus e o DNP3, que também se utilizavam de protocolos de comunicação serial (como RS232 e RS485), mas que, mesmo melhorando alguns aspectos da comunicação ainda tinham suas limitações para serem aplicados em todas as interfaces entre reles de uma subestação. Portanto estes protocolos seriais tiveram uma grande aplicação em subestações, mas apenas na função de transmitir sinalizações para o sistema de automação e para transmitir comando do sistema de automação para os equipamentos. Funções de proteção, intertravamento e leitura de variáveis para proteção continuaram a serem feitos através dos contatos físicos dos reles pelo envio de sinal elétrico a outro rele (de forma “fiada”).

Ainda com o avanço da eletrônica os reles passaram a ter maior capacidade de processamento, por isso passaram a serem capazes de concentrar várias medições de variáveis como tensão e corrente elétrica, com amostragens cada vez menores. Com estas informações os reles passaram a efetuar cálculos para informar dados como potencia ativa (Watts), potencia reativa (Var), oscilografias, etc. Desta forma o rele passou a ser chamado de IEDs (*Intelligent Eletronic Device*). A figura 11 ilustra exemplos das tecnologias dos dispositivos de proteção elétrica. Consequentemente, a chave de um bom sistema de comunicação seria usar a capacidade dos IEDs para publicarem suas variáveis em uma rede de comunicação tanto da perspectiva de visualização de dados quanto para uso em serviços de intertravamento

e proteção. A figura 12 mostra um esquema de como a arquitetura dos sistemas de automação de subestações tem se modificado com a evolução tecnológica, onde os sinais ditos “fiados” dão lugar a redes de comunicação capazes de transferir enormes quantidades de variáveis.

Figura 11- Evolução dos dispositivos de proteção elétrica.
Fonte: Schweitzer Engineering Laboratories, 2010

Segundo Mackiewicz, a rede de comunicação deveria atender aos seguintes requerimentos:

- Alta velocidade na comunicação IED-IED;
- Ser parte da rede de serviços (utilitários) da empresa;
- Alta disponibilidade;
- Entrega de pacotes garantida;
- Baseada em normas;
- Interoperabilidade entre diversos fabricantes;
- Suporte para tráfego de amostras de tensão e corrente;
- Suporte a transferências de arquivos;

- Ser de fácil configuração;
- Suportar segurança de rede.

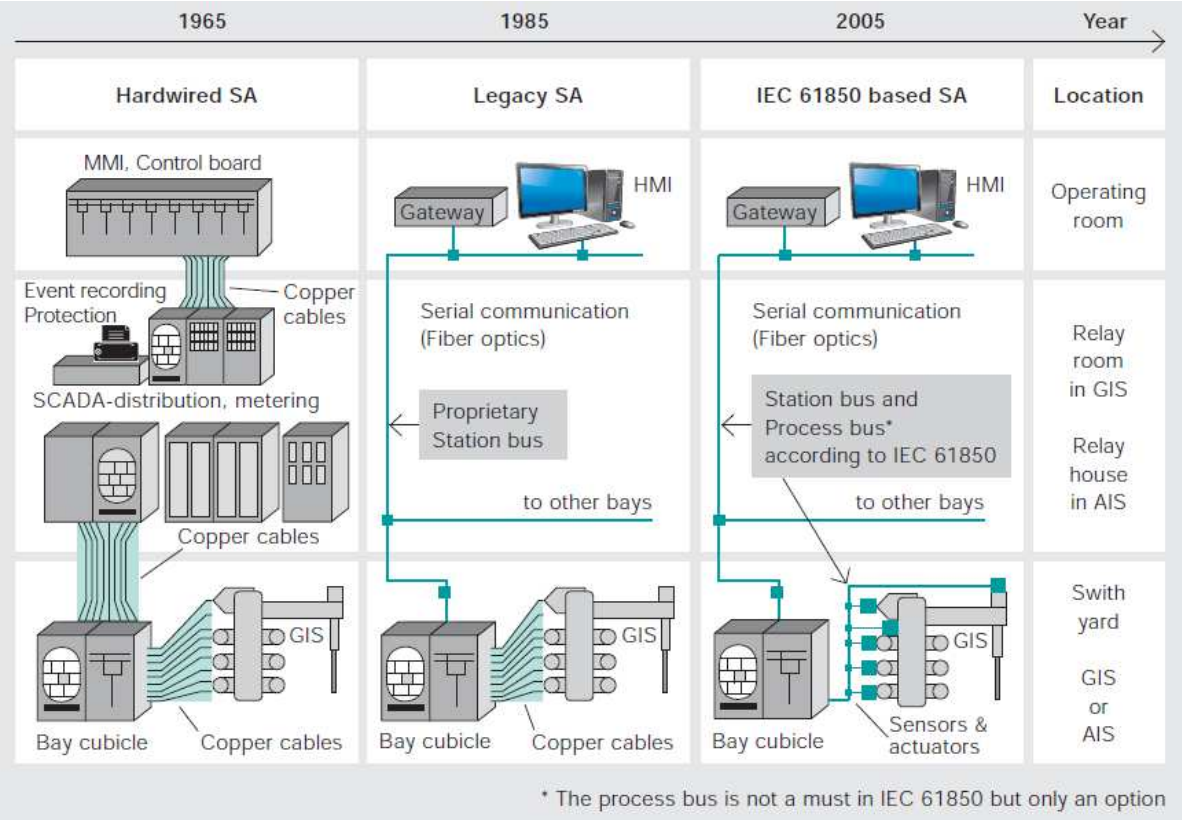


Figura 12- Desenvolvimento da arquitetura de Automação de Subestações.

Fonte: ABB, 2010

Com essas especificações, iniciou-se o trabalho de desenvolvimento da rede da "próxima geração". A arquitetura da rede de comunicação foi resultado de um trabalho iniciado pelo EPRI *(Electric Power Reserch Institute*) e que resultou na elaboração do UCA (Utility *Communication Architecture*) em 1988, que é um conjunto de regras para comunicação entre aplicações. Este trabalho gerou um perfil de protocolos recomendados para as diversas camadas do modelo OSI. Além disso, resultou em definições de modelagem de dados e serviços abstratos. Os conceitos e fundamentos deste trabalho (UCA) se tornaram a base para um outro trabalho feito pelo Comitê Técnico numero 57 (TC57) da IEC, o qual resultou na norma internacional IEC-61850 – *Communication Network and Systems in*

Substations. Desta forma foi introduzida a rede ethernet como forma de transferência de dados no sistema de automação de subestações.

A figura 13 apresenta a estrutura da norma IEC-61850 composta por dez capítulos, onde ela aborda vários aspectos da comunicação em uma subestação.

Partes	Descrição
1	Introdução e visão geral
2	Glossário
3	Requisitos gerais
4	Gerenciamento de sistema e projeto
5	Requisitos de comunicação para modelos de funções e dispositivos
6	Linguagem de descrição de configuração para comunicação em Subestações relacionada a IEDs
7	Estrutura básica de comunicação para Subestação e equipamentos de alimentadores (Subdivido em 4 partes)
8	Mapa de serviços de comunicação específicos (MMS – Manufacturing Message Specification)
9	Mapa de serviços de comunicação específicos (Valores amostrados)
10	Testes de conformidade

Figura 13- Estrutura da norma IEC-61850

Fonte: Petenel, 2012

Os capítulos três, quatro e cinco da norma identificam regras para funções gerais e especificas que serão usadas na comunicação. Estas regras são usadas para ajudar na definição de serviços e modelagem de dados, protocolos de aplicação e lança a base para os protocolos de camada de transporte, rede, enlace e físico. A norma, no seu capitulo sete, construiu uma modelagem abstrata dos dados e serviços que independe de protocolos de comunicação. Também descreveu e definiu o funcionamento do protocolo GOOSE (*Generic Object Oriented Substation Events*). Com a definição de dados e serviços abstratos, no capitulo 8 ela insere estas definições dentro de um protocolo existente, o MMS (*Manufacturing Messaging*

Specification). Na figura 14 vemos uma representação da modelagem de dados definido pela norma, na configuração seria representado por IEDxLDxXCBR1PosStVal, referente a sinalização de um disjuntor (XCBR), por exemplo. Na figura 15 vemos a uma representação ilustrando aplicação dos capítulos da norma, da modelagem de um disjuntor virtual até a interação com disjuntor real.

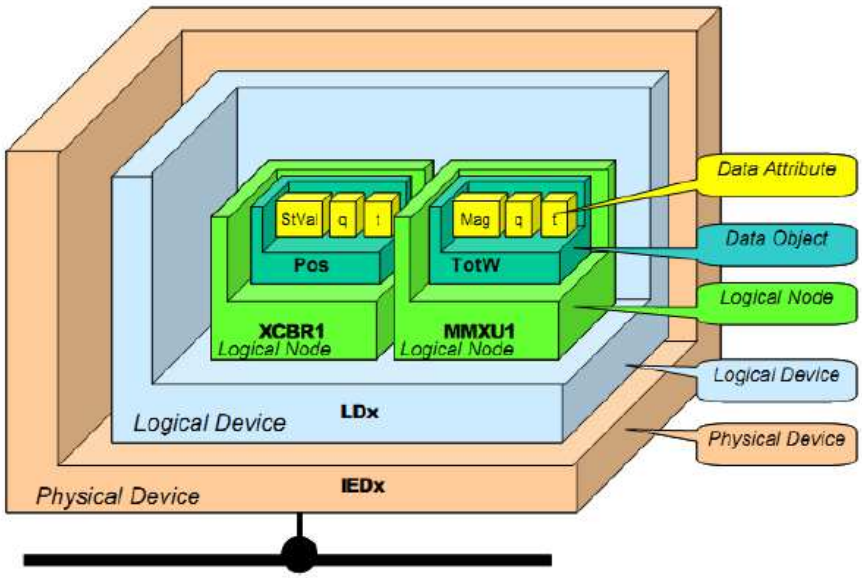


Figura 14- Modelagem de dados pela IEC-61850.

Fonte: IEC 61850-1 TR Ed2, 2012

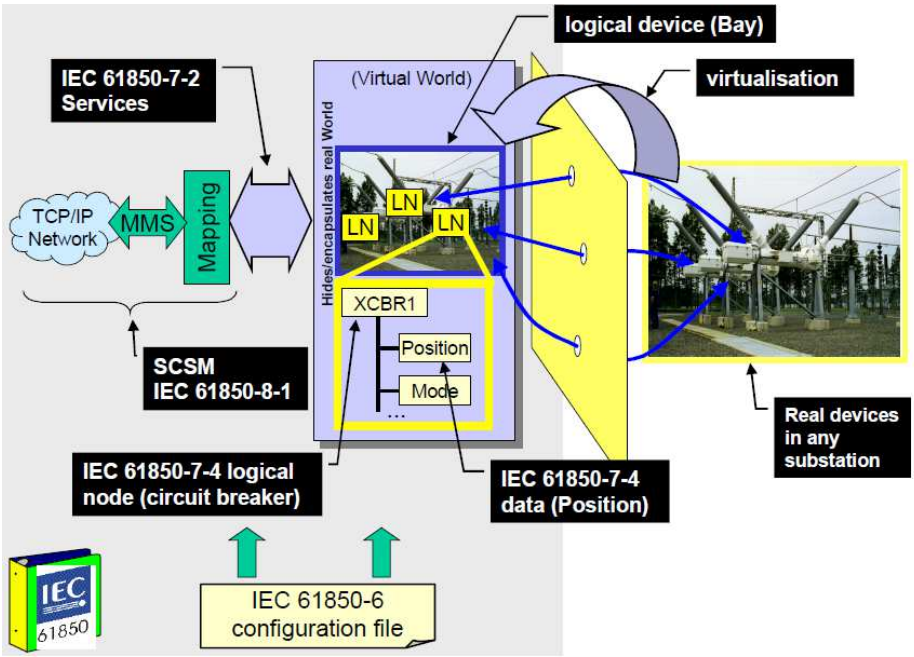


Figura 15- Modelo conceitual da aplicação da norma IEC-61850.

Fonte: IEC 61850-7-1 Ed1, 2003

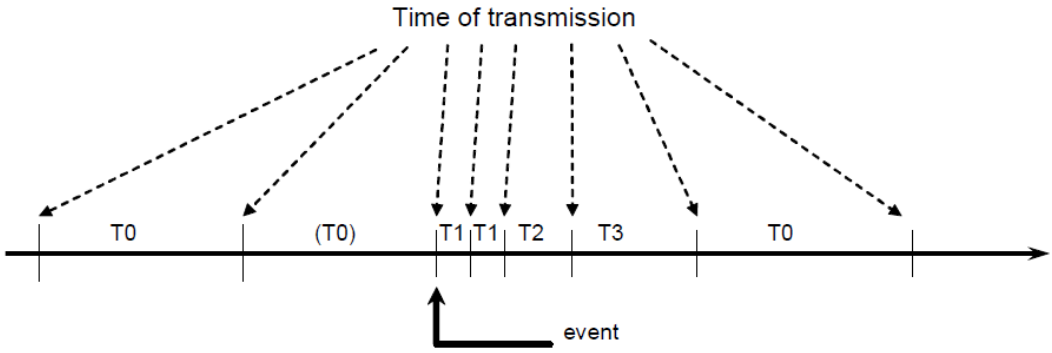
Da perspectiva do sistema, haveria uma quantidade significativa de configurações a serem feitas e muitas variáveis a serem consideradas para que um sistema de comunicação, definido nesta norma, funcionasse. Diante de tal dificuldade, a norma definiu no seu capitulo seis, uma linguagem de configuração chamada *Substation Configuration Language* (SCL) baseado na linguagem XML. Desta forma, toda a comunicação da subestação pode ser definida através de um arquivo em formato de XML, e cada IED da rede seria parte deste arquivo geral de comunicação. A intenção da criação destes arquivos de configuração de comunicação, segundo Mackiewicz, é diminuir a falha humana diante de tantas variáveis a serem manipuladas.

Finalmente no seu capitulo dez a norma define a metodologia de teste para determinar a conformidade dos protocolos implementados nos equipamentos que irão operar na rede da subestação.

2.7 GOOSE

O protocolo GOOSE tem a função de prover um modo rápido e confiável a distribuição de dados em uma rede Ethernet. Também permite a entrega simultânea de um mesmo pacote de informações a mais de um dispositivo físico através do uso de serviços *multicast*.. Resumidamente a mensagem GOOSE, do ponto de vista da rede, é endereçada por endereços MAC *multicast* de destino, portanto é um pacote camada dois do modelo OSI. Possui um cabeçalho GOOSE para controle dos serviços e o campo chamado GOOSEData, que contem as informações referentes ao processo (sinalização de disjuntores e proteções, por exemplo). Como foi dito, as mensagens são endereçadas para um endereço *multicast*, esta mensagem será recebida por todos os IED’s instalados na rede, mas apenas os IED’s “assinantes” desta mensagem (programados para receber mensagem com aquele endereço *multicast*) irão processar a informação, enquanto os demais descartarão. A figura 16 ilustra os tempos de transmissão

da mensagem. Enquanto não houver nenhuma modificação das variáveis contidas em GOOSEData a transmissão será feita em T0, estas transmissões servem para que os IED's assinantes da mensagem assumam que a associação entre estes e o IED publicador da mensagem está íntegra. Na ocorrência de um evento, que cause a mudança de uma variável contida em GOOSEData, a transmissão do pacote será imediata. Para garantir a entrega dos pacotes ao assinante haverão retransmissões do mesmo pacote inicialmente no tempo T1, e posteriormente em tempos maiores (T2 e T3) até que retorne a condição de estabilidade T0.



T0	retransmission in stable conditions (no event for a long time).
(T0)	retransmission in stable conditions may be shortened by an event.
T1	shortest retransmission time after the event.
T2, T3	retransmission times until achieving the stable conditions time.

Figura 16- Tempos de transmissão de mensagens GOOSE.

Fonte: IEC 61850-8-1, 2004

Segundo a norma IEC 61850-8-1 (2004) o cabeçalho do pacote GOOSE é formado pelos seguintes campos:

- Dataset: Contêm o nome Objeto de Referencia que esta publicando o pacote;
- AppID (*Application Identifier*): Contêm um identificador do dispositivo gerador do pacote;
- GocBRef (GOOSE *control block reference*): Contêm o nome de referencia do pacote;
- T (*time stamp*): Contêm o tempo no qual o capo STNum foi incrementado;

- StNum (*state number*): Contêm o contador incremental de cada mudança de variável do campo GOOSEData (contador de eventos);
- Test: quando em nivel lógico 1, indica que os valores da mensagem não devem ser usados para propósitos de processo;
- ConfRev (*configuration revision*): Deve conter o numero de vezes que a configuração do Data-set foi alterada;
- NdsCom (*Needs Commissionong*): Contêm o parâmetro NdsCom configurado no IED (nível lógico 1 ou 0);
- GOOSEData [1...n]: Informações configuradas no IED para serem transmitidas;
- *Value*: Numero de variáveis contidos em GOOSEData.

Portanto, pelas características da mensagem GOOSE, esta é usada para mensagens de alta prioridade dentro da rede, para transmitir informações vitais para o correto funcionamento do processo. Além das configurações do pacote GOOSE, os IED's possuem configurações para compor o cabeçalho 802.1Q, desta forma a mensagem pode ser priorizada em uma rede com excesso de mensagens. Do ponto de vista da topologia da rede, estas são informações trocadas horizontalmente, entre IED's.

2.8 MMS

MMS é um padrão internacional *(International Organization for Standardization* – ISO9506) concebido para dar suporte à troca de dados em tempo real e proporcionar a supervisão e controle de informações entre dispositivos de rede e aplicações de computadores. Este protocolo provê um sistema genérico de mensagens para comunicação entre diferentes dispositivos industriais. O MMS apenas especifica a comunicação entre um cliente e um servidor e não o funcionamento interno das entidades. Com esta estratégia, o MMS permite total flexibilidade na sua implementação (Nguyen, 2013). Segundo Pham (2013), o padrão define que:

- Objetos padronizados devem existir em todo dispositivo, nos quais operações como leitura, escrita, sinalização de eventos etc. podem ser executados. O padrão define a existência de um objeto principal chamado de *Virtual Manufacturing Device* (VMD) no qual todos outros objetos do dispositivo como Variáveis, Domínios, Arquivos, etc. estão englobados. (A norma define uma variedade de objetos, entre eles, os citados anteriormente);
- Define o padrão para troca de mensagens entre cliente e servidor para o controle e monitoração dos objetos citados anteriormente;
- Define regras de codificação para mapeamento das mensagens, para que assim o pacote seja formado pelos respectivos bytes e seja finalmente transmitido.

O protocolo MMS funciona sobre a pilha de camadas OSI descrita na figura 17.

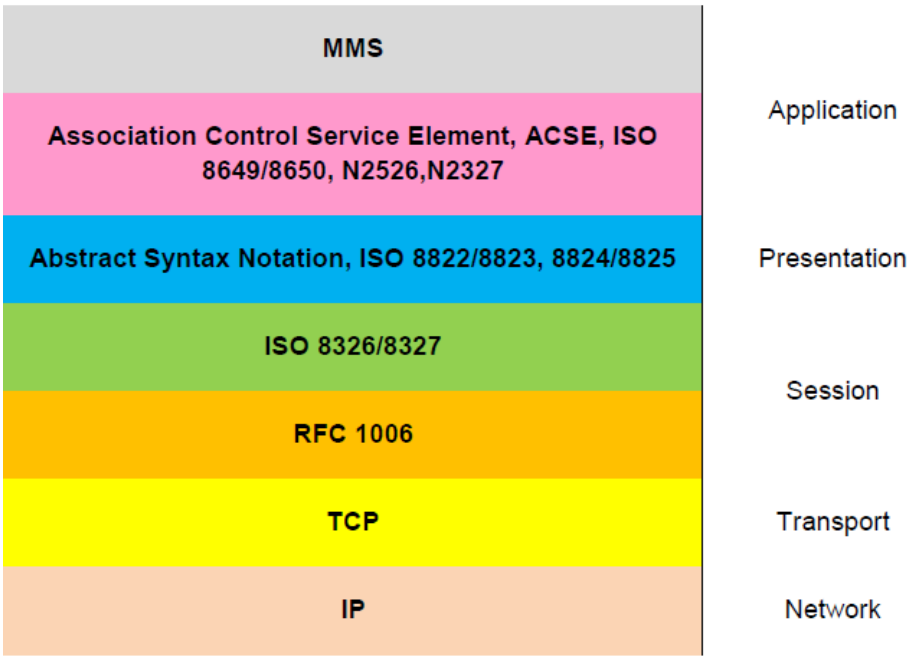


Figura 17- Pilha de camadas de comunicação OSI para MMS.

FONTE: Nguyen , 2013

Segundo Nguyen (2013), uma razão para a norma IEC 61850 definir o MMS é que este pode suportar modelos de dados complexos

além de suportar os serviços definidos pela norma IEC. Teoricamente, modelos de dados e serviços poderiam ser implementados em qualquer protocolo. Entretanto seria muito difícil e pesada a tarefa de tentar mapear objetos e serviços da IEC 61850 em protocolos que suportam apenas leitura, escrita e serviço de "*report*" para variáveis simples contidas em registradores e acessadas por um endereço numérico apenas.

Em resumo, MMS é um protocolo que funciona com o mecanismo cliente-servidor (ilustrado na figura 18), suporta serviço com necessidade de confirmação e sem necessidade de confirmação. Devido a suas características, na automação de subestações é aplicado na comunicação entre IED e supervisório (aplicação em um computador), ou seja do ponto de vista da topologia de rede é uma comunicação vertical. Esta comunicação é utilizada para transmitir variáveis de monitoração dos IED's para o supervisório e para transmitir comando do supervisório para os IED's, desta forma os tempos envolvidos para a troca destas mensagens não são críticos para o funcionamento do processo da subestação, em comparação com o protocolo GOOSE.

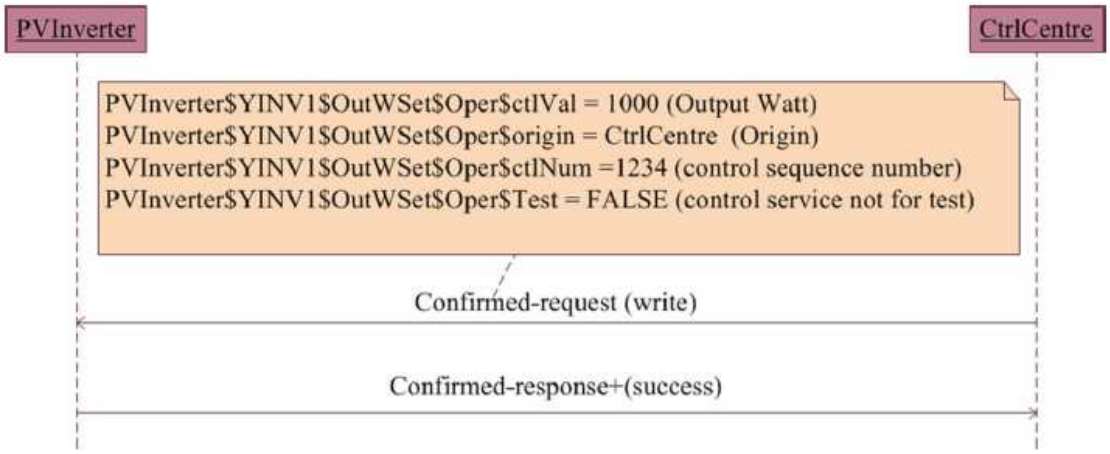


Figura 18-Exemplo da troca de mensagens (Confirmed request) MMS entre Cliente (CtrlCentre) e servidor (PVInverter).

Fonte: Nguyen, 2013

3. ESTUDO DE CASO

Nesta seção será descrito o trabalho realizado para coleta de dados e análise dos dados das redes de comunicação das subestações de uma planta industrial.

3.1 TOPOLOGIA FÍSICA

A topologia física da rede de comunicação Ethernet na qual este trabalho foi baseado, será representada em duas partes.

A primeira parte, referente a figura 19, é composta primeiramente pelos servidores de conectividade. Esses servidores têm a função ler as variáveis dos IED's e transmitir comandos aos IED's através do protocolo MMS. Alguns destes servidores ainda possuem a função de monitorar os equipamentos de rede através do protocolo SNMP (*Simple Network Management Protocol*). São chamados servidores de conectividade por propiciarem ao supervisório (que utiliza serviços OPC) se conectarem com os IED's. O servidor de conectividade é conectado a um *Backbone* de *switches*. A instalação dos *switches* de *backbone* foi feita em três locais estratégicos da planta industrial, propiciando fácil interconexão entre a subestação e o *backbone*, escalabilidade para futuras ampliações e redundância de caminhos para o tráfego da rede.

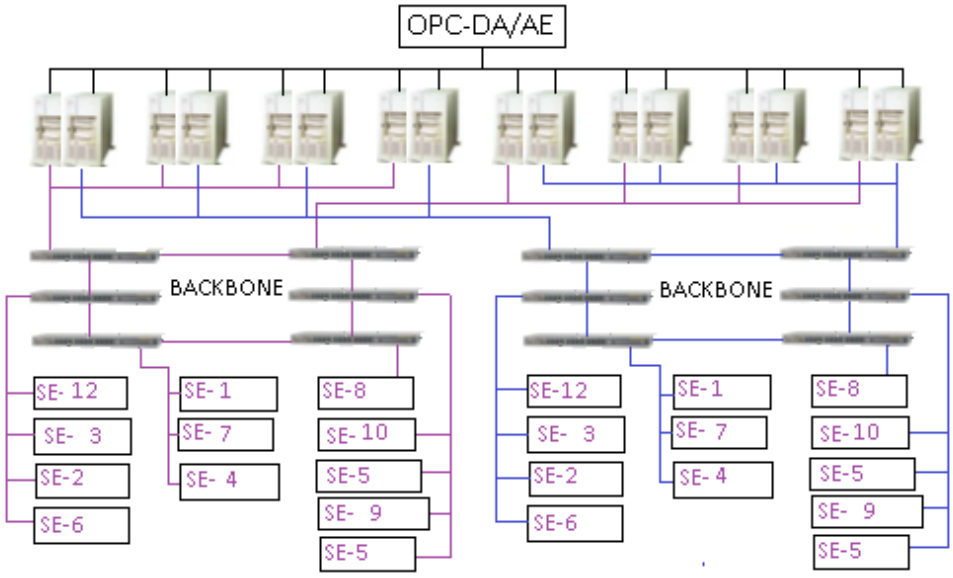


Figura 19: Topologia da rede: Backbone

Fonte: O Autor

Como é possível observar na figura 19, a rede foi concebida de maneira totalmente redundante. Todos os servidores, *switches* e cabos de fibra ótica possuem redundância, desta forma a conexão com as subestações também é redundante. Portanto pode-se perceber que esta é uma rede concebida para ser confiável (ter alta disponibilidade). Como foi dito anteriormente, alguns servidores tem a função de monitorar os equipamentos de rede tais como *switches* e servidores, quando um destes equipamentos falha, é gerado um alarme no supervisório que terá de ser reconhecido e tratado pela equipe de manutenção, que finalmente restabelecerá o equipamento, conferindo à rede sua total confiabilidade.

A segunda parte da rede, referente a figura 20, representa uma das subestações que estão conectadas ao *backbone*.

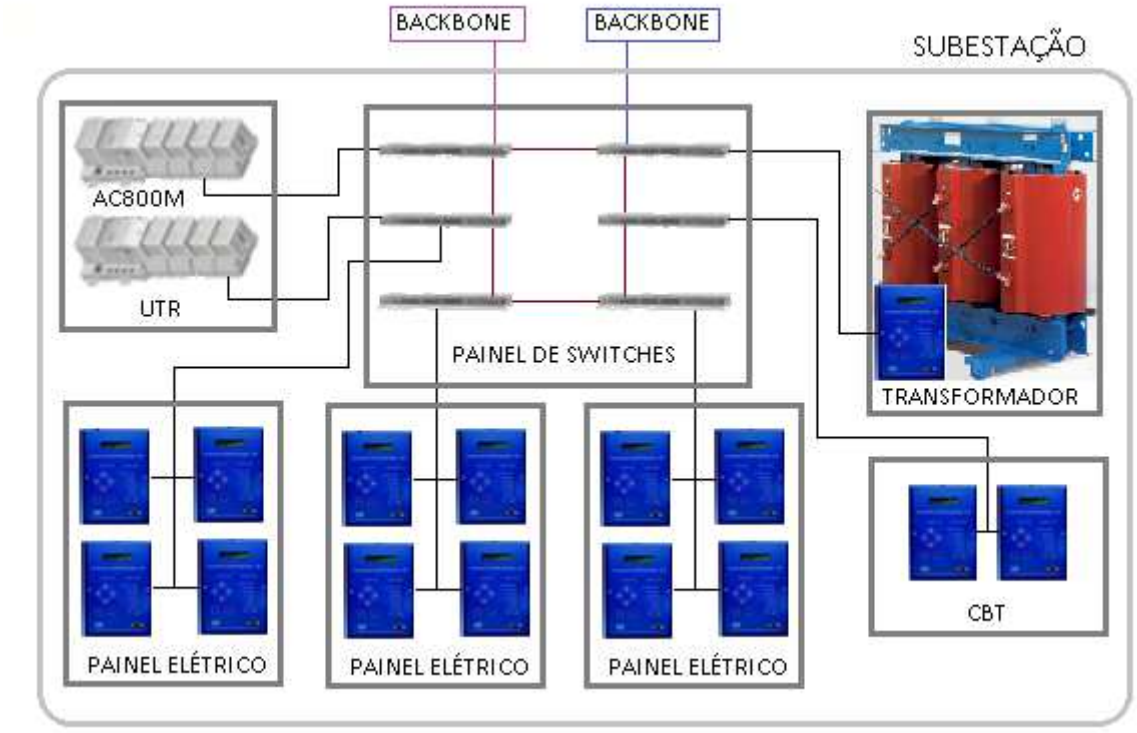


Figura 20: Topologia da rede: Subestação

Fonte: O Autor

É possível observar que há duas conexões da subestação com o *backbone*, sendo que cada conexão é feita através de um *switch* diferente para conferir confiabilidade à rede. Há o painel de *switches*, que possui uma quantidade variável de *switches* conforme o tamanho

da subestação, sendo que em todos os casos os *switches* são ligados em anel (exceto no caso de haver apenas dois *switches* no painel). Este painel fornece conectividade a todos os IED's da rede (cada IED é conectado diretamente à porta de um *switch*). Cada IED possui uma função na rede elétrica, seja controlar um disjuntor (como os IED's dos painéis elétricos) ou apenas ler sinais e transmitir estes sinais para outros IED's que irão usar estas variáveis (como os IED's instalados em transformadores). Ainda na figura 20 é possível observar uma representação da UTR (Unidade Terminal Remota). Esse é um painel onde está o CLP (controlador lógico programável) da subestação, que entre outras funções, também pode comandar ler variáveis e transmitir comandos aos IED's. Uma de suas funções nas subestações é transmitir o comando de descarte elétrico aos IED's, este comando será melhor explicado posteriormente.

3.2 TOPOLOGIA LÓGICA

A rede retratada através das figuras 19 e 20 possui necessita de algumas configurações para o bom desempenho da rede. Uma das principais configurações feitas nos *switches* foram a separação dos diversos tipos de trafego em VLAN's. As VLAN's existentes nesta rede são:

1- MONITORAÇÃO E ADMINISTRAÇÃO DO BACKBONE.
2- MMS SE-12
3- MMS SE-6
4- MMS SE-3
5- MMS SE-2
6- MMS SE-1
7- MMS SE-5
8- MMS SE-11
9- MMS SE-8
10- MMS SE-4
11- MMS SE-10
12- MMS SE-9
13- MMS SE-7

14- GOOSE DESCARTE ELÉTRICO PRINCIPAL

15- GOOSE DESCARTE ELÉTRICO SECUNDÁRIO

X – GOOSE INTERNO DA SUBESTAÇÃO (PODE SER QUALQUER NUMERO QUE NÃO COINCIDA COM OUTRA VLAN EXISTENTE)

Os *switches* do *backbone* (figura 19) possuem todas as VLAN's listadas configuradas, exceto a VLAN X, usada apenas nas subestações. Assim, cada interface do servidor é conectada a uma porta do *switch* pertencente a uma VLAN (MMS SE-xxxx). Como foi visto na seção 2.5 (VLAN), através das portas *trunk* e do *tag* 802.1Q nos pacotes *ethernet*, o tráfego é corretamente encaminhado apenas para a sua respectiva subestação, pois, nos *switches* que fazem a conectividade com as subestações, suas interfaces também estão configuradas com suas respectivas VLAN's. Como a comunicação entre o servidor e IED ocorre através do protocolo MMS (exceto nos casos de configuração e transferências de arquivo), podemos perceber que o tráfego no *backbone* é principalmente formado por pacotes MMS dentro de suas respectivas VLAN's (por isso do nome das VLAN's serem MMS SE-xxxx).

Nas subestações, os switches são configurados com quatro VLAN's:

- VLAN PARA TRÁFEGO MMS (NUMERO DE 2 A 13 DEPENDENDO DA SUBESTAÇÃO)
- VLAN GOOSE DESCARTE ELÉTRICO PRINCIPAL (NUMERO 14)
- VLAN GOOSE DESCARTE ELÉTRICO SECUNDARIO (NUMERO 15)
- VLAN PARA GOOSE INTERNO DA SUBESTAÇÃO.

As interfaces dos *switches* das subestações que conectam com os IED's foram configuradas como *trunk*, para que assim o IED tenha a possibilidade de enviar pacotes nas VLAN MMS e VLAN GOOSE, tendo em vista que o IED produz pacotes GOOSE com o *tag* 802.1Q.

A porta do *switch* que se conecta com o *backbone* recebeu uma configuração de bloqueio da VLAN PARA USO INTERNO DA

SUBESTAÇÃO. Desta forma, mesmo sendo uma porta *trunk*, o *switch* irá bloquear todo tráfego da referida VLAN. Como foi dito anteriormente o pacote GOOSE possui um endereço de destino *multicast*, que seria encaminhado para todas as portas do *switch*, inclusive para o *backbone* e posteriormente para outras subestações. O uso da VLAN PARA USO INTERNO DA SUBESTAÇÃO evita que os pacotes GOOSE gerados pelos IED's sejam encaminhados para fora da subestação, podendo causar lentidão em toda a rede.

As duas VLAN's que ainda não foram abordadas, a VLAN GOOSE DESCARTE ELÉTRICO PRINCIPAL (NUMERO 14) e a VLAN GOOSE DESCARTE ELÉTRICO SECUNDÁRIA (NUMERO 15), São usadas para a função de descarte elétrico das subestações. Como pode ser visto na figura 20, há um controlador (CLP) conectado na rede. Este controlador, além de poder ler e enviar algumas variáveis para os IED's através de GOOSE, ele tem a função de receber as mensagens GOOSE produzidas por outro controlador instalado na SE-12. Este último controlador é responsável por contabilizar a capacidade das fontes de energias (geradores e concessionária de energia elétrica) e contabilizar a demanda de energia. Caso a capacidade das fontes de energia seja menor que a demanda (no caso de uma das fontes geradoras ser desligada) o controlador enviará uma mensagem GOOSE contendo o numero da prioridade das cargas que devem ser descartadas através das VLAN's 14 e 15 .Estas mensagens serão lidas por todos os controladores das subestações, que irão recorrer a uma tabela previamente configurada relacionando cada carga com uma prioridade. Desta forma, de acordo com o nível de prioridade do descarte recebido, o controlador enviará mensagens de desligamento às suas cargas que estão contidos naquele nível de prioridade.

A figura 21 representa o esquema da topologia da rede contendo a SE-12 e a SE-5 interligadas pelo *backbone*. Também foi representada a inter-relação entre as duas subestações e o *backbone*, através dos protocolos GOOSE e MMS.

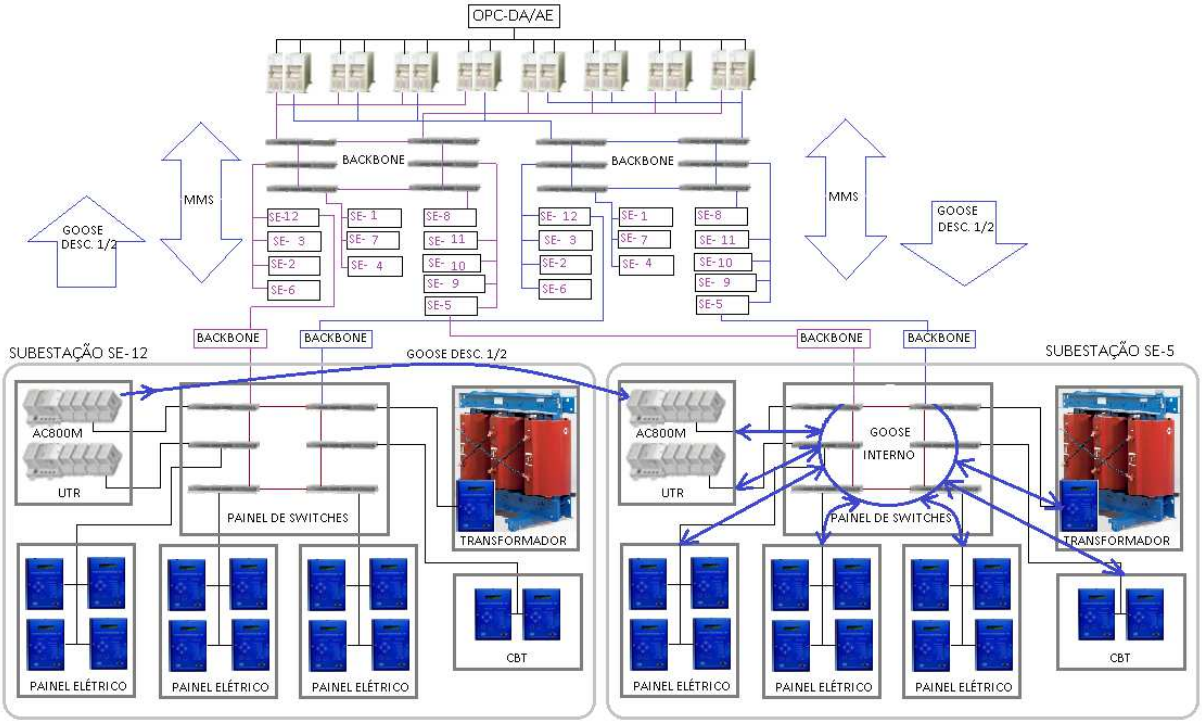


Figura 21: topologia: esquema de inter-relação entre duas subestações e o backbone.
Fonte: O Autor

3.3 SISTEMA ELÉTRICO

Após vermos como os IED's estão inseridos na topologia física e lógica da rede de comunicação, convém observar de forma resumida como os diversos IED's estão inseridos no sistema elétrico.

A grande maioria dos IED's tem a função de controlar disjuntores. Estes disjuntores estão inseridos em um sistema elétrico, seja para energizar um painel, energizar um motor ou fazer paralelismo entre duas fontes de energia. Alguns IED's não controlam diretamente um disjuntor especifico, podem ser responsáveis por atuar em mais de um disjuntor, como no caso de IED's com proteção de sobrecorrente diferencial, e alguns IED's possuem funções auxiliares como fornecer variáveis para outros IED's atuarem em seus disjuntores, como no caso de IED's instalados em transformadores.

A figura 22 ilustra o esquema do painel de alimentadores das subestações. Cada disjuntor representado no esquema (símbolo quadrado) possui um IED responsável por controlá-lo. A subestação em questão é a SE-12, onde estão localizados os geradores da planta

industrial, bem como os painéis de distribuição da alimentação elétrica.

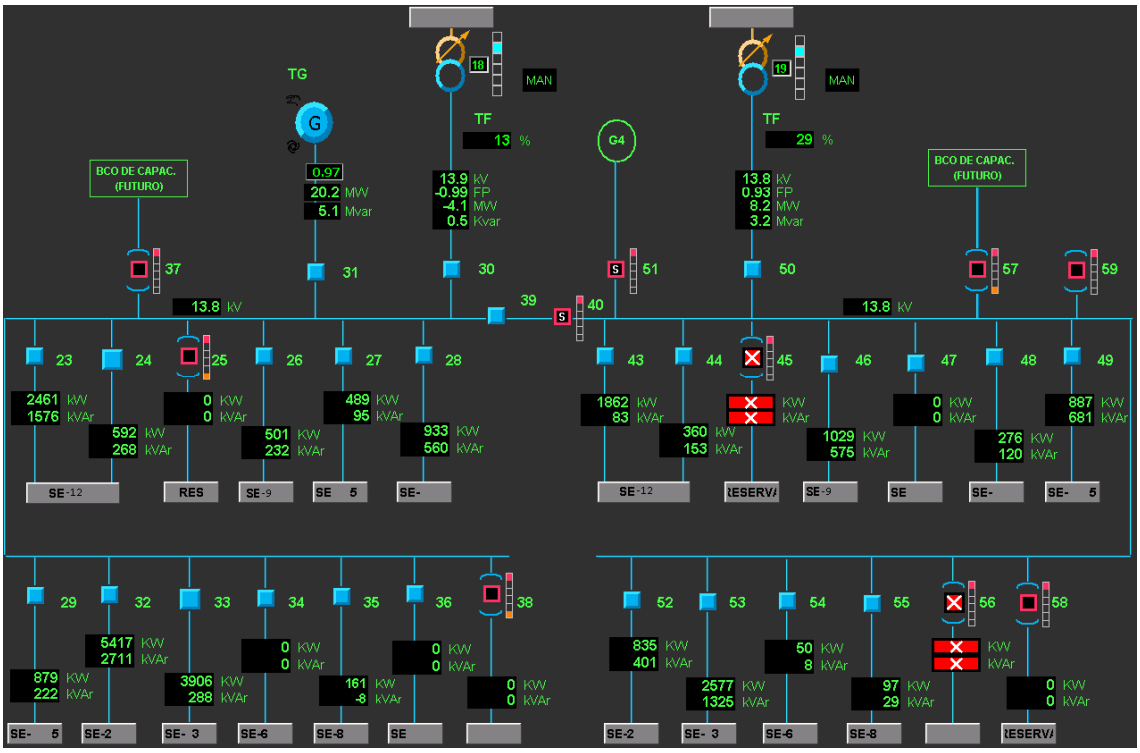


Figura 22: Visão geral do esquema elétrico dos alimentadores das subestações.

FONTE: O Autor

Na figura 23 vemos o esquema geral de uma das subestações. Nesta figura percebemos a existência de cinco painéis na subestação, sendo que apenas os disjuntores de entrada e de paralelismo estão representados.

Na figura 24 vemos o esquema de um dos painéis da subestação. Onde é possível perceber os disjuntores de alimentação e paralelismo, bem como os disjuntores das cargas do painel, que podem ser motores ou outros painéis.

É importante destacar que dependendo da função de um IED na rede elétrica, o comportamento dele rede de comunicação pode ser diferente. Pois há IED's que possuem diversos tipos de intertravamentos atuando sobre si através do protocolo GOOSE, existem IED's responsáveis por mais sinalizações no supervisório através do protocolo MMS. Isto será abordada novamente na seção de análise do tráfego de rede.

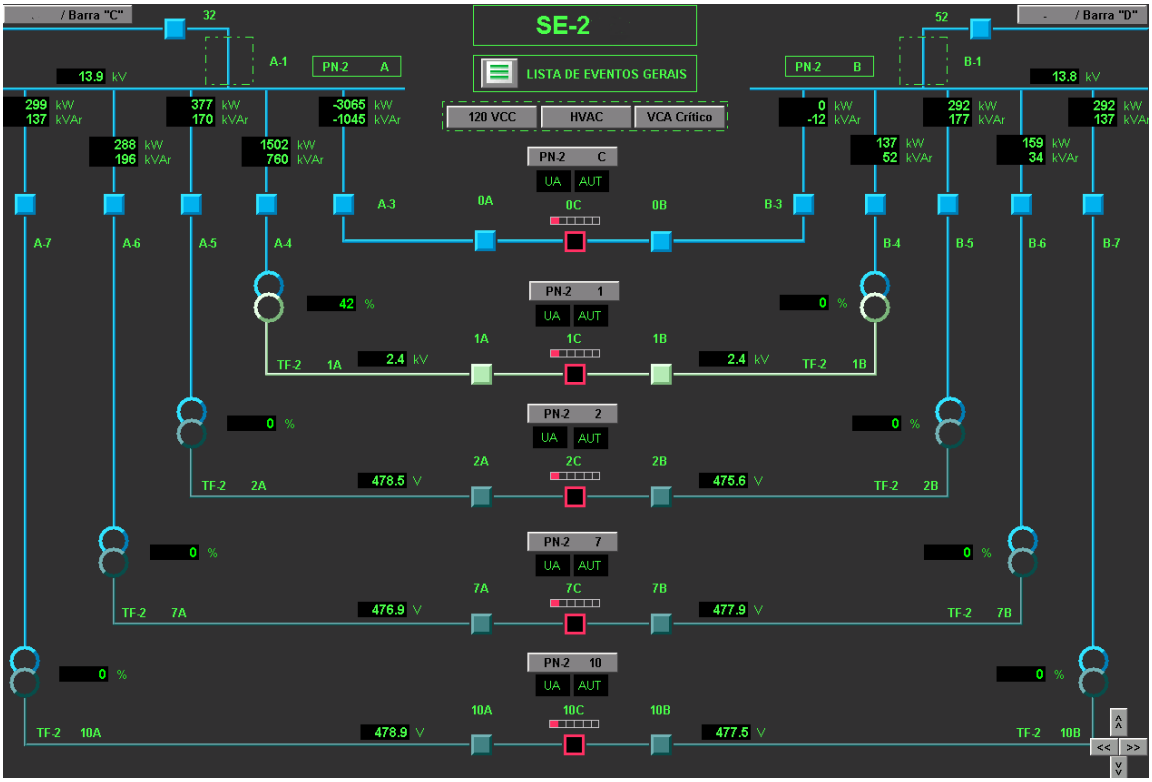


Figura 23: Esquema geral da rede elétrica de uma subestação

Fonte: O Autor

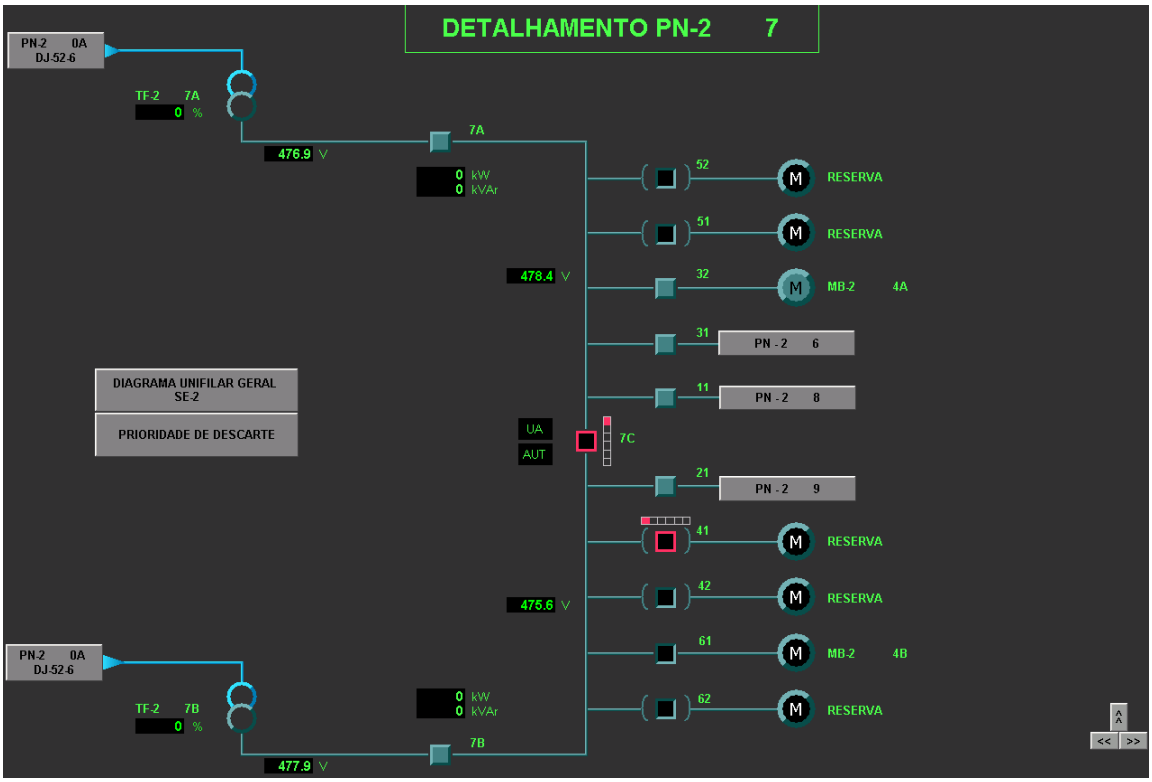


Figura 24: Esquema elétrico de uma painel da subestação.

Fonte: O Autor

3.4 CAPTURA DE PACOTES

A captura dos pacotes foi feita através da função *Mirroring port* (Espelhamento de porta) existentes nos switches Ruggedcom. Na figura 25 há uma representação de como feita a ligação do notebook à rede de comunicação. A configuração do switch foi acessada através da porta de console (porta serial), através deste acesso o switch era configurado para espelhar o tráfego de entrada e saída de determinada interface e enviá-la para a porta ethernet onde o notebook estava conectado. O acesso à configuração do switch via porta console tinha como objetivo não interferir na rede criando tráfego que não existe em condições normais.

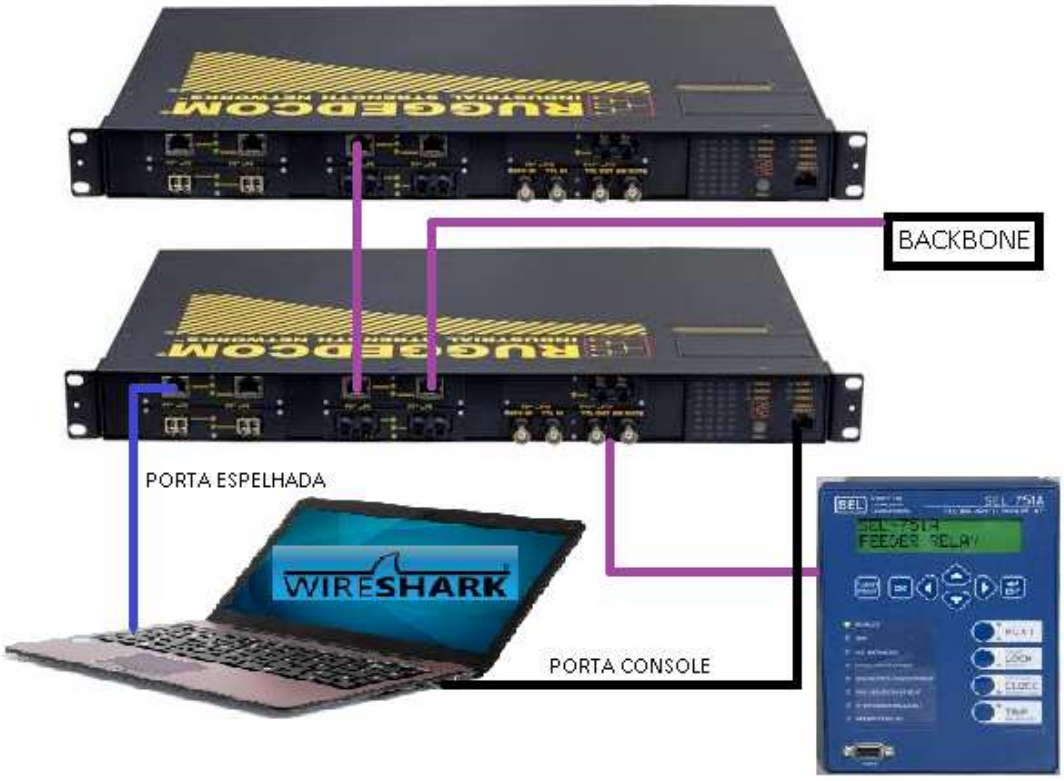


Figura 25: Esquema de ligação do notebook na rede.

Fonte: O Autor

A escolha das portas dos switches que seriam monitoradas foram feitas por amostragem obedecendo alguns critérios:

- IED's de cargas do painel, foram escolhidos apenas um de cada lado do painel, sendo que os IED's reservas não foram escolhidos. Por exemplo, no painel da figura 24

foram monitorados os IED's dos disjuntores 32 (lado A) e 61 (lado B).

- IED's dos disjuntores de entrada e interligação do painel eram todos monitorados. Por exemplo, no painel da figura 24 foram monitorados os IED's dos disjuntores 7A, 7B e 7C.
- IED's dos disjuntores de entrada de alta tensão (alimentação dos transformadores foram todos monitorados). Por exemplo, no esquema da figura 23 foram monitorados os disjuntores A3, A4, A5, A6, A7, B3, B4, B5, B6 e B7.
- IED's das entradas e interligação das barras de alimentação principal. Por exemplo, na figura 22 foram monitorados os IED's dos disjuntores 39, 40, 30, 31 e 50.
- IED's dos alimentadores das subestações, excluindo os disjuntores reserva. Por exemplo, na figura 22, foram monitorados os disjuntores 23, 24, 27, etc.
- IED's das proteções diferenciais das barras da figura 22.
- Cartões do controlador da subestação (controlador representado na figura 20 no painel chamado UTR).
- Todas as interfaces entre switches.

As monitorações foram feitas por um período de dois minutos em cada porta do switch escolhida para monitoração. Este seria um tempo adequado para que a captura de pacotes não deixasse de captar algum trafego normal na rede que ocorresse a cada dois minutos no mínimo.

3.5 ANÁLISE DO TRÁFEGO

3.5.1 Configuração da rede

Através da análise das capturas realizadas foi possível verificar o correto funcionamento do RSTP nas redes das subestações. Na figura 26 há um exemplo dos resultados das capturas efetuadas nas interfaces entre switches. Na figura é possível verificar que a rede é

composta por quatro switches, estes switches estão ligados fisicamente em uma topologia anel. Mas com a operação do RSTP, é possível identificar que a porta 11 do switch 3 (SW3_P11) possui uma taxa média de tráfego muito inferior às outras, além do fato de que o tráfego é formado apenas por pacotes com endereços de destino *multicast* ou *broadcast*, (como é o caso do GOOSE por exemplo). Portanto a figura resume os dados coletados de uma porta que esta apenas no estado de "escuta", ou seja não encaminha os pacotes que chegam a esta porta e também não encaminha pacotes por esta porta.

SUBEST.	EQUIP.	Avg. Pack/s	Avg. Pack size (bytes)	Avg. MBit/s	GOOSE Bytes (%)	STP Bytes (%)	UDP Bytes (%)	TCP Bytes (%)	ARP Bytes (%)	LLDP Bytes (%)
SE-1	SW1_P11	66282	188022	0,1	48,14	0,48	1,75	48,27	1,26	0,11
SE-1	SW1_P9	71330	196184	0,112	42,96	0,43	1,03	54,35	1,13	0,09
SE-1	SW2_P9	71726	190224	0,109	51,84	0,44	1,63	44,85	1,15	0,1
SE-1	SW2_P11	54213	190358	0,083	57,44	0,58	1,37	39,39	1,09	0,13
SE-1	SW3_P9	53773	189988	0,082	56,47	0,59	1,63	40,09	1,1	0,13
SE-1	SW3_P11	29519	193537	**0,046**	96,9	1,04	1,16	0	0,67	0,23
SE-1	SW4_P9	70522	194350	0,11	97,93	0,44	0,98	0	0,56	0,09
SE-1	SW4_P11	78872	199737	0,126	44,82	0,38	0,91	52,77	1,04	0,08

Figura 26: Exemplo dos dados obtidos através da captura entre switches.

Fonte: O Autor

Através das capturas foi possível constatar o correto funcionamento das VLAN's configuradas para trafegar os pacotes do sistema de descarte elétrico. Os pacotes que trafegam nestas VLAN's (14 e 15, conforme seção 3.6) devem ser os únicos pacotes GOOSE que trafegam entre subestações. Na figura 27 há um exemplo de um pacote capturado em uma das interfaces de entrada da rede da subestação SE-1. Conforme pode ser visto no pacote capturado pelo Wireshark, mostrado na figura 27, vemos que, através do nome de referencia do pacote GOOSE (gocbRef), pelo nome do objeto que está publicando o pacote (dataset) e pelo endereço MAC do equipamento que gerou o pacote, que este pacote GOOSE foi gerado na SE-12 e chegou na SE-5 Este comportamento foi observado em todas a subestações.

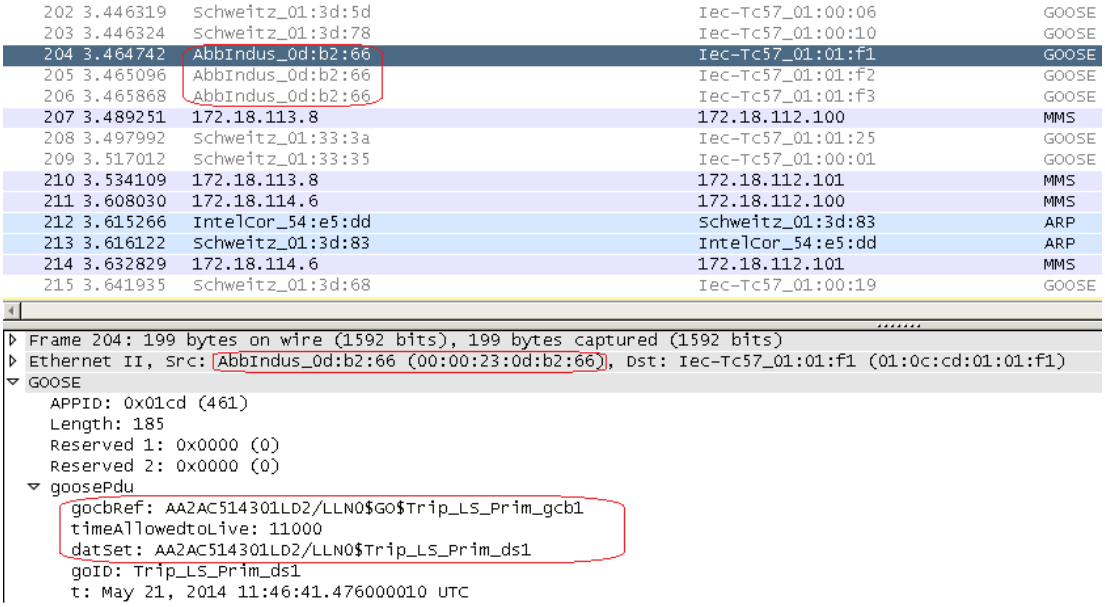


Figura 27: Pacote referente ao descarte elétrico capturado em em uma subestação.

Fonte: O Autor

Através das capturas também foi constatado que os pacotes GOOSE gerados nas subestações não estão saindo da subestação através da rede. Através do espelhamento das portas de interface entre subestação e *backbone* é possível verificar que apenas os pacotes GOOSE do sistema do descarte elétrico trafegam nestas portas.

3.5.2 Carregamento da Rede

Após a inserção dos dados coletados em planilha, foi possível obter algumas informações sobre as redes das subestações. Primeiramente foi obtido o gráfico da figura 28. Este gráfico mostra algumas informações importantes das redes de cada subestação como: média de pacotes por segundo (Avg. Pack./s), média dos tamanhos dos pacotes (Avg. Pack size [bytes]), média de tráfego em kilobits por segundo (Avg. kBits/s).

Por este gráfico primeiramente percebemos que dificilmente haverá um problema de sobrecarga nas redes das subestações, tendo em vista que as portas dos switches são configuradas para 100Mbps (exceto a porta que interligam o a subestação ao backbone que são configuradas para 1Gbps).

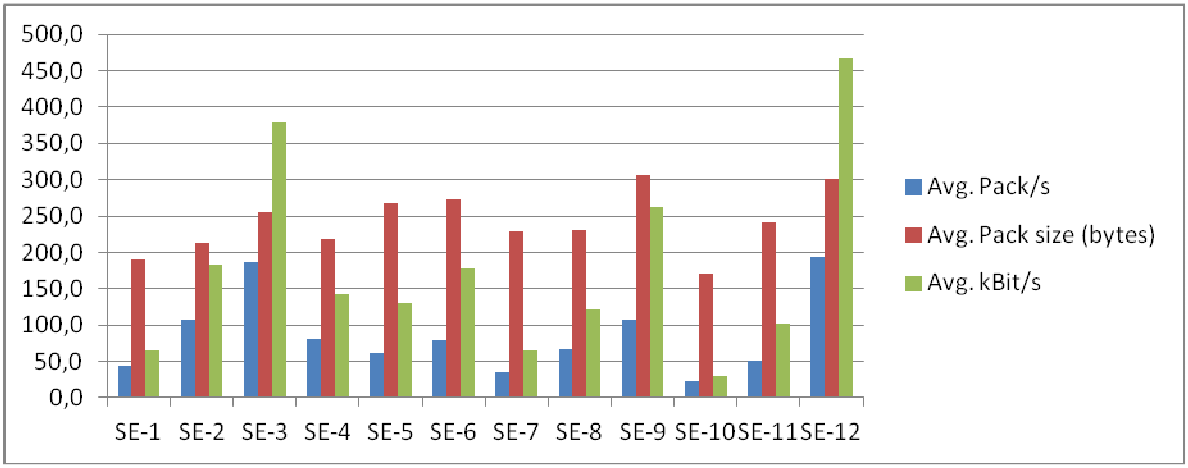


Figura 28: taxas médias pacotes por segundo, tamanho médio dos pacotes e trafego médio. Comparação entre subestações diferentes.

Fonte: O Autor

Nas coletas percebemos que a porta mais de switch mai carregada possuía pouco mais de 1Mbps de tráfego e esta localizado na subestação com mais alto trafego de acordo com o gráfico, a SE-12.

As variações dos tamanhos médios dos pacotes obteve uma variação entre as diversas subestações que ficou entre 170,8 bytes na SE-10 a 306,3 bytes na SE-9. A taxa média de pacotes por segundo obteve uma variação de 23,5 Pack./s na SE-10 a 194,3 Pack./s na SE-12. Desta forma percebemos que, comparada com a variação dos tamanhos dos pacotes a variação do tráfego de pacotes na rede é muito maior. Assim concluímos que o carregamento da rede (Kbits/s no gráfico) é influenciado principalmente pela taxa de geração de pacotes pelos dispositivos instalados na rede.

Com as informações acima é importante acrescentar uma informação importante para a análise: a quantidade de IED's por subestação. Na tabela da figura 29 está listada a quantidade de IED's por subestação. Com isto é interessante analisar o tráfego em relação a quantidade de IED's. No gráfico da figura 30 vemos o gráfico que relaciona o tráfego (em Kbits/s) com a quantidade de IED's.

SE	Quantidade IEDs
SE-1	43
SE-2	101
SE-3	72
SE-4	55
SE-5	54
SE-6	40
SE-7	34
SE-8	55
SE-9	12
SE-10	48
SE-11	67
SE-12	107

Figura 29: quantidade de IED's por subestação

Fonte: O Autor

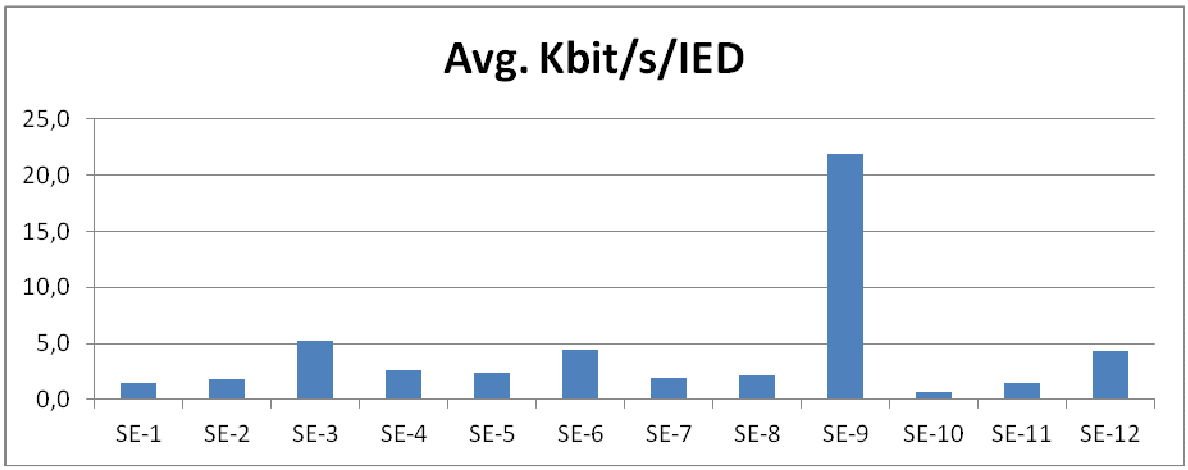


Figura 30: Relação do tráfego (em kbits/s) com a quantidade de IED's por Subestação.

Fonte: O Autor

Este gráfico nos informa que na SE-9 há uma característica interessante que não pôde ser percebida no gráfico da figura 28. Como a SE-9 é de pequenas proporções (com apenas 12 IED's) esta característica não chega a ser um problema. Isto reflete uma característica da configuração da subestação feita pela empresa que a comissionou. Como cada subestação foi construída e comissionada por diferentes empresas, percebemos também características diferentes nas redes. Analisando de forma mais detalhada o tráfego desta subestação percebe-se que, além do fato dos IED's gerarem mais pacotes GOOSE em relação a outras subestações, os pacotes

GOOSE são duplicados entre dois endereços multcast de destino como pode ser visto na figura 31.

No.	Time	Source	Destination	Protocol
1	0.000000	Schweitz_01:b3:cb	Iec-Tc57_01:00:09	GOOSE
2	0.000289	Schweitz_01:b3:cb	Iec-Tc57_01:01:09	GOOSE
3	0.012344	Schweitz_01:b3:cb	Iec-Tc57_01:00:09	GOOSE
4	0.012618	Schweitz_01:b3:cb	Iec-Tc57_01:01:09	GOOSE
5	0.037428	Schweitz_01:b3:cb	Iec-Tc57_01:00:09	GOOSE
6	0.037709	Schweitz_01:b3:cb	Iec-Tc57_01:01:09	GOOSE

Figura 31: amostra de captura da SE-9 mostrando duplicação de pacotes GOOSE

Fonte: O Autor

Isto é uma provável falha de configuração nos IED's das subestações, que não surtiria outro efeito se não tornar a rede mais carregada e exigir dos IED's capacidade de processamento duplicada.

Como veremos na próxima seção, o tráfego das redes das subestações é composta principalmente por pacotes GOOSE. Com isto é interessante atentarmos para quantos disparos GOOSE ocorrem na rede. Como foi visto na seção 2.7 na figura 16, o protocolo GOOSE possui um tempo de transmissão de regime normal e tempos de transmissão mais curtos após algum evento (disparo). No gráfico da figura 32 vemos a quantidade de disparos por subestação.

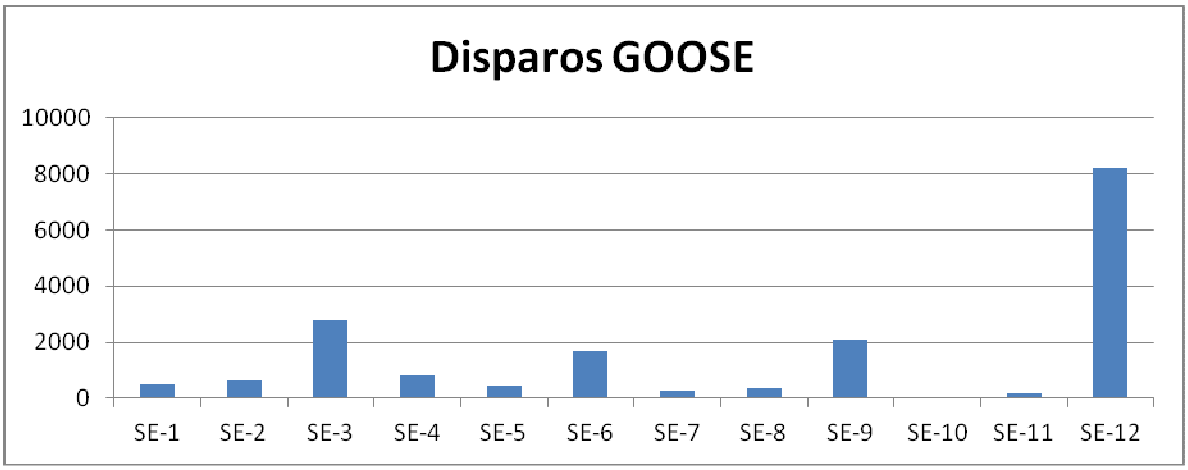


Figura 32: quantidade de disparos GOOSE por subestação

Fonte: O Autor

Nesta figura fica evidente que a SE-12 possui uma quantidade grande de disparos GOOSE, sabendo que após o disparos se seguirão transmissões em tempos mais curtos (como na figura 19) isto poderia ser um problema em potencial para os IED's envolvidos nestas transmissões e recepções de tais pacotes, já que isto demandaria

mais capacidade de processamento dos IED's. Ao analisar de forma mais detalhada as capturas da SE-12 verificamos que, dos 107 IED's existentes na SE-12, aproximadamente um terço (1/3) de todo o tráfego desta rede é gerado por apenas 8 IED's. Estes IED's controlam os disjuntores da subestação de distribuição em 69000 Volts (69kV). Através das capturas foi observado que estes 8 IED's foram configurados para que, a cada disparo GOOSE, haja 7 retransmissões sequenciais (com o variável sqNum = 0). Na figura 34 há um gráfico Disparo GOOSE X Tempo (s) no qual se demonstra o comportamento destes IED's. Nos demais IED's desta subestação foi configurado para que houvesse 3 retransmissões sequenciais. Nas demais subestações não há estas retransmissões, ou seja, após o pacote gerado no disparo (com o variável sqNum = 0) os outros pacotes já começam a aumentar o tempo das transmissões até chegar ao regime normal. Na figura 33 foi demonstrado este comportamento.

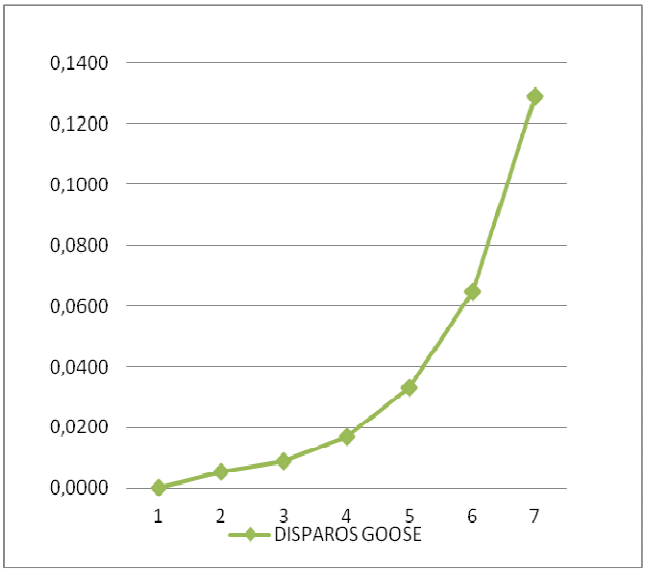


Figura 33: Grafico DisparoXTempo das subestações.

Fonte: O Autor

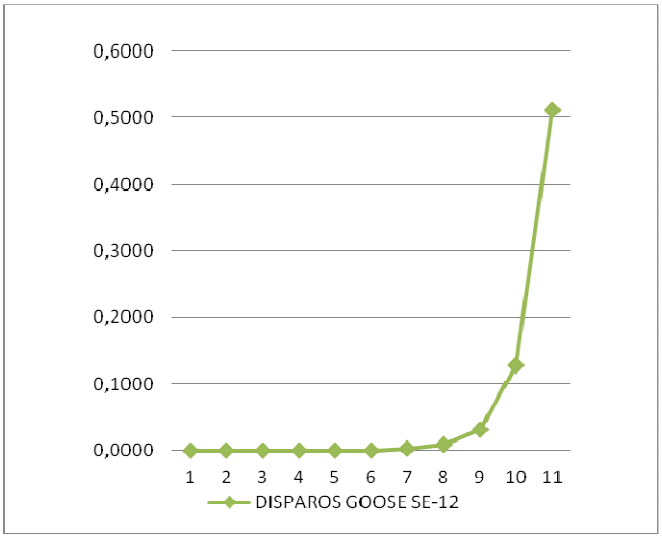


Figura 34: Grafico DisparoXTempo da SE-12

Fonte: O Autor

Também foi feita uma média dos dados coletados pelas funções dos dispositivos conectados a rede, como pode ser visto na figura 35.

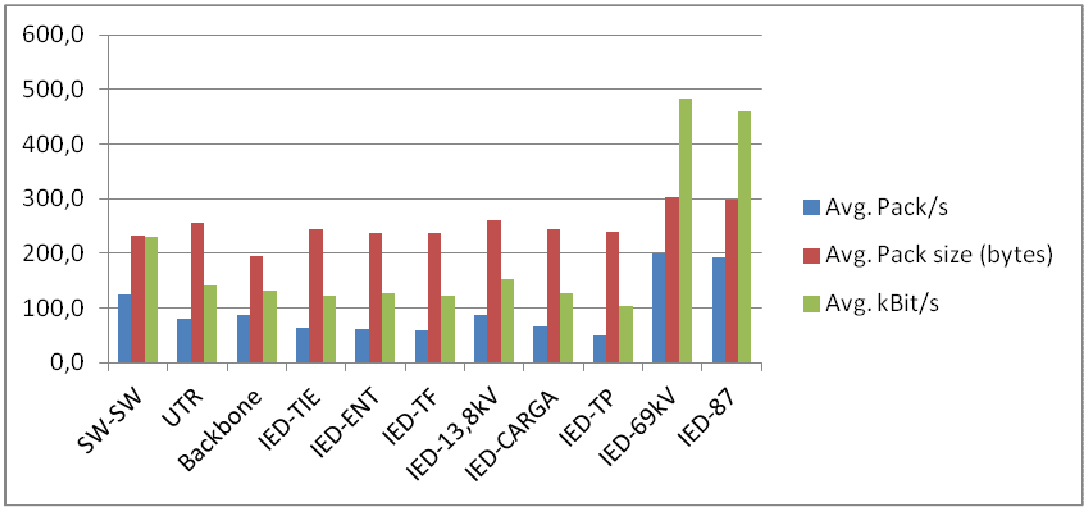


Figura 35: taxas médias pacotes por segundo, tamanho médio dos pacotes e trafego médio. Comparação entre dispositivos com funções diferentes.

Fonte: O Autor

Este gráfico foi feito com a intenção de encontrar comportamentos adversos que determinados tipos de dispositivos pudessem ter na rede e qual seria a sua influencia na rede. Percebe-se no gráfico uma maior variação nos dispositivos “IED-69kV” e “IED-87”, mas como estes dispositivos estão instalados na rede da SE-12, já vimos a causa da sua elevada taxa de tráfego em comparação com outros dispositivos.

3.5.3 Comportamento da Rede

Além das informações obtidas nas seções anteriores. Também foi elaborado um levantamento contendo qual a parcela de cada protocolo de comunicação no tráfego total da rede. Desta forma fica documentado o comportamento das redes numa situação tida como normal, para que, caso haja problemas futuros relacionados a rede de comunicação, tenhamos algo a que comparar as coletadas a serem realizadas.

Os protocolos foram separados da seguinte forma:

GOOSE – protocolo de camada 2 de comunicação entre IED's

STP – Protocolo Spannig Tree para redundância de caminhos na rede.

UDP – Protocolo de camada de transporte que, nas redes das subestações, é usado principalmente pelo protocolo SNMP. Também encontrado na rede alguns protocolos como Netbios Name Service e serviços de domínio, que provavelmente são devidos a alguma configuração indevida nos servidores do supervisório da rede.

TCP – Protocolo da camada de transporte que, nas redes das subestações, é usado para comunicação entre IED's e servidores através do protocolo MMS.

ARP – Protocolo para resolução de endereços de rede.

LLDP – *Link Layer Discovery Protocol* – Protocolo utilizado pelos switches da Ruggedcom para obterem informações básicas dos switches vizinhos.

Todo o tráfego coletado na rede foi separado dentro dos protocolos citados.

Na análise por subestação a grande maioria das subestações tem um tráfego parecido com o apresentado na figura 36, com poucas variações. Neste gráfico observamos que o protocolo GOOSE é predominante na rede. Em segundo lugar temos o protocolo TCP utilizado pelo protocolo MMS. Os demais protocolos somados não chegam a representar 4% do tráfego da rede. Ou seja, os protocolos GOOSE e MMS são responsáveis por, pelo menos 96% do tráfego.

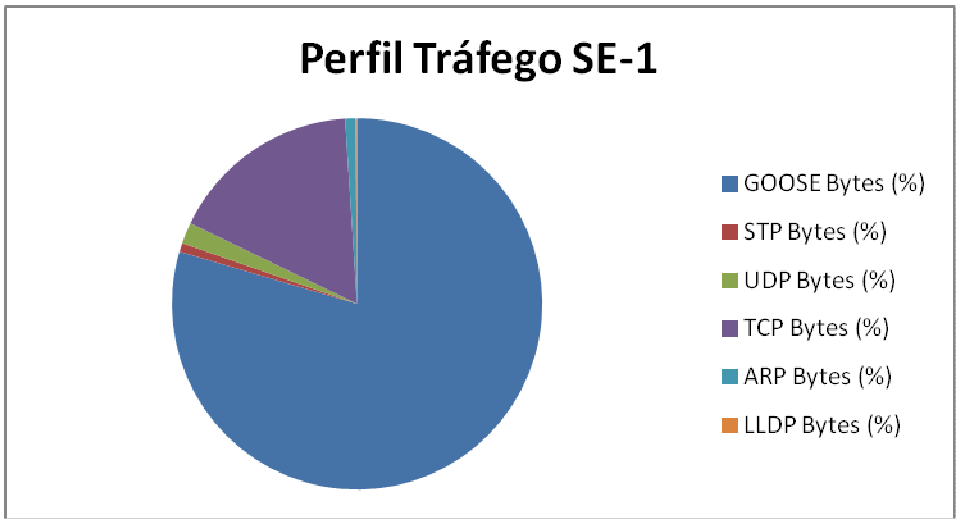


Figura 36: Composição do tráfego da SE-1

Fonte: O Autor

Foram encontradas algumas variações, como no caso da SE-10 representada na figura 37. O tráfego desta subestação possui a menor parcela do protocolo GOOSE e, em contrapartida é a que possui a maior parcela de outros protocolos.

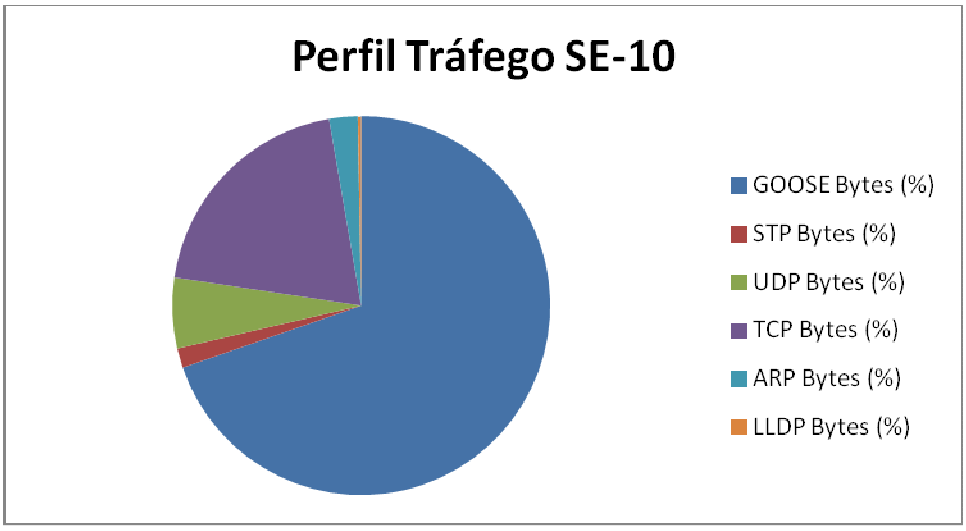


Figura 37: Composição do tráfego da SE-10

Fonte: O Autor

Ao verificar as informações da figura 28, da figura 30 e da figura 32 vemos que esta subestação possui o menor tráfego de rede. Os IED's desta subestação não geram uma elevada quantidade de pacotes GOOSE em comparação com as demais subestações. Como, os outros protocolos permanecem quase com o mesmo tráfego das

outras subestações, eles representam uma parcela maior do tráfego da SE-10.

Ao contrário desta situação, há o caso da SE-12, mostrado na figura 38. Nesta subestação os IED's geram uma elevada quantidade de pacotes GOOSE. Desta forma quase que a totalidade do tráfego da SE-12 é composta pelo protocolo GOOSE. A razão disto também foi vista na seção anterior.

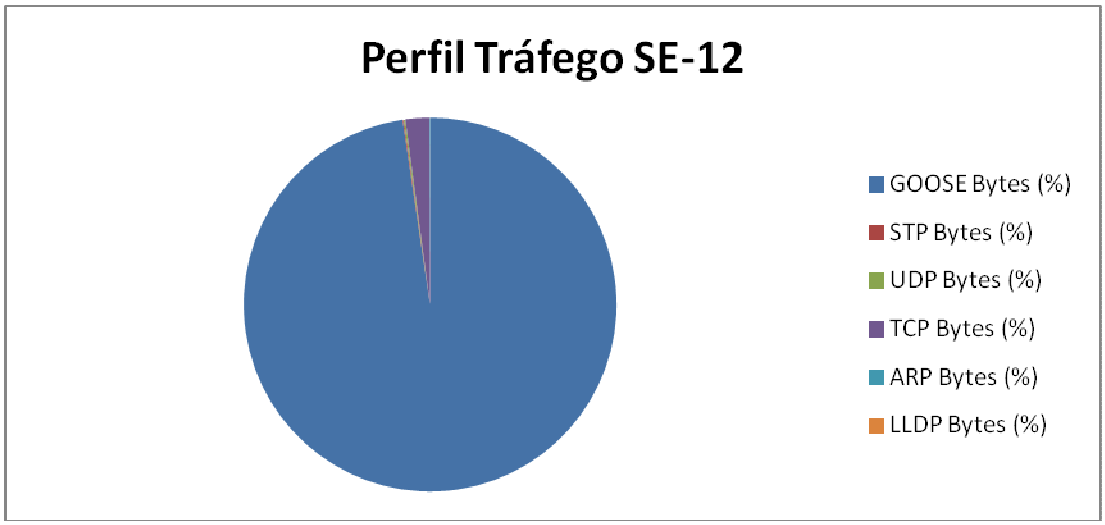


Figura 38: Composição do tráfego da SE-12

Fonte: O Autor

A análise da composição do tráfego também foi feita por dispositivos obtendo-se a média de cada subestação.

Como pontos que valem destacar, vemos a composição do tráfego das interfaces das subestações com o backbone na figura 39. O tráfego é quase que totalmente composto pelo protocolo TCP utilizado pelo protocolo MMS. A parcela de GOOSE neste gráfico é mínima (0,4%), e é devido apenas ao sistema de descarte elétrico.

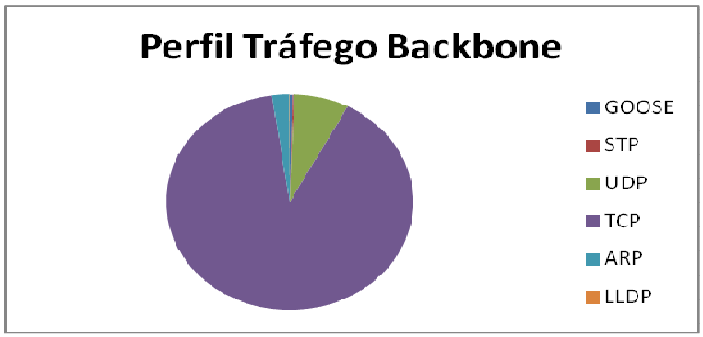


Figura 39: Composição média do trafego das interfaces com backbone.

Fonte: O Autor

Percebemos também a composição do tráfego médio entre switches visto na figura 40. Também há predominância do protocolo GOOSE mas com uma grande parcela dos pacotes MMS (TCP).

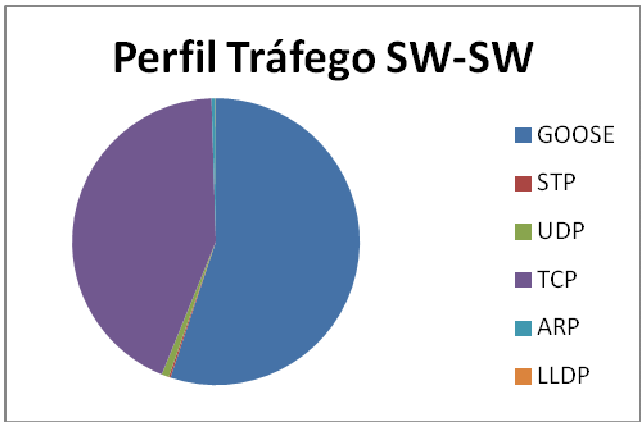


Figura 40: Composição média do trafego entre switches.

Fonte: O Autor

Importante destacar também o comportamento dos IED's na rede de comunicação de acordo com a função desempenhada no sistema elétrico. Na figura 41 vemos três perfis diferentes de comunicação. Os IED's de entrada (IED-ENT) são responsáveis por muitas sinalizações e eventos no sistema supervisório, isto significa que, entre outros tipos de IED's, estes possuem o maior tráfego MMS (TCP). IED's instalados no sistema 13,8kV (IED-13.8kV) possuem menos sinalizações e eventos requisitados pelo supervisório, portanto possuem menor tráfego de protocolo MMS (TCP).

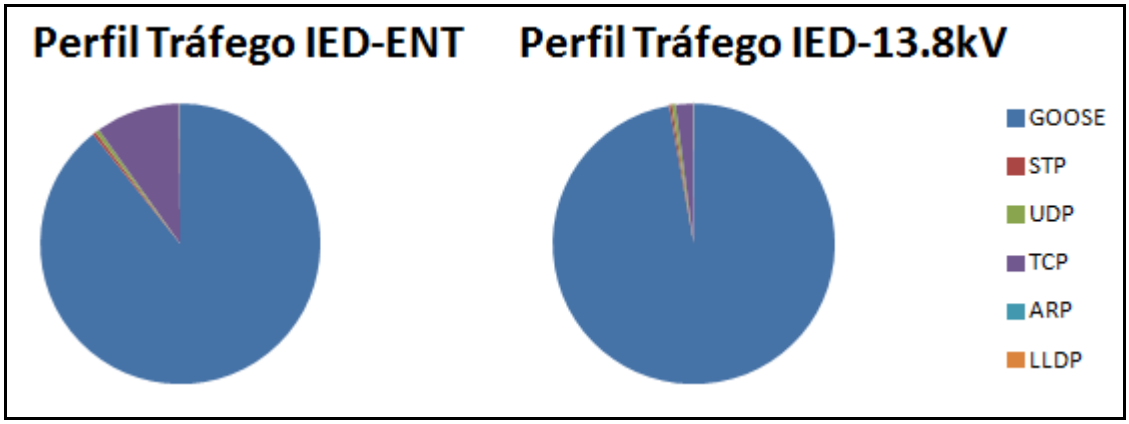


Figura 41: Perfis de tráfego dos IED de entrada de painéis e IED's no sistema de 13,8kV.

Fonte: O Autor

4. CONCLUSÃO

No capitulo 1 deste trabalho buscou-se contextualizar o leitor com a realidade das novas redes de comunicação de subestações impostas pela norma IEC-61850, apresentar os objetivos e a importância deste trabalho no diagnostico de prováveis problemas de rede.

No capitulo 2 foi apresentado uma pesquisa bibliográfica dos dispositivos de rede abordados neste trabalho como os switches e os IED's. Efetuou-se uma breve descrição dos principais protocolos de comunicação envolvidos nas análises realizadas. E foi apresentada uma breve descrição da norma IEC-61850 dando ênfase aos aspectos abordados neste trabalho

Finalmente este trabalho visou a coleta de dados para a obtenção de informações relativas ao estado das redes de comunicação das subestações de uma planta industrial. Desta forma verificou-se que, nas redes analisadas, não apresentaram problemas sérios que comprometessem a disponibilidade das redes ou dos dados trafegados por ela, que justificassem uma intervenção imediata.

Entretanto seria necessário um estudo mais aprofundado em algumas configurações de dispositivos das redes das subestações para verificar prováveis erros de configuração. Mas neste caso não por que haja risco à rede, mas por haver risco de mau funcionamento dos dispositivos devido a erros de configuração.

Com este trabalho obteve-se também um registro de "comportamento base" das redes analisadas. Assim, no caso de problemas de rede futuros, poderemos comparar dados de um provável comportamento de falha de rede com o "comportamento base" registrado neste trabalho.

Para trabalhos futuros sugere-se efetuar analise da rede baseado em dados coletados apenas com pacotes de entrada na interface do switch. Pois assim teríamos apenas os pacotes gerados pelos dispositivos na análise da rede, sendo desconsiderados os pacotes *multicast* de saída que são encaminhadas para todas as

portas do switch. Uma análise destas informações poderia acrescentar outras informações a análise realizada neste trabalho.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ABB Asea Brown Boveri Ltd, **Review: Special Report IEC 61850**. Zurique. ABB Group R&D and Technology, 2010. 8p.

BEUREN, Ilse Maria. Trajetória da construção de um trabalho monográfico em contabilidade. **LONGARAY, André Andrade et al; BEUREN, Ilse Maria (Org.). Como Elaborar Trabalhos Monográficos em Contabilidade. São Paulo: Atlas**, p. 80-93, 2003.

CISCO. **CCNA** Exploration **4.0 – Acessando a WAN**. Disponível em: <http://www.cisco.ct.utfpr.edu.br/material/CCNA4.0/Modulo4>. Acesso em: 11 de junho de 2015.

FILIPPETTI, Marco Aurélio. **Cisco CCNA 4.1 – Guia de Estudo Completo**. Florianópolis: Visual Books, 2009. p. 34-36.

INTERNATIONAL ELETROTECHINICAL COMMISSION, **IEC-61850-7-1**: Communication networks and systems in substations: Basic communication structure for substation and feeder equipment – principles e models. Primeira Edição. Genebra: IEC, 2012

INTERNATIONAL ELETROTECHINICAL COMMISSION, **IEC-TR-61850-1**: Communication networks and systems in substations: Introduction and Overview. Primeira Edição. Genebra: IEC, 2003. 15p

INTERNATIONAL ELETROTECHINICAL COMMISSION, **IEC-61850-8-1**: Communication networks and systems in substations:Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. Primeira Edição. Genebra: IEC, 2004. 68p, 70-71p.

KUROSE, James F. **Redes de Computadores e a Internet: uma abordagem top-down**. São Paulo: Pearson Education do Brasil, p. 383, 2010

MACKIEWICZ, R. E. Overview of IEC 61850 and Benefits. In: **Power Systems Conference and Exposition, 2006. PSCE'06. 2006 IEEE PES**. IEEE, 2006. p. 623-630.

NGUYEN, A. D.; **Integration of IEC 61850 MMS and LTE to support remote control communication in electricity distribution grid**. Holanda: University of Twente, 2013. 14p, 48p, 51p.

PEREIRA, Roberto Martins; SPRITZER, Ilda Maria de Paiva Almeida. Automação e digitalização em subestações de energia elétrica: um estudo de caso. **Revista Gestão Industrial**, v. 3, n. 04, p. 147-160, 2007.

PETENEL, Fernando; PANAZIO, Cristiano. **Análise de uma rede Smart Grid usando a norma IEC 61850 e dados de medições**. XXX Simpósio Brasileiro de Telecomunicações. 2012.

PHAM, Giang T.; **Integration of IEC 61850 MMS and LTE to support smart metering communications**. Holanda: University of Twente, 2013. 22-23p.

SIEMENS, **Treinamento de Automação de Sistemas Elétricos Industriais – Modulo I**, p. 7-9, Rio de Janeiro, 2013.

SCHWEITZER ENGINEERING LABORATORIES, Redes de Comunicação em Subestações de Energia Elétrica – Norma IEC 61850. **Revista O Setor Elétrico**, p. 56-57, 2010.

TANENBAUM, Andrews S. **Redes de Computadores** (4 Edição). 2003, p. 950. Rio de Janeiro: Editora Campus. 2003. P 950, 263.