Gerenciamento de Redes HFC: Nagios vs. Visium

Elaborador:	Renan Aparecido Casseta
Orientador:	Rogério Nunes de Freitas

FACULDADE DE TECNOLOGIA DE AMERICANA

Renan Aparecido Casseta

Gerenciamento de Redes HFC: Nagios vs. Visium

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação

Americana, 18 de Maio de 2020.

Banca Examinadora:

_____

Rogério Nunes de Freitas (Presidente)

Mestre

Fatec Americana

_____

Edson Roberto Gaseta

Mestre

Fatec Americana

_____

Ana Lúcia Spigolon

Especialista

Fatec Americana

SUMÁRIO

1 INTRODUÇÃO

É indiscutível que o monitoramento dos ativos de rede é de fundamental importância para o bom funcionamento da infraestrutura de T.I. (Tecnologia da Informação). Com o crescimento da Internet no final dos anos 90, passamos a ter sistemas e redes cada vez maiores e mais complexas, com um grande número de equipamentos, diferentes tecnologias e fabricantes.

Em consequência disso, aconteceu uma grande evolução nas ferramentas de monitoramento, pois as organizações buscam cada vez mais a disponibilidade de seus serviços, identificando falhas e perdas de conexão de maneira proativa, o que outrora era identificado apenas de forma reativa.

2 Objetivo deste documento

Como a migração do monitoramento da rede HFC (Hybrid Fiber-Coaxial) do Nagios para o Visium Live reduziu o tempo de análise dos incidentes emergenciais de infraestrutura e consequentemente o tempo de recuperação da falha por parte da equipe de campo?

Este relatório técnico visa demonstrar as vantagens obtidas pelo NOC (Network Operations Center) de uma grande empresa do setor de telecomunicações, ao realizar a migração para uma nova ferramenta de monitoramento, o Visium Live, onde anteriormente era utilizado apenas o Nagios, para monitorar toda a sua infraestrutura de rede HFC em 84 cidades do estado de São Paulo.

O objetivo geral ao longo do relatório será comparar as funcionalidades presentes em ambas às ferramentas e demonstrar as novas funções que o Visium Live trouxe ao departamento, que contribuíram de maneira positiva para que houvesse a otimização no tempo de análise dos incidentes, a redução no tempo de recuperação das falhas de infraestrutura e o aumento dos incidentes identificados de maneira proativa, através de alarmes.

3 Referencial Teórico

Durante esse capítulo serão abordados conceitos, ferramentas e protocolos referentes ao monitoramento de rede, de forma a facilitar o entendimento dos pontos que serão discutidos no decorrer deste relatório técnico.

3.1 Gerenciamento de rede

Quando se fala em gerenciamento de rede, Saydam (1996, p. 581) declara que:

> *Gerenciamento de rede inclui a implementação, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer as exigências operacionais, de desempenho e de qualidade de serviço a um custo razoável.*

Uma parte fundamental no gerenciamento de redes é o NOC (***Network Operations Center*** ou Centro de Operações de Rede), que segundo Kurose (2013) é um departamento responsável por monitorar todos os aspectos de uma rede e o desempenho dos serviços todos os dias do ano, 24 horas por dia, utilizando processos e ferramentas.

A ***International Organization for Standardzation*** (ISO) 7498-4 segmenta o gerenciamento de rede em cinco áreas:

- Gerenciamento de Desempenho;
- Gerenciamento de Falhas;
- Gerenciamento de Configuração;
- Gerenciamento de Contabilização;
- Gerenciamento de Segurança.

No cenário deste relatório, o NOC tem como foco o gerenciamento de desempenho e falhas de uma rede HFC, ou seja, manter a rede operando dentro das condições predefinidas, detectando e sanando os problemas que estejam impactando ou possam vir a impactar os clientes desta rede.

3.2 Rede HFC (Híbrida Fibra-Coaxial)

Segundo Kurose (2013), uma rede pode ser denominada híbrida fibra-coaxial quando o sinal chega através de um cabo de fibra ótica ao terminal de distribuição da região (*node* ou nó óptico) e a partir dela é utilizado o cabo coaxial para chegar às casas e apartamento dos clientes, conforme apresentado na figura 1. Cada *node*, equipamento que transforma o sinal de luz para RF (radiofrequência), tem capacidade para atender de 500 a 5000 residências.

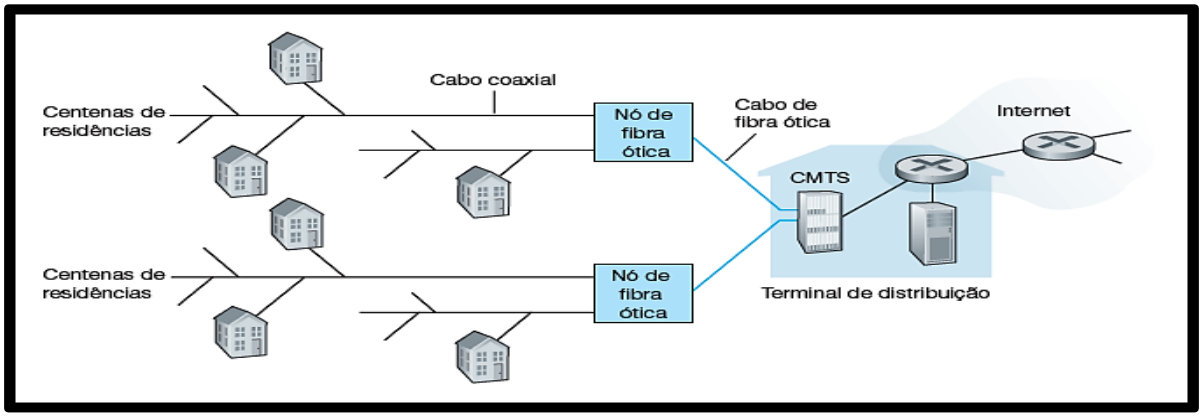
Para que o assinante acesse a Internet a cabo é necessário utilizar um *cable modem* (modem a cabo), conectando-o ao computador através da porta *Ethernet*.

Ainda a respeito da rede coaxial, Kurose (2013, p. 34), declara:

> *Uma característica importante do acesso a cabo e o fato de ser um meio de transmissão compartilhado. Em especial, cada pacote enviado pelo terminal viaja pelos enlaces downstream até cada residência e cada pacote enviado por uma residência percorre o canal upstream até o terminal de transmissão. Por essa razão, se diversos usuários estiverem fazendo o download de um arquivo em vídeo ao mesmo tempo no canal downstream, cada um recebera o arquivo a uma taxa bem menor do que a taxa de transmissão a cabo agregada. Por outro lado, se há somente alguns usuários ativos navegando, então cada um poderá receber páginas da Web a uma taxa de downstream máxima, pois esses usuários raramente solicitarão uma página ao mesmo tempo. Como o canal upstream também e compartilhado, e necessário um protocolo de acesso múltiplo distribuído para coordenar as transmissões e evitar colisões.*

A Figura 1 exibe uma rede de acesso híbrida fibra-coaxial.

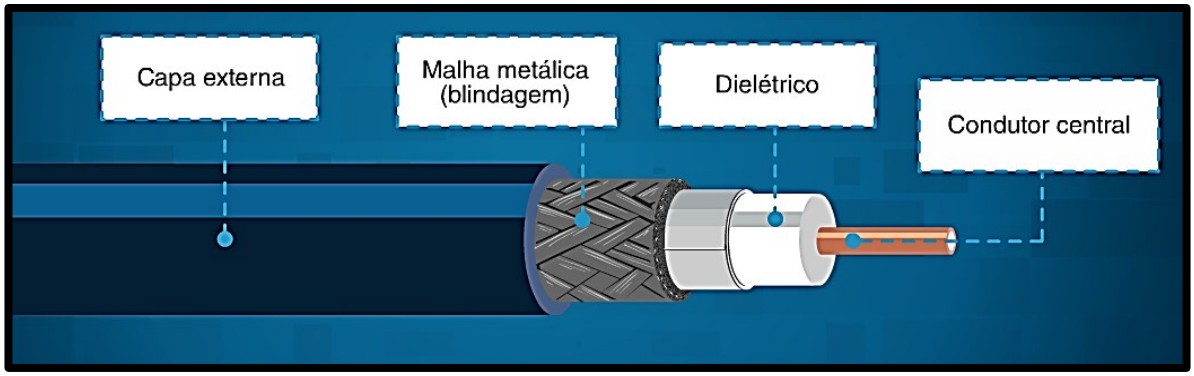
Figura 1- Rede de acesso híbrida fibra-coaxial



Fonte: KUROSE, Jim; ROSS, Keith (2013)

O cabo coaxial, de acordo com Kurose (2013), é constituído de dois condutores de cobre concêntricos, podendo alcançar taxas altas de transmissão de dados devido a essa configuração. Dessa forma, os cabos coaxiais tornaram-se muito comuns em sistemas de televisão e Internet a cabo. Na Figura 2 pode-se identificar os principais componentes da estrutura de um cabo coaxial.

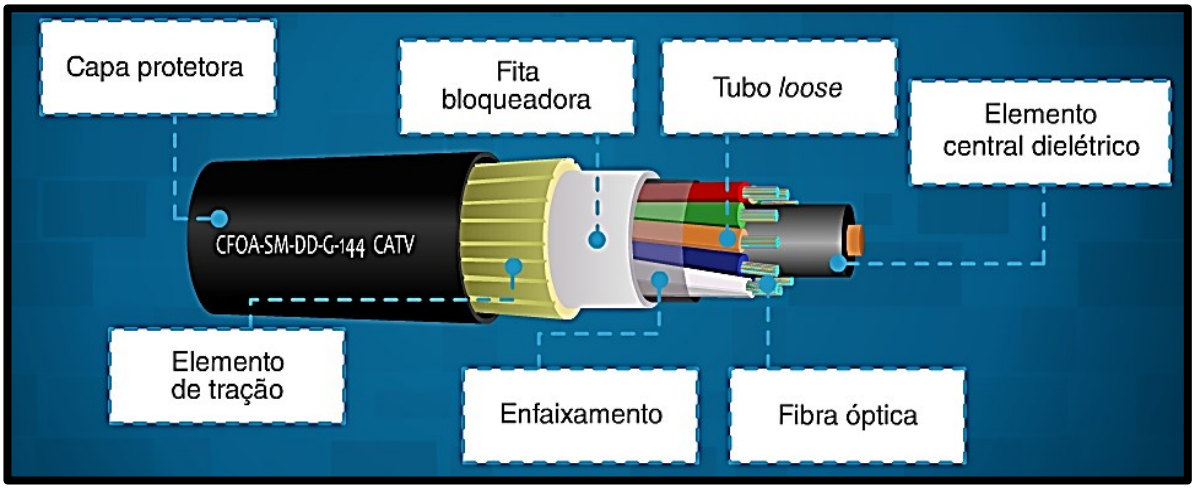
Figura 2- Estrutura do cabo coaxial



Fonte: Site de treinamento interno

A fibra ótica é um meio delgado e flexível que conduz pulsos de luz, cada um deles representando um bit. Fibras óticas são imunes à interferência eletromagnética, têm baixíssima atenuação de sinal até cem quilômetros (KUROSE, 2013). Na Figura 3 pode-se observar todos os itens que compõem a estrutura de um cabo de fibra óptica.

Figura 3- Estrutura do cabo de fibra óptica



Fonte: Site de treinamento interno

3.3 Protocolo SNMP (*Simple Network Management Protocol*)

Segundo Kocjan (2014), o protocolo SNMP foi desenvolvido, no final dos anos 80, para monitorar e gerenciar sistemas e dispositivos conectados a uma rede, atuando na camada de aplicação do TCP/IP e utilizando o protocolo de transporte UDP na porta 161.

Como demonstrado na Figura 4, o SNMP é usado para transmitir informações e comandos entre uma entidade gerenciadora e um agente que os executa em nome da entidade dentro de um dispositivo de rede gerenciado. (KUROSE, 2013).

Ele tem como seu principal objetivo estabelecer um padrão para a comunicação, independente do fabricante do equipamento, e facilitar a troca de informações entre os dispositivos, enviando notificações caso haja falha em algum serviço ou dispositivo.

Referente às principais utilizações do protocolo SNMP, Kurose (2013, p. 591), afirma:

> *A utilização mais comum do SNMP é em um modo comando-resposta, no qual a entidade gerenciadora envia uma requisição a um agente, que a recebe, realiza alguma ação e envia uma resposta a requisição. Em geral, uma requisição é usada para consultar (recuperar) ou modificar (definir) valores de objetos MIB associados a um dispositivo gerenciado. Um segundo uso comum do SNMP é para um agente enviar uma mensagem não solicitada, conhecida como mensagem trap, à entidade gerenciadora. As mensagens trap são usadas para notificar uma entidade gerenciadora de uma situação excepcional que resultou em mudança nos valores dos objetos MIB.*

Ainda segundo Kurose (2013), para o monitoramento da rede HFC, o SNMP fornece uma funcionalidade importante, o SNMP *trap*, que permite um agente enviar uma notificação ao gerente de que seu status foi alterado, o que pode indicar que há uma falha naquele dispositivo. Em uma rede gerenciada utilizando o protocolo SNMP temos três componentes importantes:

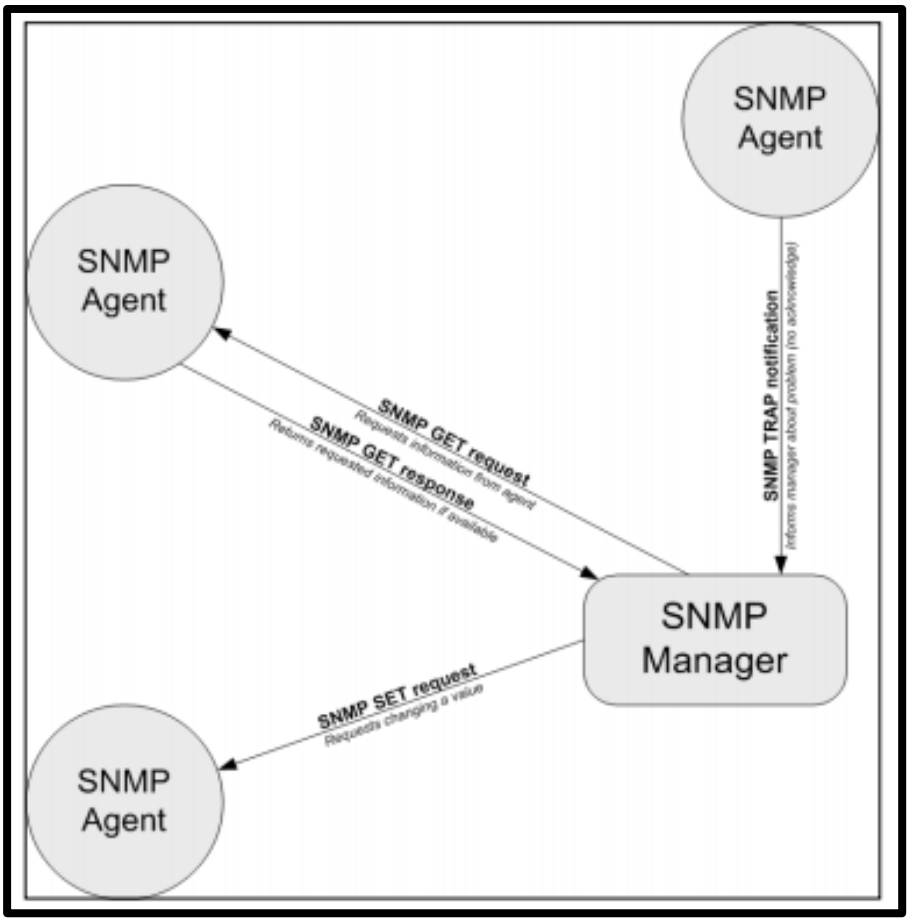
- **Gerente**: Interface de gerenciamento que envia e recebe requisições SNMP aos agentes.
- **Agente**: Está associado ao dispositivo ou sistema que está presente na rede, seu papel é responder as requisições realizadas pelo gerente e encaminhar notificações caso haja mudança de status ou atinja algum parâmetro previamente configurado, através do SNMP trap.
- **MIB (*Management Information Base*):** Base de dados com objetos que podem representam o status dos dispositivos da rede.

Ao utilizar o SNMP para o gerenciamento da rede, podemos obter diversas vantagens e benefícios, como exemplo:

- Pode ser utilizado para gerenciar dispositivos de diversos fabricantes;
- Consome poucos recursos da rede;
- Aumento da disponibilidade dos sistemas, serviços e dispositivos presentes na rede;
- Agilidade na identificação de falhas na rede.

A Figura 4 mostra o modelo de gerenciamento de SNMP.

Figura 4- Modelo de gerenciamento do SNMP



Fonte: KOCJAN, Wojciech (2014)

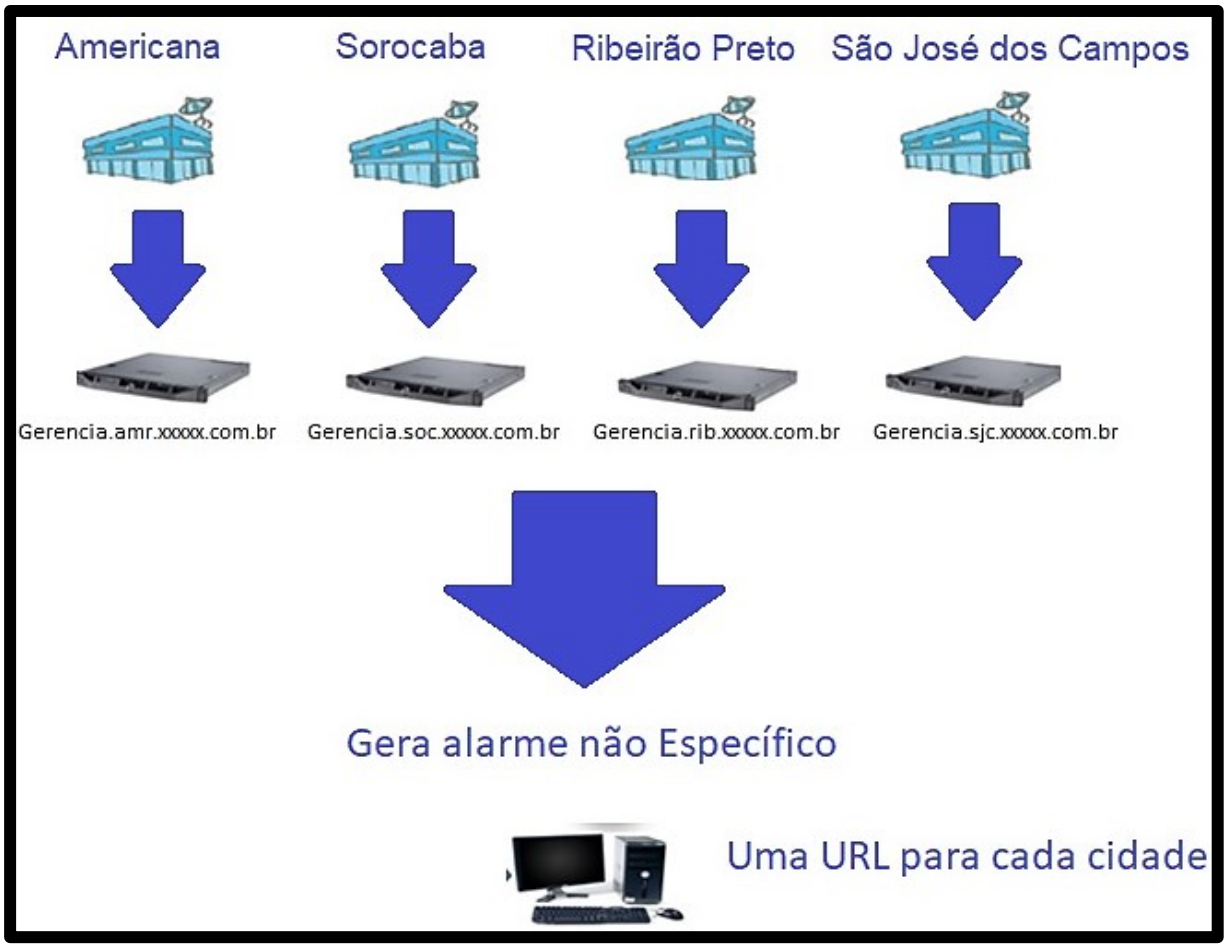
3.4 NAGIOS

De acordo com Kocjan (2014), o Nagios é uma ferramenta de código aberto para monitoramento de sistemas, redes e infraestrutura, desenvolvida por Ethan Galstad. A aplicação oferece recursos de monitoramento e alarmes para os serviços e ativos monitorados.

Os servidores do Nagios são responsáveis pela coleta de informações diretamente dos pontos de concentração (*Heandend*), realizando requisições ao CMTS (***Cable Modem Termination System***) através do protocolo SNMP. O CMTS é um equipamento instalado no *headend* para liberação do sinal de retorno, realizando a comunicação com a rede HFC através das placas cable, que faz a interface entra o CMTS e o sinal RF da rede HFC.

A Figura 5 mostra a antiga infraestrutura utilizada pela empresa, em que cada operação possuía um servidor Nagios, dessa forma havia uma página web do Nagios para cada cidade, totalizando 64 páginas de monitoramento para as cidades do interior de São Paulo e 20 para as cidades da região metropolitana de São Paulo.

Figura 5- Estrutura do Nagios



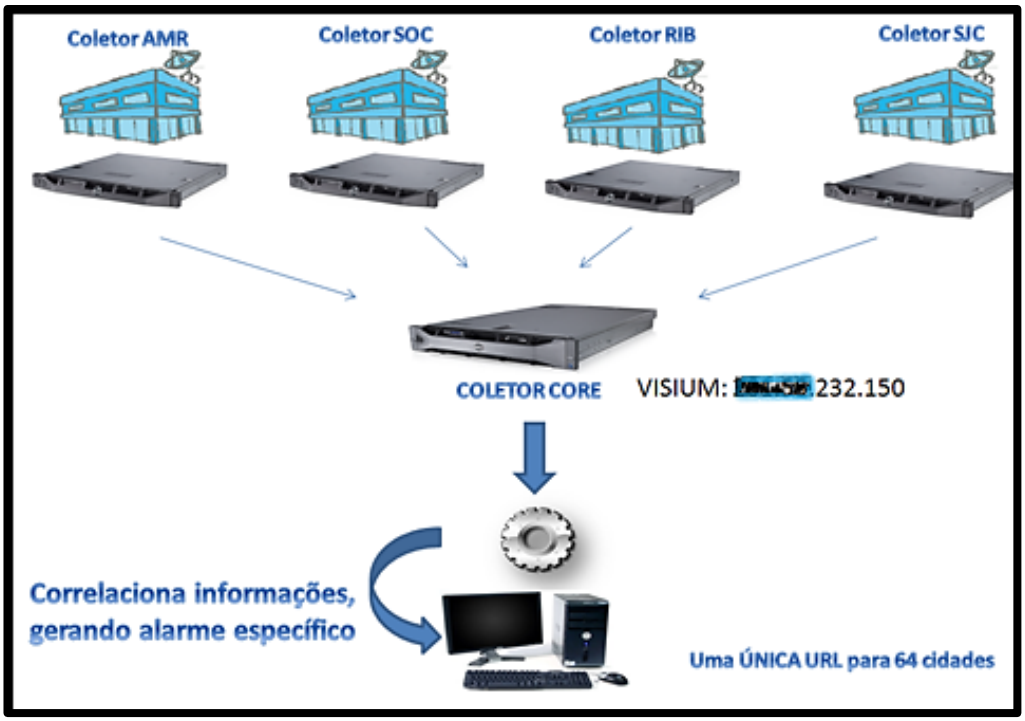
Fonte: Autor

3.5 Visium Live

Segundo Humberto Pinheiro, CEO da Visium Soluções em TI, o Visium Live é uma solução de monitoramento e gerência de incidentes de infraestrutura para rede HFC, modular, escalável e baseada no protocolo SNMP.

Conforme Figura 6, a estrutura do Visium também utiliza um servidor (Coletor Visium) para cada operação, que é responsável por efetuar as requisições SNMP aos equipamentos, realizar coletas e tratamento de dados de monitoração e encaminha-los ao núcleo de inteligência, o servidor Coletor Core, que consolida os dados de todos os servidores de coleta, disponibilizando em apenas uma página Web, o monitoramento de todas as operações.

Figura 6- Estrutura do Visium Live



Fonte: Autor

4 Comparando funcionalidades em comum

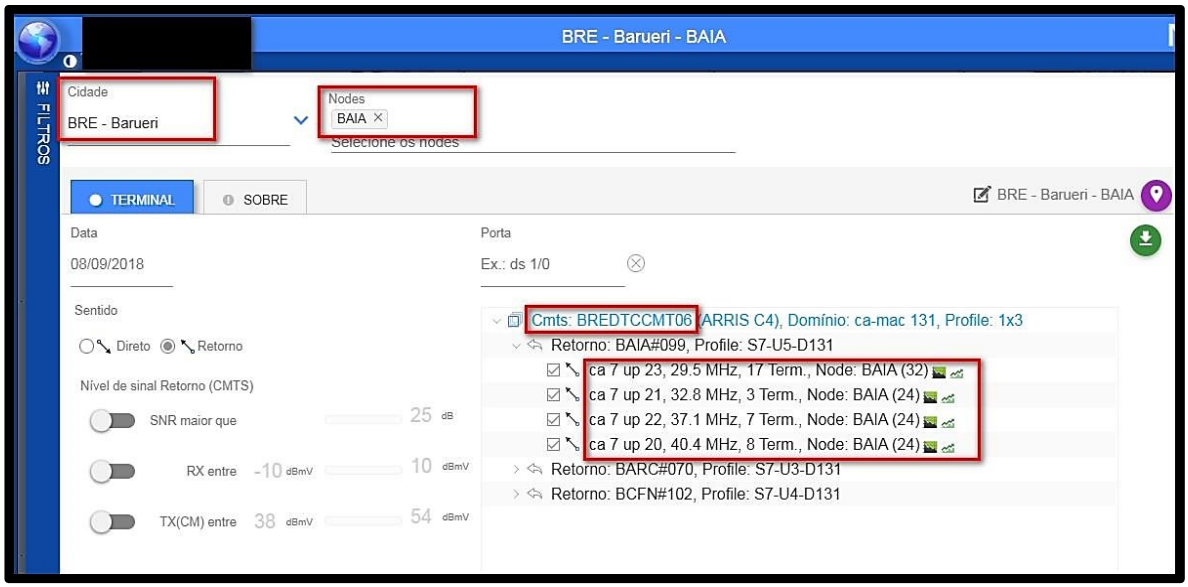
As funcionalidades das ferramentas são utilizadas para monitorar a rede HFC, gerando gráficos de fácil visualização para o usuário final, auxiliando na identificação e acompanhamento de eventos massivos.

Nesse capítulo serão comparadas as funcionalidades em comum nas duas ferramentas.

4.1 Consulta node

Para realizar uma consulta a um *node* no Nagios, primeiramente é necessário saber em qual CMTS e placa *cable* esse node está alocado. Para obter essa informação é preciso acessar outro sistema interno, que contém esses dados sobre os *nodes*, como pode ser visto na Figura 7.

Figura 7- Sistema de consulta interface



Fonte: Autor

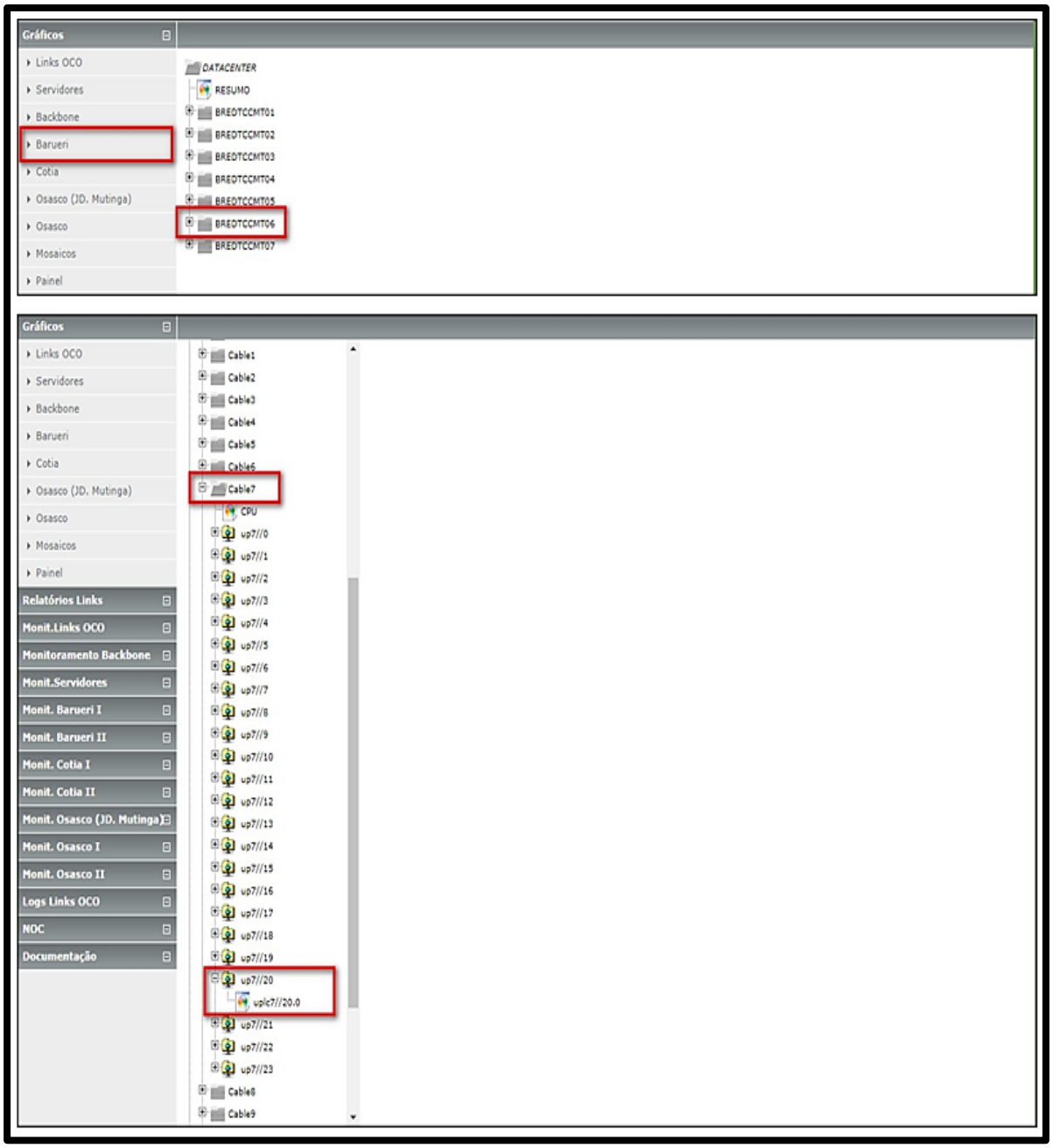
Com essas informações, o próximo passo é acessar o Nagios da cidade desejada e inserir o usuário e senha, conforme Figura 8.

Figura 8- Tela de *login* do Nagios

Fonte: Autor

Após o *login* ter sido realizado com sucesso, na barra lateral, seleciona-se a opção de gráficos, conforme Figura 9. Em gráficos, seleciona-se a cidade, o CMTS e as placas *cable* que foram obtidos anteriormente.

Figura 9- Seleção do CMTS e placa *cable*



Fonte: Autor

Seguindo todos esses passos, o gráfico do node desejado será exibido, conforme Figura 10, e o analista poderá começar a sua análise, podendo verificar os níveis de ruído e quantidade de clientes online em determinada placa.

Figura 10- Gráfico Nagios

Fonte: Autor

Diferente da consulta no Nagios, no Visium Live não é necessário realizar consultas em outros sistemas e seguir diversos passos para a visualização dos gráficos dos *nodes*.

Após o login no sistema, acessar no menu superior a opção de gráficos e em seguida, no menu lateral, a opção *node*, conforme Figura 11.

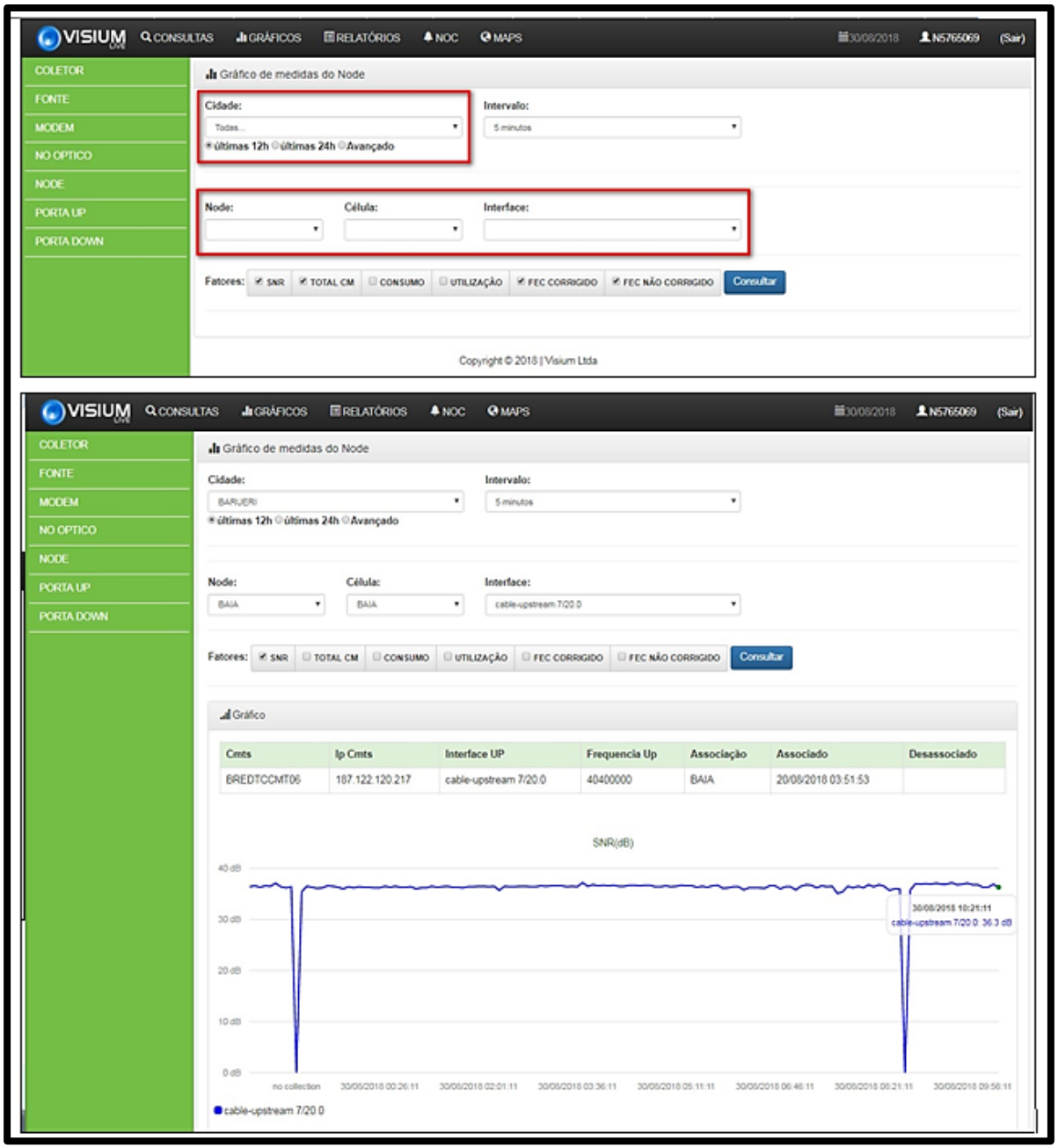
Figura 11- Interface do Visium Live

Fonte: Autor

E então, como pode ser visto na Figura 12, é necessário apenas selecionar a cidade, o *node* e os itens que deseja visualizar e o gráfico será exibido.

Dessa forma o analista consegue iniciar a sua análise de maneira mais rápida, se comparado ao Nagios.

Figura 12- Seleção do node no Visium Live



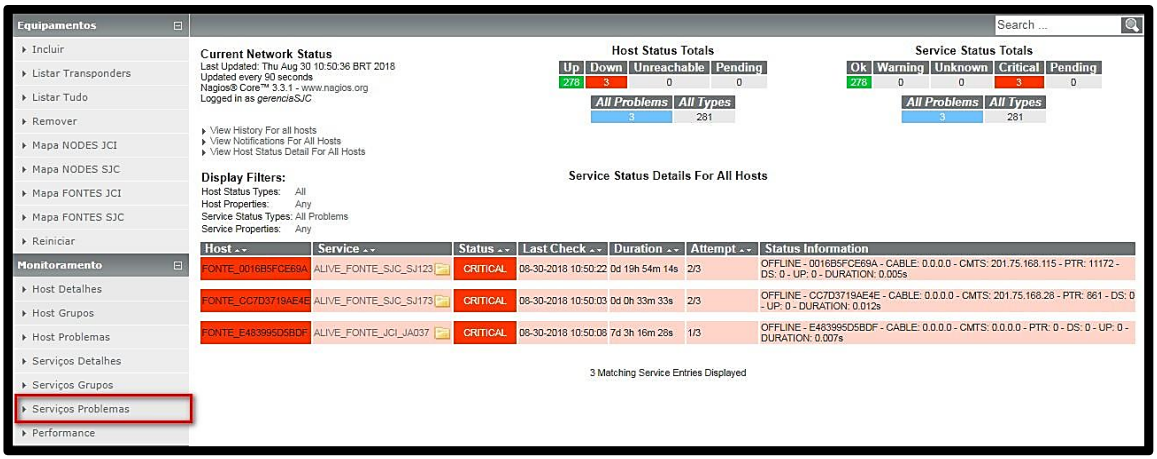
Fonte: Autor

4.2 Consulta e monitoramento de fontes

No Nagios Fontes tudo o que podemos obter de informação é se o *cable modem* da fonte está alarmado e o endereço em que ela está localizada. Não temos informações adicionais referentes ao banco de baterias, por exemplo.

Após o login no Nagios Fonte da cidade, selecionamos a opção Serviços Problemas no menu lateral, conforme Figura 13. Nessa tela são exibidas todas as fontes que estão com o status *down*, ou seja, as fontes que estão com o MAC do *cable modem* off-line.

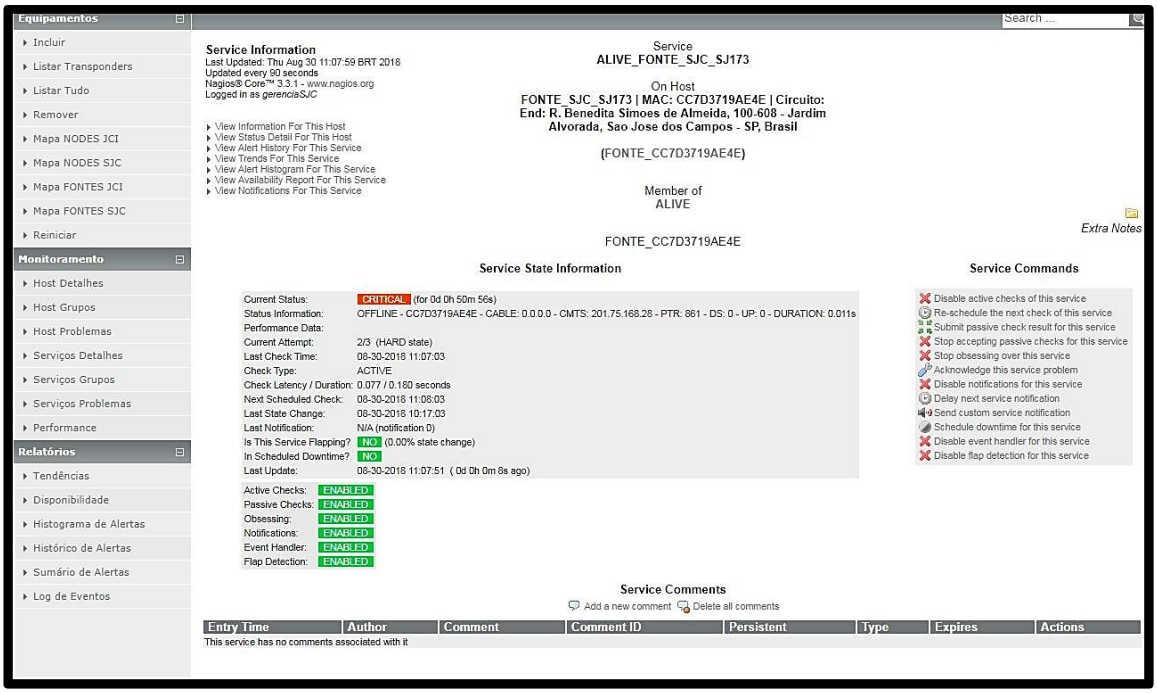
Figura 13- Interface do Nagios Fonte



Fonte: Autor

Ao selecionar a fonte desejada, podem-se visualizar alguns detalhes técnicos, endereço e o tempo que o serviço está apresentando falha, conforme Figura 14.

Figura 14- Detalhes de um alarme de fonte

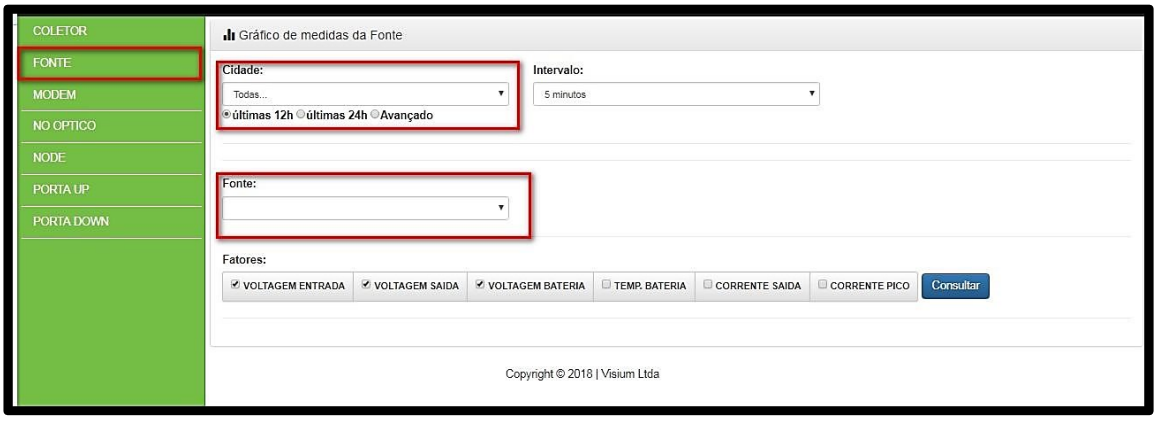


Fonte: Autor

O grande diferencial do monitoramento de fontes do Visium é a capacidade de verificar informações sobre o banco de baterias, além de todas as outras informações já obtidas pelo Nagios, como detalhes técnicos, tempo de indisponibilidade e endereço em que está localizado o equipamento.

Como mostra a Figura 15, pode-se acessar esses dados através da opção fonte do menu lateral e em seguida selecionando a cidade e o *node*.

Figura 15- Seleção da fonte

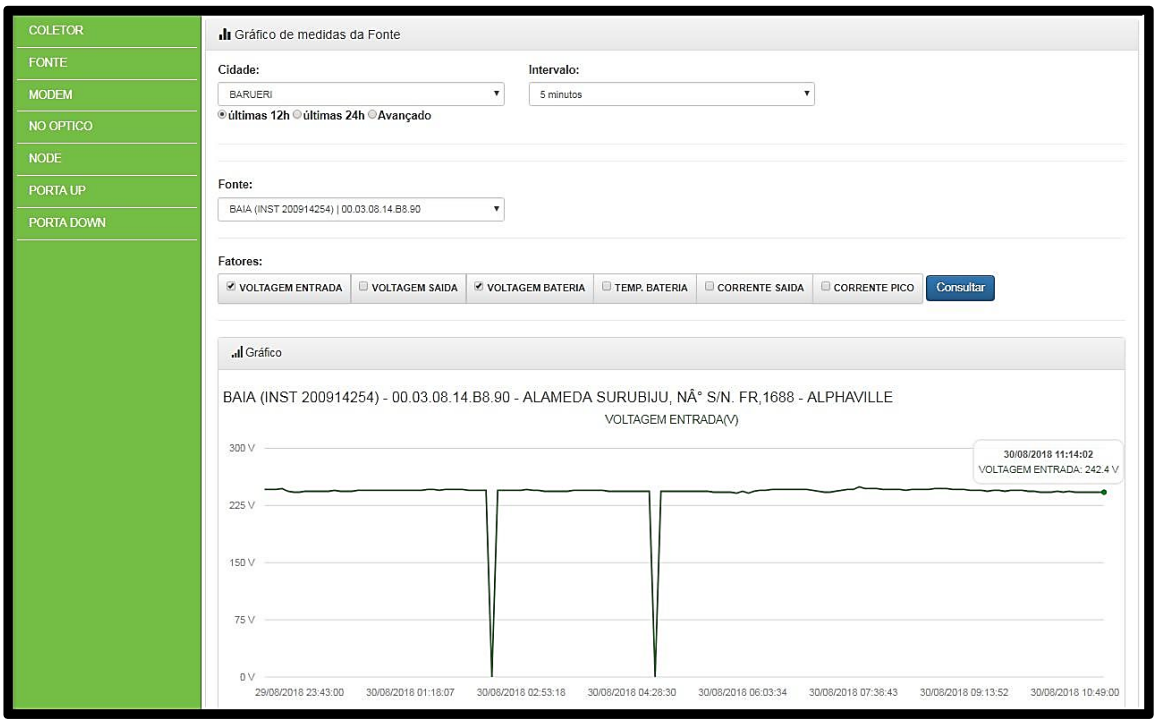


Fonte: Autor

Nos gráficos referentes ao banco de baterias é possível identificar o momento em que houve uma falha de energia externa, o momento em que as baterias assumiram e o principal, o tempo de autonomia das baterias, sendo possível deslocar o técnico para acionar o gerador com maior assertividade.

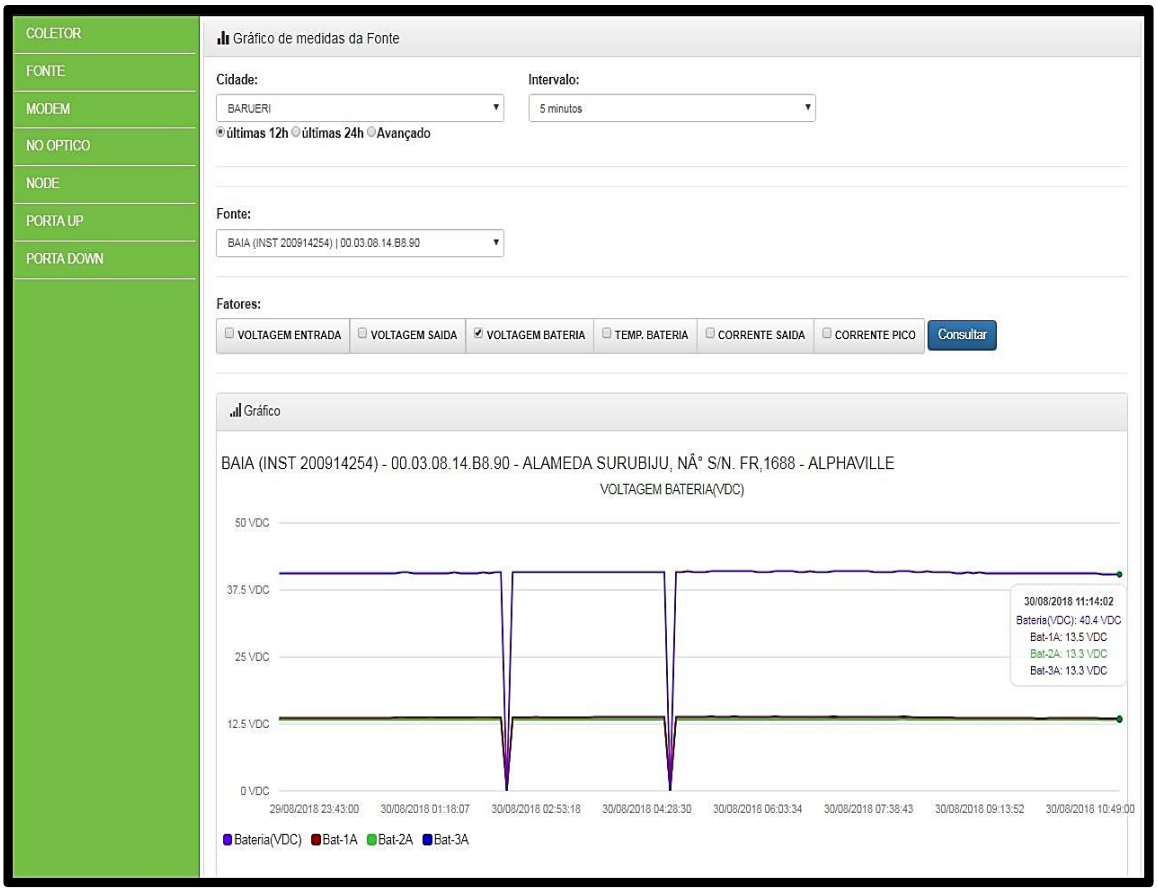
Nas figuras 16 e 17, respectivamente, é possível verificar se há voltagem de entrada na fonte e autonomia da bateria, caso haja falha na alimentação de energia por parte da concessionária.

Figura 16- Gráfico voltagem de entrada da fonte



Fonte: Autor

Figura 17- Gráfico representando a autonomia da bateria da fonte



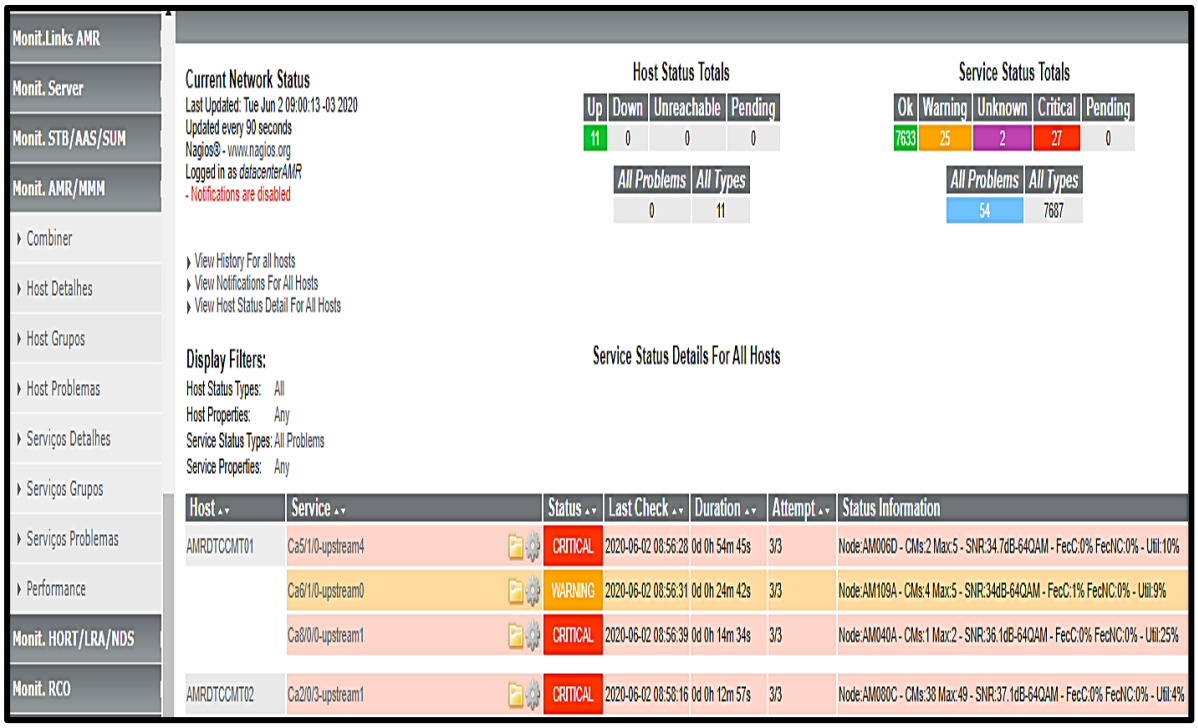
Fonte: Autor

4.3 Painel de alarmes

O Nagios oferece um painel de alarmes simples e sem opções de filtros, tornando o monitoramento dos serviços complicado, resultando na demora na identificação de possíveis problemas massivos. Conforme figura 18, ele pode ser acessado selecionando a aba monitoramento, a opção Serviços Problemas e o *Status Critical* no canto direito superior.

Para complicar ainda mais a situação, é necessário abrir uma página web para cada cidade que se deseja monitorar.

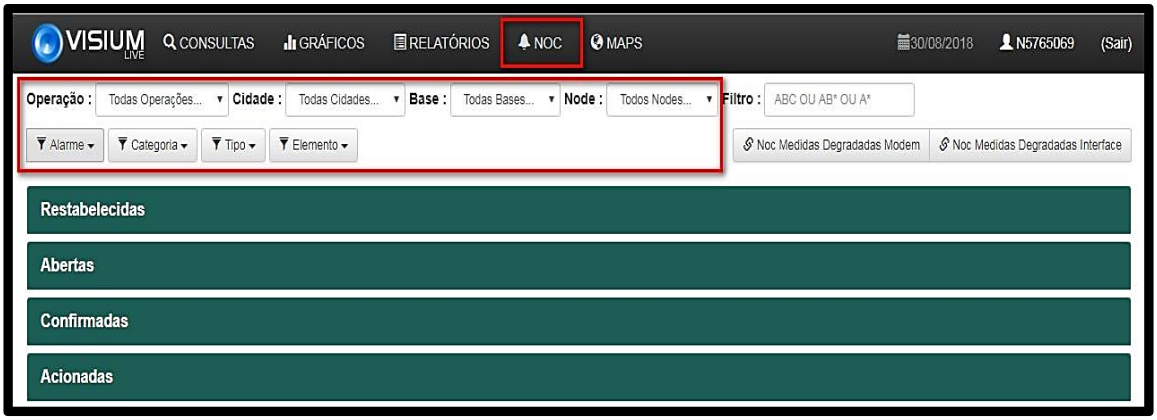
Figura 18- Painel de alarmes do Nagios



Fonte: Autor

De acordo com a Figura 19, ao acessar a aba NOC no menu superior, temos acesso ao painel de alarmes do Visium, que conta com diversos filtros e abas para segmentar o tratamento dos alarmes, dessa forma temos um painel organizado, o que torna a identificação dos incidentes mais fácil e rápida.

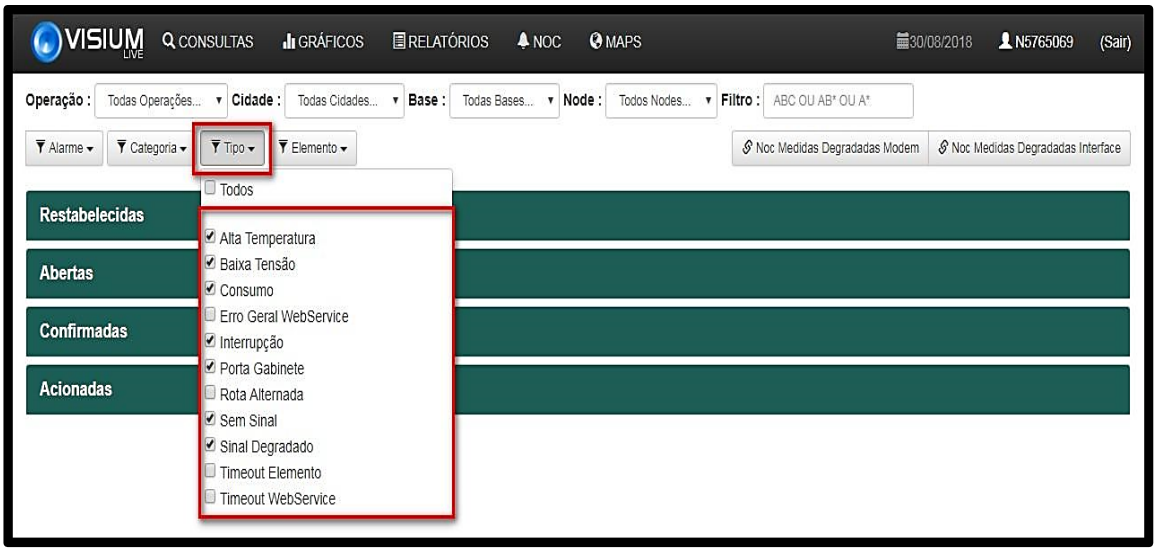
Figura 19- Interface painel de alarmes Visium Live



Fonte: Autor

No filtro 'Tipo' selecionam-se os tipos de alarmes, conforme Figura 20. Os alarmes mais comuns são os de interrupção e degradação de sinal.

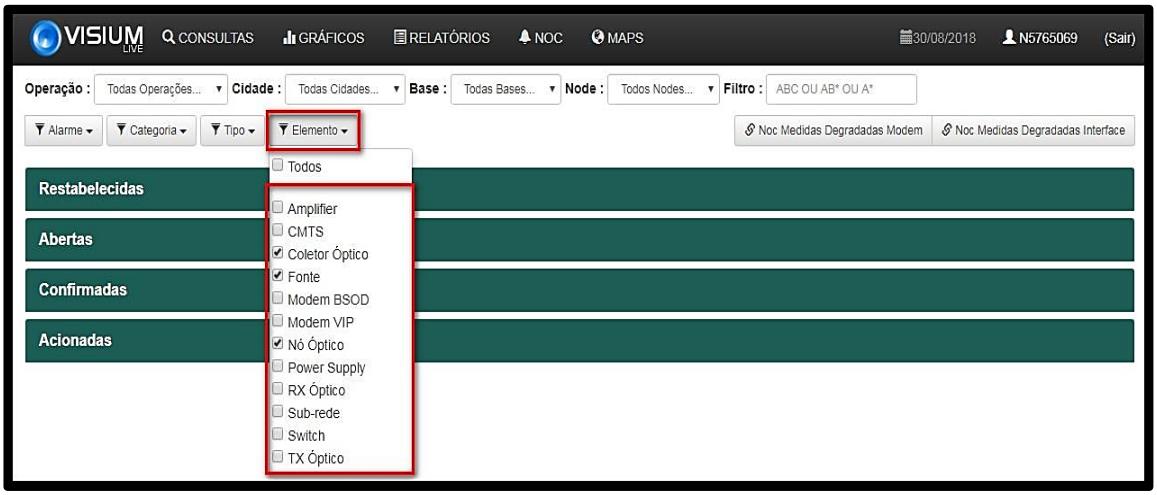
Figura 20- Filtros do painel de alarme



Fonte: Autor

A Figura 21 mostra a opção ‘Elemento’ onde são selecionados quais ativos de rede serão exibidos os alarmes, tendo como os principais elementos a serem monitorados os coletores e os nós ópticos (*nodes*).

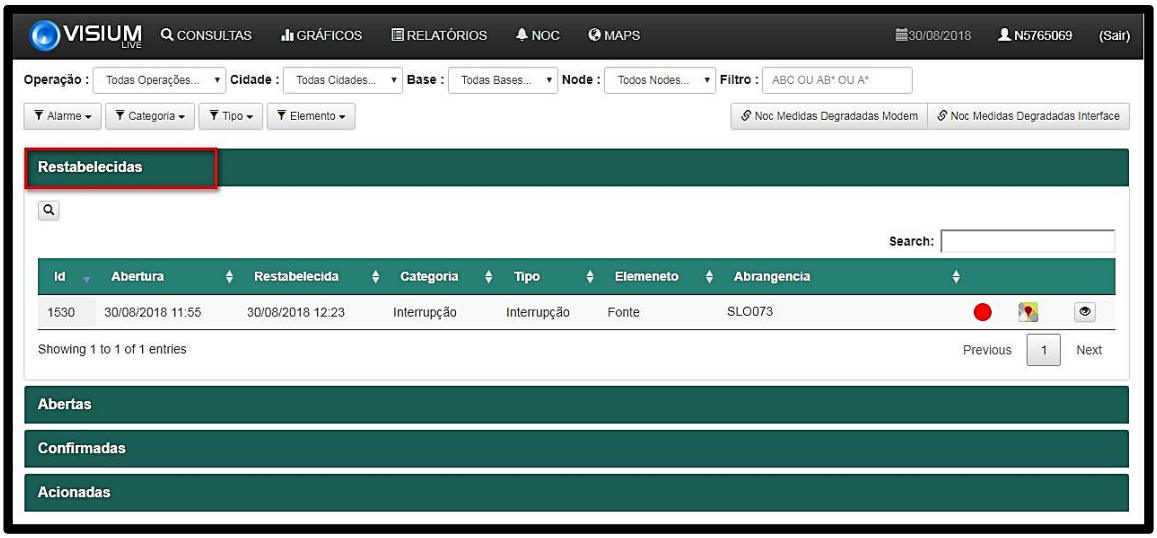
Figura 21- Filtro para a seleção de equipamento



Fonte: Autor

Na aba dos alarmes restabelecidos são exibidos os alarmes em que os problemas já foram sanados, como mostra a Figura 22. Esses alarmes ficam em monitoramento durante 15 minutos e caso não haja nova falha são finalizados automaticamente.

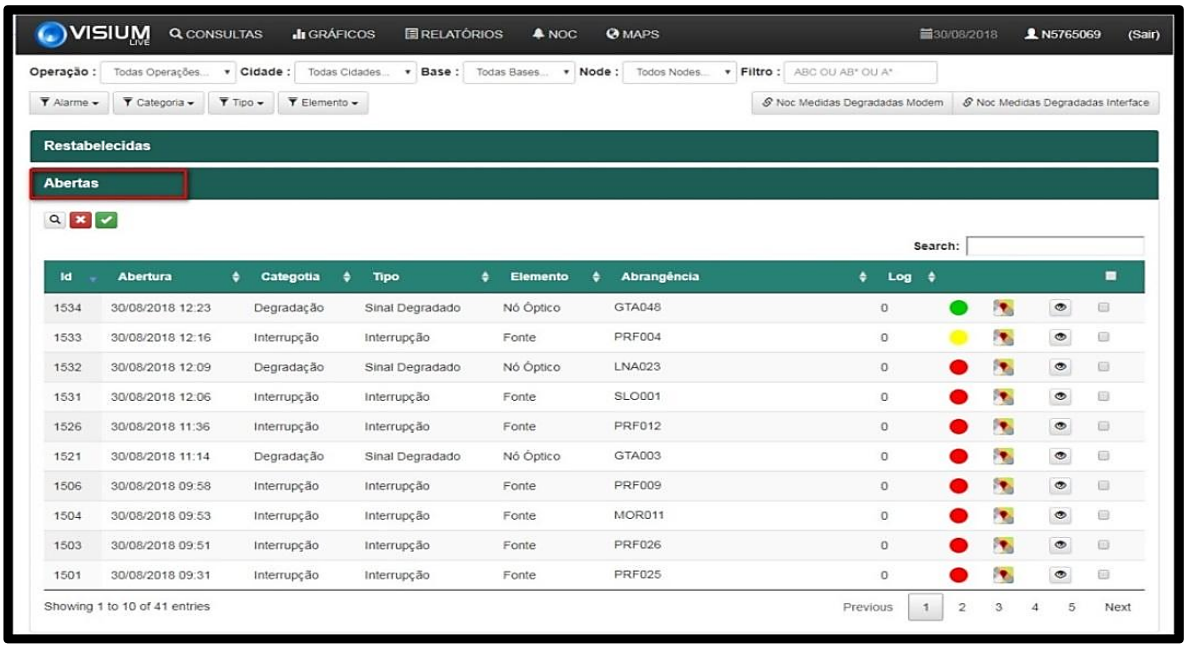
Figura 22- Aba de alarmes restabelecidos



Fonte: Autor

A aba ‘Abertas’ demonstra os alarmes que ainda não foram tratados e seguem os filtros que foram definidos no menu superior, conforme Figura 23.

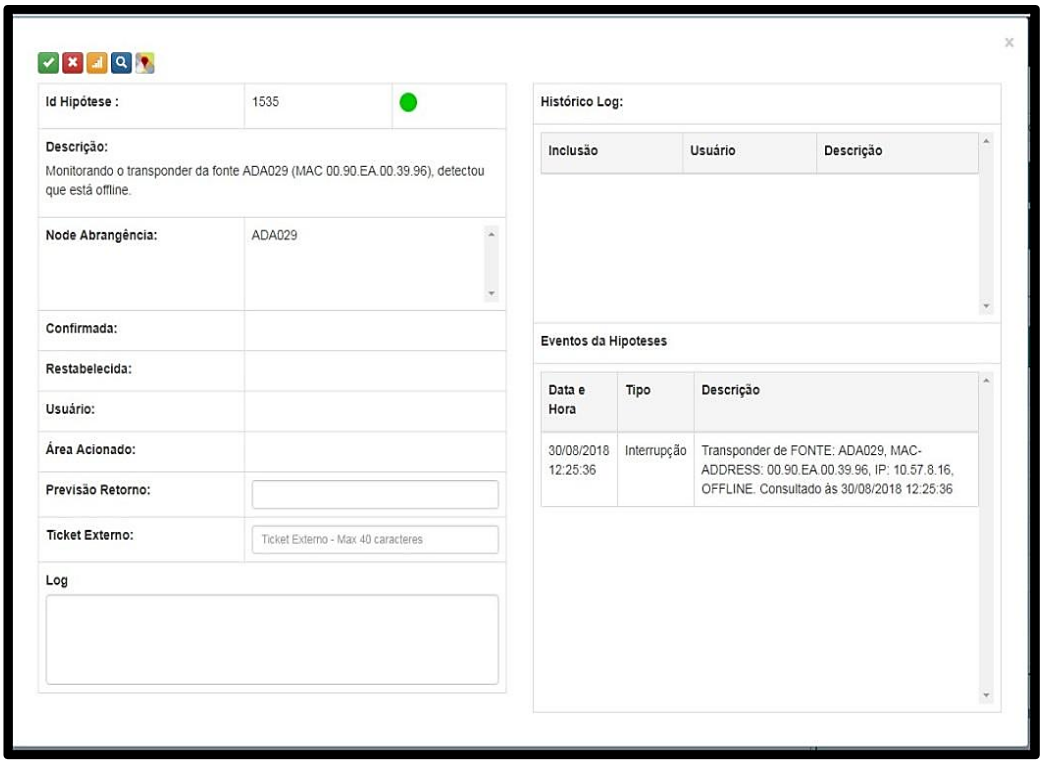
Figura 23- Aba de alarmes novos



Fonte: Autor

De acordo com a Figura 24, ao clicar sobre o alarme pode-se visualizar os detalhes técnicos sobre o possível problema.

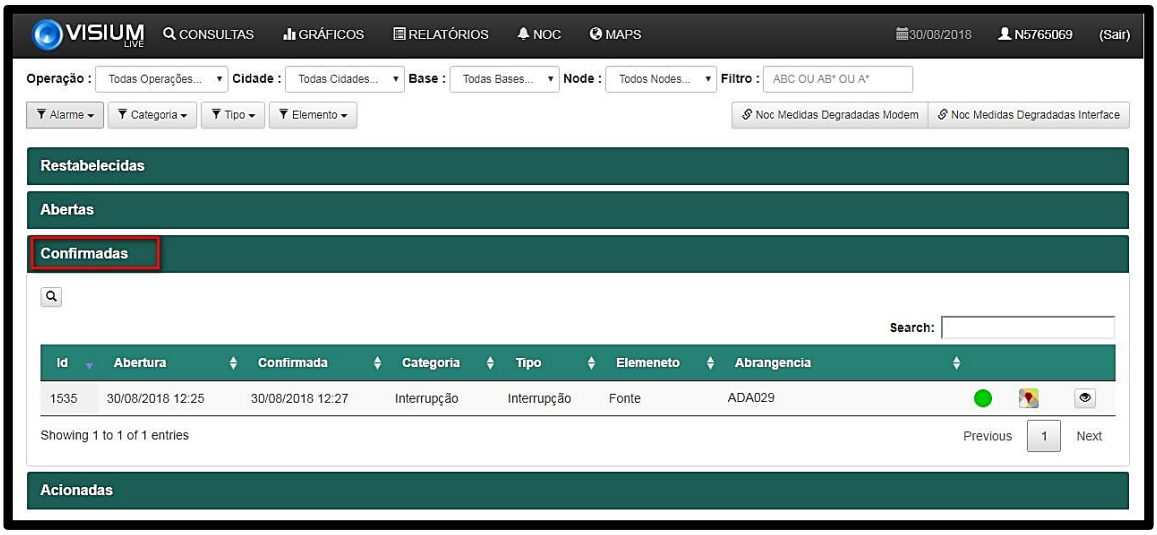
Figura 24- Detalhes de um alarme novo



Fonte: Autor

Na figura 25, pode-se visualizar a aba dos alarmes que foram confirmados e estão em tratamento, ao entrar nos detalhes o analista, caso o alarme seja procedente, realizara o acionamento, encaminhando o alarme para a aba de acionados, conforme figura 26.

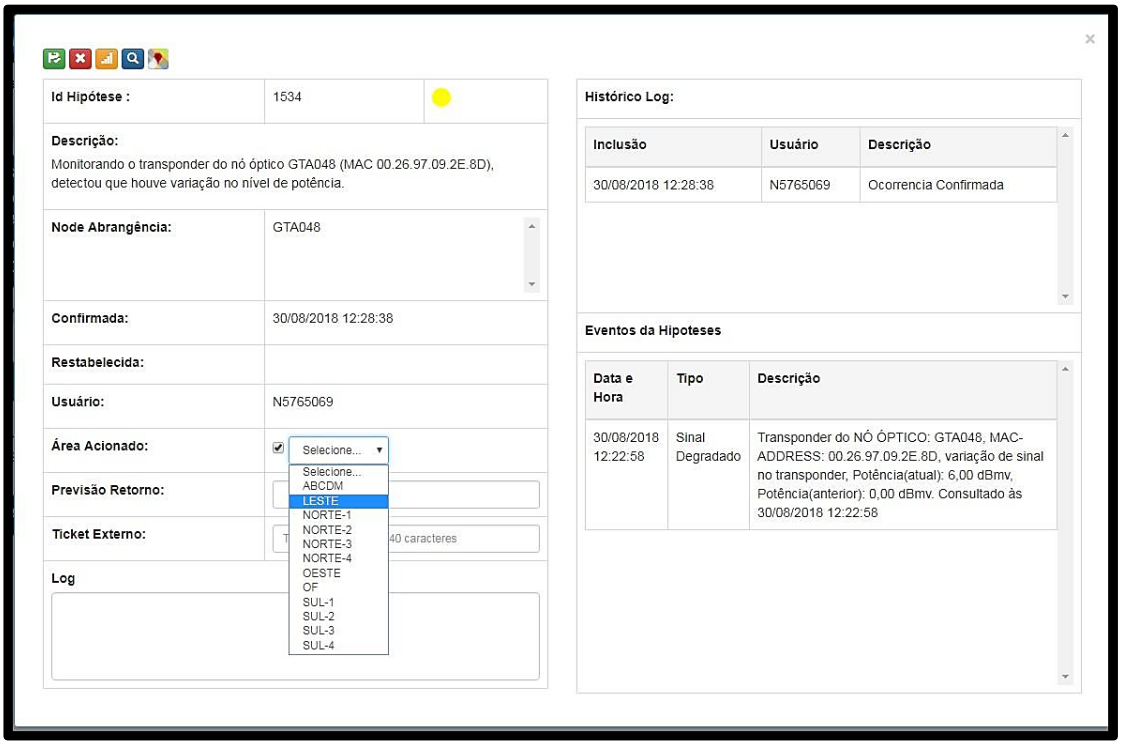
Figura 25- Aba de alarmes em análise



Fonte: Autor

Na figura 26 é possível ver detalhes de um alarme, identificado uma variação de sinal para o Nó Óptico, sendo ruído na rede gerando intermitência e lentidão para os usuários.

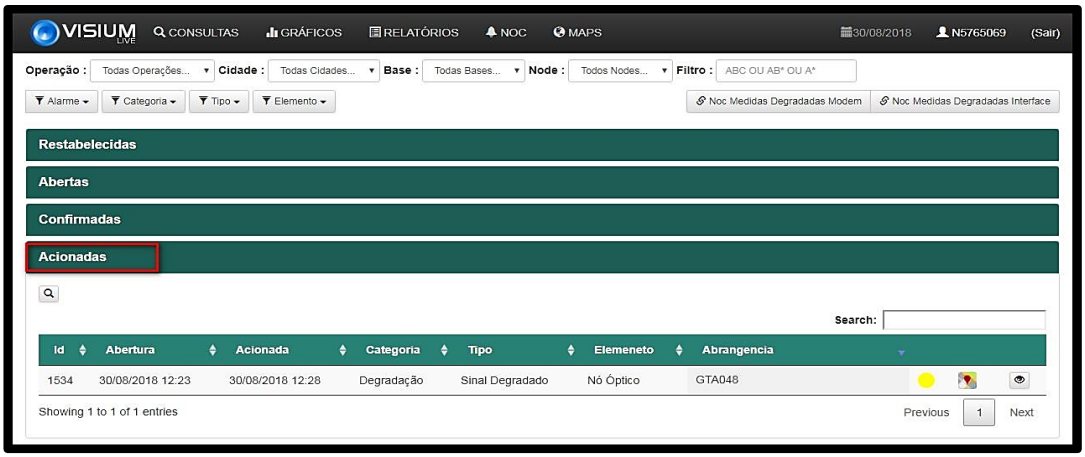
Figura 26- Detalhes de um alarme em tratamento



Fonte: Autor

Na aba ‘Acionadas’ estão todos os alarmes em que foi identificado problema de infraestrutura e a equipe de campo está acionada para a verificação e correção da falha, conforme Figura 27.

Figura 27- Aba de alarmes encaminhados para campo



Fonte: Autor

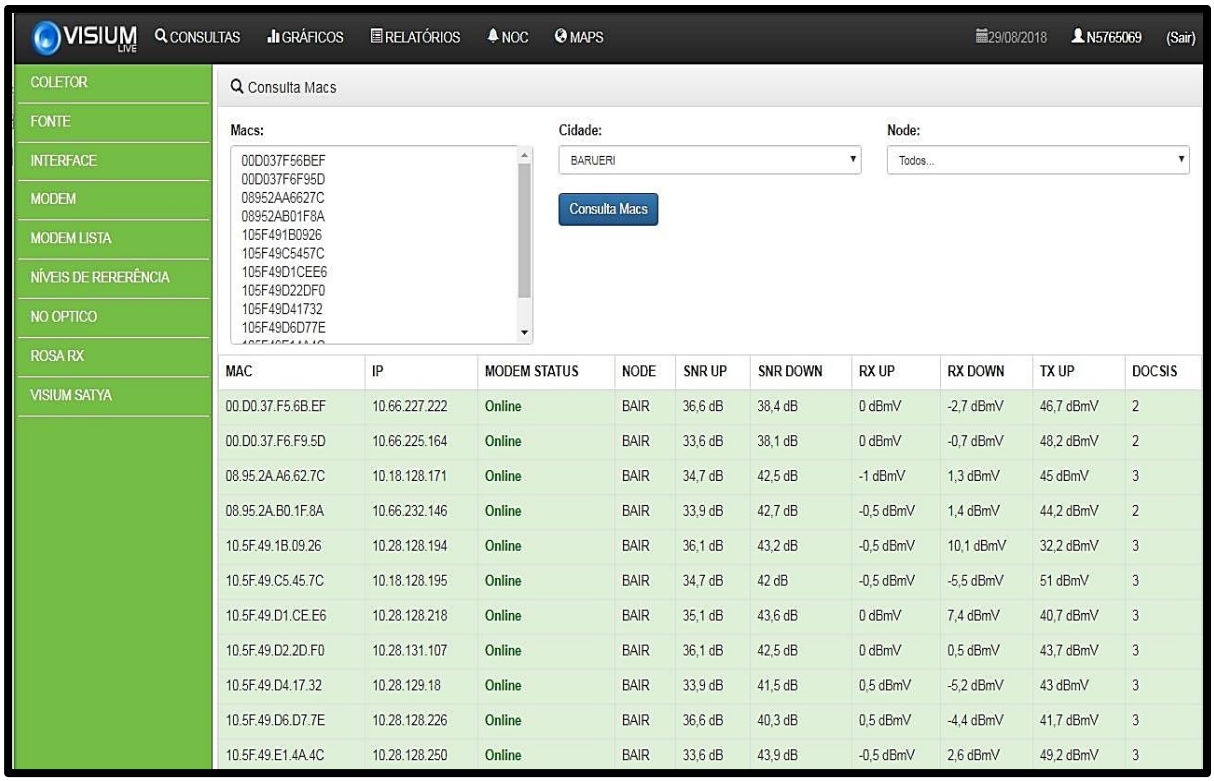
5 Funcionalidades presentes apenas no Visium Live

A Ferramenta Visium Live possui algumas semelhanças com o NAGIOS na questão de gerenciamento de redes HFC, porem possui algumas funcionalidades diferentes qual serve de grande auxilio para a análise de trafego e garantia de qualidade de sinal, funcionalidades que otimizam o serviço e diminui o tempo necessário para tratativas de falhas, garantindo que o SLA (Service Level Agreement) seja cumprido, veremos a seguir essas funcionalidades.

5.1 Consulta massiva de MACS

Através da funcionalidade de consulta modem lista, o analista pode fazer a verificação de um grande bloco de MACS de uma só vez, como pode ser visto na Figura 28, dessa forma têm-se um aumento no tempo de consulta dos níveis de sinal durante o fechamento de incidentes ou ao realizar testes com o técnico de campo. Anteriormente essa consulta poderia ser realizada através de outro sistema, porém apenas um MAC por vez, o que tornava essa consulta demorada e maçante.

Figura 28- Consulta massiva de MACS

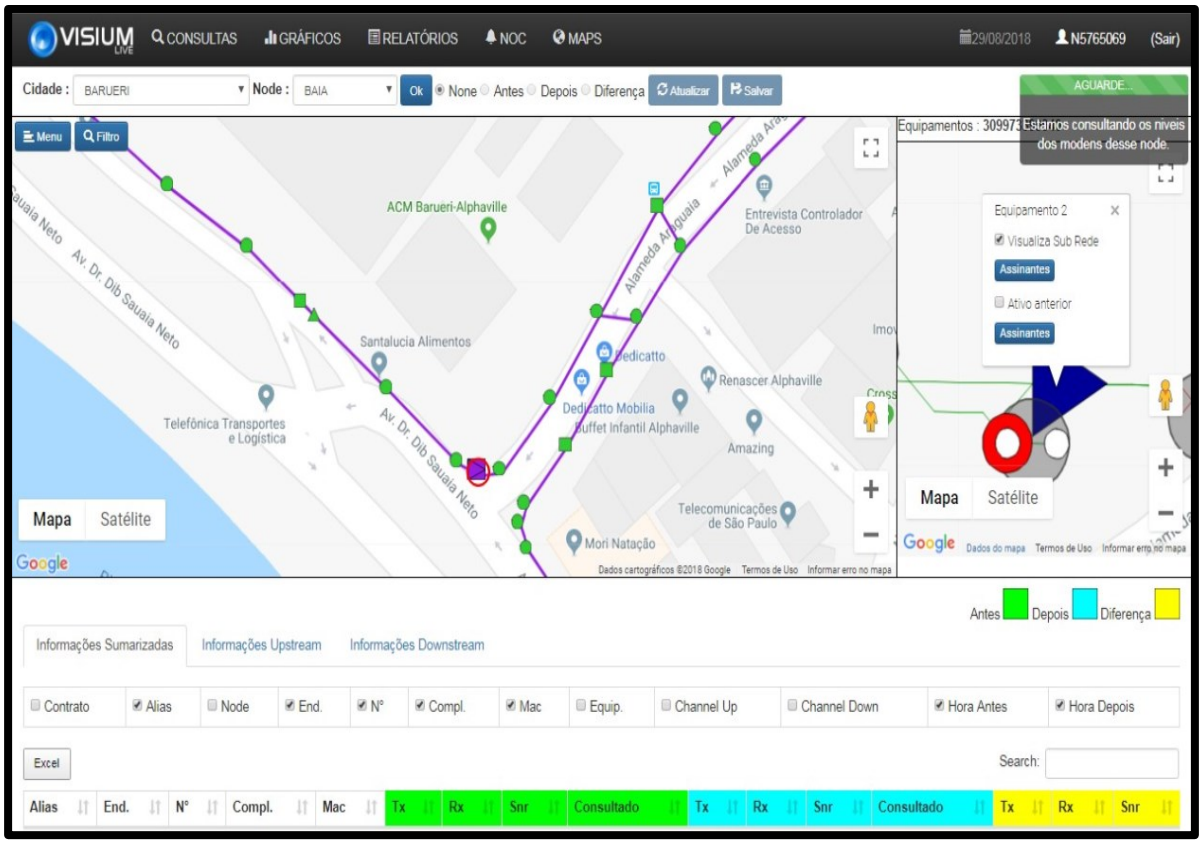


Fonte: Autor

5.2 Níveis de referência

Na funcionalidade chamada níveis de referência, que pode ser vista na figura 29, o analista pode selecionar um equipamento de rede, consultar os níveis de sinal de todos os assinantes conectados naquele equipamento, salvar esses dados e depois realizar uma consulta futura e comparar as duas consultas, a fim de identificar a mudança dos níveis de sinal.

Figura 29- Interface da funcionalidade níveis de referência

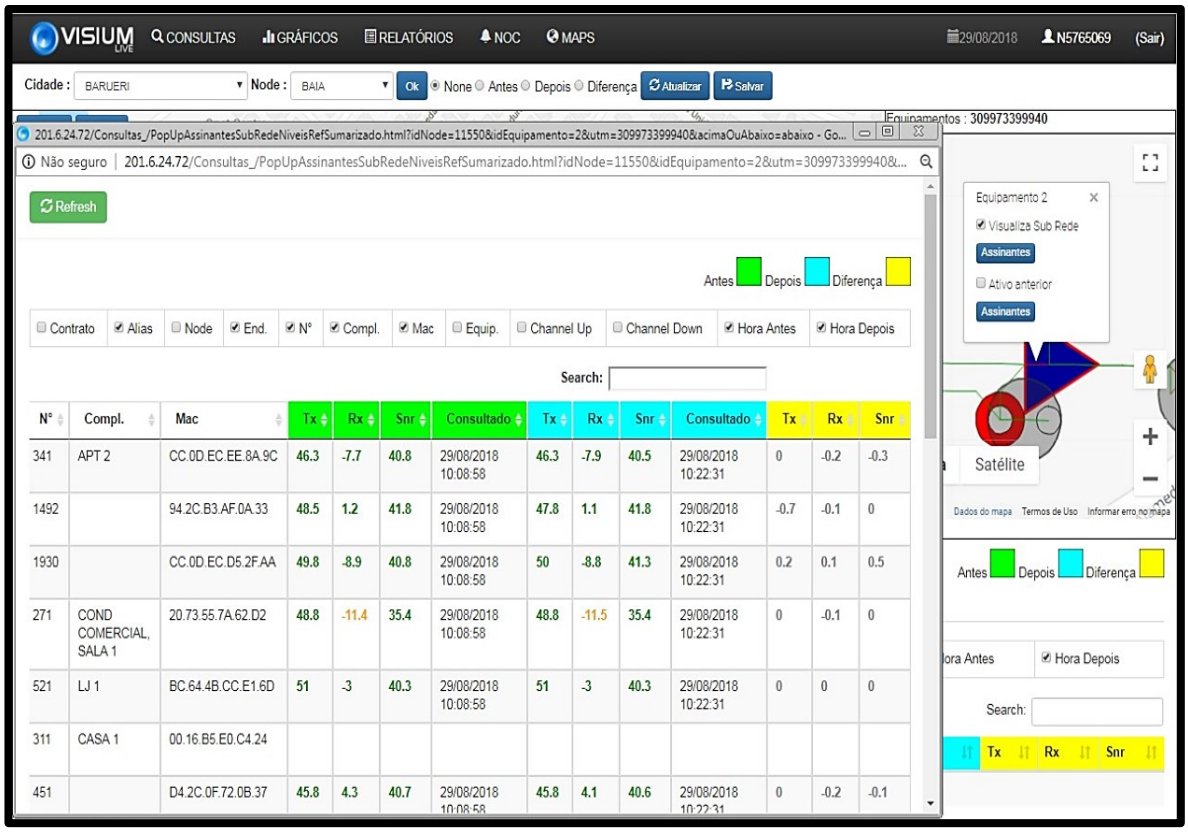


Fonte: Autor

O pré e pós manobra é um processo utilizado para comparar os níveis de sinal antes e depois da manutenção, coletando evidências de que houve melhoria após a intervenção técnica. A principal função dos níveis de referência no departamento é auxiliar no pré e pós-manobra, pois como se pode verificar na Figura 30, a ferramenta tornou a visualização dos níveis antes e depois da manutenção muito fácil e rápida.

Esse processo, antes da implementação do Visium Live era realizado, em média, por seis analistas, devido à demora na obtenção das evidências de que os níveis pós-manutenção estavam dentro do padrão, agora é realizada por dois analistas.

Figura 30- Consulta de MACS antes e depois



N°	Compl.	Mac	Tx	Rx	Snr	Consultado	Tx	Rx	Snr	Consultado	Tx	Rx	Snr
341	APT 2	CC.0D.EC.EE.8A.9C	46.3	-7.7	40.8	29/08/2018 10:08:58	46.3	-7.9	40.5	29/08/2018 10:22:31	0	-0.2	-0.3
1492		94.2C.B3.AF.0A.33	48.5	1.2	41.8	29/08/2018 10:08:58	47.8	1.1	41.8	29/08/2018 10:22:31	-0.7	-0.1	0
1930		CC.0D.EC.D5.2F.AA	49.8	-8.9	40.8	29/08/2018 10:08:58	50	-8.8	41.3	29/08/2018 10:22:31	0.2	0.1	0.5
271	COND COMERCIAL, SALA 1	20.73.55.7A.62.D2	48.8	-11.4	35.4	29/08/2018 10:08:58	48.8	-11.5	35.4	29/08/2018 10:22:31	0	-0.1	0
521	LJ 1	BC.64.4B.CC.E1.6D	51	-3	40.3	29/08/2018 10:08:58	51	-3	40.3	29/08/2018 10:22:31	0	0	0
311	CASA 1	00.16.B5.E0.C4.24											
451		D4.2C.0F.72.0B.37	45.8	4.3	40.7	29/08/2018 10:08:58	45.8	4.1	40.6	29/08/2018 10:22:31	0	-0.2	-0.1

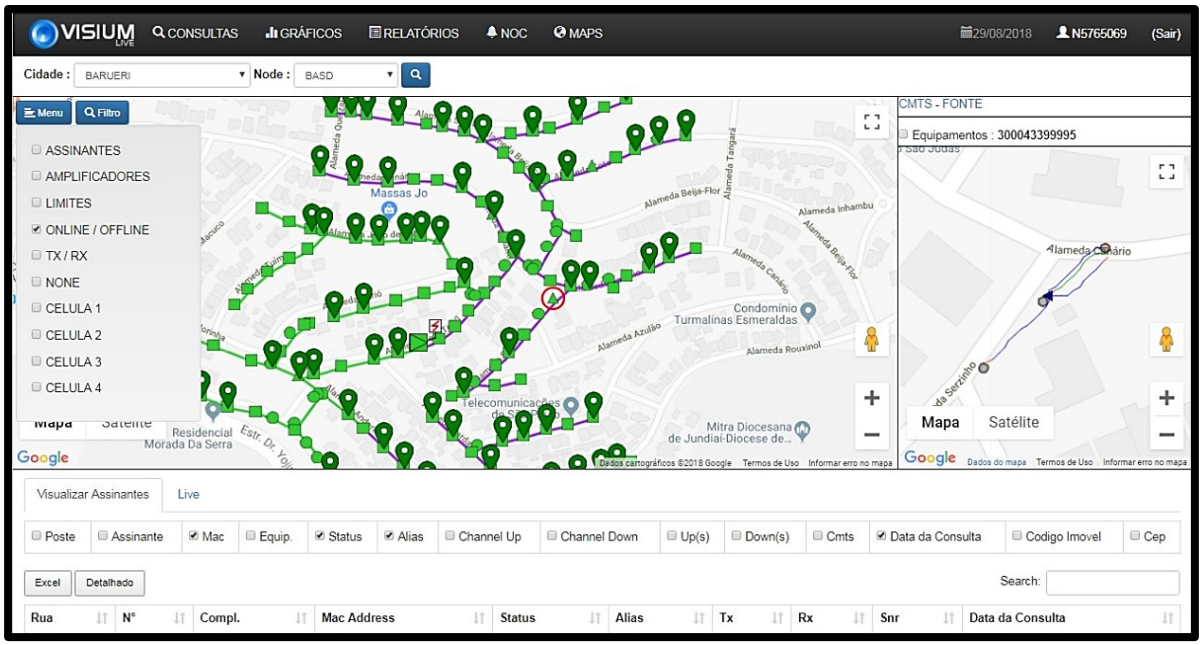
Fonte: Autor

5.3 Maps

O *Maps* oferece visualização detalhada da topologia da rede, conforme Figura 31, e se podem consultar os *cable modems* de todos os assinantes conectados ao equipamento selecionado, como por exemplo, o *node*, amplificador, divisor ou *tap* (equipamento passivo que conecta o cliente à rede), como pode ser visto na Figura 32. Porém, sua principal função é determinar o possível ponto da falha nos casos de interrupção de sinal, como veremos de forma detalhada durante o capítulo 5, onde será demonstrado um caso real.

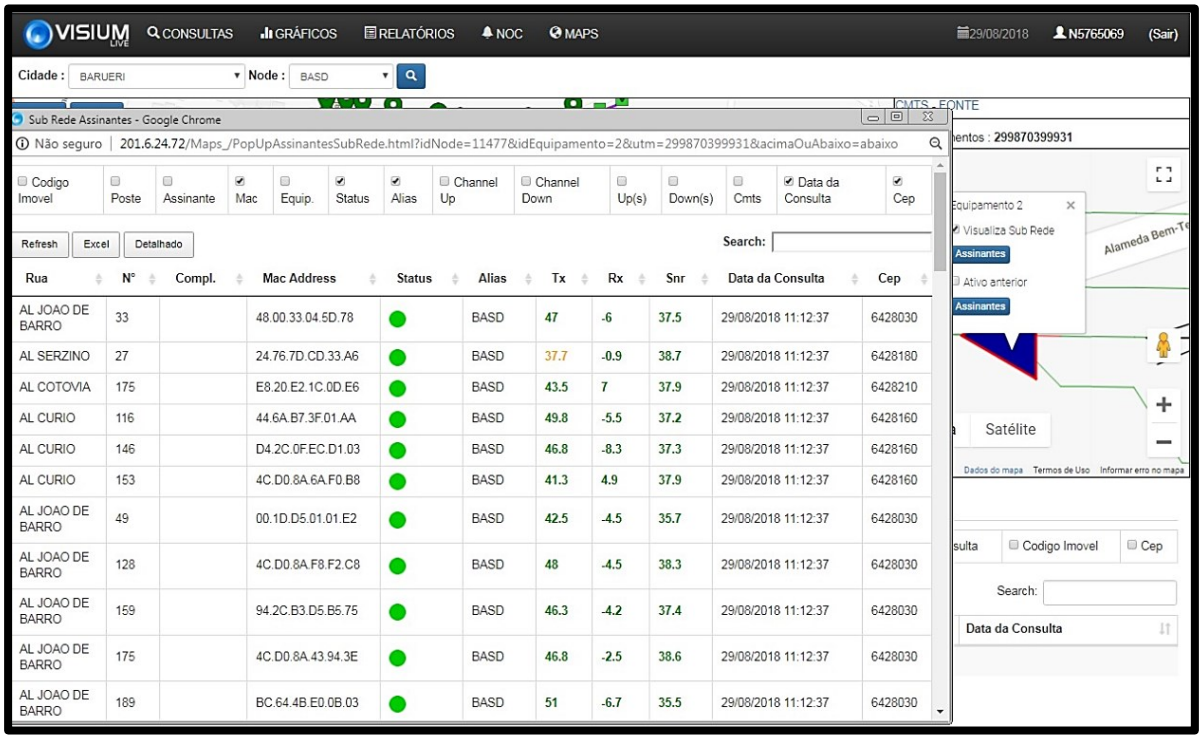
O tempo ganho com essa funcionalidade impacta diretamente nos indicadores de negócio da empresa, reduzindo drasticamente o tempo médio de recuperação, auxiliando diversas operações a atingir o SLA de 90 minutos.

Figura 31- Interface *Maps*



Fonte: Autor

Figura 32- Consulta dos níveis de todos os clientes do *node*



Fonte: Autor

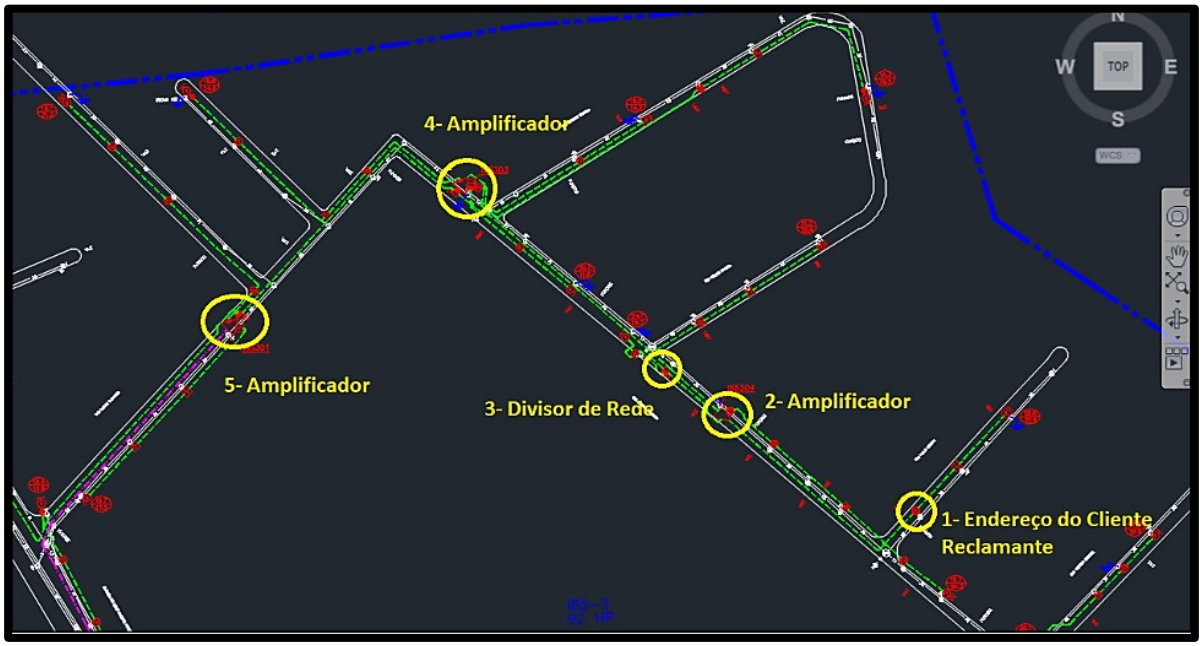
6 Exemplo utilizando incidente real

Neste capítulo, será mostrado como era realizada a tratativa de um incidente sem sinal antes da implementação do Visium Live e compará-lo ao método utilizado agora.

Sem o auxílio do Visium Live, normalmente o técnico era encaminhado para o endereço do reclamante, no ponto 1 da Figura 33, onde realiza a medição dos sinais e verifica se o *tap* está queimado, oxidado ou com água, caso o equipamento esteja dentro do padrão, mas com ausência ou degradação do sinal, é necessário voltar a rede e ir para o ponto 2, o amplificador, onde são verificados os níveis de sinal e conexões, caso o sinal já esteja chegando fora do padrão na entrada do amplificador, é necessário voltar a rede novamente, dessa vez ao divisor, identificado pelo ponto 3, onde serão realizados os mesmo procedimentos realizados no tap.

Nesse exemplo da Figura 33, o técnico teria que voltar a rede até o ponto 5, onde foi trocado o amplificador que estava queimado, como pode ser visto no fechamento do incidente na Figura 35.

Figura 33- Projeto de rede no CAD

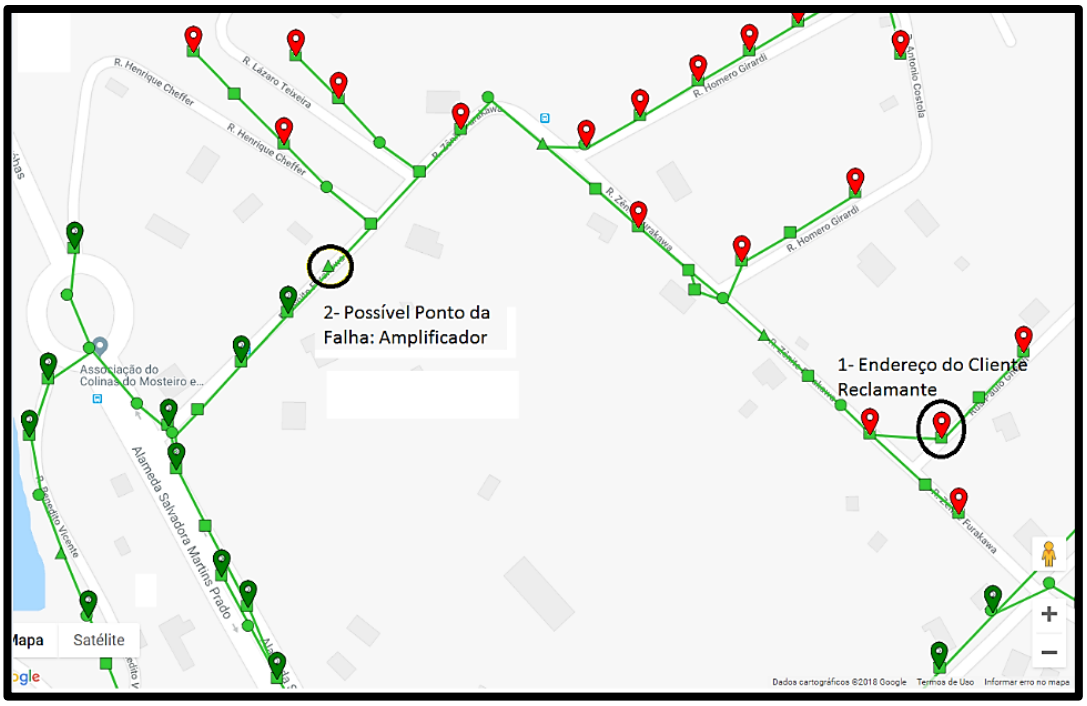


Fonte: Autor

Ao realizar a tratativa pelo Visium Live, através da funcionalidade *Maps*, ao visualizar a topologia já é possível identificar que o amplificador, ponto 2 na Figura 34, é o ponto da falha, pois a partir dele todos os assinantes estão *offline*, indicado pelos pontos em vermelho.

Utilizando esse método, o técnico vai direto no ponto da falha e, consequentemente, consegue resolver o problema em um tempo muito menor, o que será comprovado no capítulo 6, através dos relatórios de tempo médio de recuperação.

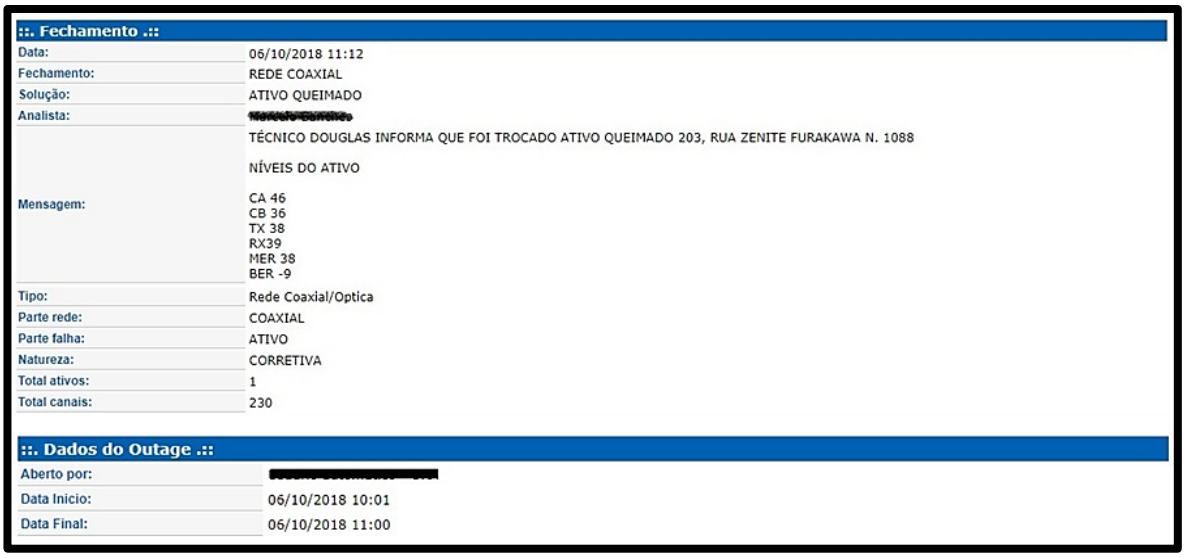
Figura 34- Projeto de rede no Visium Live



Fonte: Autor

Na Figura 35 temos a resolução do incidente, onde foi constatado que o amplificador identificado pelo Visium Live como o ponto de falha, estava queimado, foi realizada a substituição do equipamento e o incidente foi finalizado com 59 minutos, ficando dentro do SLA de 90 minutos.

Figura 35- Fechamento do incidente



::. Fechamento .::

Data:	06/10/2018 11:12
Fechamento:	REDE COAXIAL
Solução:	ATIVO QUEIMADO
Analista:	[redacted]
Mensagem:	TÉCNICO DOUGLAS INFORMA QUE FOI TROCADO ATIVO QUEIMADO 203, RUA ZENITE FURAKAWA N. 1088 NÍVEIS DO ATIVO CA 46 CB 36 TX 38 RX39 MER 38 BER -9
Tipo:	Rede Coaxial/Optica
Parte rede:	COAXIAL
Parte falha:	ATIVO
Natureza:	CORRETIVA
Total ativos:	1
Total canais:	230

::. Dados do Outage .::

Aberto por:	[redacted]
Data Inicio:	06/10/2018 10:01
Data Final:	06/10/2018 11:00

Fonte: Autor

7 Resultados

Logo após os primeiros meses de uso da nova ferramenta, foi possível identificar uma melhora significativa em diversos indicadores, nesse relatório o foco será na queda do tempo médio de recuperação dos incidentes e o aumento no número de incidentes proativos.

7.1 Queda no Tempo Médio de Recuperação (TMR)

Com o uso do Visium Live, o tempo de análise foi otimizado e o analista é capaz de encaminhar o técnico no ponto exato da falha, por consequência houve queda significativa no tempo de recuperação dos incidentes de interrupção. Em algumas cidades já foi possível alcançar o SLA de 90 minutos, como pode-se ver na Tabela 1.

Tabela 1- Tempo médio de recuperação

TMR	jul/18	ago/18	set/18	out/18	nov/18	dez/18	jan/19	fev/19	mar/19	abr/19	mai/19	jun/19
Americana	164	194	191	179	117	170	119	110	104	92	85	89
Aparecida	89	83	91	77	72	88	82	69	51	55	61	57
Campinas	139	129	140	124	94	112	97	90	88	74	69	70
Bauru	189	212	175	146	127	108	92	97	74	78	76	84
Santos	154	151	143	129	113	176	124	121	118	123	109	112
Sorocaba	161	134	142	162	147	131	128	112	104	109	98	94

Fonte: Autor

7.2 Aumento no Número de Incidentes Proativos

Utilizando o painel de alarmes do Visium Live, uma grande parte dos incidentes de interrupção de sinal é identificada antes da reclamação do cliente, gerando uma grande economia para a empresa, pois quando o cliente liga e o incidente já está aberto, essa ligação fica retida na URA (unidade de resposta audível), que informa ao assinante que a área está em manutenção, caso o incidente ainda não esteja aberto, essa ligação é direcionada ao atendente na central de relacionamento. O custo de uma ligação retida na URA é de R$ 0,80 centavos e a que passa para o atendente é de, em média, R$ 8,80 reais.

Através da Tabela 2 pode-se identificar o aumento nos incidentes abertos de maneira proativa, ou seja, sem que houvesse reclamação dos assinantes.

Tabela 2- Incidentes proativos

	Incidentes	Abertos pela Monitoração	% Abertos pela Monitoração
Julho	901	89	10%

Agosto	817	64	8%
Setembro	869	78	9%
Outubro	917	127	14%
Novembro	804	198	25%
Dezembro	1134	427	38%
Janeiro	715	271	38%
Fevereiro	858	301	35%
Março	805	278	35%
Abril	896	292	33%
Maio	980	312	32%
Junho	1008	372	37%

Fonte: Autor

8 Conclusões e considerações finais

Com o objetivo de analisar os impactos operacionais que recaem sobre o NOC e a empresa como um todo, verificou-se que um aspecto muito relevante são as ferramentas utilizadas para o gerenciamento da rede HFC. Observou-se, após a mudança do Nagios para o Visium Live, um aumento significativo na produtividade dos analistas, sobretudo aqueles que são responsáveis pelo monitoramento de alarmes e abertura proativa de incidentes de interrupção de sinal.

Não se trata apenas de uma mudança nas atividades cotidianas do NOC, mas um quadro geral de melhorias para a empresa, causando impacto positivo tanto tecnicamente quanto financeiramente. Dessa forma, pode-se dizer que a mudança entre ferramentas foi altamente benéfica para a companhia, como pôde ser visto no capítulo 6, através da redução do tempo médio de recuperação, auxiliando as operações a atingir o SLA no restabelecimento dos serviços em incidentes de interrupção de sinal, e com potencial de ganhos financeiros, pois ao abrir incidentes proativos, a grande maioria das ligações dos clientes são retidas na URA, e não passam ao atendente, gerando uma economia de aproximadamente R$ 8,00 por ligação.

REFERÊNCIAS BIBLIOGRÁFICAS:

Canal de Retorno. Disponível em: <http://www.net.atenalms.com.br>. Acesso em: 19 Out. 2019.

Nagios, The industry standard in IT infrastructure monitoring. Disponível em: <https://www.nagios.com/products/nagios-xi >. Acesso em: 02 Out. 2019.

KOCJAN, Wojciech. **Learning Nagios 4.** 2 ª Edição. Birmingham: Packt Publishing, 2014.

KUROSE, Jim; ROSS, Keith. **Redes de computadores e a Internet**: uma abordagem top-down. 6ª Edição. São Paulo: Pearson, 2013.

VISIUM Soluções em TI e telecom. Disponível em: <http://www.visium.com.br/visium_suite_5.html>. Acesso em: 25 Nov. 2019.