



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

FI/GTL/23
18 a 21 de Outubro de 2015
Foz do Iguaçu - PR

GRUPO - XV

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

**SOLUÇÃO DE ROTEAMENTO DINÂMICO NA INTERLIGAÇÃO
DA REDE DOS AGENTES AO SSC DO ONS**

Demétrius Mendonça da Silva(*)
ONS – Operador Nacional do Sistema Elétrico

Antônio José Alegria Filho
ONS – Operador Nacional do Sistema Elétrico

Cristian Tatsuro Kogachi
ONS – Operador Nacional do Sistema Elétrico

Geraldo Pinto Ribeiro
ONS – Operador Nacional do Sistema Elétrico

Gilson Fernando da Silva
ONS – Operador Nacional do Sistema Elétrico

Rodrigo Marques de Melo Santiago
ONS – Operador Nacional do Sistema Elétrico

RESUMO

A solução de Roteamento Dinâmico na Interligação da Rede dos Agentes aos SSC do ONS foi concebida para preservar a supervisão dos agentes, em caso de falha em um dos links de comunicação de forma rápida, automática e transparente. Além disso, essa solução foi projetada para também atender aos requisitos de contingenciamento de um Centro de Operação Principal por um Centro de Operação Backup. Posto isto, tornou-se necessário que as redes de telecomunicações envolvidas no processo de aquisição de dados dos Agentes alterassem as rotas dos fluxos de dados e voz, a partir da utilização de protocolos de roteamento dinâmico e de contingenciamento automático que preservassem a supervisão elétrica dos Agentes, tanto pelo Centro de Operação Principal como também através do Centro de Operação Backup.

Além do aspecto de contingenciamento e disponibilidade, a solução levou em consideração também todos os requisitos de segurança cibernética, isolamento do tráfego através de VLAN, filtros de rotas e controles de acesso, de forma a garantir que as comunicações do ONS com um determinado Agente não fossem afetadas pela comunicação com um outro e nem que um Agente pudesse acessar outro através da rede do ONS.

PALAVRAS-CHAVE

Comunicação de Dados em Tempo Real, Disponibilidade das Comunicações, Roteamento Dinâmico, Contingenciamento dos Canais de Comunicação.

1.0 - INTRODUÇÃO

O ONS opera o SIN com apoio de um novo Sistema de Supervisão e Controle, denominado REGER (Rede de Gerenciamento de Energia). O REGER foi concebido de forma a atender o Procedimento de Rede Submódulo 2.7 no qual foi definido que um SSC do ONS deve operar com alta disponibilidade e plena capacidade de contingenciamento. As principais características de contingenciamento previstas no PR 2.7 são as seguintes:

(a) Cada centro regional pode ser atendido por qualquer SSC do ONS. Em condições normais será atendido por aquele localizado nas suas próprias instalações;

(*) Rua Júlio do Carmo, n° 251 Cidade Nova – CEP 20.211-160 Rio de Janeiro, RJ, – Brasil
Tel: (+55 21) 3444-9042 – Fax: (+55 21) 3444-9009 – Email: demetrius@ons.org.br

(b) Cada SSC possui um sistema de aquisição de dados local (SAL) e um sistema de aquisição de dados remoto (SAR) em outra localidade de uma mesma região metropolitana;

(c) Os Agentes são responsáveis, com relação aos equipamentos na rede de supervisão, por fornecer recursos de supervisão e controle em dois sistemas de aquisição de dados designados pelo ONS, sendo um local (SAL) e outro remoto (SAR). SAL e SAR são sistemas de aquisição de dados (front-end) do ONS que operam numa arquitetura de alta disponibilidade, sendo o (SAL) localizado no Centro de Operação de propriedade do ONS (COSR), e o outro (SAR), localizado em outra instalação designada pelo ONS.

Antes deste conceito de SAL e SAR, os Agentes entregavam os canais de telecomunicações de dados e voz em uma mesma localidade. Desta forma, os Agentes que utilizam protocolos IP nos seus Sistemas de Supervisão e Controle configuravam seus roteadores com um endereço IP Virtual, permitindo ao ONS criar rotas estáticas para aquisitar os dados, ficando transparente por qual canal deveria ser feita a aquisição e o contingenciamento dos canais de telecomunicações.

Com a entrada em operação do SAL e SAR, tornou-se inviável configurar um endereço IP Virtual nos roteadores de forma a viabilizar a configuração de rotas estáticas devido ao fato dos mesmos estarem em redes e localidades distintas. Inicialmente, para solucionar este problema, o controle do contingenciamento dos canais de telecomunicações foi transferido para o SSC. No SSC foram então configurados endereços IP fictícios para as remotas/front-end dos Agentes, sendo um IP fictício para cada canal de telecomunicação, simulando desta forma a existência de duas remotas/front-ends. Posto isso, a solução completa do problema era realizada nos firewalls, através dos quais criavam-se rotas distintas estáticas para cada canal de comunicação e também era feita a conversão através de NAT dos endereços IP's fictícios para o endereço IP real da remota/front-end. Entretanto, para o contingenciamento ocorrer, era necessário o SSC se desconectar de uma remota/front-end para então se conectar na outra, o que acarretava uma queda temporária da aquisição de dados durante o contingenciamento dos canais de telecomunicações.

Para resolver os problemas relatados acima, o ONS projetou um novo esquema de roteamento, permitindo que as rede de telecomunicações envolvidas no processo de aquisição de dados dos Agentes alterassem as rotas dos fluxos de dados e voz de forma ágil, transparente e automática utilizando técnicas e protocolos de roteamento dinâmico. Este novo processo foi batizado de Roteamento Dinâmico do SSC e preserva a supervisão elétrica dos Agentes conectados aos Centros de Operação do ONS em caso de falha em um dos circuitos de comunicação com o Agente.

2.0 - ARQUITETURA DOS AMBIENTES ENVOLVIDOS NO PROJETO DE ROTEAMENTO DINÂMICO

Visando um melhor entendimento da solução de roteamento proposta, vamos detalhar as arquiteturas dos ambientes envolvidos para aquisição de dados dos Agentes pelo ONS.

2.1 Rede Operativa do ONS (ROP)

Os requisitos de sincronismo e de contingenciamento de Centros do Reger impuseram a necessidade de se implementar uma rede de comunicação de alta disponibilidade e com severos requisitos de qualidade. Isto posto, o ONS contratou uma rede para a interligação dos Centros de Operação, que suporta tolerância a falhas no nível N-2, além dos requisitos de 99,99% de disponibilidade, latência máxima inferior a 100ms e perda de pacotes menor do que 1%. A ROP foi concebida, inicialmente, para atender exclusivamente a comunicação entre os Centros do ONS e ITAIPU. A figura 1 representa a arquitetura definida para a ROP.

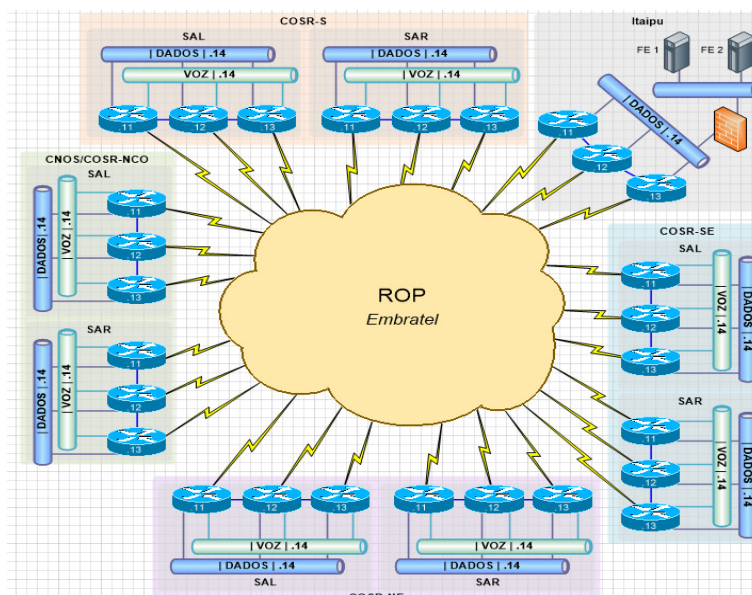


Figura 1 – Rede Operativa - ROP

2.2 Arquitetura da Rede de Aquisição de Dados utilizada atualmente pelo ONS

A arquitetura de rede padrão utilizada no processo de integração de Agentes está representada na figura 2. Existem variantes dessa topologia, localizadas do lado do Agente, em decorrência do fato de existirem Agentes que possuem mais de uma instalação com comunicação direta com o COSR do ONS.

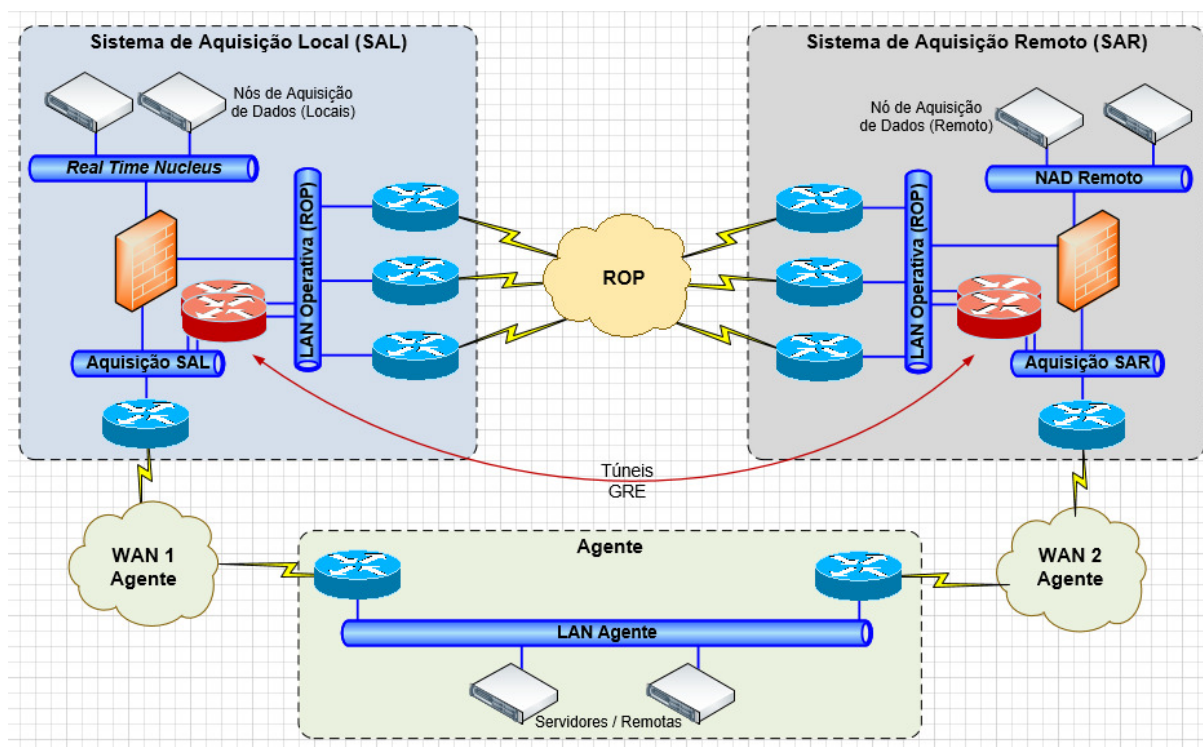


Figura 2 - Arquitetura da rede existente entre os Agentes e o ONS para a aquisição de dados

Entretanto, independentemente das variações existentes, todas necessitam atender os requisitos estabelecidos no Módulo 13 dos Procedimentos de Rede, assim como as premissas estabelecidas no projeto roteamento dinâmico. A saber:

- Disponibilizar, no mínimo, um link de acesso no SAL e outro no SAR;
- Utilizar equipamentos de rede monitoráveis;
- Topologia da rede LAN do SAL e do SAR idênticas;
- Uso exclusivo de uma rede LAN para atender cada Agente;
- Filtragem do tráfego de rede dos Agentes através de ACL's e VLAN;

- Utilizar somente os protocolos de roteamento dinâmico OSPF, BGP e EIGRP;
- Utilizar protocolos de contingenciamento automático HSRP ou VRRP, no lado do Agente;
- Alta disponibilidade nos ativos de rede do ONS;
- A perda de supervisão de um Agente só poderá ocorrer caso os dois links estejam inoperantes;
- Segregação do tráfego dos Agentes com o tráfego da ROP, através de túnel GRE (4 túneis).

De forma a garantir, durante a ocorrência de um incidente, a continuidade da supervisão sistêmica de um centro de operação principal por um centro de operação backup do ONS, tornou-se necessário que um Agente disponibilizasse um link de comunicação no SAL e outro no SAR. A comunicação de dados entre os servidores de aplicação do ONS, localizados no SAL, com os servidores dos Agentes deverá ser realizada, prioritariamente, pelo link instalado no SAL, com o objetivo de não depender da ROP.

Havendo perda de comunicação, seja na interface LAN ou na WAN do roteador instalado no SAL ou com o par deste roteador instalado na rede LAN do Agente, a comunicação entre os servidores de aplicação do ONS com os servidores do Agente passará então a trafegar através da ROP e do link de comunicação do Agente instalado no SAR. Assim que for reestabelecida a comunicação do link do Agente instalado no SAL ou do seu par instalado na rede LAN do Agente, o tráfego de dados voltará através desse link.

Para isto, tornou-se necessário utilizar os seguintes critérios:

- 1- Sempre que possível, utilizar o mesmo protocolo de roteamento dinâmico nos dois links de acesso dos Agentes;
- 2- Utilizando-se o mesmo protocolo de roteamento dinâmico nos dois links de acesso dos Agentes, o menor custo deverá ser atribuído para o link do SAL;
- 3- Utilizando-se protocolos de roteamento distintos, o protocolo com distância administrativa menor deverá ser utilizado para atender o link do SAL;
- 4- Os mesmos critérios mencionados de 1 a 3 deverão ser utilizados na rede LAN do Agente.

3.0 - O PROJETO

Além de atender os Procedimentos de Rede no Submódulo 2.7 e no módulo 13, o REGER foi concebido de tal forma que os dados de tempo real recebidos por um sistema de supervisão e controle (SSC) sejam disponibilizados para qualquer outro SSC que solicitar esses dados.

Posto isso, cada SSC tem como função principal dar suporte ao SSC local. Adicionalmente, os SSC-BSB, SSC-REC e o SSC-RIO tem uma função secundária de serem o sistema de backup de um ou mais centros de controle em caso de falha provisória de um SSC. A lista abaixo mostra as funções de backup entre os sistemas de supervisão e controle do ONS:

- SSC-BSB é o sistema de backup do SSC-RIO, SSC-FLN e SSC-REC;
- SSC-RIO é o sistema de backup do SSC-BSB para a função de CNOS;
- SSC-REC é o sistema de backup do SSC-BSB para a função de COSR-NCO.

3.1 – Planejamento

O planejamento do projeto foi pautado através da realização das seguintes etapas:

- Criação de protótipo da solução de roteamento dinâmico em conformidade com as premissas apresentadas;
- Elaboração da especificação técnica dos equipamentos de rede, considerando-se:
 - ✓ *Throughput* para atender um tráfego médio de 100 kbps por Agente;
 - ✓ Alta disponibilidade com fontes e placas controladoras redundantes;
 - ✓ Capacidade de configuração de protocolos de contingenciamento automático HSRP, VRRP e GLBP;
 - ✓ Capacidade de configuração de protocolos de roteamento dinâmico EIGRP, BGP, OSPF e IS-IS;
 - ✓ Capacidade de configuração de NAT, PAT e SNAT;
 - ✓ Capacidade de configuração de ACL's.
- Nivelamentos técnicos envolvendo as equipes do ONS, Embratel e a empresa de consultoria técnica TEN;
- Preparação do ambiente de teste;
- Elaboração e homologação do caderno de teste contemplando:
 - ✓ Realização de testes de interoperabilidade contemplando protocolos de contingenciamento automático (HSRP ou VRRP) e protocolos de roteamento dinâmico, totalizando 9 testes;
 - ✓ Testes de disponibilidade contemplando a desconexão lógica e física das interfaces WAN e LAN do roteador do Agente instalado no SAL, no SAR e nos roteadores instalados na rede LAN do Agente;
 - ✓ Testes com objetivo de garantir alta disponibilidade através do desligamento de um dos roteadores CORE (CISCO 3900) do SAL e do SAR;

- ✓ Testes de falha simultânea nos dois roteadores CORE do SAL;
 - ✓ Testes de falha simultânea nos dois roteadores CORE do SAR;
 - ✓ Testes de segurança através da configuração de VLAN, ACL e filtros nos roteadores com o objetivo de garantir somente a publicação e recebimento das redes LAN que atendem os servidores de aplicação, tanto do ONS quanto do Agente.
 - ✓ Documentação e elaboração de relatório técnico contendo o resultado de todos os testes realizados junto com o procedimento de integração de um Agente ao centros do ONS.
 - ✓ Hardenização dos ativos de rede;
 - ✓ Integração de pelo menos 2 Agentes em cada centro do ONS com suporte técnico da contratada utilizando roteamento dinâmico.
- Documentação da solução e elaboração de procedimentos de integração de Agentes.

3.2 – Premissas

As premissas que foram levadas em consideração no desenvolvimento neste projeto foram as seguintes:

- Preservar o chaveamento automático entre os links de comunicação dos Agentes;
- A perda da supervisão só deverá ocorrer caso os dois links estejam inoperantes;
- O ambiente de interligação dos Agentes no SAL e no SAR devem ser idênticos;
- Todos os centros de operação do ONS devem estar padronizados;
- Levar em consideração todos os requisitos de segurança do REGER;
- Não depender do provedor da ROP no processo de integração de Agentes;
- Apresentar facilidade de manutenção.

3.2.1 Ambiente de testes

A simulação da arquitetura de aquisição de dados dos Agentes foi realizada em Florianópolis e modelada da seguinte forma:

- Utilização/empréstimo dos canais da ROP entre Florianópolis e Brasília para simular os links de um Agente. No SAR de Brasília foi instalada uma remota simulando a instalação de um Agente.
- Simulou-se o link 1 do Agente através de um link constituído pelos roteadores 3 do SAR do CNOS e do SAL do COSR-S;
- Simulou-se o link 2 do Agente através de um link constituído pelos roteadores 2 do SAR do CNOS e pelo roteador 3 do SAR do COSR-S;
- Simulou-se a rede LAN do Agente utilizando-se o ambiente do SAR do CNOS/COSR-NCO;
- Os links do Agente instalados no SAL e no SAR do COSR-S e no SAR do CNOS utilizaram uma AS (Autonomus System) diferente da rede ROP.

A preparação do ambiente e a realização do caderno de teste foram realizados envolvendo as equipes técnicas do ONS, da Embratel e da prestadora de serviço TEN.

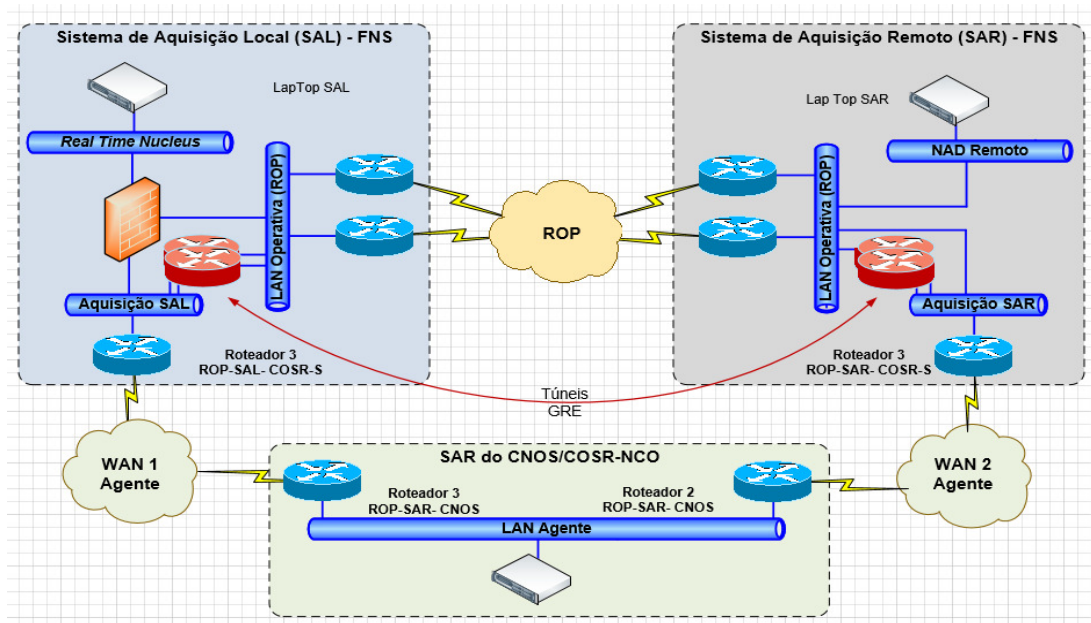


Figura 3 - Arquitetura do ambiente de testes

3.3 – Implantação do Roteamento Dinâmico

Para implantação definitiva da solução, foi produzido um plano detalhado a ser executado em horários agendados e aprovados pelas Salas de Controle do ONS.

Em cada *site*, foram configurados os roteadores redundantes CORE (CISCO 3900) operando como um *cluster* através de um endereço IP virtual. Para isso, utilizou-se o protocolo de alta disponibilidade HSRP nas interfaces LAN da rede “Aquisição” desses roteadores.

Entre os sistemas de aquisição (SAL e SAR) de cada Centro, foram configurados túneis GRE (*Generic Routing Encapsulation*) através da ROP (rede MPLS – *Multiprotocol Label Switching*). Esses túneis são formados ponto a ponto, de forma que temos quatro túneis GRE entre os pares de roteadores de cada *site*.

O protocolo GRE é um tipo de encapsulamento de roteamento genérico, desenvolvido pela Cisco, que pode encapsular uma grande variedade de tipos de protocolos dentro de túneis IP, criando uma ligação virtual entre o SAL e o SAR através de uma rede IP. O túnel encapsula os pacotes com um cabeçalho adicional. Esses, por sua vez, contêm toda a informação necessária para que exista um roteamento com sucesso desde a origem do túnel até ao seu destino. Esta travessia pode ser realizada em uma rede WAN privada ou pública.

3.3.1 Interoperabilidade entre protocolos de roteamento

Atualmente, os ativos de camada 3 disponíveis no mercado atuam, concomitantemente, com diversos tipos de protocolos de roteamento dinâmico – sejam eles livres (como BGP e OSPF) ou proprietários (como EIGRP). Além disso, os roteadores podem ser configurados de tal forma que os protocolos possam conversar entre si, trocando suas tabelas de roteamento. Isso proporciona interoperabilidade entre os *front-ends* do ONS e dos Agentes. Apesar do ONS recomendar o uso do protocolo OSPF (por ser eficiente e não proprietário) e o não uso do RIP (por trabalhar simplesmente com algoritmo vetor de distância), o Agente pode fazer uso de outro, que possa já estar em operação no *backbone* da operadora, por exemplo.

Os equipamentos Cisco utilizados no projeto permitiram selecionar, através de listas, rotas específicas a serem redistribuídas entre os protocolos. Isto contribuiu para se ter tabelas de roteamento mais sucintas, filtrando, por exemplo, rotas indesejadas vindas de roteadores de Agentes e aumentando, desta forma, a segurança no envio dos dados.

Rotas concorrentes oriundas de diferentes protocolos são escolhidas de acordo com a distância administrativa. A Tabela 1 apresenta os valores padrão das distâncias administrativas dos roteadores Cisco:

Tabela 1 – Valores padrão de distâncias administrativas em ativos Cisco. [Ref 1.]

Origem da rota	Valores padrão	Origem da Rota	Valores padrão
Interface conectada	0	IS-IS	115
Rota estática	1	RIP	120
Rota sumária no EIGRP	5	EG	140
BGP Externo	20	ODR	160
EIGRP Interno	90	EIGRP Externo	170
IGRP	100	BGP Interno	200
OSPF	110	Desconhecido	255

Assim, rotas OSPF, por exemplo, têm preferência (na tabela de roteamento) em relação a rotas BGP Interno. Tais valores podem ser alterados de acordo com a necessidade.

3.3.2 Segurança

As listas de redistribuição, assim chamadas, foram definidas e implantadas nos roteadores *Core* de modo a recebermos e divulgarmos apenas as rotas que nos interessassem – rotas para as redes locais e redes de *front-ends* dos Agentes. Outras configurações realizadas foram as listas de controle de acesso (ACL) e acesso seguro (SSH) aos roteadores, além da criptografia de senhas dos arquivos de configuração.

Os serviços do ONS são visíveis pelos Agentes sempre através de endereços IP traduzidos, preservando as informações internas dos servidores e evitando a conexão direta com os seus reais endereços IP's. A rede que os Agentes “enxergam” é a rede “Aquisição” (rede de trânsito), conectada diretamente aos *firewalls*, onde são realizados os NATs (*Network Address Translation*) necessários.

Além disso, em conformidade com as boas práticas de segurança, realizou-se a *hardening* dos ativos de rede (roteadores e switch) em que foram habilitados os seguintes recursos: autenticação e autorização, segmentação

por VLANs, desativação de serviços inseguros HTTP, FTP e TELNET e ativação dos HTTPS, SCP e SSH, *banner* com alerta e configuração de *backup* automático das configurações dos ativos para repositório interno.

3.4 Resultados

Todos os testes descritos no item 3.1 foram considerados consistentes, satisfatórios e os mesmos foram comprovados através da coleta de evidências. Os testes pelos quais fez-se necessário dar shutdown nas interfaces LAN e WAN dos roteadores instalados no SAL, SAR e na rede LAN do Agente apresentaram um tempo de convergência da rede inferior a 30 segundos.

4.0 - CONCLUSÃO

O conceito de roteamento dinâmico, em tomar decisões de encaminhamento de acordo com condições e mudanças de tráfego e/ou topologia, caracteriza-se pela flexibilidade e eficiência em condições adversas.

O esforço em realizar o projeto e, maior ainda, em “ajustar” as conexões com os Agentes em atendimento à nova arquitetura, é compensado em relação aos ganhos obtidos. Para um melhor entendimento dos mesmos, segue um resumo do cenário anterior, com uso do roteamento estático, através do qual tínhamos:

- Configuração manual e complexa a cada entrada de um novo Agente;
- Manutenção de scripts, rotas estáticas e NATs nos firewalls;
- Configuração de roteamento e NAT nos servidores NADs do SAR (previstos inicialmente também para trabalharem com roteamento a partir de configurações adequadas em seus sistemas Linux);
- Gerência de objetos com endereços IP fictícios nos firewalls e servidores DNS;
- Grande demanda de recursos de memória e processamento nos firewalls. *“While each connection uses two entries in the flow tables, connections involving NAT uses four entries instead of two. NAT requires heavy CPU and memory usage. Although NAT travels in flowpath, it functions in slowpath.” [Ref 2.];*
- Utilização de uma interface GigabitEthernet do servidor NAD do SAR para possibilitar o roteamento, pelo qual poderia ser utilizada em agregação (bonding) com intuito de aumentar a disponibilidade e throughput do mesmo;
- Segregação de tráfego na camada de enlace;
- Documentação e passagem de conhecimento complexas;

4.1 Ganhos Obtidos

Dentre os ganhos obtidos com a adoção do roteamento dinâmico nas comunicações de longa distância entre *sites* do ONS e com Agentes, destacam-se:

- Contingenciamento de fluxo de comunicação (roteamento) automático, sem necessidade de intervenção manual, em que as rotas são aprendidas automaticamente a partir de mudanças na topologia;
- Não há necessidade de criação de scripts e rotas estáticas adicionais;
- Menor consumo de recursos dos firewalls e servidores NADs remotos;
- Diminuição de regras NAT nos firewalls para cerca de 1% do total do cenário anterior;
- Segregação de tráfego na camada de rede;
- Redução de acionamentos de sobreaviso das equipes de O&M em decorrência da automatização da solução de contingenciamento automático entre os links de comunicação sem necessidade de intervenção humana;
- Durante a preparação do ambiente do roteamento dinâmico, descobriu-se uma forma de substituir uma rede denominada RAOP, com disponibilidade mensal de 98%, responsável pela coleta de dados de frequência provenientes de 7 subestações, com um custeio anual de R\$ 207.000,00. Essa rede foi substituída roteando-se os dados provenientes dessas subestações através da rede dos Agentes e da rede ROP até o Centro CNOS/COSR-NCO. Destaca-se que a utilização dessa nova modelagem de aquisição da coleta de frequência elevou a disponibilidade de 98% pra 99,98% sem nenhum encargo financeiro adicional para o ONS.
- Manutenção, documentação e passagem de conhecimento mais simples.

5.0 - BIBLIOGRAFIA

- [1] CISCO SYSTEMS, O que é distância administrativa, Informe Técnico, disponível em http://www.cisco.com/cisco/web/support/BR/8/84/84574_admin_distance.html. Referenciar Tabela 1.
- [2] LAMY, P., IP Platforms Best Practices for Performance, Check Point, disponível em https://sc1.checkpoint.com/sc/SolutionsStatics/sk39777/IP_Platforms_Best_Practices_for_Performance_010810.ppt. Referenciar texto do 5º bullet do capítulo 4.0.
- [3] DONAHUE, Gary A., Redes Robustas, Editora O'Reilly
- [4] RANJBAR, Amir, Troubleshooting and Maintaining Cisco IP Networks (TSHOOT), Ciscopress
- [5] TEARE, Diane, Implementing Cisco IP Routing (Route), Ciscopress

6.0 - DADOS BIOGRÁFICOS



Demétrius Mendonça da Silva – Graduado em Engenharia Elétrica pela UFRJ (1992); Especialização em Análise de Sistema pela PUC-RIO (1995); MBA em Aspectos Institucionais do Setor Elétrico - CAISE pela PUC-RIO (2010); Pós-graduação em Computação Aplicada e Automação pela UFF (2012). É atualmente Especialista na Gerência de Infraestrutura e SSC do COSR-SE.

Endereço eletrônico: demetrius@ons.org.br.



Antonio José Alegria Filho – Graduado em Engenharia de Telecomunicações pela PUC-RIO (1998). Atualmente Analista de TI Senior na Gerência de Infraestrutura e SSC do COSR-SE.

Endereço eletrônico: alegria@ons.org.br.



Cristian Tatsuro Kogachi - Graduado em Engenharia Elétrica – UFSC / Universidade Federal de Santa Catarina; Graduado e Administração de Empresas – UDESC / Universidade do Estado de Santa Catarina – 1999; Pós Graduado em Engenharia Biomédica – UFSC / Universidade Federal de Santa Catarina - 2000. E atualmente Engenheiro de Sistemas de Potência Sênior na Gerência de Infraestrutura e SSC do COSR-S.

Endereço eletrônico: cristian@ons.org.br.



Geraldo Pinto Ribeiro – Graduado em Química pela Universidade Federal Rural de Pernambuco - UFRPE (1982); Especialização em Redes de computadores pela Universidade Federal de Pernambuco - UFPE. É atualmente Analista de Sistemas especialista na Gerência de Infraestrutura e SSC do COSR-NE.

Endereço eletrônico: geraldo@ons.org.br.



Gilson Fernando da Silva – Graduado em Matemática pela UnB (1996); Especialização em Redes e Telecomunicações pelo IESB (2009); MBA em Aspectos Institucionais do Setor Elétrico - CAISE pela PUC-RIO (2014)). É atualmente Analista de Sistemas Senior na Gerência Infraestrutura e SSC do CNOS/COSR-NCO.

Endereço eletrônico: gilson@ons.org.br.



Rodrigo Marques de Melo Santiago – Graduado em Engenharia Elétrica com ênfase em Telecomunicações pela UFRN (2008). Atualmente, atua como Eng. de Infraestrutura no ONS.

Endereço Eletrônico: rsantiago@ons.org.br.