WHITE PAPER

Solução de latência ultrabaixa para empresas de energia elétrica

Em 2003, a região nordeste dos EUA sofreu o maior apagão de energia da história do país. Por dois dias, 50 milhões de clientes de oito estados e partes de Ontário ficaram sem energia, o que resultou em perdas econômicas estimadas em US$ 6 bilhões. A principal causa do corte de energia: incapacidade de reconhecer, avaliar e entender as insuficiências e a deterioração de setores da rede elétrica em áreas remotas, uma história conhecida do gerenciamento da infraestrutura crítica. De danos à reputação e multas caras a perdas financeiras diretas em bilhões de dólares, a confiabilidade da rede no nível da infraestrutura crítica era (e ainda é) uma das principais preocupações do setor de serviços públicos.

Além de causar danos ao sistema e a equipamentos que são caros para consertar, as falhas no sistema de energia podem resultar em interferências nas operações normais do sistema. Interferências graves podem até mesmo desestabilizar o sistema e gerar apagões em grande escala. A eliminação das falhas é, portanto, um componente integral do design, da manutenção e das operações do sistema de transmissão e distribuição de energia. Os esquemas de proteção desenvolvidos para identificar e eliminar falhas atendem a uma variedade de objetivos em toda a rede:

- Remover o elemento avariado do resto do sistema.
- Limitar ou evitar danos a equipamentos.
- Evitar oscilações graves de energia ou instabilidade do sistema.
- Minimizar efeitos adversos no consumo dos clientes.
- Manter a capacidade de transferência do sistema de energia.
- Prevenir a ocorrência de lesões pessoais.

Energia para manter as luzes acesas
Saiba mais

Esquemas, aplicações e convergência

Um método comumente implementado em subestações da rede elétrica é um esquema de proteção assistido por comunicação na rede remota (WAN). Esse tipo de esquema facilita a coordenação e o compartilhamento de dados entre dispositivos de proteção e possibilita o emprego de métodos que aumentam a confiança, seletividade, segurança e velocidade do esquema. Comunicações confiáveis possibilitam a implementação de esquemas de comparação diferenciados, como proteção diferencial da corrente de linha (87L).

As redes remotas (WAN) são usadas para transmitir canais multiplexados de proteção, além de outros serviços da subestação (voz, teleproteção, telemetria, vídeo, controle e automação, e-mail e LAN corporativa), e se tornaram uma parte integral e necessária dos sistemas modernos de proteção de rede.

TDM/SONET foram amplamente adotadas em todo o setor de rede elétrica como a tecnologia preferencial de transporte de rede remota (WAN), porque fornece baixa latência, determinismo e desempenho com assimetria mínima. Contudo, o setor apresenta uma tendência nítida de adesão à rede Ethernet e baseada em pacotes para todas as aplicações e todos os serviços de energia, incluindo proteção. A motivação para abandonar os sistemas baseados em TDM, principalmente os sistemas SONET e SDH, é impulsionada pelo desejo de convergir as redes de TI e OT e padronizar um conjunto comum de interfaces a fim de reduzir despesas de capital e operacionais. A migração para tecnologias de rede baseadas em pacotes, como Carrier Ethernet, criou o desafio de desenvolver serviços de teleproteção que forneçam o determinismo e o desempenho garantido, necessários à proteção de aplicações.

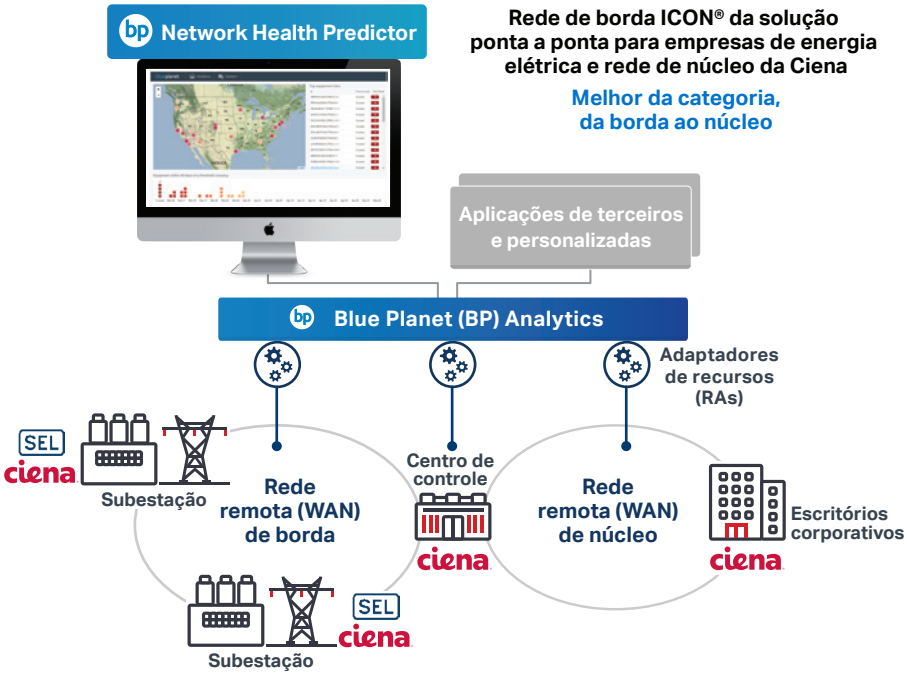

Figura 1. Rede de borda ICON da solução ponta a ponta para empresas de energia elétrica e rede de núcleo da Ciena

A motivação para abandonar os sistemas baseados em TDM, principalmente os sistemas SONET e SDH, é impulsionada pelo desejo de convergir as redes de TI e OT e padronizar um conjunto comum de interfaces a fim de reduzir despesas de capital e operacionais.

Evitar outra interrupção de energia como a de 2003 requer uma solução com latência baixíssima e desempenho de failover muito rápido. Se ocorrer falha no sistema de energia, os esquemas de proteção assistidos por comunicação de toda a rede remota (WAN) operam para isolar a falha e evitar instabilidade relacionada à falha. Os tempos de religamento da infraestrutura principal da linha de transmissão precisam estar na casa dos milissegundos. Se a condição da falha do sistema de energia não for detectada nem comunicada com a menor das latências, vários equipamentos podem ser danificados e grandes porções da rede elétrica podem ser afetadas.

Para solucionar esses desafios, a Ciena buscou uma solução de ponta para a subestação de energia, fornecida pela Schweitzer Engineering Labs (SEL).

A solução de transporte de pacotes determinísticos SEL ICON (Integrated Communications Optical Network) fornece o tráfego crítico e a latência determinística em uma rede de transporte Ciena Carrier Ethernet. O conceito é preservar as características de desempenho de TDM, que estão disponíveis na plataforma ICON SONET, sem prejudicar desempenho durante o transporte em uma rede Carrier Ethernet como um protocolo de transporte de rede remota (WAN).

Mais sobre a Ciena e a solução SEL

Resultados de teste de latência e failover do encapsulamento SONET por meio de um núcleo Ciena Carrier Ethernet

Os resultados de teste a seguir demonstram que é possível usar o conceito de VSN (Virtual SONET Network) da SEL ICON para oferecer consistentemente baixa latência, baixa assimetria de canal e restauração extremamente rápida do sistema OT para falhas de redes de núcleo e redes de borda. Esses resultados de desempenho atendem aos requisitos das aplicações de proteção.

Vários padrões especificam os requisitos de desempenho do canal de comunicação das aplicações da subestação de energia elétrica. Ao considerar os requisitos de desempenho especificados nas normas IEEE 1646 e IEC TR 61850-90-12 e incluir os requisitos do fabricante de relés em termos de assimetria e restauração, podemos estabelecer um resumo dos requisitos de desempenho do canal de comunicação das aplicações de proteção (Tabela I).

Esquema	Latência (ms)	Assimetria (ms)	Restauração (ms)
Proteção 87L	5	< 0,5	5
Proteção piloto	8	5	5
Deslocamento de transferência direta	10	5	5

Tabla I. Requisitos de rendimiento del canal de comunicaciones para circuitos de protección

Teste e resultados de desempenho de latência

Os casos de teste a seguir fornecem dados de desempenho de encapsulamento de serviços usando SEL ICON em uma rede de núcleo Carrier Ethernet (nó IT WAN Ciena 3930/ 3932). Essa rede usou a topologia indicada na Figura 2.

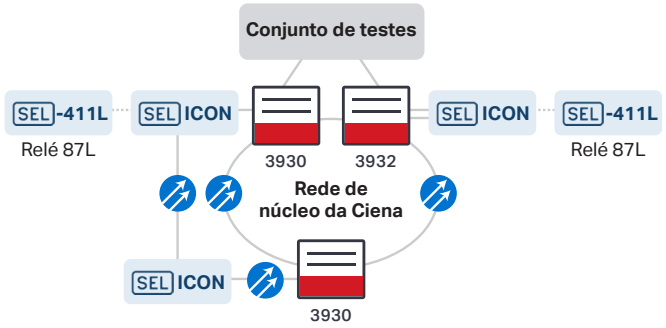

Figura 2. Teste de topologia de rede

Para estabelecer um conjunto de dados de linha de base, dois relés 87L foram conectados a um jumper de fibra ótica (Figura 3).

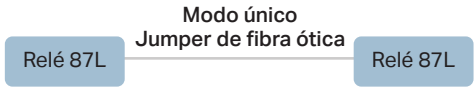

Figura 3. Teste de topologia de rede

Em seguida, os relés 87L de linha de base foram conectados a uma VSN de três nós. As informações sobre latência e assimetria foram registradas para fins de comparação com os dados do relé de linha de base. A Figura 4 mostra a topologia do sistema de teste VSN.

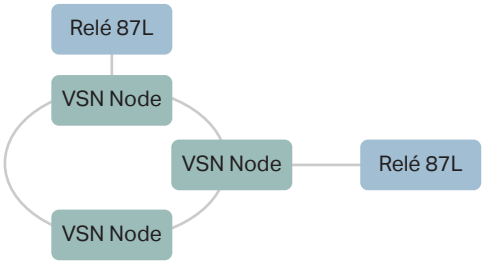

Figura 4. Rede de teste VSN

A rede de teste VSN foi expandida para a topologia exibida na Figura 1. A rede remota (WAN) Ciena Carrier Ethernet de três nós foi inserida para atuar como a rede de núcleo. Dessa forma, a VSN foi encapsulada por meio da WAN e os relés 87L continuaram conectados à VSN. Foi usado um conjunto de testes para gerar tráfego de rede, simulando condições típicas de carga de tráfego. Isso foi feito para confirmar se a rede de núcleo poderia usar as configurações de QoS para dar à VSN maior prioridade em relação a outro tráfego de rede e manter o desempenho determinístico. Para o núcleo da rede Ciena Carrier Ethernet, a VSN recebeu uma F-RCoS (Fixed Resolved Class of Service) equivalente a 0 e o tráfego do conjunto de teste recebeu uma F-RCoS de 7.

O teste foi executado em nós de rede remota (WAN) de núcleo Ciena Carrier Ethernet indicados na Figura 1. Em cada teste, foi usado um relé 87L para estabelecer um circuito de proteção 87L. Recursos de medição interna dos relés foram usados para avaliar a latência e a assimetria do canal. Os parâmetros de desempenho de latência e assimetria foram registrados para a implementação da rede Carrier Ethernet. Uma série de cinco medições separadas foram realizadas em cada teste, e a média das latências e assimetrias foi calculada.

A Tabela II mostra os resultados comparados aos dados de base e VSN apenas. Cada dispositivo de borda VSN OT usou um buffer de flutuação de fase (jitter) de tamanho variável, com base no PDV da rede de núcleo para otimizar a latência por meio da rede de núcleo de TI. Foi usada uma configuração de PDV para ajustar o tamanho do buffer de flutuação de fase (jitter). Para a rede Carrier Ethernet, foi usado um PDV de 50 µs.

Os resultados do teste na Tabela II mostram que a rede Ciena Carrier Ethernet introduziu apenas uma latência adicional de ida e volta de 1 ms comparada às configurações de linha de base e VSN apenas. A rede de núcleo introduziu um mínimo de assimetria. Os resultados estão bem dentro dos requisitos de desempenho do canal de comunicação para circuitos de proteção 87L resumidos na Tabela I.

Parâmetro	Linha de base (ms)	VSN (ms)	VSN e Carrier Ethernet (ms)
Latência (RTD)	0,1	0,1	1,1
Assimetria	0,0	0,0	0,04

Tabela II. Resultados de teste de desempenho do canal de comunicação

O mais importante é que o teste confirmou que as configurações apropriadas de QoS podem ser definidas para dar aos circuitos VSN a prioridade suficiente em relação a outros serviços, a fim de garantir a entrega determinística de quadros VSN e, assim, preservar a integridade e a periodicidade dos dados SONET encapsulados.

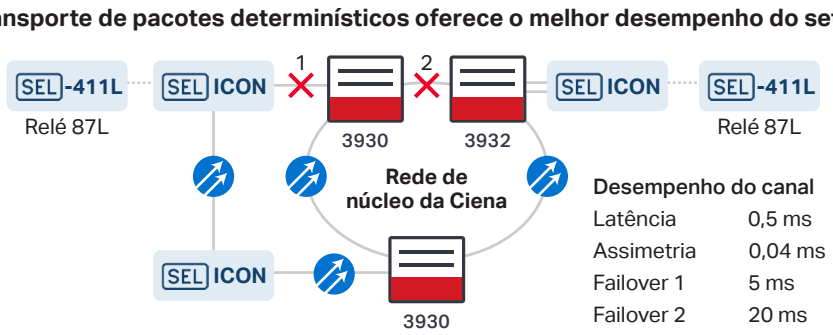

Figura 5. Resultados de teste de failover de rede de núcleo e de borda

Resultados do teste de reparação da rede

O desempenho de reparação da rede em termos de caminhos VNS pode ser otimizado com o provisionamento de túneis ponta a ponta desprotegidos por meio da rede de núcleo. A reparação da rede é então realizada pelo dispositivo de borda VSN OT, e não pela rede de núcleo.

Os seguintes testes de reparação foram realizados para avaliar o desempenho comparativo dos failovers de rede de borda em relação à de núcleo. O teste de failover da rede de núcleo envolveu dividir a fibra no link, como mostra a Figura 5 (Failover 1) e incumbir a rede de núcleo da execução de um failover no caminho redundante, no lado oposto do anel. No teste de failover da rede de borda indicado na Figura 5 (Failover 2), um link do dispositivo de borda OT para o nó da rede remota (WAN) Ciena Carrier Ethernet foi desfeito e a rede de borda OT executou a reparação.

Os resultados do teste de failover na Figura 5 mostram que é possível obter uma vantagem de desempenho significativa com o uso da rede de borda OT para realizar a reparação da rede.

Resumo

As empresas de serviços públicos estão implementando redes de energia altamente inteligentes para melhorar a eficiência operacional, atender às demandas do consumidor e cumprir determinações governamentais. Essas redes inteligentes são baseadas em uma rede de comunicação bidirecional que deve ser altamente confiável e ter baixa latência, além de ser fácil de instalar e operar.

Este documento demonstrou que uma abordagem VSN é o melhor método para oferecer proteção de missão crítica e controlar o tráfego do sistema em uma rede remota (WAN) Carrier Ethernet, ao mesmo tempo que garante que os atributos de desempenho do canal de comunicação atendem aos requisitos especificados nas normas IEEE 1646 e IEC TR 61850-90-12. Ela soluciona elegantemente o desafio de migrar circuitos de proteção baseados em TDM para Ethernet sem afetar o desempenho da rede. O design, planejamento e implementação da rede OT são simplificados para redes complexas com elementos de rede de núcleo e de borda de subestação que envolvem uma combinação de tecnologia de transporte e equipamentos do fabricante.

Essa solução utiliza um modelo de provisionamento simplificado que pode ser facilmente dimensionado à medida que a topologia da rede muda e cresce. O uso de túneis ponta a ponta por meio da rede de núcleo Carrier Ethernet com a mais alta configuração de QoS abaixo do NMS garante que o desempenho de circuitos críticos se mantenha conforme ocorrem mudanças na rede, o que evita a necessidade de gerenciar individualmente cada circuito de proteção. Além disso, embora o tráfego tenha maior prioridade, o atraso de todo o outro tipo de tráfego pode ser insignificante (um máximo de 0,1 µs por link de rede para uma rede de núcleo 10 GbE).

Faça suas perguntas na Comunidade da Ciena