



**XXI SNPTEE  
SEMINÁRIO NACIONAL  
DE PRODUÇÃO E  
TRANSMISSÃO DE  
ENERGIA ELÉTRICA**

Versão 1.0  
23 a 26 de Outubro de 2011  
Florianópolis - SC

**GRUPO -15**

**GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS - GTL**

**SOLUÇÃO PARA MONITORAMENTO DE REDES CONVERGENTES**

**José Flávio de Souza Dias Júnior(\*)  
ELETROBRAS ELETRONORTE**

**RESUMO**

Solução técnica e economicamente viável para monitoramento de redes Ethernet convergentes implantada com sucesso na Regional de Transmissão do Pará – CPA da Eletrobras Eletronorte.

**PALAVRAS-CHAVE**

Redes Convergentes, Monitoramento, Ethernet, IP

**1.0 - INTRODUÇÃO**

A Eletrobras Eletronorte atua no sistema elétrico nacional principalmente como geradora e transmissora de energia elétrica. Possui diversas unidades geograficamente distantes umas das outras, as quais são interligadas por um grande e complexo sistema de telecomunicações.

Como a maioria das empresas deste perfil, possui diversas e importantes redes internas, como a da operação, supervisão, medição e corporativa, as quais normalmente são convergidas para uma única rede a fim de facilitar o seu controle e reduzir custos de transmissão de dados.

A arquitetura básica desta solução de monitoramento de redes convergentes consiste em coletar e armazenar em tempo real informações sobre cada pacote trafegado pela rede, possibilitando a análise sobre a carga e tipos de dados que transpõem a rede convergente, além de possibilitar e facilitar a inferência de informações que ajudam na detecção de invasão e mau uso da rede.

**2.0 - REDES CONVERGENTES**

A indústria de telecomunicações procura, há alguns anos, orientar sua tecnologia de maneira a tornar os operadores competitivos em um ambiente caracterizado pela concorrência e aumento da desregulamentação. As redes de comunicação convergentes, com interfaces abertas e capacidade para transmitir voz, dados, imagens, som e vídeo, exploram plenamente as tecnologias de ponta para oferecer serviços sofisticados e aumentar as receitas dos operadores, reduzindo despesas de investimentos e custos de operação (4).

O conceito convergência pode ser definido de várias maneiras, mas fundamentalmente é a integração dos serviços de: dados, voz e vídeo, ou comumente chamado de triple play, em um único serviço. As redes de nova geração devem seguir os seguintes preceitos (3):

- a. Qualidade de serviço (QoS) – mudança da filosofia da rede de dados de menor esforço (best effort) para alta-qualidade (high-quality) e tempo real;

(\*) Eletrobras Eletronorte - Regional de Transmissão do Pará, Bloco B – CEP 66.077-830 Belém, PA – Brasil  
Tel: (+55 91) 3210-8281 – Email: joseflaviojr@eletronorte.gov.br

- b. Confiabilidade – garantir os SLA's, ou seja, os requisitos mínimos aceitáveis para o serviço proposto, mesmo durante falha de elementos;
- c. Escalabilidade – capacidade para crescer da menor para a maior rede;
- d. Uso eficiente dos recursos – economizar investimentos em infraestrutura;
- e. Operação simplificada da rede – reduzir custos operacionais.

### 3.0 - MONITORAMENTO

Segundo Bartle (1), monitoramento é a observação e o registro regular das atividades de um projeto ou programa. É um processo rotineiro de acúmulo de informações do projeto em todos os seus aspectos. Monitorar é checar o progresso das atividades do projeto, ou seja, uma observação sistemática e com propósitos.

Monitorar é também dar um retorno sobre o projeto aos seus colaboradores, implementadores e beneficiários. A criação de relatórios permite que todas as informações reunidas sejam usadas na tomada de decisões em prol da aperfeiçoamento da performance do projeto.

No caso da Eletrobras Eletronorte, dentre os principais objetivos com o monitoramento das redes convergentes, podemos citar:

- a. Estatística – quantificar, classificar e estipular o consumo de cada rede e serviço;
- b. Suporte e Qualidade – auxiliar na alocação, configuração e utilização de recursos;
- c. Segurança – observar o comportamento da rede e identificar possíveis invasões, vírus e outros maus usos.

### 4.0 - SOLUÇÃO PARA MONITORAMENTO DE REDES CONVERGENTES

A arquitetura básica desta solução consiste em coletar e armazenar em tempo real informações sobre cada pacote trafegado pela rede, analisando-os periodicamente de forma estratégica.

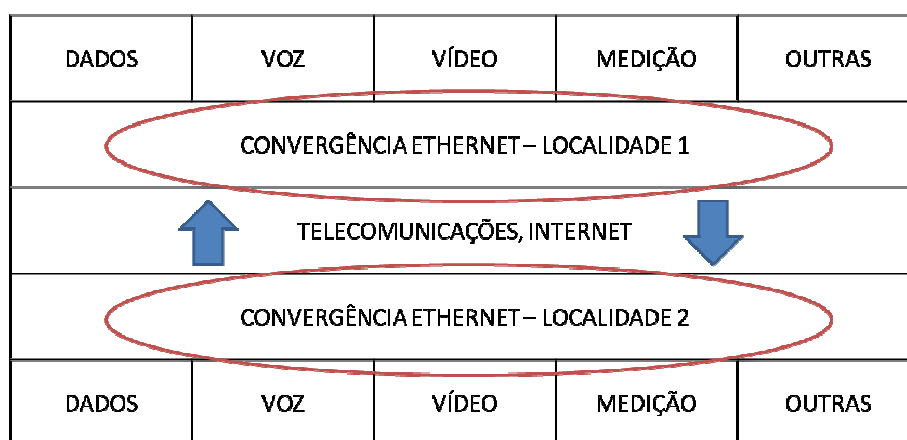


FIGURA 1 – Foco do monitoramento na arquitetura comum de redes convergentes

A Figura 1 demonstra em forma de camadas que o monitoramento se concentra na transposição das redes convergentes, isto é, a coleta de dados ocorre após a convergência, ainda em Ethernet, garantindo absorção de 100% de todo o tráfego entre duas localidades.

#### 4.1 Metodologia

O monitoramento realizado com esta solução é composto por 5 etapas:

- 1ª. Interceptação dos pacotes em tráfego
- 2ª. Coleta sintetizada de todo o tráfego
- 3ª. Armazenamento contínuo em disco

4ª. Processamento analítico dos dados armazenados

5ª. Geração de relatórios diversos

As 3 primeiras etapas são agrupadas no processo denominado Coleta, realizado concomitantemente a um outro processo responsável pelas últimas 2 etapas, o qual denomina-se Análise.

A Coleta fica em execução constante, esperando, capturando, resumindo e armazenando cada pacote da rede. Já a Análise fica em eterna dependência da Coleta, processando, inferindo e gerando/atualizando cada relatório solicitado de acordo com os dados até então registrados.

#### 4.2 Implementação

A solução foi implementada com um computador pessoal com hardware moderado, por exemplo Core 2 Duo, 2 GB de memória, 250 GB de disco e placa de rede Gigabit Ethernet. O computador é conectado a uma porta-espelho do switch responsável pela convergência da rede, através da qual se tem acesso a todos os dados trafegados, os quais são resumidos e armazenados em disco para análise especializada, que pode ser feita remotamente com a instalação de uma segunda placa de rede.

Tanto a Coleta quanto a Análise foram compostas totalmente com softwares livres, desenvolvidos em padrão largamente aceito e devidamente testados, o que reduziu o custo da solução ao custo de um computador pessoal, pois não foi necessária a aquisição de licenças e nem de consultoria/treinamento específico.

A Figura 2 demonstra a infraestrutura da solução.



FIGURA 2 – Infraestrutura básica da solução de monitoramento

##### 4.2.1 Intercepção dos pacotes em tráfego.

A intercepção é realizada ligando-se um computador-monitor a uma porta-espelho do switch responsável pela convergência da rede, como se pode ver na Figura 3. Este computador deve possuir uma placa de rede com velocidade compatível com a carga total da convergência e deve ser colocada em modo promíscuo a fim de se obter todos os pacotes, além de não interferir na rede.

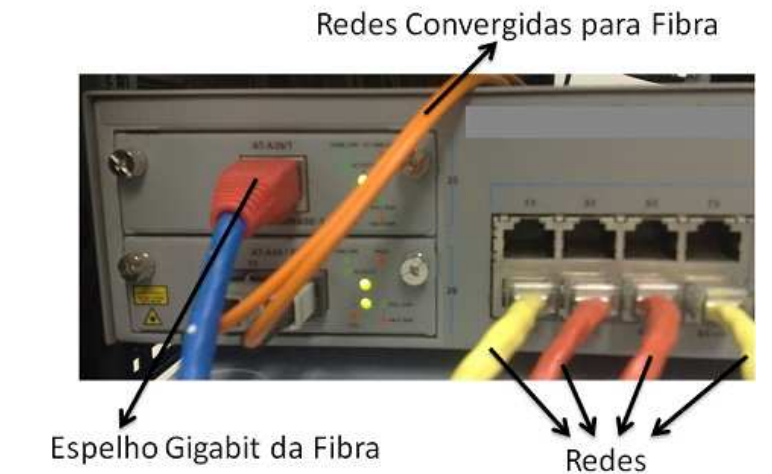


FIGURA 3 – Exemplo de interceptação: espelhamento da convergência

#### 4.2.2 Coleta sintetizada de todo o tráfego e Armazenamento contínuo em disco.

As etapas 2 e 3 são praticamente atendidas com a ferramenta TCPDump (5), software livre para captura e armazenamento de pacotes Ethernet. Vale ressaltar que a Aranha (2) conta com uma eficiente ferramenta de controle de espaço livre, a qual elimina dados mais antigos na necessidade de se armazenar dados recentes.

#### 4.2.3 Processamento analítico dos dados armazenados.

Esta solução, para fins de processamento e análise estratégica dos pacotes coletados, aconselha a ferramenta Aranha (2), a qual reconhece o formato de armazenamento da TCPDump (5) e oferece uma gama de utilidades como: análise a medida que pacotes são armazenados, controle de espaço livre em disco, geração de diversos relatórios portáteis e personalizáveis, etc. Além do mais, a Aranha é software livre e implementada em Java, podendo facilmente agregar novas funcionalidades através de reimplementação ou componentização. Contudo, para fins de análise individual mais aprofundada de cada pacote coletado, a solução aponta a ferramenta de análise de protocolos Wireshark (6).

#### 4.2.4 Geração de relatórios diversos.

Como antes mencionado, a solução usufrui dos recursos da ferramenta Aranha (2), a qual gera relatórios portáteis e personalizáveis. Vale ressaltar que tais relatórios também são periodicamente atualizados, refletindo em seus resultados as informações extraídas dos pacotes até então coletados.

Os relatórios normalmente são gerados no formato CSV, sendo possível com ele, por exemplo, a plotagem de gráficos com ferramentas de planilhas eletrônicas. Contudo, a Aranha fornece ferramentas de plotagem e amostragem de dados autoatualizáveis, como podemos verificar nas Figuras 4 e 5.

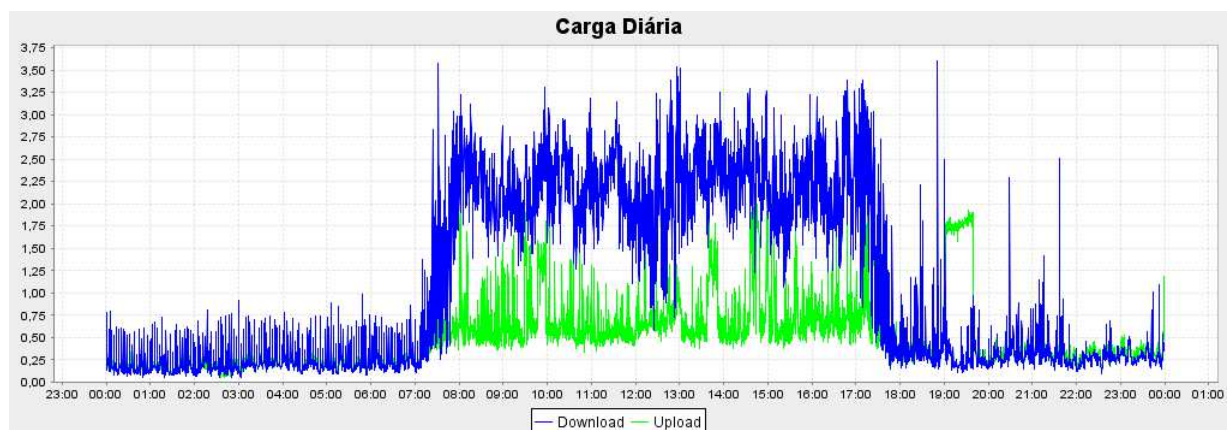


FIGURA 4 – Exemplo de Relatório de Carga Total Diária em Mbps

A Figura 4 exemplifica a ferramenta de plotagem de carga em Mbps, a qual é totalmente personalizável. Ela pode conter inúmeras séries referenciando IP's, MAC's e/ou QoS. Os IP's ainda podem ser mascarados; exemplo: "10.0.\*.\*".


Medição Individual						
PE = 31095033 / PR = 31095033						
BE = 13475160767 / BR = 13475160767						
Nodo	PE	PR	BE	BR	PT	(BT)
10.61.116.65	10,5	10,1	27,3	4,3	10,3	15,8
10.61.116.93	5,2	5,4	13,0	4,2	5,3	8,6
10.5.0.10	3,7	2,6	8,6	0,9	3,1	4,8
10.54.0.122	1,3	2,3	0,2	7,6	1,8	3,9
10.61.116.45	2,2	2,0	7,1	0,4	2,1	3,7
10.5.0.6	6,2	6,0	4,2	2,5	6,1	3,4
10.98.0.10	1,8	1,5	5,0	0,3	1,6	2,6
10.5.2.25	7,0	4,7	1,7	3,5	5,9	2,6
10.61.116.54	6,9	9,5	2,7	2,5	8,2	2,6
10.5.5.24	1,1	1,1	1,9	0,4	1,1	1,1
10.5.3.136	0,4	0,6	0,2	1,7	0,5	0,9
10.5.5.10	0,7	0,4	1,7	0,2	0,5	0,9
10.5.2.238	0,5	0,3	1,2	0,4	0,4	0,8
	1-PE	2-PR	3-BE	4-BR	5-PT	6-BT
P=Pacotes B=Bytes E=Enviados R=Recebidos T=Total						
Ranking: +  - Passo=1 P-Pausar						

FIGURA 5 – Exemplo de Medição Individual de Pacotes e Bytes por IP, em %

Podemos verificar na Figura 5 a contabilização de pacotes (PE=enviados, PR=recebidos, PT=total) e bytes (BE=enviados, BR=recebidos, BT=total) por IP, sendo possível também a contabilização por MAC. O período dessa medição é configurável e autoatualizável. No exemplo, a medição está ordenada por BT (Bytes Total), em percentagem quanto ao total geral.

## 5.0 - CONCLUSÃO

O monitoramento permite a mensuração da rede, identificando seus pontos fortes e fracos, e auxilia na garantia de qualidade do serviço, alinhando estrategicamente a Tecnologia da Informação e Comunicação com os objetivos da corporação e, neste caso, do sistema elétrico nacional.

Vale ressaltar a devida importância do monitoramento desse tipo de rede, pois nela trafegam importantes e sigilosos dados de operação e supervisão de equipamentos elétricos, os quais devem funcionar ininterruptamente com qualidade.

O monitoramento de redes convergentes permite quantificar, classificar e estipular o consumo de cada rede e serviço, auxiliando na alocação e configuração de recursos, principalmente os relacionados com roteadores e demais equipamentos para telecomunicação.

Esta solução permite observar o comportamento da rede e identificar possíveis invasões, vírus e outros maus usos, como downloads indevidos e usufruto de ferramentas corporativamente proibidas. Além disso, utiliza softwares livres na base da arquitetura, amplamente aceitos e utilizados no mundo, garantindo um núcleo funcional consistente e estável, além de obter melhorias constantes e reduzir custos de licença. E os resultados são confiáveis e exatos, pois a análise é baseada em histórico completo de período de tempo da rede (coleta contínua de todo tráfego com sistema de armazenamento dedicado).

Quanto à implantação, dada a importância dos serviços de rede no contexto do sistema elétrico nacional, o custo financeiro desta solução é desprezível economicamente.

## 6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) BARTLE, P. Handbook of Monitoring. <http://www.scn.org/cmp/hemon.txt>, Dezembro 2003.

(2) JÚNIOR, J.F.D.S.D. Aranha. <http://www.joseflavio.com/aranha/>, 2010.

- (3) LIOTINE, M. Mission-Critical Network Planning. Artech House Telecommunications, 2003.
- (4) NASSIF, A.T. Redes da próxima geração: aspectos técnicos, econômicos e cenários de migração. Dissertação de Mestrado. Departamento de Engenharia Elétrica, Universidade de Brasília, 2004. Brasil.
- (5) JACOBSON V., LERES C., MCCANNE S. et al. TCPDump. <http://www.tcpdump.org/>, 2010.
- (6) COMBS, G. et al. Wireshark. <http://www.wireshark.org/>, 2010.

## 7.0 - DADOS BIOGRÁFICOS

Nome: José Flávio de Souza Dias Júnior

Naturalidade: Tucuruí-PA, Brasil, 25 de abril de 1985

Graduação: Universidade Federal do Pará-UFPA, Belém-PA, 2009

Experiência profissional: Eletrobras Eletronorte, 2007-Hoje, Téc. em Processamento de Dados