PROTEÇÃO E SUPERVISÃO DE SISTEMAS ELÉTRICOS NUMA ESTRATÉGIA SMART GRID COM REDES IP DE NOVA GERAÇÃO

POWER SYSTEMS PROTECTION AND SUPERVISION IN A SMART GRID STRATEGY USING NEW GENERATION IP NETWORKS

Carlos Alberto Malcher Bastos[1], Joberto Sérgio Barbosa Martins[2], José Augusto Suruagy Monteiro[2], Anilton Salles Garcia[3], Ana Elisa Ferreira[3], João Marcos da Silva[1] e Walter da Costa Pinto Neto[2]

[1]Universidade Federal Fluminense, Departamento de Engenharia de Telecomunicações
cmbastos@telecom.uff.br, jmarcos@midiacom.uff.br, anaelisa@telecom.uff.br

[2]Universidade Salvador, NUPERC - Núcleo de Pesquisa em Redes e Computação
joberto@unifacs.br, suruagy@unifacs.br, wcpneto@gmail.com

[3]Universidade Federal do Espírito Santo, Departamento de Informática
anilton@inf.uff.br

Resumo
Este artigo apresenta um posicionamento sobre a arquitetura, o plano de controle e a gerência para redes e infraestruturas de telecomunicações das operadoras de energia num cenário de solução Smart Grid (SG) fazendo uso das redes IP. As novas redes IP são apresentadas, o cenário Smart Grid é introduzido e um modelo de arquitetura e seus aspectos de gerência são discutidos. Os autores argumentam sobre a necessidade da utilização de múltiplas soluções tecnológicas para o atendimento dos requisitos de proteção e supervisão, discutem a adoção de um plano de controle integrador e avaliam os impactos na solução de gerência e na engenharia de tráfego como elementos de controle e otimização da solução.

Palavras-chave: Smart Grid; Proteção, Supervisão; Sistemas Elétricos; Redes IP de Nova Geração; GMPLS (Generalized Mutiprotocol Label Switching); DCN (Dynamic Circuit Network).

Abstract
This position paper, presents an overview of the architecture, control plane and management for the network and telecommunications infrastructure of an energy utility company in a Smart Grid (SG) solution scenario, using IP networks. The new IP networks are presented, a Smart Grid scenario is introduced, and its architecture model and management issues are discussed. The authors argue about the need of using multiple technological solutions to satisfy protection and supervisory requirements; discuss the adoption of an integrating control plane, and evaluate its impact on the management solution and in the traffic engineering as the solution control and optimization elements.

Keywords: Smart Grid; Protection; Supervision; Power Systems; New Generation IP Networks; GMPLS (Generalized Mutiprotocol Label Switching); DCN (Dynamic Circuit Network).

1 NOVA GERAÇÃO DE REDES IP

A Internet, como é conhecida hoje, é uma rede suportada por tecnologias básicas desenvolvidas há mais de 30 anos, que evoluiu de uma rede de pesquisa interconectando algumas instituições, para uma rede global que permite a troca de informação, serviços e comunicação em todo o mundo. Seu papel, tamanho e complexidade ultrapassaram em muito qualquer previsão de seus criadores e, em suma, a Internet se tornou a rede núcleo da sociedade e da economia moderna. Acompanhando e fomentando este crescimento, as redes corporativas também adotaram o modelo IP, possibilitando sua integração em escala mundial. O uso comercial e social generalizado da Internet e das redes IP apresenta, neste contexto, novos e importantes desafios de pesquisa e desenvolvimento.

Muitos pesquisadores em todo o mundo já identificaram algumas limitações da arquitetura da rede IP atual e concordam que necessitamos de uma nova abordagem para o desenho das redes IP do futuro e da denominada Internet do Futuro (IF). Diferentes estudos e propostas têm sido apresentados tanto para resolver as limitações do modelo atual do IP como para desenvolver uma nova e próxima geração de rede (*New and Next Generation Networks*) com capacidades inovadoras em uma perspectiva compatível com as demandas e necessidades de serviços das instituições atuais e da sociedade da informação como um todo.

As “Redes de Próxima Geração” (*Next Generation Networks* – NGN) e as “Redes de Nova Geração” (*New Generation Networks* – NWGN) juntamente com a “Internet do Futuro” [1]são as principais iniciativas em pesquisa e desenvolvimento em curso pela comunidade internacional.

As Redes de Próxima Geração (NGNs) constituem fundamentalmente numa abordagem da área de telecomunicações que procura definir a arquitetura e os padrões necessários para que as redes IP possam suportar os serviços de telecomunicações como um todo. As NGNs incluem aspectos como a integração de serviços de dados, voz e imagem numa perspectiva de telecomunicações e negócios associados.

As Redes de Nova Geração (NWGNs) é ousadia pura e além da Internet atual. Neste sentido, implica em repensar a arquitetura IP e seus protocolos avaliando a factibilidade de profundas mudanças arquiteturais na rede de suporte atual da Internet, de instituições e de empresas como um todo (baseada em IP). A abordagem NWGN inclui aspectos como o roteamento baseado em fluxos (OpenFlow), novos protocolos de identificação e endereçamento, além de novas facilidades para a gerência e segurança da rede.

A iniciativa da "Internet do Futuro", por sua vez, constitui uma abordagem inovadora e diferenciada que busca soluções para uma utilização da Internet e da Web numa escala e aplicabilidade beirando a generalização. Em efeito, a sociedade atual deseja que a Internet possa suprir a maioria das suas necessidades em termos de aplicações em rede tais como a multimídia, telefonia, acessos banda larga, privacidade e mobilidade, para citar algumas delas.

De maneira geral as iniciativas de novas redes IP apresentam um conjunto de características relevantes e comuns tais como:

- Alta disponibilidade em termos de velocidade e banda passante;
- Elevada integração funcional com uma verticalização acentuada das funcionalidades;
- Orientação para a virtualização de serviços, equipamentos e elementos funcionais;
- Integração web acentuada - aspectos semânticos e de integração de dados;
- Elevada confiabilidade operacional em termos de resiliência, sobrevivência e capacidade de recuperação de falhas;
- Tendência acentuada para uma elevação do nível de autonomia dos elementos e componentes (computação e serviços autonômicos); e
- Provisionamento da Qualidade de Serviço (QoS) com base nos serviços e/ou aplicações demandantes.

Estas novas características funcionais das redes IP de próxima ou de nova geração integradas à Internet/web são significativas para um conjunto de aplicações novas ou

legadas que podem vir a se beneficiar da evolução tecnológica das redes e, dentre estas, avaliaremos neste artigo a perspectiva das soluções Smart Grid (SG) em redes IP.

Entre os principais projetos que desenvolvem os novos princípios das redes IP, as novas tecnologias e novos cenários de aplicação para a "nova geração" temos:

- *Internet2* (Internet2) [2] – A Internet2 é um consórcio de redes avançadas nos EUA. Liderada pelas comunidades de pesquisa e educação desde 1996, a Internet2 promove o desenvolvimento de novas aplicações e pesquisas fortemente baseadas em uma rede com capacidades elevadas e fazendo uso de tecnologias revolucionárias para a Internet.
- *Global Environment for Network Innovations* (GENI) [3]– Este projeto, patrocinado pela *National Science Foundation*, visa suportar experimentos que variam desde novas pesquisas relacionadas ao desenho da infraestrutura de redes até sistemas distribuídos para os aspectos teóricos subjacentes do valor social, econômico e tecnológico das redes.
- *Future Internet Research and Experimentation* (FIRE) [1][4] – O FIRE tem o suporte do programa *Information and Communication Technologies* (ICT) da Comunidade Europeia. O FIRE trata as novas expectativas que estão emergindo para a Internet provendo um ambiente de pesquisa para a investigação e a validação experimental de ideias altamente inovadoras e revolucionárias. O projeto FIRE envolve o *FIRE Facility* (uma rede experimental) e o *FIRE experimentally-driven research* (pesquisa multidisciplinar visionária).
- *Gigabit European Academic Network* (GÉANT) [5] – A GÉANT é uma rede de alta capacidade que inclui mais de trezentas instituições de pesquisa e educação em 32 países através de 34 redes nacionais e regionais para educação e pesquisa. Atualmente, o projeto GÉANT está direcionado para o desenvolvimento e implementação de ferramentas e serviços, para que a comunidade de pesquisa e educação possa conseguir o melhor desempenho possível da rede. A GÉANT é gerenciada pela DANTE (*Delivery of Advanced Network Technology to Europe*).

2 PROTEÇÃO E SUPERVISÃO DE SISTEMAS ELÉTRICOS NUMA ESTRATÉGIA SMART GRID COM REDES IP DE NOVA GERAÇÃO

Existe uma grande demanda para uso das redes IP (inclusive a Internet) em aplicações as mais diversas possíveis que exigem, dentre outros requisitos, uma alta disponibilidade, uma elevada confiabilidade e garantias estritas de qualidade de serviço. Como exemplo, temos as aplicações em tempo real, aplicações científicas (*e-science*) e de negócios e as aplicações de proteção, supervisão e controle num estilo Smart Grid [6][7] [8].

A proteção e a supervisão de sistemas elétricos é um problema importante, antigo e de interesse de toda a comunidade de sistemas elétricos que tem sido tratado e implantado de forma limitada com o uso principalmente de enlaces dedicados e soluções centralizadoras (Figura 01).

Esta solução tem uma tendência clara a evoluir na quase totalidade de seus aspectos de implantação, operação e gerência. A título de exemplo, temos a utilização de novos equipamentos de proteção e comandos de teleproteção baseados na norma IEC61850 [9][10]. Esta norma, em resumo, especifica os requisitos internos às subestações procurando automatizá-las e está em estudo uma especificação para sua utilização num ambiente distribuído das linhas de transmissão.

A solução Smart Grid (SG) representa de forma bastante abrangente a ideia geral de evolução dos sistemas de proteção, supervisão e controle dos sistemas de geração e distribuição de maneira geral [11][12].

Do ponto de vista dos sistemas elétricos e operadoras de energia, a solução SG constitui-se num componente crítico do processo de modernização destes fazendo uso de uma infraestrutura de redes e telecomunicações. O SG pode ser entendido, em resumo, como uma infraestrutura de redes e telecomunicações com um conjunto de sistemas, aplicações, facilidades funcionais e características técnicas tais como interoperabilidade com sistemas legados, comunicação bidirecional, capacidade de recuperação de falhas,

alto desempenho e segurança, dentre outras. O SG deve se constituir numa solução integradora para os elementos do modelo conceitual adotado na área de energia (NIST *Reference Model*) tais como a geração, transmissão, distribuição, operação, provedores de serviço e usuários finais.

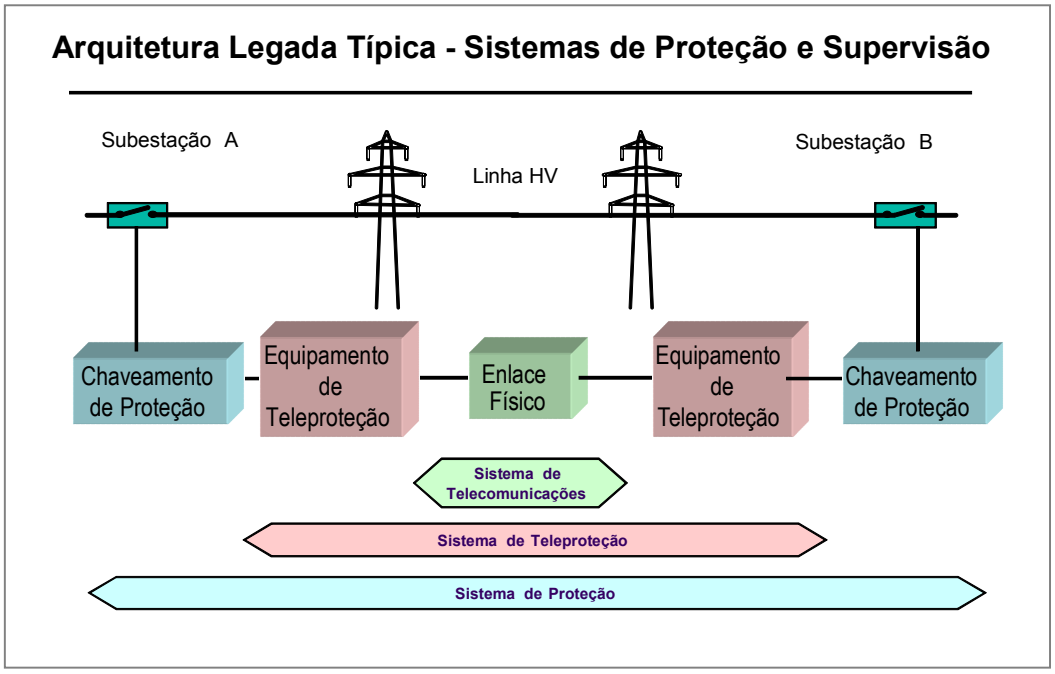

Figura 01 – Sistema Legado Típico de Proteção, Teleproteção e Telecomunicações em Operadoras de Sistemas Elétricos

Retomando a questão dos sistemas atuais e legados, é fato que os sistemas de potência energizados com tensões elétricas altas em três fases podem sofrer falhas devido a inúmeras causas, tais como problemas de isolamento elétrico, mau tempo, animais, falhas de manuseio que, por sua vez, interrompem o fluxo de energia. De forma a evitar-se distúrbios na rede elétrica e grandes colapsos desta, medidas de proteção e requisitos rígidos são empregados para a prevenção e compensação das falhas. Normalmente, diferentes requisitos existem dependendo da abrangência geográfica do sistema a ser protegido, pois sistemas de proteção de falhas podem atuar localmente sobre geradores, transformadores e outros elementos importantes, como em uma usina

geradora/subestação, ou podem atuar de forma distribuída protegendo as linhas de transmissão em alta tensão.

Em termos práticos, existem na maioria das operadoras do sistema elétrico duas redes quase paralelas:

- Uma Rede Operativa, usada principalmente para supervisionar e telecomandar subestações ou pequenas usinas geradoras desatendidas, e
- Uma Rede de Proteção normalmente dedicada, limitada e desprovida de melhores recursos tecnológicos para a proteção dos sistemas elétricos.

O estudo e a avaliação de novas alternativas de implantação e operação para as Redes de Proteção, Supervisão e Controle de Sistemas Elétricos constitui-se então um aspecto importante para as operadoras de energia motivadas principalmente pela existência de novos recursos tecnológicos, serviços, funcionalidades e características para as redes IP de nova geração. O desenho de uma integração e evolução conjunta para as Redes Operativa e de Proteção permite uma economia de escala, de operação e de manutenção de interesse da comunidade.

3 MODELOS DE ARQUITETURA DE REDES IP – DIVERSIDADE DE SISTEMAS E APLICAÇÕES

As novas aplicações sobre IP (*IP-based applications*) estão levando as redes IP ao seu limite tecnológico. Aplicações distribuídas que requerem garantias estritas, como a computação em grade (*GRID Computing*), a computação em nuvem (*Cloud Computing*), a Proteção e Supervisão de Sistemas Elétricos, as aplicações médicas, o controle aéreo e urbano e a automação veicular, entre outras, fazem uso de tecnologias e serviços diversificados baseados no IP e têm suas arquiteturas específicas moldadas segundo os seus respectivos requisitos funcionais e operacionais.

De maneira geral, percebe-se que um caminho possível para a solução de um determinado problema mais setorial passa, em princípio, pela identificação e avaliação de

uma arquitetura ou arcabouço de solução envolvendo as alternativas tecnológicas baseadas ou relacionadas ao IP para as tecnologias, serviços e protocolos existentes.

Este novo perfil de utilização das redes IP exige cada vez mais garantias de desempenho e disponibilidade de rede, incluindo a interconexão em alta capacidade. Para atender a estes requisitos, têm sido desenvolvidas ao longo dos anos diversas melhorias na pilha de protocolos original, com o acréscimo de novas facilidades e capacidades para o controle, a gerência, a medição, a segurança e a engenharia de tráfego.

Na seção seguinte consideramos uma adequação do modelo de operação das redes IP especificamente para o caso da proteção, supervisão e controle de sistemas elétricos num contexto Smart Grid.

3.1 Redes de Proteção, Controle e Supervisão de Sistemas Elétricos num Contexto IP Smart Grid

Os sistemas de proteção foram, até então, fundamentalmente baseados numa operação com enlaces confiáveis dedicados e independentes, resultando numa efetiva separação entre as Redes Operativas e de Proteção.

Uma solução alternativa para uma nova geração de redes de proteção e supervisão de sistemas elétricos num contexto Smart Grid pode ser obtida com base na utilização de canais protegidos, confiáveis, redundantes e de alto desempenho sobre uma estrutura dinâmica e compartilhada de rede de pacotes baseada no IP.

Como alternativas efetivas para a implantação de uma nova geração de redes de proteção e supervisão e controle destacamos as seguintes alternativas tecnológicas:

- Sistema de Proteção e Supervisão basedo em Redes IP Ópticas com sinalização GMPLS (*Generalized Multiprotocol Label Switching*) [13]; e
- Provisionamento de circuitos dinâmicos de rede com DCN (*Dynamic Circuit Network*) [14].

De maneira geral, a solução baseada numa arquitetura de redes IP ópticas com GMPLS leva a uma solução de provisionamento de serviços e recursos mais estática para a

proteção, supervisão e o controle dos sistemas elétricos. Por outro lado, a solução baseada no DCN leva a uma solução de rede híbrida e dinâmica quanto ao provisionamento de serviços e recursos de maneira geral.

Outra distinção básica e relevante entre as duas alternativas propostas é baseada no fato do DCN ser uma solução mais orientada para uma operação envolvendo múltiplos domínios administrativos enquanto que a solução estática baseada no GMPLS é orientada e focada para um cenário de operação baseado num único domínio administrativo.

Segue uma apresentação das arquiteturas correspondentes e uma discussão sobre as funcionalidades, tecnologias, serviços e protocolos envolvidos nas mesmas com suas vantagens, desvantagens e demais aspectos operacionais e mercadológicos.

3.2 Proteção e Supervisão com Redes IP Ópticas e GMPLS

A arquitetura ilustrada na figura 02 indica os componentes arquiteturais básicos para uma Rede de Proteção, Controle e Supervisão de Sistemas Elétricos com base em redes IP ópticas e com o plano de controle e sinalização baseado no GMPLS.

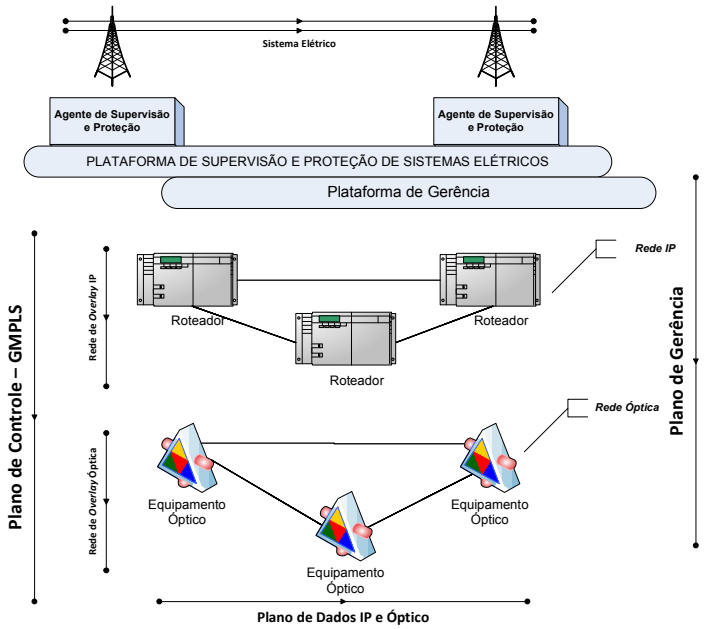

Figura 02: Arquitetura IP Óptica com GMPLS para a Proteção e Supervisão de Sistemas Elétricos

Na arquitetura proposta existem dois níveis funcionais distintos e independentes do ponto de vista do plano de dados. São eles o nível de comutação e roteamento IP e o nível de comutação e roteamento óptico que, do ponto de vista da arquitetura para o controle, supervisão e proteção de sistemas elétricos, podem ser abstraídos como redes sobrepostas (*overlay networks*) independentes.

A sinalização é o elemento integrador desta arquitetura e o GMPLS é o protocolo de sinalização assumido na implantação da solução que deve provisionar circuitos nas redes de overlay IP e óptica.

O requisito básico suportado pela arquitetura proposta com relação à Rede de Proteção é o provisionamento de um canal lógico sobre uma rede IP Óptica, onde este canal lógico apresenta os seguintes requisitos funcionais (Figura 03):

- Provisionado sob demanda;
- Alta velocidade;
- Mecanismos de detecção e recuperação de falhas eficiente e compatível com os requisitos do setor (50 mseg máximo);
- Confiável;
- Redundante; e
- Integrado com a solução de Rede Operativa.

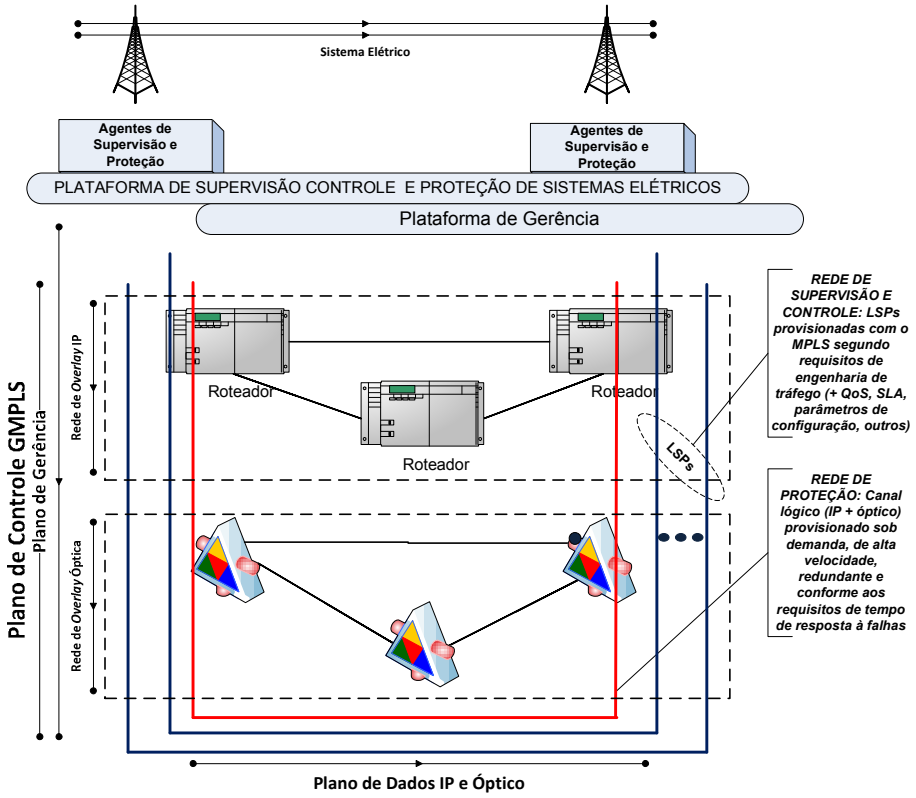

Figura 03 – Provisionamento de Canais Lógicos para a Rede de Proteção e Supervisão de Sistemas Elétricos

Com relação à Rede de Supervisão e Controle, a arquitetura proposta permite o provisionamento de circuitos MPLS (*LSPs – Logical Switched Paths*) através da rede de roteadores segundo um dimensionamento, alocação e distribuição de tráfego que pode seguir uma estratégia de engenharia de tráfego. Assim sendo, a arquitetura proposta garante alguns ganhos relevantes, a saber:

- Permite a efetiva integração entre a Rede Operativa e a Rede de Proteção na medida em que utiliza a mesma infraestrutura de redes sobrepostas para o provisionamento de circuitos com diferentes características e requisitos funcionais (canais de supervisão e canais de proteção).
- Permite a "verticalização" na implantação dos canais da Rede de Proteção.

A verticalização funcional é um aspecto arquitetural relevante que permite e viabiliza a implantação dos canais de proteção na medida em que estes exigem o

atendimento de um conjunto de requisitos que não são normalmente atendidos pelas redes de pacotes tradicionais. A verticalização perpassa, inter-relaciona e integra os planos funcionais (Figura 04) e é uma abordagem de projeto atual que tem sido proposta e utilizada nas redes de nova geração e na Internet do Futuro. A abordagem tem sido comumente referenciada como "design do zero" (*clean slate design*) e teve suas origens em alguns desenvolvimentos de novas abordagens e paradigmas de rede como, a título de exemplo, o roteamento de fluxo aberto (*open flow routing*).

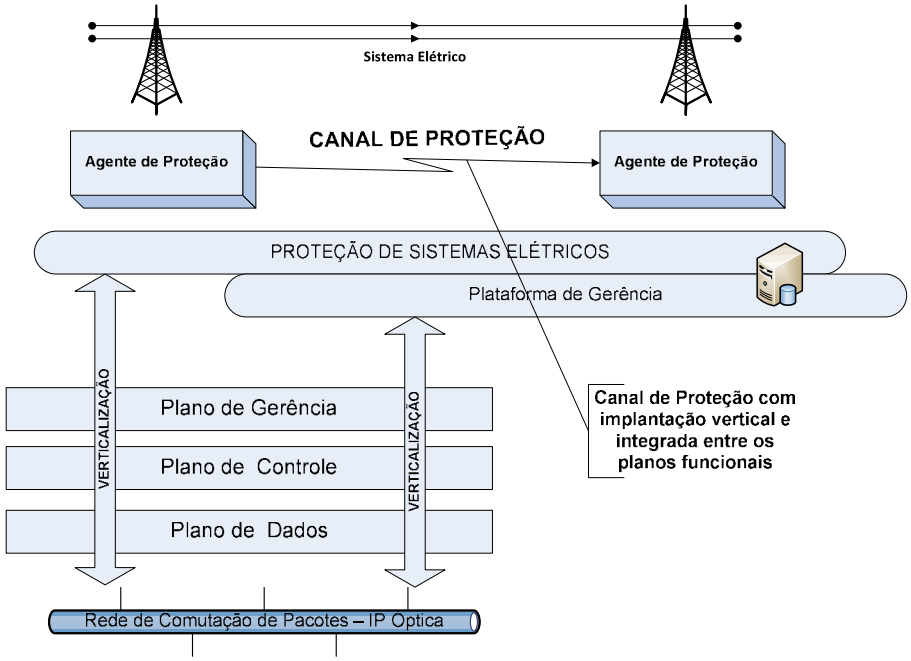

Figura 04 – Design para a Proteção de Sistemas Elétricos

3.3 Proteção e Supervisão com Tecnologia DCN (*Dynamic Circuit Network*)

A solução DCN (*Dynamic Circuit Network)* [15] é um serviço dinâmico de provisionamento de circuitos entre diferentes domínios administrativos. Ela foi desenvolvida em parceria da Internet2 com a ESNet, MAX, USC ISI East e a George Mason University, sendo a base para o seu serviço ION (*Interoperable On-Demand Network*) [16]. Os circuitos são estabelecidos entre usuários que, normalmente, requerem uma grande quantidade de banda dedicada, incluindo conexões confiáveis por períodos variando de

minutos a dias. Circuitos ópticos dedicados podem ser alocados para aplicações que requerem mais banda.

Nas redes DCN a gerência e o controle das múltiplas redes são realizados de forma transparente, automática e dinâmica. A gerência e controle no DCN estabelecem conexões com diferentes granularidades, cruzando múltiplos domínios administrativos com requisitos estritos de desempenho. Os usuários DCN são autenticados, existe uma negociação de parâmetros de operação e faz-se uma monitoração dos mesmos para o estabelecimento, desativação e manutenção dos circuitos. Além disso, DCN faz isolamento e diagnóstico de falhas e bilheta o serviço de forma coordenada em cada um dos domínios envolvidos. Assim, a solução DCN desenvolve uma solução para os planos de gerência e controle numa estratégia multi-domínio.

Uma das soluções usada na Internet2 para a implementação e suporte da solução DCN é o DRAGON (*Dynamic Resource Allocation via GMPLS Optical Networks*) [17]. O projeto DRAGON desenvolveu a tecnologia usada para construir uma infraestrutura de rede que permite o provisionamento dinâmico de seus recursos para estabelecer caminhos determinísticos em uma rede de pacotes, atendendo assim aos requisitos dos vários tipos de usuários finais.

O AutoBAHN (*Automated Bandwidth Allocation across Heterogeneous Networks*) é um sistema desenvolvido pela GÉANT para permitir a alocação dinâmica de circuitos. O AutoBAHN é o resultado de pesquisas para automatizar o estabelecimento de circuitos fim a fim interdomínio com garantia de capacidade [18]. Outra solução é o UCLP (*User Controled Light Paths*) [19] que permite o estabelecimento de circuitos intra e interdomínio através do uso de Serviços Web (*Web Services*). Diferentemente dos outros dois projetos, o UCLP usa o plano de gerência, via protocolo TL1, em vez do plano de controle para interagir com os equipamentos.

A utilização da solução DCN como suporte à implementação das soluções de proteção e supervisão de sistemas elétricos segue as seguintes premissas arquiteturais e de projeto:

- O DCN é utilizado como elemento de projeto no escopo das interconexões em sistemas administrativos distintos que, em efeito, corresponde a um requisito importante numa estratégia SG onde diversas operadoras de energia devem necessariamente interconectar seus sistemas de forma a otimizar os recursos em termos de Países ou regiões de atendimento ao usuário;
- A solução DCN é utilizada como alternativa para os canais fora de banda (*out-of-band*) na solução de operação e gerência do Smart Grid.

3.4 GMPLS como Plano de Controle Integrador

As soluções de proteção e supervisão com Redes IP Ópticas e com o DCN fazem uso efetivo do plano de controle da rede através da utilização de um protocolo de sinalização. Em ambas as propostas o protocolo de sinalização é um elemento fundamental e integrador.

No caso específico da solução com Redes IP Ópticas e GMPLS, tem-se uma estrutura com domínio administrativo, em princípio, único, multi-tecnológica (MPLS, Ethernet, SONET/SDH, WDM, outra) e multi-nível. Por solução multi-nível, entende-se que os domínios ou regiões de atuação dos Sistemas Elétricos podem operar em diferentes áreas/regiões de roteamento ou virtualmente através de fronteiras entre regiões ou áreas. O aspecto multi-tecnológico inerente às Redes de Proteção e Supervisão de sistemas elétricos faz com que seja necessária a implementação de uma solução de rede híbrida envolvendo capacidades tanto da rede IP como da rede óptica.

No caso específico da solução DCN tem-se as mesmas considerações anteriores acrescentando-se novos requisitos de operação derivados da característica de uma atuação entre múltiplos domínios administrativos. Neste contexto, tem-se a ressaltar que o protocolo de sinalização opera numa estratégia multisserviço e com múltiplas políticas de administração e gerência de recursos. Estes requisitos são necessários na medida em que as solicitações de provisionamento de circuitos por parte dos usuários DCN deve ser

transparentemente repassadas entre diversos domínios administrativos envolvidos no estabelecimento dos circuitos.

A partir destas considerações, faz-se necessário definir um protocolo de sinalização que seja capaz de lidar com a integração proposta, ou seja, tratar a questão da integração multi-tecnológica, multi-nível e, no caso do DCN, multi-domínio levando a uma solução efetiva de "rede híbrida". Nossa escolha de protocolo de sinalização para o plano de controle integrador foi o GMPLS (*Generalized Multiprotocol Label Switching*) [13]. Segue uma descrição de suas características mais importantes à luz da aplicação em foco.

O GMPLS estende o plano de controle (sinalização) do roteamento IP (roteadores) que, tipicamente, utiliza o MPLS (*Multiprotocol Label Switching*) e faz uso de protocolos de sinalização como o RSVP-TE (*Resource Reservation Protocol – Traffic Engineering*) e o CR-LDP (*Constraint Routing – Label Distribution Protocol*), entre outros. Em efeito, o GMPLS estende a operação da sinalização, antes restrita aos roteadores IP e à comutação de pacotes para outros equipamentos de rede que, como exemplo, comutam no tempo (comutadores e multiplexadores ópticos), em comprimentos de onda (multiplexadores WDM e equipamentos "*cross-connects*") e/ou usando recursos físicos como fibras ópticas (apagadas ou não).

Com relação às soluções de proteção e supervisão com Redes IP Ópticas e com o DCN, a unificação do plano de controle permite a integração necessária entre os equipamentos de comutação IP e de comutação óptica utilizados nestas soluções.

Um aspecto arquitetural relevante a considerar é o estabelecimento, encerramento, manutenção e gerência de circuitos fim a fim.

No caso da "Rede Operativa", esses circuitos são solicitados pelos usuários através de suas respectivas aplicações com o suporte de uma aplicação de "Engenharia de Tráfego" de forma a permitir que o "plano de dados" transporte eficientemente os dados dos usuários (Figura 05). Em outras palavras, a solução proposta cria LSPs (*Label Switched Paths*) através dos equipamentos envolvidos com base num planejamento de distribuição de tráfego que considera uma estratégia de otimização com engenharia de tráfego.

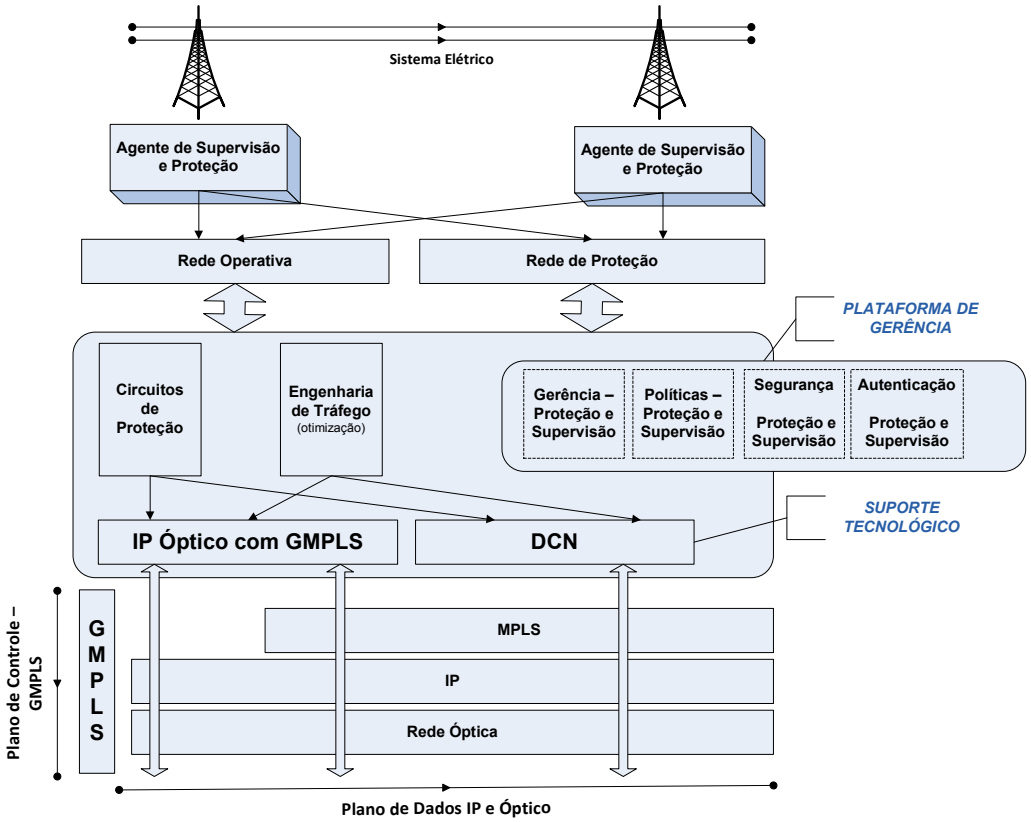

Figura 05 – Circuitos (LSPs) para as Redes de Proteção e Supervisão

No caso da "Rede de Proteção" os circuitos específicos de proteção são também criados através dos protocolos citados. No entanto, dado os requisitos do circuito de proteção, o estabelecimento, encerramento, monitoração e manutenção deste ocorre de forma estática sem levar em conta nenhuma abordagem de otimização como no caso da rede operativa.

A evolução do MPLS para GMPLS estendeu os protocolos de sinalização, RSVP-TE (*Resource reSerVation Protocol – Traffic Engineering*) e CR-LDP (*Constraint Routing – Label Distribution Protocol*), e os protocolos de roteamento, OSPF-TE (*Open Shortest Path First – Traffic Engineering*) e IS-IS-TE (*Intermediate System to Intermediate System – Traffic Engineering*), para acomodar as características das redes ópticas, Ethernet, SDH (*Synchronous Division Multiplexing*) e TDM (*Time Division Multiplexing*). Um novo protocolo, o LMP (*Link Management Protocol*) foi também introduzido para gerenciar e

manter o bom funcionamento dos planos e controlar os dados entre dois nós vizinhos. O LMP é um protocolo baseado em IP que inclui extensões para RSVP-TE e CR-LDP. A tabela 1 sumariza estes novos protocolos e as extensões que podem ser utilizadas pelo GMPLS [13].

Tabela 1 – Protocolos de Suporte e Extensões para o GMPLS

Protocolos		Descrição
Roteamento	OSPF-TE IS-IS-TE	Protocolos de roteamento para descobrir a topologia da rede e anunciar a disponibilidade de recursos (ex. banda ou proteção). Os principais desenvolvimentos são: • Anúncio de proteção de enlace (1+1, 1:1, desprotegido, tráfego extra). • FA-LSP (*forwarding adjacency*) implementação para melhorar a escalabilidade. • Anúncio e recebimento de informação em um enlace IP usando "enlace ID" • Descoberta de rota alternativa diversa do caminho principal (*shared-risk link group*).
Sinalização	RSVP-TE CR-LDP	Protocolos de sinalização para estabelecer LSPs. Os principais desenvolvimentos são: • "*Generic Labels*" permitem o uso conjunto de comutação de pacotes e comutação óptica na mesma rede. • Estabelecimento de LSPs bidirecionais. • Sinalização para estabelecimento de caminhos de backup (informação de proteção). • Associação rápida de rótulo (*label*) via rótulo sugerido. • Suporta a comutação de "agregados" (*waveband)* – agregados de comprimentos de onda são comutados em conjunto.
LMP - Gerência de Enlace		– Gerência de canal de controle: Estabelecimento através de negociação de parâmetros do enlace (ex. mensagens de *keep-alive*) e usado para assegurar a integridade do enlace (*hello*). – Verificação de conectividade do enlace: Assegura a conectividade física entre vizinhos usando uma mensagem de teste similar ao *ping*. – Correlação das propriedades dos enlaces: Identificação das propriedades dos enlaces entre nós adjacentes (ex. mecanismos de proteção). – Isolamento de Falhas: Isola falhas simples ou múltiplas no interior do domínio óptico.

3.5 Plano de Gerência para a Proteção e Supervisão no Contexto das Redes IP de Nova Geração – Um Posicionamento

Uma atividade de grande importância na operação das Redes de Proteção e Supervisão de Sistemas Elétricos é a sua gerência. Existem inúmeras e diversas

abordagens para a gerência de redes como um todo e, dentre estas, o modelo TMN (*Telecommunication Management Network*), definido pelo ITU-T (*International Telecommunications Union – Telecommunications*) na série de recomendações M.3000, provê um arcabouço para permitir a interconexão e comunicação entre redes e sistemas de suporte à operação (*OSS - Operations Support System*) e o plano de gerência (Figura 06).

O TMN, do ponto de vista da abordagem adotada para as Redes de Proteção e Supervisão de Sistemas Elétricos, é a nossa referência de implementação na medida em que define as áreas funcionais e as camadas lógicas que podem ser aplicadas à gerência. No entanto, em termos de um posicionamento visando uma solução arquitetural para as Redes Operativas e de Proteção, sua implementação é revista e estendida para atender as necessidades das redes IP de nova geração. De forma similar ao plano de controle, existem desafios importantes para a gerência e a nossa abordagem neste tópico é focada na identificação das camadas lógicas mais importantes para a aplicação considerada e um posicionamento quanto às soluções adotadas para estas.

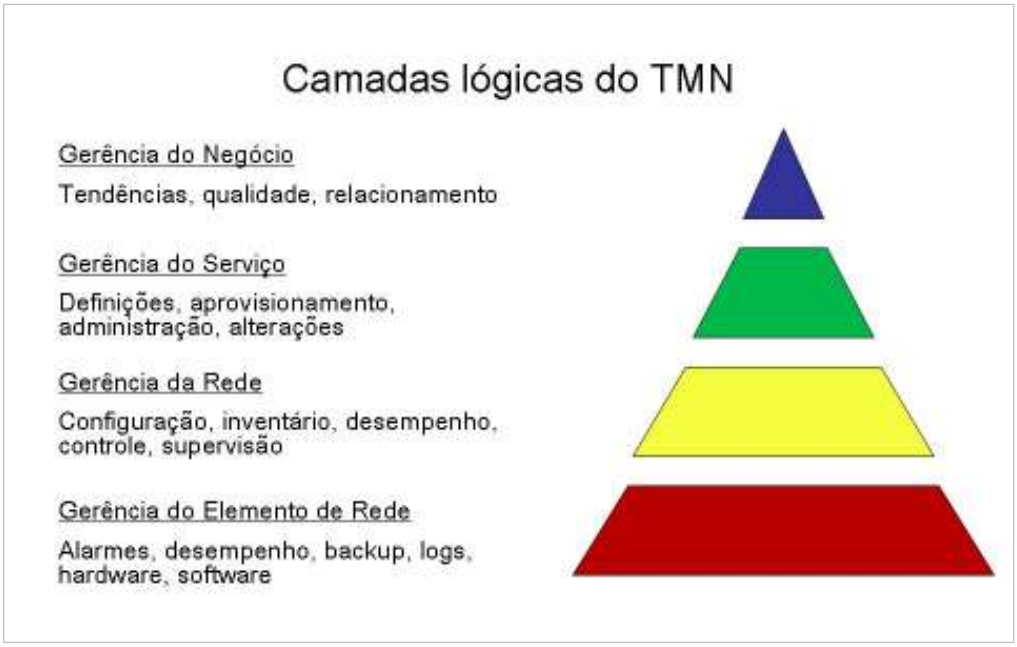

Figura 06 – Camadas Lógicas do TMN

As cinco áreas funcionais do TMN mostradas na tabela 2, conhecidas como FCAPS (*Fault, Configuration, Accounting, Performance, Security*), são implementadas para permitir que usuários com diferentes perfis possam atuar em diferentes camadas da rede e com diferentes níveis de abrangência.

Tabela 2 - Áreas Funcionais do TMN

Um tópico atual de pesquisa é o gerenciamento baseado em políticas e autonomia [20][21], especificando os parâmetros de comportamento dos vários elementos de rede. Para implementar esta proposta deve haver comunicação dentro do plano de gerência, entre as plataformas de medição e monitoração e o OSS. Também deve ser feita a validação do tráfego entrante com as políticas de operação da rede. Uma abordagem sugerida pelo projeto HYMAN [22] é o uso de meta-políticas previamente definidas para serem comparadas através de mecanismos de validação com as necessidades do usuário. A meta-política consiste de um conjunto de regras que especificam o nível de qualidade de serviço para os diferentes usuários.

A gerência de redes híbridas e multicamadas com o uso de recursos de diferentes tipos de comutação, granularidades, virtuais ou não, necessita de novas formas de monitoração. Falhas de equipamentos, problemas de desempenho e segurança se tornam mais críticos e de solução mais difícil devido ao seu impacto nas várias camadas e serviços da rede. Um gerenciamento efetivo requer monitoração, interpretação e controle dos recursos distribuídos. Do ponto de vista da monitoração, o principal problema é a multidimensionalidade e variabilidade da rede. Novos caminhos devem ser encontrados para obter as informações básicas sobre a carga e a utilização dos recursos individuais neste tipo de rede, cuja estrutura muda aleatoriamente de acordo com as solicitações dos usuários. Sistemas distribuídos de gerência, explorando as vantagens dos agentes móveis, softwares que se movem na rede entre suas diferentes entidades, são uma possibilidade de lidar com o gerenciamento de redes dinâmicas. O uso de agentes móveis permite ao sistema de gerência se adaptar também dinamicamente às alterações de redes DCN, SAC, DTN e outras. Entretanto, o uso exclusivo de agentes móveis pode levar a um aumento desnecessário do tráfego de gerência, sobrecarregando o plano de gerência. Uma abordagem em discussão é o uso de sistemas que combinam a centralização de tarefas triviais e a descentralização através dos agentes móveis para tarefas complexas, permitindo uma solução mais realista.

3.6 Engenharia de Tráfego – Otimização para a Rede Operativa

Um dos objetivos da implantação de uma estrutura de suporte de rede comum para as Redes Operativas e de Proteção é a otimização do uso dos recursos disponíveis pelas operadoras de energia mantendo o atendimento às demandas dos usuários e assegurando que a disponibilidade e qualidade acordadas (SLAs – *Service Level Agreements*) serão cumpridas.

A “Engenharia de Tráfego” [23] é o método pelo qual o desempenho de uma rede e a distribuição do seu tráfego pode ser otimizado, analisando dinamicamente, previsto e regulado. A engenharia de tráfego permite adaptar os vários fluxos de tráfego de acordo

com a disponibilidade de recursos da rede (enlaces, banda, desempenho, outros), visando a meta conjunta de assegurar o bom desempenho e o uso eficiente destes recursos.

Do ponto de vista das redes operativa e de proteção a engenharia de tráfego é assegurada pela implantação de um módulo na plataforma de proteção e supervisão que opera segundo os princípios básicos deste tipo de aplicação, a saber, medição, análise, modelagem e controle.

Em resumo, o tráfego e a rede devem ser medidos e identificados. A ferramenta para medição e monitoração da rede deve informar a topologia da rede, o estado operacional dos enlaces e equipamentos da rede, incluindo configuração e parâmetros de desempenho e os fluxos de tráfego e suas características.

Estes dados também são úteis para outras atividades como planejamento de capacidade, visualização da rede e bilhetagem. Então as modificações a fazer na rede devem ser planejadas considerando as heurísticas e meta-políticas definidas para a rede, física ou sobrepostas, e para os serviços. A eficiência deste passo depende de uma visão acurada e atualizada do estado da rede (*snapshot*), ou seja, da frequência e da assertividade das medições realizadas. Finalmente um operador ou um sistema automatizado faz as configurações.

A engenharia de tráfego é aplicada tanto durante a operação normal como em caso de falha. Em caso de falha, o objetivo é preservar ao máximo possível o desempenho dos fluxos e restaurar o estado operacional da rede. Durante a operação normal a meta é a melhoria operacional executando ações preventivas e para otimização da rede, por exemplo, permitindo o aumento de fluxos ou a melhoria de parâmetros relacionados à qualidade. A cada fluxo de dados incluído ou excluído, a rede deve ser revista para verificar a sua capacidade de lidar com o novo fluxo e o impacto da inclusão ou exclusão sobre o desempenho da rede e a distribuição dos outros fluxos. Decisões táticas e estratégicas também podem vir a ser um motivo para utilizar a engenharia de tráfego na rede: um novo acordo de interconexão leva a priorizar o encaminhamento do tráfego através de uma interface, ou o suporte a um novo serviço oferecido para os usuários, etc.

Adicionalmente o estabelecimento de circuitos e a computação de caminhos devem ser feitos usando as informações de medição e monitoração, de forma que seja possível alcançar os objetivos da aplicação. Uma vez que as métricas sejam definidas e mapeadas nos parâmetros das várias tecnologias, é necessário identificar as heurísticas que vão resultar em boas entradas para os algoritmos de computação de caminhos. Todas estas informações são essenciais para fazer a correta modelagem da rede.

4 CONSIDERAÇÕES FINAIS

Uma adequação da arquitetura das redes IP compreendendo um conjunto específico de alternativas tecnológicas utilizando redes ópticas, redes híbridas (DCN) e um plano de controle integrador (GMPLS) com funcionalidades de garantia de qualidade de serviço e otimização de recursos de rede via a engenharia de tráfego permite a utilização de redes comutadas para a supervisão e controle dos sistemas elétricos.

Este novo modelo de rede desenvolvido para o setor se configura no escopo das soluções Smart Grid como elemento integrador da geração, transmissão, distribuição, operação, provedores de serviço e usuários finais. A arquitetura e tecnologias constituintes permitem o atendimento de um conjunto mínimo de requisitos fundamentais no contexto do Smart Grid tais como alta capacidade de processamento de mensagens, comunicação bidirecional, alta disponibilidade, segurança, confiabilidade e a detecção e recuperação de falhas, dentre os mais relevantes.

REFERÊNCIAS

[1] Subharthi P., Jianli P., Jain R. Architectures for the Future Networks and the Next Generation Internet: A Survey. *Computer Communicaton*, v. 34, n. 1, p. 2-42, 2011.

[2] Internet2. Site Institucional. Disponível em: <http://www.internet2.edu/about/>. Acesso em 12 ago. 2011.

[3] GENI. Global Environment for Network Innovations. Disponível em: <http://www.geni.net/>. Acesso em 12 ago. 2011.

[4] European Commission. **Future Internet Research and Experimentation – An Overview of the European FIRE Initiative and its Projects**. Luxembourgo: Office for Official Publications of the

European Communities, 2008.
[5] GEANT Network. Disponível em:< http://www.geant.net/>. Acesso em 12 ago. 2011.
[6] Gobena, Y.; Durai, A.; Birkner, M.; Pothamsetty V.; Varakantam, V. Practical Architecture Considerations for Smart Grid WAN Network, In: Power Systems Conference and Exposition (PSCE), 2011 IEEE/PES, page(s): 1 - 6, 2010.
[7] Yang T.; Zhang Z.; Li A.; Wu J.; Wei M.; "New IP QoS Algorithm Applying for Communication Sub-Networks in Smart Grid", Power and Energy Engineering Conference (APPEEC), 2010 Asia-Pacific, p. 1 - 4, 2010.
[8] Yong-Hee J. QoS Requirements for the Smart Grid Communications System. *IJCSNS International Journal of Computer Science and Network Security*, v. 11, n. 3, 2011.
[9] Mackiewicz, R.E. Overview of IEC 61850 and Benefits. In: IEEE Power Systems Conference and Exposition (PSCE), 2006.
[10] Sidhu, T. S.; Gangadharan, P. K. Control and Automation of Power System Substation using IEC61850 Communication. In: Proceedings of 2005 IEEE Conference on Control Applications (CCA), 2005.
[11] Budka K.; Deshpande J.; Doumi T.; Madden M.; and Mew T. Communication Network Architecture and Design Principles for Smart Grids. *Bell Labs Technical Journal Special Issue: Green Information and Communications Technology (ICT) for Eco-Sustainability*, v. 15, n. 2, p. 205–227, 2010.
[12] Farhangi, H. The Path of the Smart Grid. *IEEE Power and Energy Magazine*, v. 8, n. 1, p. 18-28, ISSN: 1540-7977, 2010.
[13] Mannie, E. Generalized Multi-Protocol Label Switching (GMPLS) Architecture, IETF, RFC 3945, 2004.
[14] Guok, C. P.; Robertson, D. W.; Chaniotakis, E.; Thompson, M. R.; Johnston, W.; Tierney, B. A User Driven Dynamic Circuit Network Implementation, In: Proceedings of the Distributed Autonomous Network Magagement Systems Workshop (DANMS 2008), IEEE GLOBECOM Workshops, 2008.
[15] Internet2 Dynamic Circuit Network. Disponível em: <http://www.internet2.edu/network/dc/. Acesso em 12 ago. 2011.
[16] Internet2. ION Service. Disponível em: <http://www.internet2.edu/ion/>. Acesso em 12 ago. 2011.
[17] Lehman, T.; Sobieski, J.; Jabbari, B. DRAGON: A Framework for Service Provisioning in Heterogeneous Grid Networks. *IEEE Communications Magazine*, v. 44, n. 3, p. 84 - 90, 2006.
[18] Sevasti, A. AutoBAHN Dynamic Circuits across Heterogeneous R&E Networks, RNP X National Education and Research Network Workshop (WRNP 2009), Maio, 2009.
[19] UCLP. User Controlled Lightpaths. Disponível em: <http://www.uclp.ca/>. Acesso em 12 ago. 2011.
[20] Bezerra, R. M. S. and Joberto, S. B. M. Network Self-Management with a Partitioning Method based on Network Density and Traffic Matrix. In: Proceedings of the 13th Asia-Pacific Network Operations and Management Symposium, 2011.
[21] Strassner, J. **Policy-Based Network Management: Solutions for the Next Generation**. Morgan Kaufmann Series in Networking. ISBN: 1558608591, 2003.
[22] Granville, L. HYMAN – Gerenciamento de Redes Híbridas e Interação com Usuários, Projeto Nova RNP, Outubro, 2008.
[23] Monteiro, J. A. S.; Bastos, C. A. M. MonCircuitos – Monitoração de Circuitos e Engenharia de Tráfego. Projeto Futura RNP. Dezembro de 2008.