Introdução

Esse documento apresenta um roteiro para utilização do programa Wireshark, para captura de mensagens Ethernet transmitidas na infraestrutura de rede do Sistema de Automação de Subestações (SAS) proposto. Cada subgrupo de alunos deve registrar o tráfego de mensagens do tipo GOOSE durante um dos ensaios realizados, para analisar o escopo de mensagens trocadas entre os IEDs, o tempo de envio de cada mensagem e seu conteúdo de *dataitens*.

Requisitos

Para a utilização desse guia, os subgrupos devem ter acesso aos seguintes elementos:

- ✓ Um computador com placa de rede conectada à mesma rede de automação e proteção do sistema elétrico de potência, e;
- ✓ Instalação do software de captura e análise de protocolos Wireshark (www.wireshark.org).

O software Wireshark é gratuito e pode ser instalado nos computadores pessoais dos alunos, para análise dos arquivos de captura de tráfego Ethernet.

Exemplo de utilização

Para coletar o tráfego de rede de mensagens GOOSE, trocadas entre os IEDs do SAS, deve-se seguir o procedimento citado a seguir.

1) Executar o software Wireshark em um dos computadores conectados à rede do SAS. Surge a tela principal do programa (Fig.1).

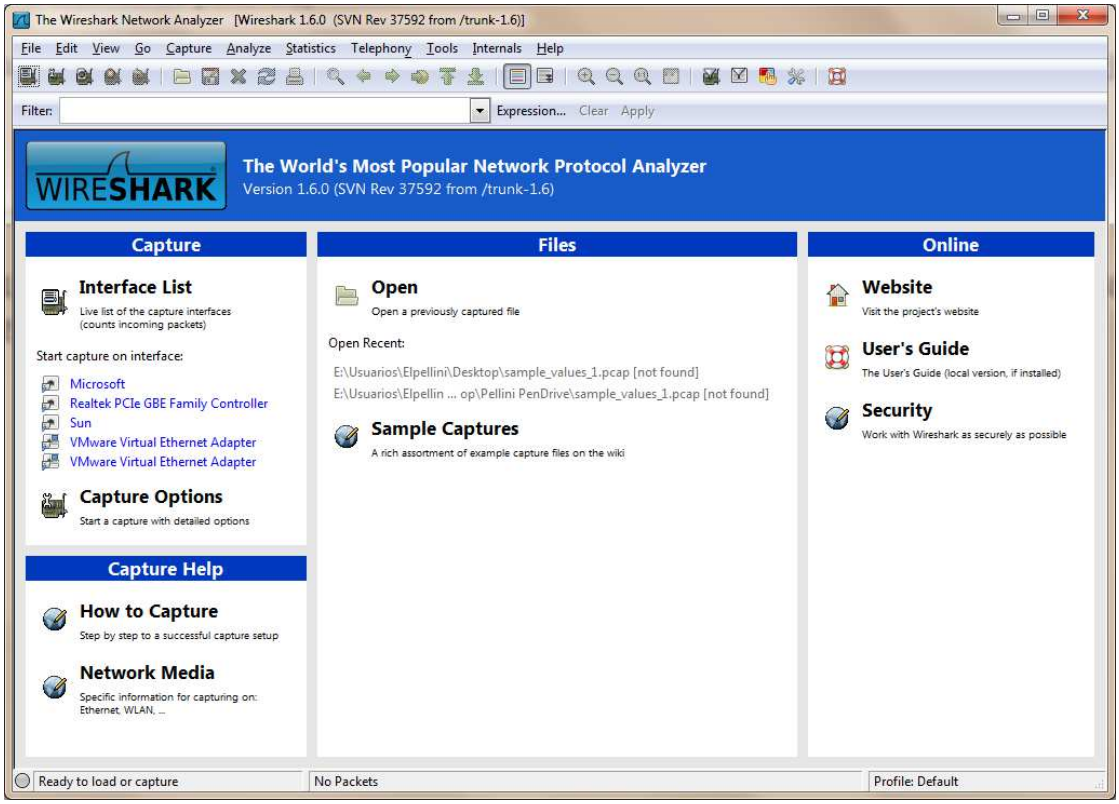

Fig. 1 - Janela principal do WireShark.

2) Na janela principal do Wireshark, acione no menu superior "**Capture**", a opção "**Interfaces**". Surge uma nova janela, como a da Fig. 2. Nessa janela, são listadas todas as interfaces de rede do computador local, capazes de produzir ou receber tráfego de rede Ethernet. Deve-se descobrir qual delas está ligada à rede do SAS, ou seja, qual interface de rede está recebendo as mensagens GOOSE publicadas pelos IEDs. Isso pode ser notado pela atividade em termos de pacotes ou pacotes/s. A interface com maior atividade, provavelmente, é a interface de rede desejada. No exemplo mostrado na Fig. 2, a interface é a denominada "Realtek PCIe GBE Family Controller...".

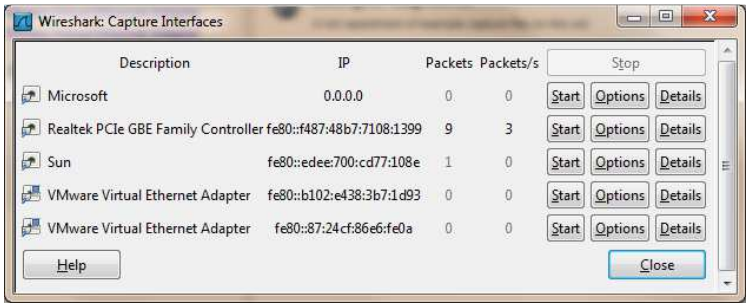

Fig. 2 - Lista de interfaces para captura de mensagens. Deve-se procurar a interface com maior atividade de rede.

3) Deve-se clicar no botão "**Options**" da interface escolhida, que dará acesso a uma janela, como a mostrada na Fig. 3.

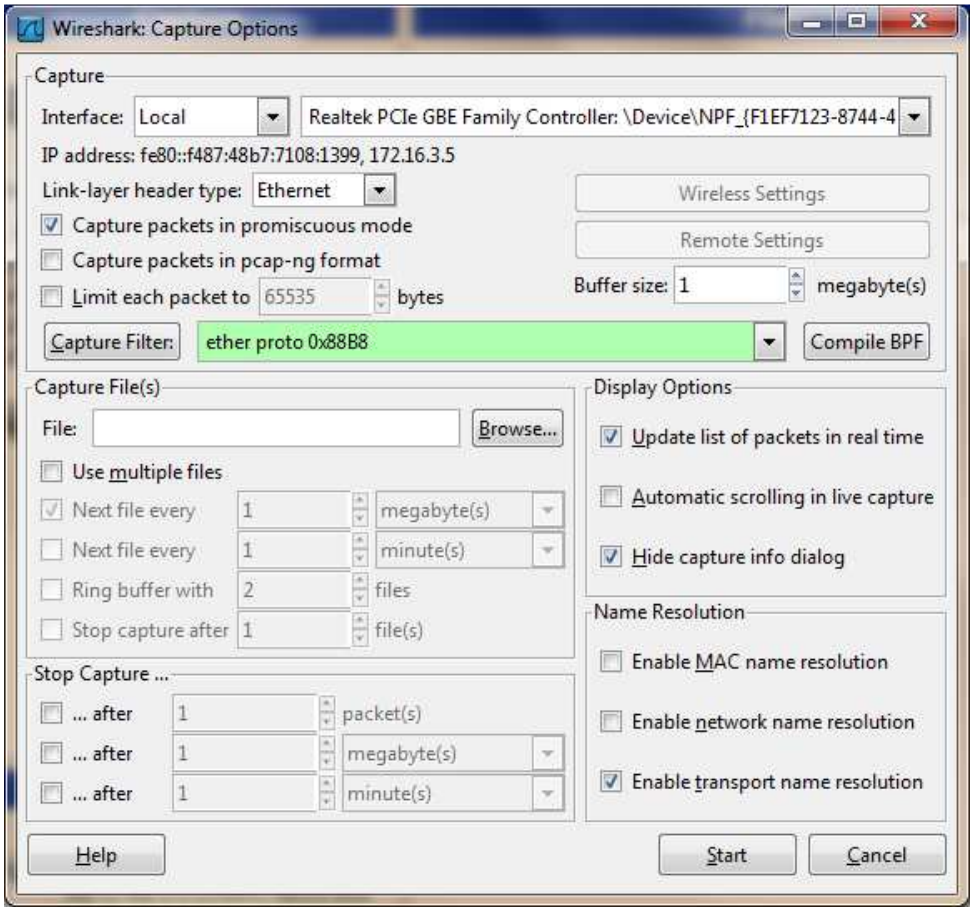

Fig. 3 - Lista de opções para a interface de rede selecionada. Deve-se atentar para que os demais campos (com exceção da Interface) estejam configurados como mostrado na figura. Atente para o campo "Capture Filter", que precisa ser "ETHER PROTO 0x88B8" .

4) Na tela mostrada da Fig. 3, assegure-se que os seguintes itens estejam checados ou habilitados:

- ✓ **Capture packets in promiscuous mode**
- ✓ **Update list of packets in real time**
- ✓ **Hide capture info dialog**
- ✓ **Enable transport name resolution**

Os demais itens devem estar desabilitados. Assegure-se que na caixa de texto ao lado do botão "**Capture Filter**", você tenha digitado:

```
ETHER PROTO 0x88B8
```

Com esses ajustes, o programa Wireshark está apto a capturar quaisquer pacotes do tipo GOOSE (Ethernet Type 0x88B8) que passam pela rede.

5) Para iniciar o processo de captura, clique então no botão "**Start**" na parte inferior da janela da Fig. 3. O programa retorna para janela principal, mostrando uma lista cronológica dos pacotes capturados, atualizada em tempo real. Isso pode ser visto na Fig. 4.

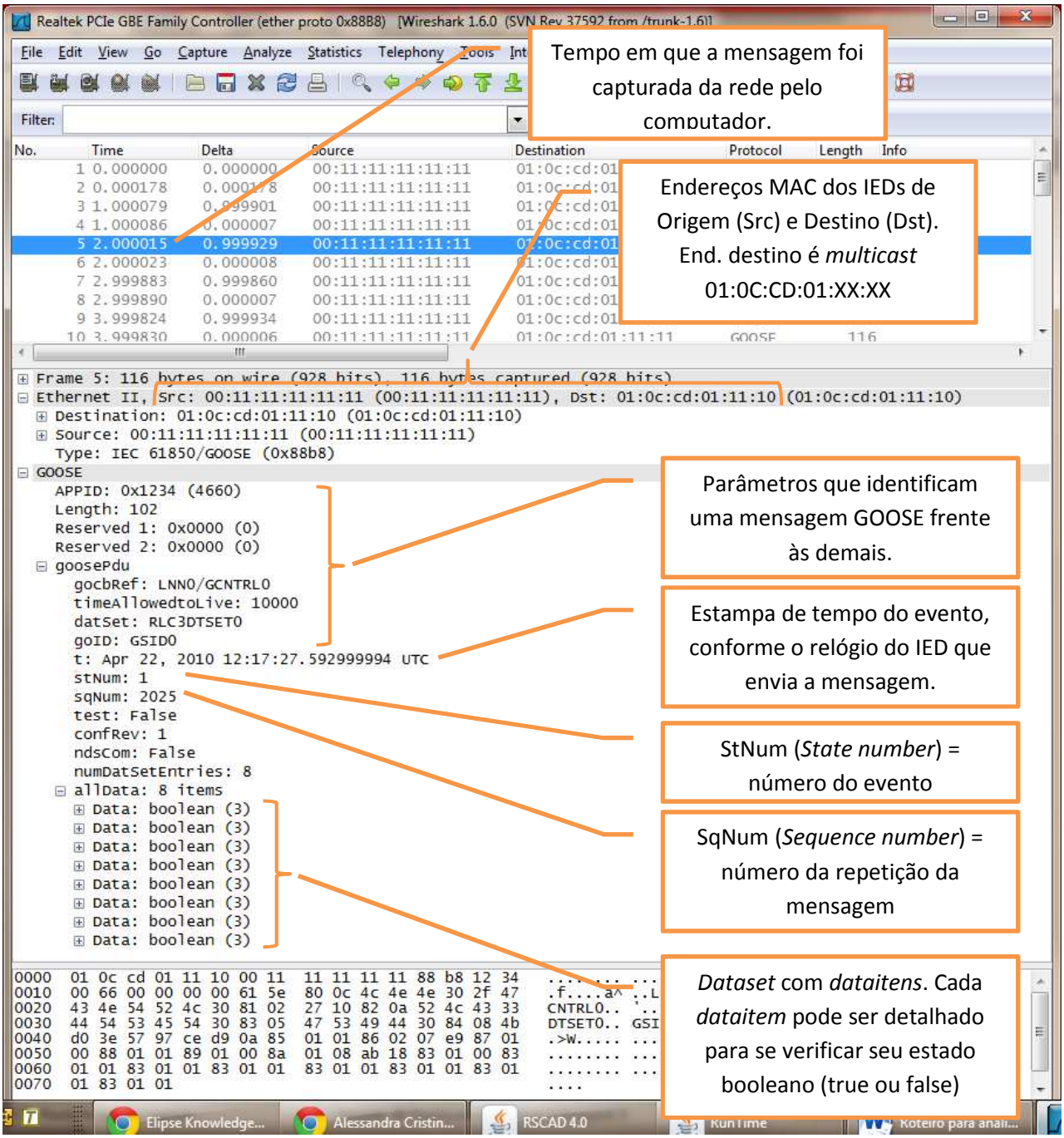

Fig. 4 – Tela do Wireshark durante a captura de mensagens GOOSE que transitam pela rede Ethernet. Na parte superior da tela há uma lista cronológica dos pacotes capturados. Na parte central da tela, uma descrição do conteúdo de um pacote GOOSE selecionado. Na parte inferior é mostrado o conteúdo, *byte* a *byte*, de cada mensagem selecionada.

6) O processo de captura é efetuado continuamente. O usuário pode interrompê-lo a qualquer momento acessando o menu "**Capture**", opção "**Stop**" (ou CTRL+E).

7) Os pacotes coletados podem ser inspecionados individualmente, bastando clicar sobre a mensagem na parte superior da janela do Wireshark. As informações da mensagem selecionada são mostradas, e o usuário pode verificar quaisquer detalhes internos do pacote GOOSE clicando-se sobre as árvores de opções, mostradas na parte central da tela.

8) Deve-se notar que **todas** as mensagens GOOSE, incluindo as repetições de cada evento, são mostradas. Para se simplificar a interpretação do fluxo de mensagens, pode-se instruir o Wireshark a filtrar as mensagens capturadas, de forma a exibir apenas aquelas enviadas nos instantes iniciais de cada evento. Para isso, deve-se escrever na caixa de texto "**Filter**" na parte superior da tela, a seguinte expressão:

```
goose.sqNum == 0
```

Atenção 1: há dois sinais de igual na expressão acima.
Atenção 2: o Wireshark é sensível a maiúsculas e minúsculas nesse campo "Filter".

Dessa, forma, apenas as mensagens GOOSE com *Sequence Number* igual a zero serão exibidas, ou seja, aquelas mensagens enviadas no instante imediato de um evento.

9) É importante notar que a estampa de tempo dos pacotes capturados pelo Wireshark está sincronizada ao relógio do computador que executa o programa. Esse relógio pode não estar sincronizado com a base de tempo usada como sincronismo para os IEDs da subestação. Dessa forma, a análise da troca de mensagens GOOSE entre equipamentos pode estar com algum atraso ou adiantamento com relação ao registro de eventos interno dos IEDs.

10) Todos os pacotes coletados pelo programa podem ser armazenados em disco para análise posterior. Para isso, deve-se clicar no menu "File", opção "Save", e escolher o nome de um arquivo para a gravação das informações coletadas. O arquivo, de formato ".pcap", pode ser transportado e aberto em qualquer computador que possua instalado o Wireshark, para posterior análises e interpretações.

Atividade para laboratório

Após o comissionamento final das subestações, durante um dos eventos que serão gerados aleatoriamente com o RTDS, cada subgrupo deve registrar o tráfego de mensagens GOOSE para análise e detalhamento. O arquivo ".PCAP" obtido deverá ser salvo e entregue via Moodle, junto com o relatório de laboratório, que deve incluir as análises comentadas a seguir.

Atenção: Sugere-se que esse tráfego seja capturado durante um evento de falta com falha de disjuntor.

Cada subgrupo deverá proceder às seguintes análises:

A) Identificar as mensagens GOOSE de cada um dos 9 IEDs configurados pelo arquivo capturado no Wireshark. Criar uma tabela mostrando: o nome do IED, o endereços MAC de origem (Src), destino (Dst) e o valor dos campo APPID e gocbRef (GOOSE Control Block Reference name) da mensagem enviada por cada dispositivo.
B) Constituir uma linha do tempo por dispositivo, mostrando o instante em que cada mensagem foi enviada pela rede Ethernet, e por qual razão. Todas as linhas do tempo devem estar sincronizadas e mostradas na mesma base de tempo. Considere a estampa de tempo de cada mensagem como sendo o tempo apresentado na coluna "Time", mostrada na lista de mensagens da Fig. 4. Verifique no registro de eventos

dos dispositivos, o tempo em que essa informação foi enviada e o tempo em que a informação foi recebida pelos outros IEDs. Um exemplo dessa análise pode ser visto na Fig. a seguir.

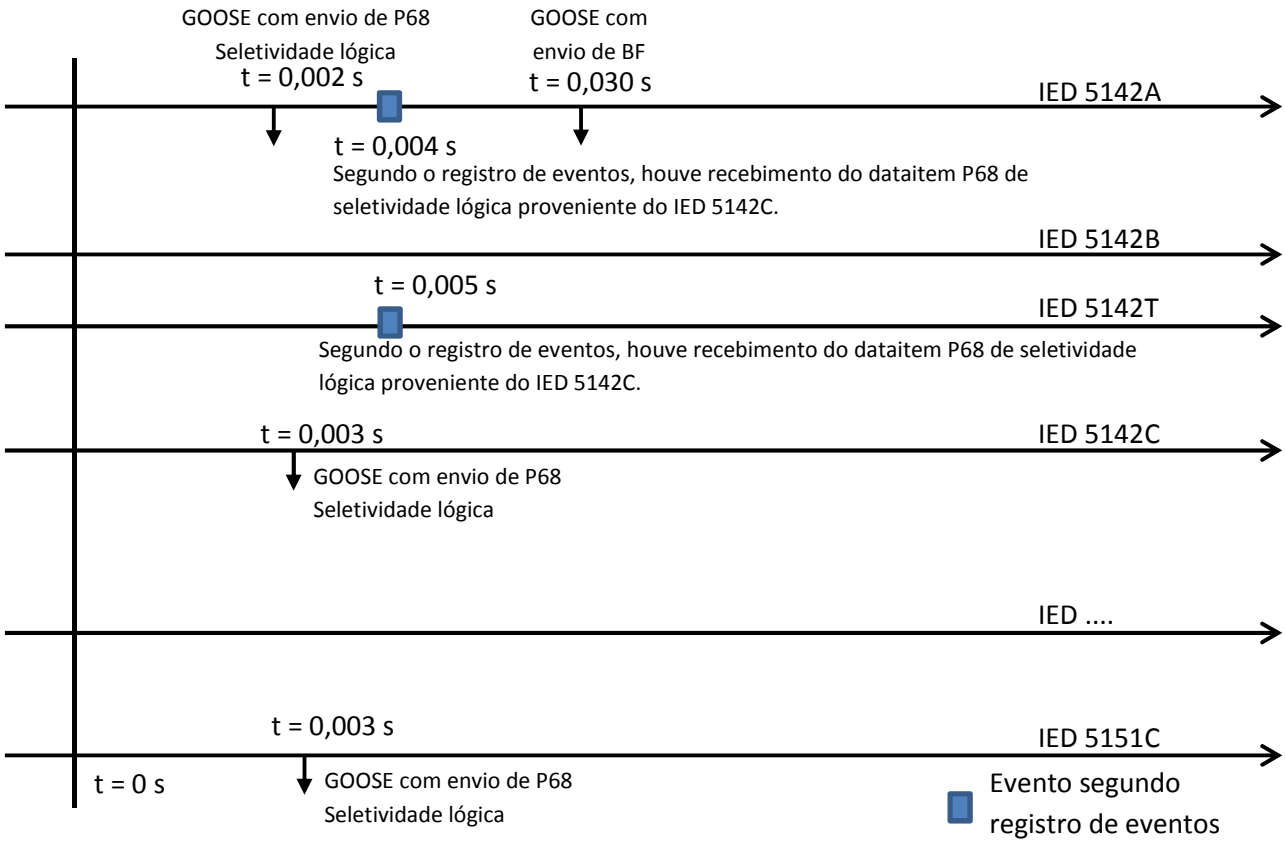

Fig. 5 – Exemplo de análise das informações enviadas pelos IEDs via GOOSE para um evento.