MANUAL DE REDES DO SFN

VERSÃO 9.4

Brasília, 14 de agosto de 2026.

CONTATOS

Gerência Integrada de Segundo Nível

E-mail: infra.rsfn@bcb.gov.br

Telefone: +55 61 3414-3012 ou +55 61 3553-3012

Gestor do Manual de Redes

E-mail: infra.rsfn@bcb.gov.br

Operadoras

CLARO NXT: 0800-7021358.

Consórcio Claro/RTM: 0800-7077400.

Lista de escalonamento disponível em www.rsfn.net.br (somente a partir da RSFN)

HISTÓRICO DE REVISÕES

Versão	Descrição das Modificações	Data da Modificação
9.4	- Adequação à Resolução BCB 598, de 05/09/2025. - Alteração da concessionária de Telmex para CLARO NXT - Adequação das referências para operadoras genéricas VERMELHA e AZUL	14 de agosto de 2026
9.3	- Ajuste na regra de comunicação entre os participantes – Seção 1.5 - Atualização da seção DNS - Capítulo 6 - Remoção do formulário do Anexo 1, que passa a ser disponibilizado diretamente no website do BCB sob a denominação de Formulário para Inclusão ou Alteração de Participante na RSFN - Alteração da tabela "Configuração de Qualidade de Serviço na RSFN", Capítulo 8, para refletir a distribuição do tráfego do PIX em canais primário e secundário - Inclusão do Glossário, Capítulo 9.	06 de outubro de 2023
9.2	- Atualização dos requisitos para conexão direta à RSFN, destacando-se a inclusão de recomendações para alta disponibilidade	11 de maio de 2021
9.1	- Inclusão da opção para conexão híbrida à RSFN - Atualização da política de QoS comtemplando a criação da classe Platina, realocação do tráfego do SPB e redefinição dos percentuais de reserva de banda para cada classe. Além disso, permitir a configuração diferenciada de circuitos dedicados do BCB e das câmaras e prestadores de serviço de liquidação e de compensação -Atualização do normativo que trata dos PSTI, incluindo a necessidade de no mínimo dois acessos redundantes e independentes entre si para comunicação entre o PSTI e os seus clientes	20 de agosto de 2020
9.0	- Adequação à Circular 3.970 de 28 de novembro de 2019: inclusão Título "Redes e PSTI" e ajustes nas demais partes do Manual - Alteração da concessionária de Primesys para Telmex	12 de fevereiro de 2020
8.2.1	- Inclusão da opção para MQ *multi-instance* - Alteração do parâmetro de *batch-size* do MQ	30 de outubro de 2018
8.2	- Exclusão da restrição de NAT 1:1 nos *firewalls* - Atualização dos procedimentos de DNS - Alteração da definição de canais do MQ	28 de agosto de 2018
8.1	- Atualização do novo modelo de QoS da RSFN - Inclusão de prefixos IP /28 para Câmaras e PSTIs - Atualização Escala de Trabalho GI2N para 24x7 - Inclusão do Perfil F para interligação na RSFN	04 de outubro de 2017
8.0	- Inclusão do domínio SPB02	16 de agosto de 2016
7.6.4	- Melhoria de texto (pág 54) - Correção do telefone da Primesys (pág 8)	5 de novembro de 2015
7.6.3	- Alteração Visão Geral – Normas de utilização da RSFN (p.7)	5 de maio de 2015
7.6.2	- Alteração Página 45, inserindo o range de portas de Homologação do domínio MES03	29 de agosto de 2014
7.6.1	- Alteração dos Endereços de hostnames	28 de janeiro de 2014
7.6	- Alteração do sistema de Qualidade de Serviço da RSFN - Inclusão do ambiente PPRO - Alteração na configuração do Serviço FTP - Alteração do e-mail de contato da equipe de infraestrutura da RSFN para infra.rsfn@bcb.gov.br	03 de dezembro de 2013
7.5.1	Atualização do Normativo que trata de PSTI	25 de setembro de 2013

7.5	Inclusão de informações sobre Política de encaminhamento do tráfego de entrada e saída de dados	11 de setembro de 2013
7.4	Inclusão de informação sobre transação para acesso à configuração do MES02 no MQConfig	5 de setembro de 2013
7.3.1	Inclusão do Manual de DNS como Anexo I	12 de março de 2013
7.3	- Referência à Circular Nº 3629 de 19 de fevereiro de 2013, inclusão dos Requisitos para o Modelo Operacional de PSTI e alteração do nome do Manual Técnico.	26 de fevereiro de 2013
7.2	- Substituição da PRED300 e PCCS400 em Homologa e Produção	8 de novembro de 2012
7.1	- Troca de menções ao PCCS400 e acréscimo do MQConfig	19 de julho de 2012
7.0	- Inclusão dos domínios MES02 e MES03	13 de julho de 2012
6.1	- Inclusão do domínio mês	9 de abril de 2009
6.0	- Inclusão da Gerência de Segundo Nível da RSFN e da Qualidade de Serviço na RSFN	20 de dezembro de 2006
5.0	- Inclusão dos campos que comprovam a emissão do COA pelo BCB no item “Diretrizes Básicas” da “Infraestrutura de Mensageria”.	02 de janeiro de 2004
4.0	- Adequação à Circular BCB 3014 - alteração da redação das “Normas de Utilização da RSFN”; - retirada do item “Sobre o Comitê Gestor da RSFN”. - Inclusão da obrigatoriedade do TTL igual a zeros para o nome do servidor MQ no item “Recomendações” - Inclusão de observação sobre perda de conectividade nos modelos 4 e 5. - Inclusão do Roteiro de Testes de Contingência da RSFN. - Inclusão da configuração obrigatória do parâmetro ADOPTMCA no servidor MQSeries.	26 de agosto de 2003
3.0	- Inclusão do Template para Roteamento do o Perfil D com roteadores da entidade no barramento RSFN e NAT do 2º prefixo /28 (Modelo 6). - Inclusão do capítulo referente infraestrutura da mensageria.	5 de novembro de 2001
2.0	- Inclusão do Template para segmentação do prefixo /27 em duas VLANs: SPB (prefixo /28) e outra para NAT (prefixo /28).	3 de setembro de 2001

ÍNDICE DE FIGURAS

Figura 1- Comunicação entre as entidades participantes da RSFN 15
Figura 2 - Preferência de comunicação na RSFN 18
Figura 3 - Perfis de Conexão com a RSFN 19
Figura 4 - Dois sites com interconexão pela rede interna 21
Figura 5 - Dois Sites, porém com apenas dois CPE 22
Figura 6 - Conexão do Perfil D com roteamento iBGP 23
Figura 7- Conexão direta do Perfil D com a célula de segurança 25
Figura 8 - Topologia com dois sites, porém com apenas dois CPE 27
Figura 9- Topologia com dois sites com interconexão pela rede interna 28
Figura 10 - Conexão do Perfil D com roteamento iBGP 29
Figura 11 -Topologia com dois sites, quatro roteadores da entidade e NAT interno 30
Figura 12 - Conexão direta do Perfil D com a célula de segurança 31
Figura 13 - Diagrama de consultas aos subdomínios na RSFN 34

ÍNDICE DE TABELAS

Tabela 1 - Faixa de Endereços dos hosts TCP/IP com máscara /27 16
Tabela 2 -Faixa de Endereços dos hosts TCP/IP com máscara /26 16
Tabela 3 - Faixa de Endereços dos hosts TCP/IP das IF com máscara /28 17
Tabela 4 - Faixa de Endereços dos hosts TCP/IP das IFs com máscara /27 17
Tabela 5 - Lista de IRS 35
Tabela 6 - Padronização de nomes de hosts 35
Tabela 7 - Parâmetro de temporização de registro 36
Tabela 8 - Filas locais (na IF) 39
Tabela 9 - Filas remotas (na IF) 40
Tabela 10 - Filas locais (no BC/Prestador) 40
Tabela 11 - Filas remotas (no BC/Prestador): 40
Tabela 12 - Domínios, ambientes e portas 42
Tabela 13 - Atributos Comuns a Todas as Filas 44
Tabela 14 - Atributos de Filas Locais 45
Tabela 15 - Atributos de Filas Remotas 45
Tabela 16 - Atributos de Alias Queues 45
Tabela 17 - Atributos de NameLists 45
Tabela 18 - Atributos de Processos 46
Tabela 19 - Atributos de Queue Managers 46
Tabela 20 - Atributos de Canais 47
Tabela 21 - Configuração das marcações de Qualidade de Serviço na RSFN 50
Tabela 22 - Configuração das marcações de Qualidade de Serviço na RSFN para circuitos dedicados 50
Tabela 23 - Configuração de Qualidade de Serviço na RSFN 51

ÍNDICE GERAL

1 REDES E PSTI 9
1.1 Alterações no Manual de Redes 9
1.2 RSFN - Rede do Sistema Financeiro Nacional 9
1.3 Serviços da RSFN 10
1.4 Participantes da RSFN 10
1.5 Comunicação entre os participantes da RSFN 11
1.6 Operadoras de serviço de comunicação da RSFN 11
1.7 Provedor de Serviços de Tecnologia da Informação - PSTI 12
1.8 Gerência Integrada de Segundo Nível da RSFN 13
2 RSFN 15
2.1 Topologia lógica da RSFN 15
2.2 Endereçamento IP na RSFN 15
2.3 Política de encaminhamento do tráfego de entrada e saída de dados 17
2.4 Conexão direta dos participantes à RSFN 18
2.5 Conexão dos participantes à RSFN por meio de um PSTI 20
2.6 Conexão híbrida à RSFN 20
3 MODELOS DE TOPOLOGIA E ENDEREÇAMENTO 21
3.1 Modelo 1 21
3.2 Modelo 2 22
3.3 Modelo 3 e modelo 6 23
3.4 Modelo 4 e modelo 5 25
4 ROTEAMENTO DA RSFN 27
4.1 Roteamento para os perfis A e B (Modelo 2) 27
4.2 Roteamento para o perfil C (Modelo 1) 28
4.3 Roteamento para o perfil D - roteadores no barramento RSFN (Modelo 3) 29
4.4 Roteamento para o perfil D - roteadores no barramento RSFN e NAT (Modelo 6) 29
4.5 Roteamento para o perfil D com *firewall* da entidade no barramento RSFN (Modelo 4) 31
4.6 Roteamento para o perfil D com *firewall* da entidade no Barramento RSFN (Modelo 5) 31
5 CONEXÃO DA INFRAESTRUTURA DOS PSTI E DOS PARTICIPANTES À RSFN 33
6 SERVIÇOS DE REDE DA RSFN 34
6.1 DNS (*Domain Name System*) 34
6.2 Servidor de tempo (time server) 36
6.3 Servidor Web da RSFN 37
6.4 Servidor FTP 37
7 INFRAESTRUTURA DE MENSAGERIA 38
7.1 Diretrizes básicas 38
7.2 Definições do MQ 38
7.3 Configuração do Servidor MQ - Opção ADOPTNEWMCA 48
7.4 Configuração do MQ - BCB 49

8 QUALIDADE DE SERVIÇO NA RSFN 50
9 GLOSSÁRIO 52

1 REDES E PSTI

Este Manual de Redes do SFN, de acordo com Circular 3.970 de 28 de novembro de 2019, tem por finalidade regulamentar os padrões técnicos das redes e dos PSTI que suportam o tráfego de dados para a comunicação eletrônica no SFN, bem como os requisitos necessários aos participantes da Rede do Sistema Financeiro Nacional (RSFN).

O Departamento de Tecnologia da Informação (DEINF) do Banco Central do Brasil (BCB) é responsável pela publicação deste Manual e designará servidores para exercerem a função de Gestor do Manual de Redes do SFN.

Caberá ao Gestor do Manual de Redes:

- estabelecer os padrões técnicos deste Manual, em consonância com a política estabelecida pelas áreas de negócio do BCB;
- acolher e avaliar requerimentos para alteração deste Manual submetidos por participantes da RSFN;
- alterar este Manual e publicá-lo no *website* do BCB;
- avaliar o impacto da inclusão de novos serviços na RSFN ou da alteração no perfil de tráfego dos serviços existentes;
- convidar ou convocar instituições e participantes interessados para discutir temas relacionados a redes de comunicação bem como alterações neste Manual;
- solicitar e avaliar relatórios produzidos pela Gerência Integrada de Segundo Nível;
- decidir sobre assuntos relativos a padrões técnicos da rede;
- supervisionar o funcionamento da RSFN no que tange aos princípios elencados na Circular 3.970 de 28 de novembro de 2019.

1.1 Alterações no Manual de Redes

O requerimento para alterações deste Manual deverá ser encaminhado ao Gestor do Manual de Redes, através de Documento de Requisitos Técnicos (DRT), cujo modelo para preenchimento está disponível para download no *website* do BCB.

Durante o processo de avaliação do DRT, o Gestor do Manual de Redes poderá solicitar complementações ou alterações no documento encaminhado pelo requisitante ou ainda consultar os participantes da RSFN e as unidades de negócio do BCB.

O Gestor do Manual de Redes efetuará as devidas adequações e publicará uma nova versão deste Manual no *website* do BCB.

1.2 RSFN - Rede do Sistema Financeiro Nacional

A RSFN é uma estrutura de comunicação de dados que tem por finalidade amparar o tráfego de informações no âmbito do SFN para serviços autorizados. A arquitetura da RSFN foi especificada tendo como premissas alta disponibilidade, desempenho e segurança.

Os detalhes técnicos da RSFN estão descritos nos capítulos 2 a 8 deste Manual.

1.3 Serviços da RSFN

A RSFN tem como objetivo principal suportar o tráfego de dados diretamente relacionados a serviços críticos, podendo, sem interferir no seu objetivo principal, suportar o tráfego de dados de outra natureza. São considerados serviços críticos:

- a transferência de recursos financeiros, de títulos e valores mobiliários e de outros ativos financeiros no âmbito do SFN;
- a realização de leilão de câmbio;
- a obtenção de informações para formação da taxa PTAX.

Somente os serviços com estudo de impacto previamente aprovados pelo BCB poderão trafegar na RSFN.

A inclusão de novo serviço ou alteração do perfil de tráfego dos serviços já existentes deverá ser previamente submetida ao Gestor do Manual de Redes, através do DRT. Havendo necessidade, deverá ser submetido Documento de Requisito de Negócios conforme Catálogo de Serviços do SFN.

Somente a unidade de negócio responsável pelo serviço ou o gestor do serviço, no caso de serviço autorregulado, poderá solicitar a inclusão ou a alteração de serviços na RSFN.

A autorização de uma instituição num dado serviço é concedida pela unidade de negócio por ele responsável ou pelo gestor do serviço, no caso de serviços autorregulados.

1.4 Participantes da RSFN

Podem ser participantes as entidades autorizadas ou em processo de homologação em pelo menos um dos serviços que utilizam a RSFN, observado o disposto no art. 3º da Circular 3.970 de 28 de novembro de 2019.

Os participantes autorizados podem se conectar à RSFN das seguintes formas:

- **direta**, devendo realizar adesão ao Acordo Operacional e ao Contrato de Prestação de Serviços de Gerência Integrada de Segundo Nível, de que tratam os itens 1.6 e 1.8, respectivamente;
- **por meio de um PSTI**, devendo escolher dentre aqueles credenciados pelo BCB e celebrar contrato específico;
- **híbrida**, em que o participante pode adotar mais de uma forma de conexão simultaneamente, observados os cenários do item 2.6.

São obrigações dos participantes da RSFN:

- contratar pelo menos uma conexão com cada operadora da RSFN, se diretamente conectado à RSFN. Caso o participante seja câmara ou prestador de serviços de compensação e de liquidação, deverá possuir pelo menos 2 sites, cada site com uma conexão de cada operadora da RSFN;
- contratar a Gerência Integrada de Segundo Nível, quando conectado diretamente à RSFN;
- solicitar ao Gestor do Manual de Redes as informações técnicas necessárias para a sua conexão à rede, informando o PSTI contratado, se for o caso;
- prestar informações ao Gestor do Manual de Redes, quando solicitado;
- utilizar certificado próprio, observados os requisitos do Manual de Segurança da RSFN;

- zelar pela guarda e integridade de suas chaves criptográficas privadas, utilizando mecanismos de segurança que garantam o acesso às chaves somente a pessoas autorizadas pelo participante;
- observar os padrões técnicos deste Manual;
- observar as regras de negócio específicas para cada serviço;
- possuir acessos redundantes e independentes entre si para a comunicação com o PSTI, quando não utilizar acesso direto à RSFN.

1.4.1 Suspensão e exclusão de participantes da RSFN

O BCB poderá suspender temporariamente da RSFN, se necessário sem aviso prévio, o participante que:

- utilizar a RSFN em desacordo com este Manual; e
- causar prejuízo à utilização da RSFN pelos demais participantes.

O BCB comunicará imediatamente a suspensão ao participante, que poderá revertê-la assim que comprovar que está apto a operar em conformidade com os padrões previsto neste Manual.

O BCB poderá excluir da RSFN, garantido o direito a ampla defesa, o participante que:

- utilizar a RSFN em desacordo com este Manual;
- colocar em risco o funcionamento normal da RSFN;
- não estiver autorizado ou em processo de homologação em pelo menos um dos serviços que utilizam a RSFN.

O participante excluído da RSFN poderá solicitar novamente a sua inclusão a qualquer momento.

1.5 Comunicação entre os participantes da RSFN

Os participantes devem observar as seguintes regras de conectividade na RSFN:

- é permitido a todos os participantes da RSFN estabelecer comunicação direta com os seus respectivos PSTI, o BCB, as IOSMF e os prestadores de serviços;
- é permitido ao BCB, às IOSMF e aos prestadores de serviços estabelecer comunicação direta com todos os participantes da RSFN;
- é permitido aos PSTI estabelecer comunicação direta com os seus clientes, o BCB, as IOSMF e os prestadores de serviços;
- é vedado aos participantes da RSFN e aos PSTI estabelecer comunicação direta entre si que não esteja prevista nos casos anteriores;
- é vedada a comunicação entre os dois *sites* de um mesmo participante via RSFN.

1.6 Operadoras de serviço de comunicação da RSFN

Operadoras de serviço de comunicação da RSFN são as empresas que proveem a infraestrutura de conectividade de rede para os participantes diretamente conectados à RSFN, os PSTI e o BCB.

Os participantes da RSFN devem selecionar as operadoras e definir o Acordo Operacional com as condições de prestação do serviço.

As operadoras selecionadas e o Acordo Operacional a ser celebrado devem ser submetidos à aprovação do BCB.

Atualmente as operadoras de telecomunicações da RSFN são a CLARO NXT TELECOMUNICAÇÕES LTDA (doravante denominada CLARO NXT ou Operadora VERMELHA) e o consórcio composto pelas empresas RTM – Rede de Telecomunicações para o Mercado LTDA e Claro S.A (doravante denominado consórcio RTM/Embratel ou Operadora AZUL).

São obrigações das operadoras de serviço de comunicação da RSFN:

- atender os níveis de serviço estabelecidos em contrato com os participantes (Acordo Operacional e demais instrumentos contratuais);
- manter neutralidade em relação aos participantes e aos PSTI;
- prover redundância em todos os segmentos da RSFN, tais como: *backbone*, entroncamentos e meios físicos, equipamentos, nós da rede e última milha;
- garantir que suas infraestruturas utilizadas para prover a RSFN são completamente independentes, ou seja, não possuem elementos comuns entre si;
- comunicar ao Gestor do Manual de Redes qualquer fato relevante relativo à sua infraestrutura que suporta a RSFN;
- certificar-se de que a instituição está apta a tornar-se participante da rede previamente a sua conexão à RSFN.

1.7 Provedor de Serviços de Tecnologia da Informação - PSTI

O PSTI é a entidade autorizada a prestar serviços de processamento de dados, para fins de acesso à RSFN, a instituições financeiras e demais instituições supervisionadas a funcionar pelo Banco Central do Brasil, nos termos da Resolução BCB nº 498, de 5 de setembro de 2025.

São obrigações dos PSTI:

- contratar a Gerência Integrada de Segundo Nível;
- prover aos seus clientes mecanismos de segurança adequados aos serviços contratados, observados este Manual, o Manual de Segurança do SFN e as demais regulamentações publicadas pelo BCB;
- quando necessário, realizar a configuração dos canais MQ no BCB utilizando o subdomínio específico da instituição, e não o subdomínio do PSTI;
- fornecer mensalmente para a Gerência Integrada de Segundo Nível da RSFN relação com todas as instituições interligadas ao provedor, detalhando: as instituições ativas, as instituições autorizadas e em ativação e/ou em homologação, além das que cancelaram seus contratos com o provedor no período. O documento deverá conter obrigatoriamente: nome da instituição, ISPB, subdomínio da RSFN e informações de contato técnico;
- fornecer e manter atualizado contato do suporte técnico qualificado tanto para seus clientes quanto para a Gerência Integrada de Segundo Nível. Esse suporte deve estar capacitado para atuar prontamente na solução de problemas que afetem os serviços prestados pelo PSTI;
- atuar na resolução de problemas que necessitem da articulação entre diversos envolvidos, como operadora de telecomunicação, operadora de última milha e clientes;

- utilizar somente a RSFN para comunicação entre PSTI e os demais participantes da RSFN que não sejam seus clientes, observando as restrições do item 1.5 deste Manual;
- prestar informações ao Gestor do Manual de Redes sempre que requisitado;
- assegurar e preservar o sigilo das informações processadas por seu intermédio;
- conectar-se à RSFN por meio de infraestrutura redundante com, no mínimo, dois *datacenters* independentes. Cada *datacenter* deverá ter acesso às duas operadoras da RSFN;
- observar os acordos de nível de serviço para todos os serviços prestados;
- certificar-se de que a instituição está apta a tornar-se participante da rede previamente a sua conexão à RSFN.

1.7.1 Comunicação entre o PSTI e seus clientes

A comunicação entre o PSTI e seus clientes poderá ocorrer utilizando:

- a RSFN;
- rede dedicada;
- rede privada compartilhada;
- a Internet.

A comunicação entre o PSTI e as instituições autorizadas deve feita por meio de um canal seguro, que garanta integridade, confidencialidade, disponibilidade e autenticidade das informações trafegadas.

No caso de utilização da Internet, o PSTI deverá implementar mecanismo de proteção contra ataques de negação de serviço distribuído (anti-DDoS) nos acessos à Internet utilizados para conexão com seus clientes.

O cliente deve utilizar no mínimo dois acessos redundantes e independentes entre si, a fim de prover alta disponibilidade, para comunicação com o PSTI. A seguir uma lista não exaustiva de combinações válidas:

- 2 circuitos da rede dedicada homologada pelo PSTI;
- 1 circuito da rede dedicada homologada pelo PSTI e 1 acesso à Internet;
- 2 acessos à Internet, providos por operadoras distintas;
- 1 circuito da rede dedicada homologada pelo PSTI e 1 circuito de rede privada compartilhada;
- 2 circuitos de rede privada compartilhada;
- 2 acessos à Internet para se comunicar com o PSTI A e com o PSTI B.

Caso o PSTI utilize formas distintas de comunicação da RSFN para prover serviços aos seus clientes, deverá ter acessos redundantes e independentes entre si, distribuído entre seus *datacenters*, a fim de prover alta disponibilidade.

1.8 Gerência Integrada de Segundo Nível da RSFN

A Gerência Integrada de Segundo Nível da RSFN – GI2N deve ser prestada por uma empresa independente das operadoras de serviço de comunicação e tem por finalidade:

- monitorar o tráfego de mensagens, arquivos e demais serviços autorizados a trafegarem na RSFN;

- monitorar a qualidade dos serviços prestados pelas operadoras;
- assessorar o Gestor do Manual de Redes nas questões relacionadas ao funcionamento da RSFN;
- acompanhar as atividades de configuração e falhas da RSFN, com funções de planejamento, monitoração, execução e documentação;
- acompanhar e auditar o funcionamento da RSFN e o cumprimento dos níveis de atendimento das operadoras de serviço de comunicação;
- comunicar ao Gestor do Manual de Redes eventuais desvios na utilização da RSFN pelos participantes e pelos PSTI;
- auxiliar na solução de requisições dos participantes não atendidos pelas operadoras;
- pesquisar e propor melhorias para a RSFN, tanto referentes ao desempenho e à estabilidade, quanto à implementação de novos serviços e de eventuais produtos que possam ser agregados;
- auxiliar no planejamento da implantação de novos serviços;
- seguir as diretrizes estabelecidas pelo BCB;
- preparar relatórios específicos sobre a RSFN quando solicitados pelo Gestor do Manual de Redes;
- encaminhar relatórios gerenciais periódicos ao Gestor do Manual de Redes sobre a utilização da RSFN.

Os participantes da RSFN devem contratar a prestadora do serviço de Gerência Integrada de Segundo Nível. A empresa selecionada e o Contrato de Prestação de Serviços de Gerência Integrada de Segundo Nível a ser celebrado devem ser submetidos à aprovação do BCB.

As atividades da Gerência Integrada de Segundo Nível serão executadas 24 horas por dia, 7 dias por semana (24x7).

Atualmente o serviço de Gerência Integrada de Segundo Nível é prestado pelo CPqD.

2 RSFN

2.1 Topologia lógica da RSFN

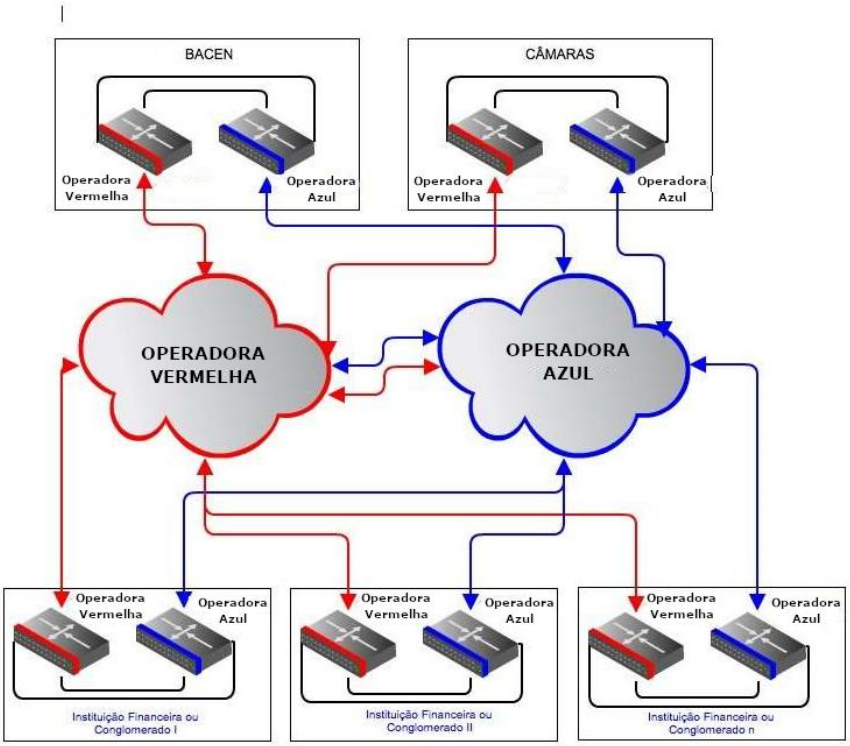


Figura 1- Comunicação entre as entidades participantes da RSFN

A RSFN é composta por duas redes MPLS, cada uma provida por uma das operadoras contratadas, interconectadas através de circuitos inter-AS. O BCB, os PSTI e os participantes se conectam em cada uma dessas redes de acordo com perfis pré-estabelecidos. A Figura 1 ilustra a comunicação na RSFN.

2.2 Endereçamento IP na RSFN

A RSFN recebeu do Comitê Gestor da Internet Brasil um bloco de endereços IP versão 4 (prefixo /18). Esse bloco foi subdivido em blocos menores (/27 ou /28), que são distribuídos aos participantes de acordo com os perfis adotados. Caso o participante adote o perfil A ou B, receberá um prefixo /28 para a VLAN de conexão com a RSFN. Para os demais perfis, receberá dois prefixos /28. O BCB, as Câmaras, os prestadores de serviços de compensação e de liquidação e os PSTI utilizarão perfil C ou D, recebendo dois prefixos /27 ou /28.

Para facilitar a administração dos endereços IP dos diferentes nós TCP/IP dentro de cada VLAN, as faixas foram padronizadas por tipo de *hosts*. Além de permitir a identificação rápida do recurso, a utilização de faixa de endereços permite definir listas de acesso e de prioridades para cada recurso da rede.

2.2.1 VLAN para Instituições com Prefixo /27

A alocação recomendada de endereços para esse prefixo está ilustrada na Tabela 1.

1º byte	2º byte	3º byte	4º byte	*host*	Tipo do *host*
X	X	X	xxx00001	1o.	Ethernet 0/0 CPE OPERADORA VERMELHA
X	X	X	xxx00010	2o.	Ethernet 0/0 CPE OPERADORA AZUL
X	X	X	xxx00011	3o.	HSRP
X	X	X	xxx00100	4o.	1o. switch
X	X	X	xxx00101	5o.	2o. switch
X	X	X	xxx00110	6o.	1o. Servidor DNS
X	X	X	xxx00111	7o.	2o. Servidor DNS
X	X	X	xxx01000	8o.	1o. Servidor MQ
X	X	X	xxx01001	9o.	2o. Servidor MQ
X	X	X	xxx01010	10o.	3o. Servidor MQ
X	X	X	xxx01011	11o.	4o. Servidor MQ
X	X	X	xxx01100	12º.	Reservado
X	X	X	...	...	Reservado
X	X	X	xxx11101	29º.	Reservado
X	X	X	xxx11110	30o.	*Firewall*

Tabela 1 - Faixa de Endereços dos hosts TCP/IP com máscara /27

Caso a instituição opte por consolidar seus prefixos /27 em um prefixo /26, a alocação dos endereços recomendada está ilustrada na Tabela 2.

1º byte	2º byte	3º byte	4º byte	*host*	Tipo do *host*
X	X	X	Xx000001	1o.	Ethernet 0/0 CPE OPERADORA VERMELHA do *site* principal
X	X	X	Xx000010	2o.	Ethernet 0/0 CPE OPERADORA AZUL do *site* principal
X	X	X	Xx000011	3o.	Ethernet 0/0 CPE Telmex do *site backup*
X	X	X	Xx000100	4o.	Ethernet 0/0 CPE OPERADORA AZUL do *site backup*
X	X	X	Xx000101	5o.	HSRP
X	X	X	Xx000110	6o.	1o. Servidor DNS
X	X	X	Xx000111	7o.	2o. Servidor DNS
X	X	X	Xx001000	8o.	1o. Servidor MQ
X	X	X	Xx001001	9o.	2o. Servidor MQ
X	X	X	Xx001010	10o.	3o. Servidor MQ
X	X	X	Xx001011	11o.	4o. Servidor MQ
X	X	X	Xx001100	12o.	Reservado
X	X	X	...	...	...
X	X	X	xx110111	55o.	Switch
X	X	X	…	…	
X	X	X	xx111011	59o.	*Firewall*
X	X	X	…	…	…
X	X	X	xx111110	62o.	*Firewall*

Tabela 2 -Faixa de Endereços dos hosts TCP/IP com máscara /26

2.2.2 VLAN para Instituições com Prefixo /28

A alocação recomendada de endereços para esse prefixo está ilustrada na Tabela 3.

1º byte	2º byte	3º byte	4º byte	*host*	Tipo do *host*
X	X	X	xxxx0001	1o.	Ethernet 0/0 CPE OPERADORA VERMELHA
X	X	X	xxxx0010	2o.	Ethernet 0/0 CPE OPERADORA AZUL
X	X	X	xxxx0011	3o.	HSRP
X	X	X	xxxx0100	4o.	1o. switch
X	X	X	xxxx0101	5o.	2o. switch
X	X	X	xxxx0110	6o.	1o. Servidor DNS
X	X	X	xxxx0111	7o.	2o. Servidor DNS
X	X	X	xxxx1000	8o.	1o. Servidor MQ
X	X	X	xxxx1001	9o.	2o. Servidor MQ
X	X	X	xxx01010	10o.	3o. Servidor MQ
X	X	X	xxx01011	11o.	4o. Servidor MQ
X	X	X	xxxx1100	12º.	Reservado
X	X	X	xxxx1101	13º.	Reservado
X	X	X	xxxx1110	14o.	*Firewall*

Tabela 3 - Faixa de Endereços dos hosts TCP/IP das IF com máscara /28

Caso a instituição opte por consolidar seus prefixos /28 em um prefixo /27, a alocação dos endereços recomendada está ilustrada na Tabela 4.

1º byte	**2º byte**	**3º byte**	**4º byte**	***host***	**Tipo do *host***
X	X	X	xxx00001	1o.	Ethernet 0/0 CPE OPERADORA VERMELHA do *site* principal
X	X	X	xxx00010	2o.	Ethernet 0/0 CPE OPERADORA AZUL do *site* principal
X	X	X	xxx00011	3o.	Ethernet 0/0 CPE OPERADORA VERMELHA do *site backup*
X	X	X	xxx00100	4o.	Ethernet 0/0 CPE OPERADORA AZUL do *site backup*
X	X	X	xxx00101	5o.	HSRP
X	X	X	xxx00110	6o.	1o. Servidor DNS
X	X	X	xxx00111	7o.	2o. Servidor DNS
X	X	X	xxx01000	8o.	1o. Servidor MQ
X	X	X	xxx01001	9o.	2o. Servidor MQ
X	X	X	xxx01010	10o.	3o. Servidor MQ
X	X	X	xxx01011	11o.	4o. Servidor MQ
X	X	X	xxx01100	12º.	Reservado
X	X	X	...	...	...
X	X	X	xxx10111	22º.	Switch
X	X	X	…	…	…
X	X	X	xxx11010	26º.	*Firewall*
X	X	X	…	…	…
X	X	X	xxx11110	30o.	*Firewall*

Tabela 4 - Faixa de Endereços dos hosts TCP/IP das IFs com máscara /27

2.3 Política de encaminhamento do tráfego de entrada e saída de dados

O critério de escolha do caminho de saída de cada entidade será definido pela configuração HSRP (*Hot Standby Router Protocol*). Nesta configuração, todos os *Hosts* da VLAN deverão apontar

para um *default gateway* virtual, onde os roteadores (CPE OPERADORA AZUL e OPERADORA VERMELHA) irão responder, sendo que um deles terá uma prioridade maior.

Os participantes serão divididos em dois grupos, de acordo com o bloco IP utilizado, de forma que uma operadora não seja mais sobrecarregada do que a outra. O circuito da OPERADORA VERMELHA terá preferência na comunicação entre entidades de mesmo grupo e o circuito da OPERADORA AZUL terá preferência na comunicação entre entidades de grupos diferentes, conforme a Figura 2.

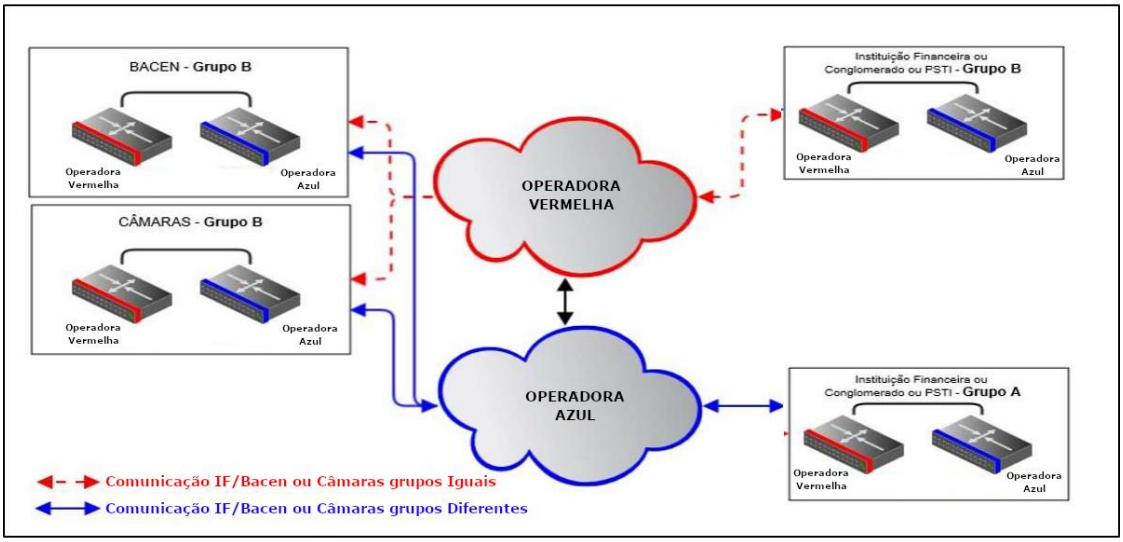


Figura 2 - Preferência de comunicação na RSFN

2.4 Conexão direta dos participantes à RSFN

Uma vez autorizado a participar da RSFN, a entidade deve solicitar a conexão às operadoras através das respectivas centrais de atendimento (ver seção Contatos no início deste Manual), disponibilizando o Formulário para Inclusão ou Alteração de Participantes na RSFN[1] (FIAP) preenchido, bem como quaisquer outras informações relevantes solicitadas pelas operadoras.

Em seguida, as operadoras encaminharão esses dados à GI2N. Se a entidade estiver autorizada a participar da RSFN, a GI2N providenciará o cadastro do nome do subdomínio informado pelo solicitante no DNS da RSFN e encaminhará ao solicitante e as operadoras as faixas de endereços IP a serem utilizadas pela entidade. Na eventual duplicidade de nomes de subdomínio, a GI2N negociará um novo nome com o solicitante.

As operadoras procederão com a inclusão do solicitante na RSFN, com disponibilização das conexões no(s) endereço(s) indicado(s) pelo solicitante, na modalidade *Turn Key*, ou seja, acesso local (par metálico, fibra óptica ou rádio). As operadoras fornecerão o roteador com o *hardware*, *software* e configurações necessários para suportar os serviços da RSFN. Esses roteadores serão de uso exclusivo para a RSFN.

Conexão dos roteadores das operadoras em barramento de rede local do participante deve ser realizada conforme modelos sugeridos no Capítulo 3**.**

Após a disponibilização dos circuitos pelas operadoras, recomenda-se ao participante realizar testes de conectividade e os testes previstos para o modelo de conexão utilizado (ver Capítulo 3).

[1] Disponível no *website* do BCB.

2.4.1 Perfis de conexão direta à RSFN

Os perfis possíveis para conexão à RSFN são os detalhados na Figura 3.

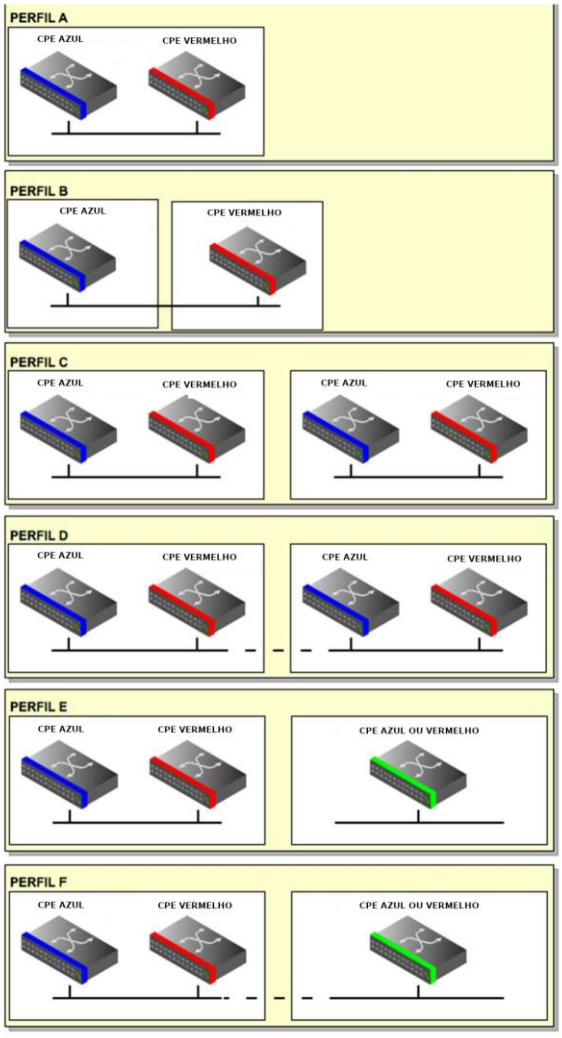


Figura 3 - Perfis de Conexão com a RSFN

2.4.2 Testes de Conectividade

Configurar uma estação com os parâmetros abaixo. Caso a instituição opte por efetuar o teste através da sua rede local, deve-se efetuar NAT.

- IP *address* do host;
- *subnet mask*: fornecida na documentação;
- *gateway*: endereço do HSRP.

Configurada a estação, **efetuar os seguintes testes:**

- *ping* no endereço IP 200.218.66.5 (HSRP do BCB);

- se OK, retirar o cabo ou desligar o modem de uma das OPERADORAS e efetuar novamente o *ping*;
- se OK, reconectar o cabo ou ligar o modem da OPERADORA desconectada no passo anterior e retirar o cabo ou desligar o modem da OUTRA OPERADORA e efetuar novamente o *ping*;
- se OK, reconectar o cabo ou ligar o modem da OPERADORA desconectada no passo anterior.

Caso algum dos testes falhe, abrir chamado na central de atendimento da operadora e reportar o procedimento e a falha.

2.5 Conexão dos participantes à RSFN por meio de um PSTI

Uma vez autorizado a participar da RSFN, a entidade deve escolher um PSTI dentre os homologados pelo Banco Central.

Em seguida, o PSTI encaminhará à GI2N as informações do novo participante. Se a entidade estiver autorizada a participar da RSFN, a GI2N providenciará o cadastro do nome do subdomínio informado pelo solicitante no DNS da RSFN. Na eventual duplicidade de nomes de subdomínio, a GI2N negociará um novo nome com o solicitante.

2.6 Conexão híbrida à RSFN

O participante poderá utilizar mais de uma forma de conexão à RSFN simultaneamente (direta ou por meio de um ou mais PSTI) quando houver possibilidade de segregação de tráfego.

São passíveis de segregação o tráfego:

- do domínio SPB01;
- do domínio SPB02;
- do grupo de domínios MES01, MES02 e MES03;
- do PIX.

Por exemplo: utiliza-se somente o PSTI A para o domínio SPB01; somente o PSTI B para os domínios MES01, MES02 e MES03; e somente a conexão direta à RSFN para o domínio SPB02.

3 MODELOS DE TOPOLOGIA E ENDEREÇAMENTO

3.1 Modelo 1

Conexão entre o *site* principal e *backup* feita por *link* interno e conexão entre a RSFN e entidade via roteadores ou *Firewall*.

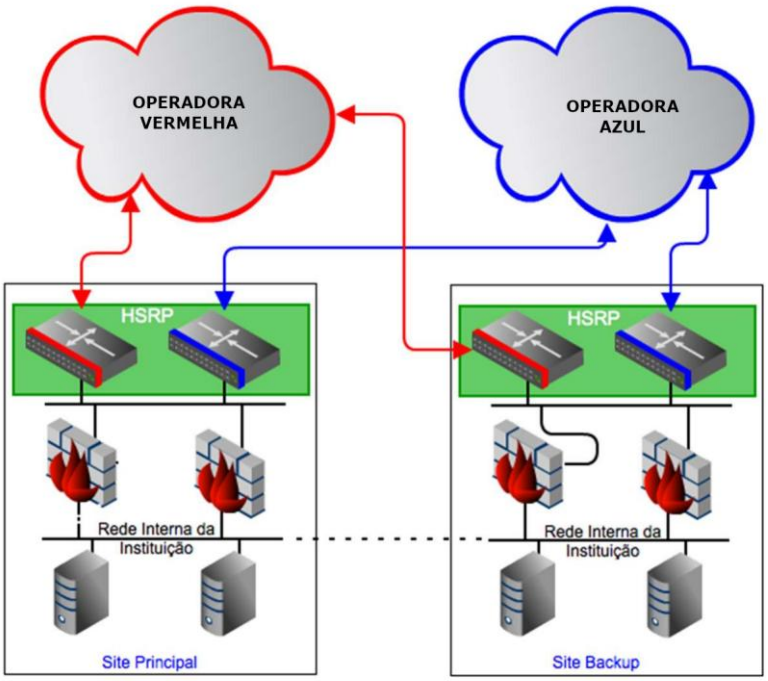


Figura 4 - Dois sites com interconexão pela rede interna

Este modelo pode ter como variante a conexão de apenas 1 *firewall* por *site*.

3.1.1 Testes

1. Queda do circuito OPERADORA VERMELHA do *site* principal
2. Queda do circuito OPERADORA AZUL do *site* principal.
3. Queda do circuito OPERADORA VERMELHA do *site backup*.
4. Queda do circuito OPERADORA AZUL do *site backup*.
5. Queda dos 2 circuitos do *site* principal.
6. Queda dos 2 circuitos do *site* principal + OPERADORA VERMELHA *site backup*.
7. Queda dos 2 circuitos do *site* principal + OPERADORA AZUL *site backup*.
8. Queda do roteador OPERADORA VERMELHA do *site* principal.
9. Queda do roteador OPERADORA AZUL do *site* principal.
10. Queda do roteador OPERADORA VERMELHA do *site backup*.
11. Queda do roteador OPERADORA AZUL do *site backup*.

12. Queda dos 2 roteadores do *site* principal.
13. Queda dos 2 roteadores do *site* principal + OPERADORA VERMELHA *site backup*.
14. Queda dos 2 roteadores do *site* principal + OPERADORA AZUL *site backup*.
15. Queda do *firewall* 1 do *site* principal.
16. Queda do *firewall* 2 do *site* principal.
17. Queda do firewall 1 do site backup.
18. Queda do firewall 2 do site backup.
19. Queda dos 2 *firewalls* do *site* principal.
20. Queda dos 2 *firewalls* do *site* principal + *firewall* 1 *site backup*.
21. Queda dos 2 *firewalls* do *site* principal + *firewall* 2 *site backup*

3.2 Modelo 2

Site Principal e *Backup* com apenas um CPE em cada.

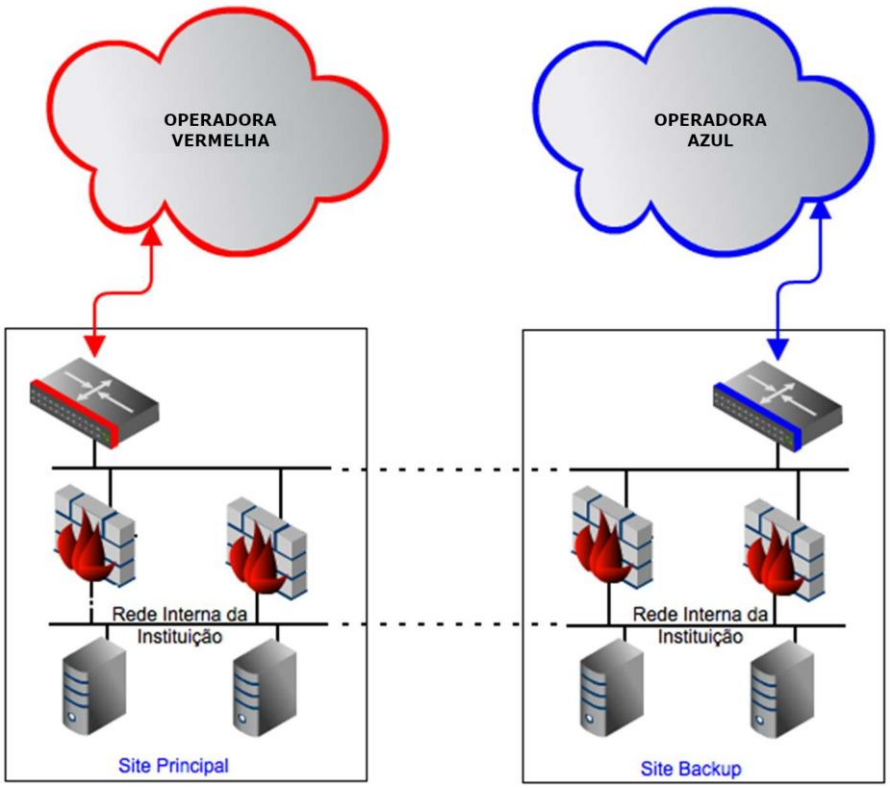


Figura 5 - Dois Sites, porém com apenas dois CPE

Este modelo pode ter como variante a conexão dos 2 CPE no mesmo *site* (sem *site backup*). Neste caso também podemos ter 1 ou 2 *firewalls*.

3.2.1 Testes

1. Queda do circuito OPERADORA VERMELHA do *site* principal.

2. Queda do circuito OPERADORA AZUL do *site backup*.
3. Queda do roteador OPERADORA VERMELHA do *site* principal.
4. Queda do roteador OPERADORA AZUL do *site backup*.
5. Queda do *firewall* do *site* principal.
6. Queda do firewall do site backup.

3.3 Modelo 3 e modelo 6

Conexão entre o *site* Principal e *Backup* feita pela extensão do barramento LAN da RSFN e conexão entre a RSFN e entidade via roteadores (que suportem roteamento BGP).

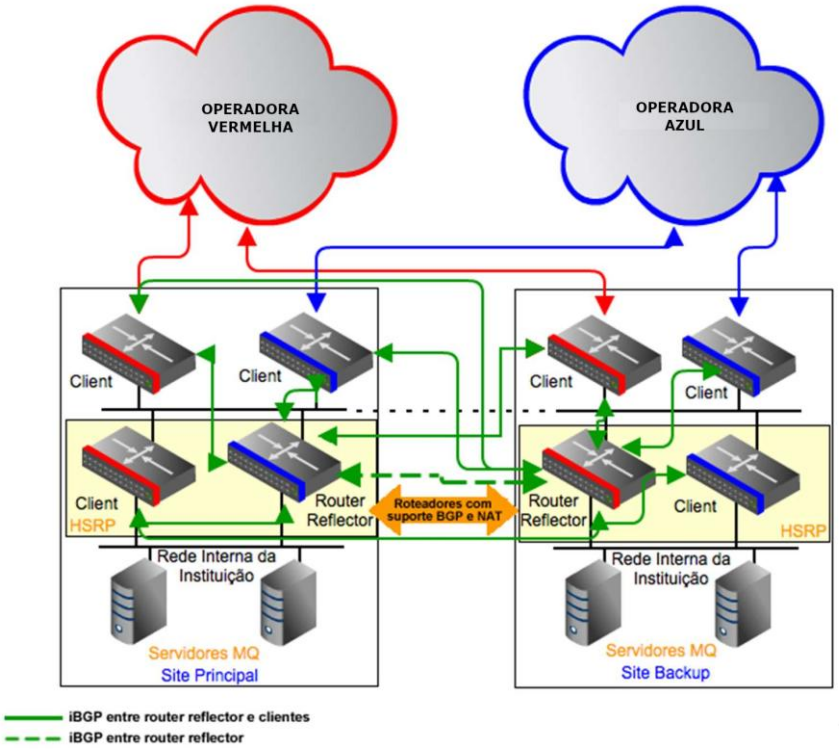


Figura 6 - Conexão do Perfil D com roteamento iBGP

Esse modelo pode ter como variantes:

1. Sites principal e *backup*, sendo que cada *site* deverá conter 2 CPE e **n** roteadores BGP (onde **n** é um número entre 1 e 2);
2. Sem *site backup*, com 2 CPE e **n** roteadores BGP no mesmo *site* (onde **n** é um número entre 1 e 2).

3.3.1 Testes

1. Queda do circuito OPERADORA VERMELHA do *site* principal.
2. Queda do circuito OPERADORA AZUL do *site* principal.
3. Queda do circuito OPERADORA VERMELHA do *site backup*.
4. Queda do circuito OPERADORA AZUL do *site backup*.
5. Queda dos 2 circuitos do *site* principal.
6. Queda dos 2 circuitos do *site* principal + OPERADORA VERMELHA *site backup*
7. Queda dos 2 circuitos do *site* principal + OPERADORA AZUL *site backup*.
8. Queda do roteador OPERADORA VERMELHA do *site* principal.
9. Queda do roteador OPERADORA AZUL do *site* principal.
10. Queda do roteador OPERADORA VERMELHA do *site backup*.
11. Queda do roteador OPERADORA AZUL do *site backup*.
12. Queda dos 2 roteadores do *site* principal.
13. Queda dos 2 roteadores do *site* principal + OPERADORA VERMELHA *site backup*.
14. Queda dos 2 roteadores do *site* principal + OPERADORA AZUL *site backup*.
15. Queda do roteador BGP 1 do *site* principal.
16. Queda do roteador BGP 2 do *site* principal.
17. Queda do roteador BGP 1 do *site backup*.
18. Queda do roteador BGP 2 do *site backup*.
19. Queda dos 2 roteadores BGP do *site* principal.
20. Queda dos 2 roteadores BGP do *site* principal + roteador BGP 1 *site backup*.
21. Queda dos 2 roteadores BGP do *site* principal + roteador BGP 2 *site backup.*

3.4 Modelo 4 e modelo 5

Conexão entre o *site* Principal e *Backup* feita pela extensão do barramento LAN da RSFN e a conexão entre a RSFN e a entidade via célula de segurança (equipamentos que não suportam roteamento BGP).

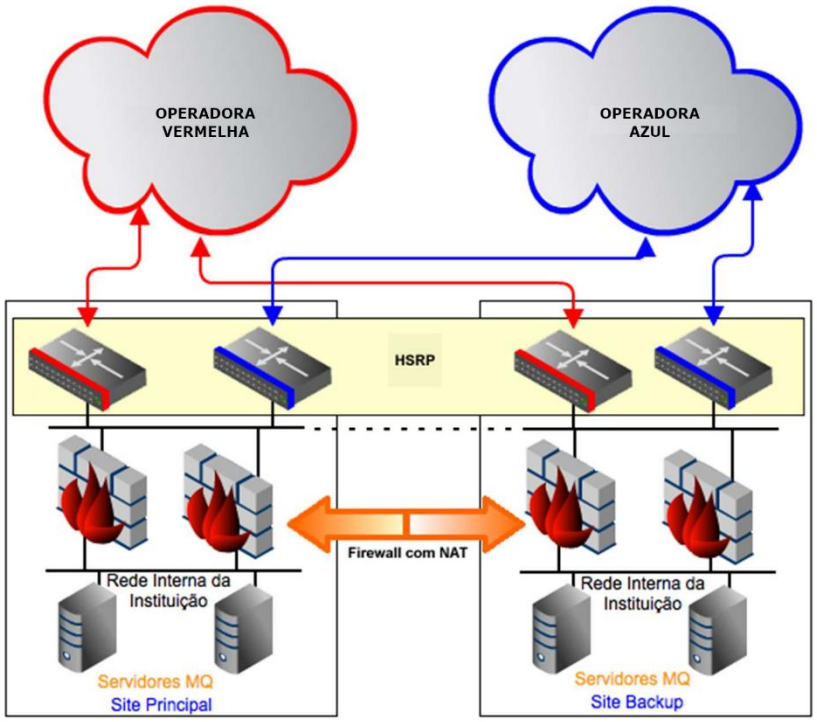


Figura 7- Conexão direta do Perfil D com a célula de segurança

3.4.1 Testes

1. Queda do circuito OPERADORA VERMELHA do *site* principal.
2. Queda do circuito OPERADORA AZUL do *site* principal.
3. Queda do circuito OPERADORA VERMELHA do *site backup*.
4. Queda do circuito OPERADORA AZUL do *site backup*.
5. Queda dos 2 circuitos do *site* principal.
6. Queda dos 2 circuitos do *site* principal + OPERADORA VERMELHA *site backup*.
7. Queda dos 2 circuitos do *site* principal + OPERADORA AZUL *site backup*.
8. Queda do roteador OPERADORA VERMELHA do *site* principal.
9. Queda do roteador OPERADORA AZUL do *site* principal.
10. Queda do roteador OPERADORA VERMELHA do *site backup*.
11. Queda do roteador OPERADORA AZUL do *site backup*.
12. Queda dos 2 roteadores do *site* principal.

13. Queda dos 2 roteadores do *site* principal + OPERADORA VERMELHA *site backup*
14. Queda dos 2 roteadores do *site* principal + OPERADORA AZUL *site backup*.
15. Queda do *firewall* 1 do *site* principal.
16. Queda do *firewall* 2 do *site* principal.
17. Queda do firewall 1 do site backup.
18. Queda do firewall 2 do site backup.
19. Queda dos 2 *firewalls* do *site* principal.
20. Queda dos 2 *firewalls* do *site* principal + *firewall* 1 *site backup*.
21. Queda dos 2 *firewalls* do *site* principal + *firewall* 2 *site backup*

4 ROTEAMENTO DA RSFN

As operadoras garantem que as rotas das VPN dos participantes da RSFN não serão divulgadas para a Internet. A operadora não deve interferir na política de roteamento dos participantes da RSFN.

Todo o tráfego das informações de entrada dos participantes não terá preferência entre os circuitos das duas operadoras; o mesmo se aplica para todo o tráfego das informações de saída dos participantes, que não terão preferência entre os circuitos, dividindo o tráfego entre as duas operadoras. Este controle é feito pelo protocolo de roteamento BGP, responsável pelo roteamento dos pacotes entre os CPE e as operadoras.

4.1 Roteamento para os perfis A e B (Modelo 2)

Apenas um site com dois CPE de cada operadora ou site principal e backup com apenas um CPE em cada.

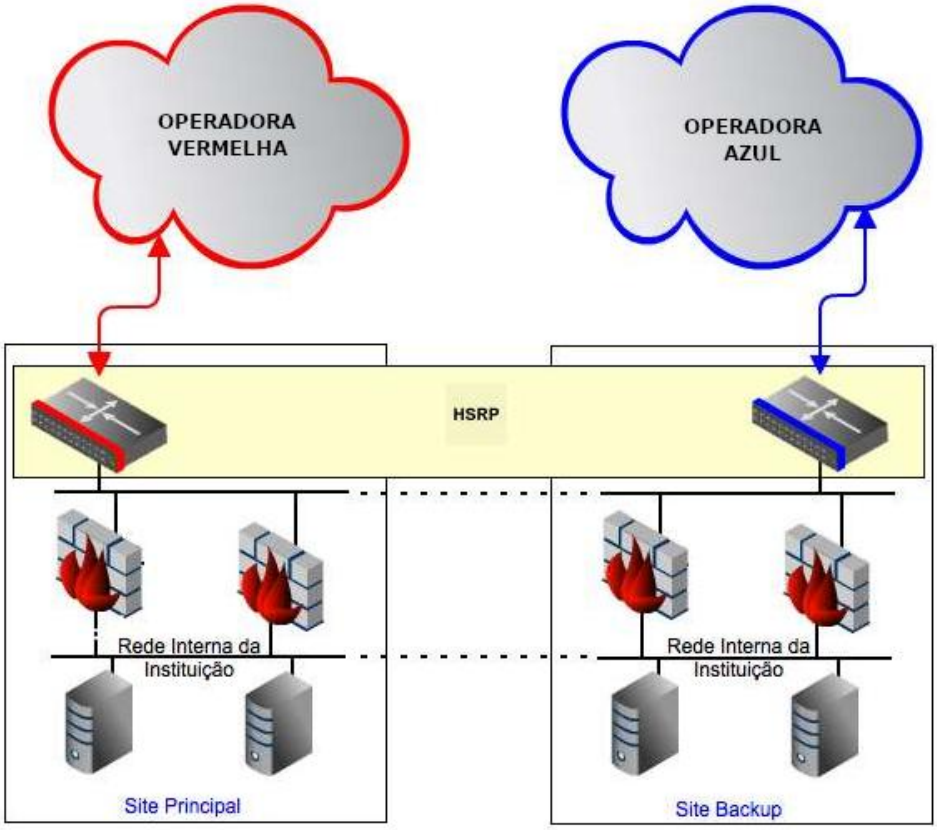


Figura 8 - Topologia com dois sites, porém com apenas dois CPE

Neste tipo de conexão, a entidade receberá apenas um prefixo de endereçamento IP e será cadastrado no DNS um registro com apenas um prefixo. Internamente deverá ser utilizado NAT sob total controle da entidade.

Na rede local da entidade, o segmento que interliga os CPE e a célula de segurança não possui nenhum protocolo de roteamento dinâmico, sendo utilizado apenas roteamento estático.

Como nesse segmento de rede local existem dois roteadores, será utilizado o protocolo HSRP. Desta forma, os *hosts* terão alternativas de acesso externo em caso de falha de um roteador, sem necessidade de configuração manual.

Os dois roteadores possuirão alocação de endereços das interfaces Ethernet. Além disso será alocado um terceiro endereço virtual, que corresponderá ao HSRP. Este endereço virtual deverá ser o mesmo em ambos os roteadores e corresponderá ao *default* gateway dos *hosts* deste segmento de rede.

4.2 Roteamento para o perfil C (Modelo 1)

Conexão entre o *site* principal e *backup* feita por link interno e conexão entre a RSFN e entidade via roteadores ou *firewall*.

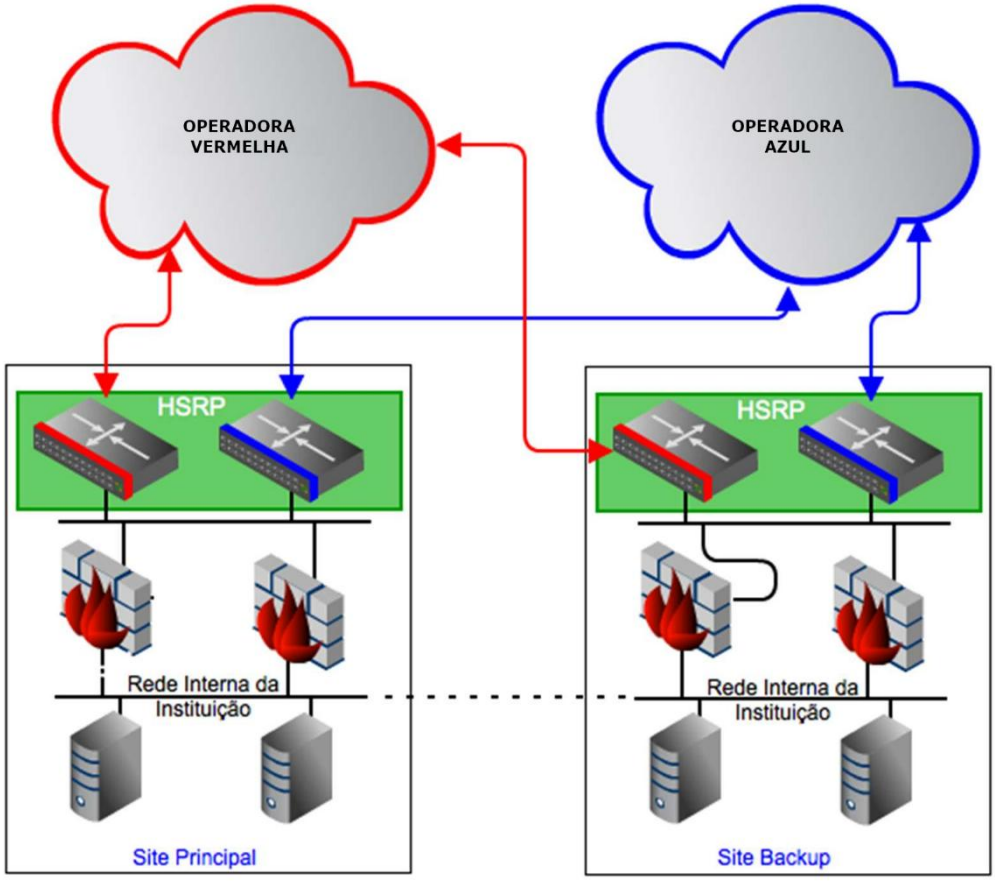


Figura 9- Topologia com dois sites com interconexão pela rede interna

Para esta topologia, a entidade será cadastrada no DNS com dois registros de prefixo - um do *site* principal e outro do *site backup*.

Sob o ponto de vista de roteamento IP, serão considerados dois participantes, isto é, tanto no *site* principal como no *site backup* serão configurados dois CPE.

Internamente deverá ser utilizado NAT em ambos os *sites* sob total controle da entidade. Isto significa que o pacote que sair do *site backup* terá um endereço diferente em relação ao *site* principal.

Como o roteamento está ativo em ambos os *sites*, no caso de um dos *sites* ficar indisponível, o outro continuará em funcionamento de forma transparente para a RSFN.

4.3 Roteamento para o perfil D - roteadores no barramento RSFN (Modelo 3)

Conexão entre o site principal e *backup* feita pela extensão do barramento LAN da RSFN e conexão entre a RSFN e entidade via roteadores (que suportem roteamento BGP).

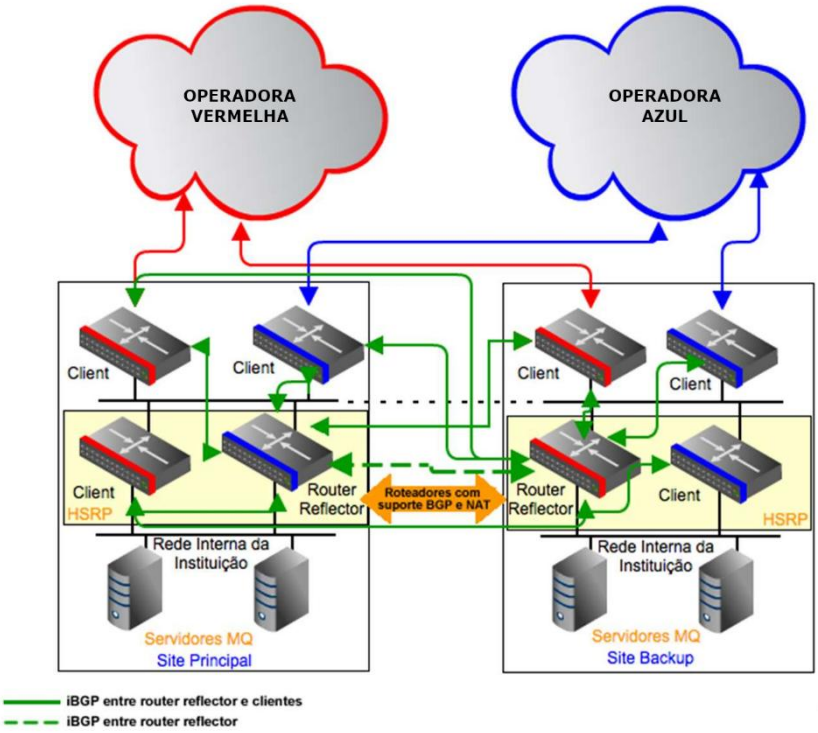


Figura 10 - Conexão do Perfil D com roteamento iBGP

Embora neste tipo de conexão os participantes recebam dois blocos de endereçamento IP, para a RSFN será anunciado apenas um único prefixo (prefixo /27 ou /26).

Caso sejam utilizados roteadores entre o barramento da RSFN e a rede da entidade, pode ser utilizado roteamento BGP entre todos os roteadores. Um dos roteadores de cada site deverá ser configurado como *route-reflector* (para reduzir o número de conexões IBGP, ficando transparente para a operadora a existência de um ou mais roteadores da entidade no barramento RSFN). Os demais roteadores deste barramento serão configurados como *route-reflector-client* e terão como *neighbor* iBGP apenas os dois roteadores da entidade (os route-reflector), como ilustrado na Figura 10. Os roteadores dos participantes deverão utilizar os endereços da interface local para as configurações BGP, em vez de utilizar interfaces *loopbacks*. Desta forma, a configuração do HSRP deverá ser nos roteadores da entidade em vez de ser nos roteadores CPE.

4.4 Roteamento para o perfil D - roteadores no barramento RSFN e NAT (Modelo 6)

Conexão entre o *site* principal e *backup* feita pela extensão do barramento LAN da RSFN, conexão entre a rede RSFN e entidade via roteadores (que suportem roteamento BGP) com blocos não sumarizados na rede da entidade. O primeiro prefixo será utilizado para a VLAN das interfaces *Ethernet* dos roteadores CPE e o segundo prefixo será utilizado para o *pool* de NAT. Divulgação do segundo prefixo a partir de roteadores internos para que os CPE possam alcançar os endereços deste prefixo a partir dos *route-reflectors*.

Este modelo visa atender à necessidade de uma entidade ter roteamento BGP em sua estrutura interna (modelo 3) utilizando *route-reflectors* e realizar o NAT em um dispositivo de rede interna e não na VLAN das interfaces *Ethernet* dos roteadores CPE utilizando ARP (**modelo 5**).

Para a RSFN, será anunciado apenas um único prefixo (prefixo /27 ou /26) e o grupo (grupo A/B) será referente ao primeiro prefixo fornecido pelo BCB (ou seja, se o primeiro prefixo for grupo A, o sumário será do grupo A).

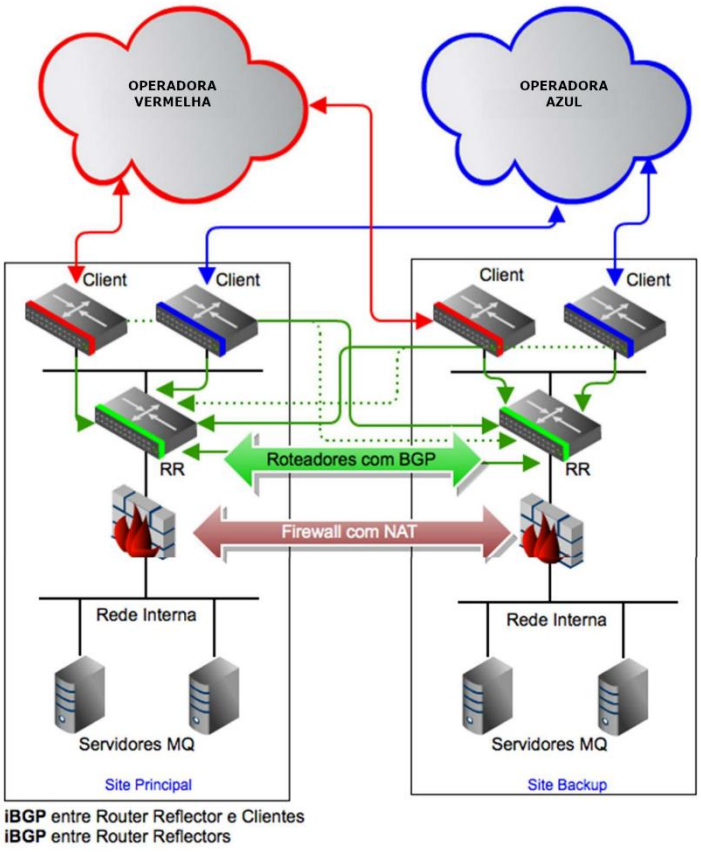


Figura 11 -Topologia com dois sites, quatro roteadores da entidade e NAT interno

Caso haja roteadores entre o barramento RSFN e a rede da entidade, deverá ser utilizado roteamento BGP entre todos os roteadores. Um dos roteadores (de cada *site*) deverá ser configurado como *route-reflector* (para reduzir o número de conexões iBGP, ficando transparente para a operadora a existência de um ou mais roteadores da entidade no barramento RSFN). Os demais roteadores deste barramento serão configurados como *route-reflector-client* e terão como *neighbor* iBGP apenas os dois roteadores da entidade (os *route-reflectors*), como ilustrado na Figura 11. Os roteadores dos participantes deverão utilizar os endereços da interface local para as configurações BGP, em vez de utilizar interfaces *loopbacks*. Desta forma, as configurações do HSRP, caso seja necessário, deverá ser nos roteadores da entidade em vez de nos roteadores CPE.

O *route-reflector* do *site* principal deverá ter a interface de rede da VLAN RSFN com o 13º endereço do primeiro prefixo e o *route-reflector* do *site* secundário o 14º. Apesar de, a partir dos CPE existirem dois caminhos para a o segundo prefixo, a opção de acesso será tomada para o vizinho (*neighbor*) com o menor endereço IP (*site* principal).

4.5 Roteamento para o perfil D com *firewall* da entidade no barramento RSFN (Modelo 4)

Conexão entre o *site* principal e *backup* feita pela extensão do barramento LAN da RSFN e a conexão entre a RSFN e a entidade via célula de segurança (equipamentos que não suportam roteamento BGP).

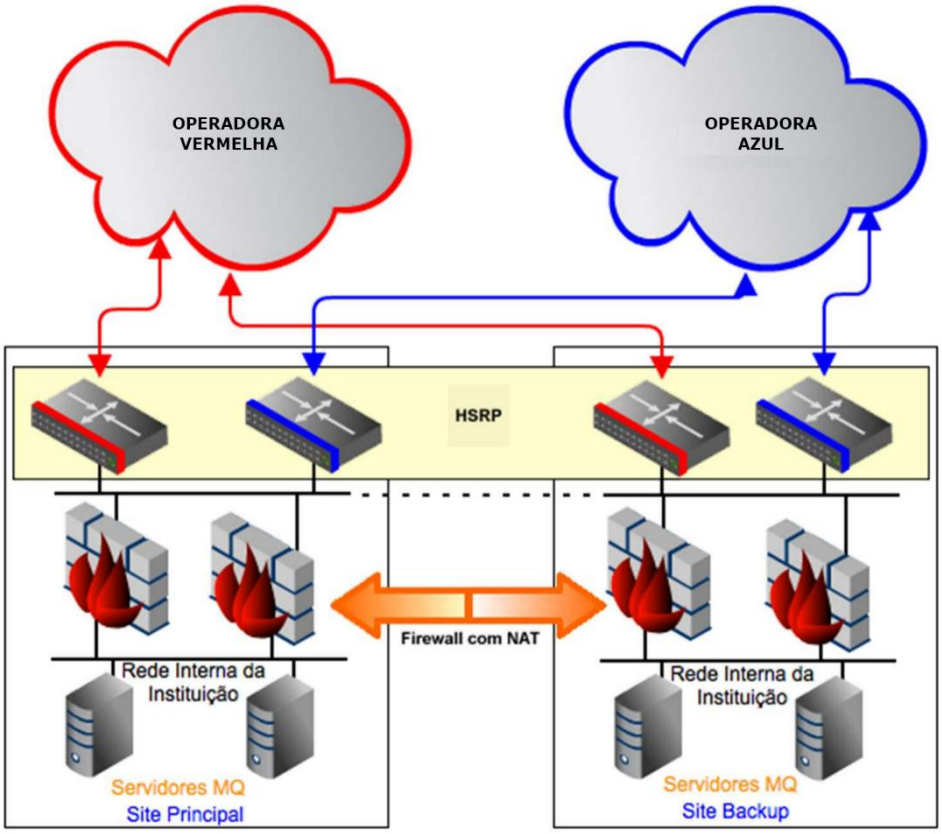


Figura 12 - Conexão direta do Perfil D com a célula de segurança

A diferença entre esse modelo e o modelo do item 4.4 é o fato de que os equipamentos de interface entre o barramento da RSFN e o da entidade não suportarem o protocolo de roteamento BGP (ou a entidade optar em não utilizar esse protocolo). Neste caso, deverá ser configurado HSRP envolvendo os 4 CPE (dois de cada *site*). Os blocos IP serão sumarizados e anunciados como único na RSFN, ou seja, /27 para os participantes com dois prefixos /28 e /26 para participantes com dois prefixos /27.

Esse modelo deverá ter garantida a comunicação entre os quatro roteadores de forma a garantir que, quando ativos simultaneamente, não haja interrupção do tráfego por ausência de comunicação entre os mesmos. A interrupção da conectividade entre os dois *sites* poderá causar perda de conectividade com a RSFN. As operadoras devem ser consultadas para maiores detalhes sobre essa característica de tráfego.

4.6 Roteamento para o perfil D com *firewall* da entidade no Barramento RSFN (Modelo 5)

Similar ao modelo 4, exceto que o bloco não é sumarizado. O primeiro prefixo será utilizado para a VLAN das interfaces *Ethernet* dos roteadores CPE e o segundo prefixo será utilizado para o *pool* de NAT. Desta forma não haverá necessidade de configurar uma tabela ARP estaticamente nos

firewalls, sendo necessária apenas a inserção de uma rota estática nos CPE indicando o *next-hop* do segundo prefixo /28.

A diferença entre este modelo em relação ao modelo 4 se refere em definir dois domínios de *broadcast*.

5 CONEXÃO DA INFRAESTRUTURA DOS PSTI E DOS PARTICIPANTES À RSFN

Os PSTI e os participantes devem observar os seguintes requisitos mínimos para conexão direta à RSFN:

- em hipótese alguma, o segmento da RSFN deve estar interligado ao segmento da intranet sem a utilização de *firewall stateful,* que permita a segregação e o controle de tráfego da/para a RSFN;
- somente o segmento da RSFN deve utilizar endereços fornecidos pela RSFN. Os demais segmentos de rede devem utilizar endereços da intranet da entidade, realizando a tradução de endereços IP, quando necessária;
- as entradas de DNS no subdomínio rsfn.net.br deverão conter exclusivamente endereços lógicos da RSFN;
- deverão ser configuradas rotas específicas para os endereços IP da RSFN, apontando para o endereço do *default gateway* virtual. A GI2N poderá orientar na configuração dessas rotas.

Para reduzir o risco de indisponibilidade nos serviços, é recomendado fortemente aos participantes que revisem periodicamente sua infraestrutura de comunicação fim-a-fim para conexão à RSFN, com o objetivo de contemplar equipamentos e caminhos redundantes, observando manter uma equiparação ao grau de redundância entregue pelo perfil de conexão contratado, item 2.4.1, de forma a evitar pontos únicos de falha desde da origem da mensagem até os CPE das operadoras da RSFN. Nesse contexto, recomenda-se que os participantes adotem centros de processamento geograficamente distintos, utilizando, por exemplo, diferentes zonas de disponibilidade de nuvens públicas, datacenters próprios ou colocação em datacenters de terceiros.

Caso o percurso da mensagem dependa de provedores de serviços, recomenda-se que essa mesma redundância seja observada, utilizando provedores distintos e sem compartilhamento de recursos entre si para a prestação do serviço. Essa recomendação aplica-se especialmente aos casos em que há necessidade de contratação de circuitos para interligar a nuvem pública onde a aplicação está hospedada e os CPE das operadoras da RSFN em outra localidade.

Também deve ser considerada a utilização de solução de balanceamento de carga para distribuir o serviço entre diferentes servidores aplicação, dentro de um mesmo site ou entre sites bem como a adoção de soluções complementares de segurança, como firewall de aplicação (WAF) e sistema de prevenção de intrusão (IPS).

Por fim, é importante ressaltar a necessidade de se validar periodicamente a alta disponibilidade na conexão à RSFN, incluindo a realização de testes de resiliência.

6 SERVIÇOS DE REDE DA RSFN

6.1 DNS (Domain Name System)

O DNS é um componente fundamental para o funcionamento dos serviços na Rede do Sistema Financeiro Nacional, sendo mandatório o uso de FQDN sempre que necessário.

6.1.1 Arquitetura de DNS

O modelo de replicação dos apontamentos de subdomínios e a forma de consultas utilizadas na RSFN estão apresentadas na Figura 13.

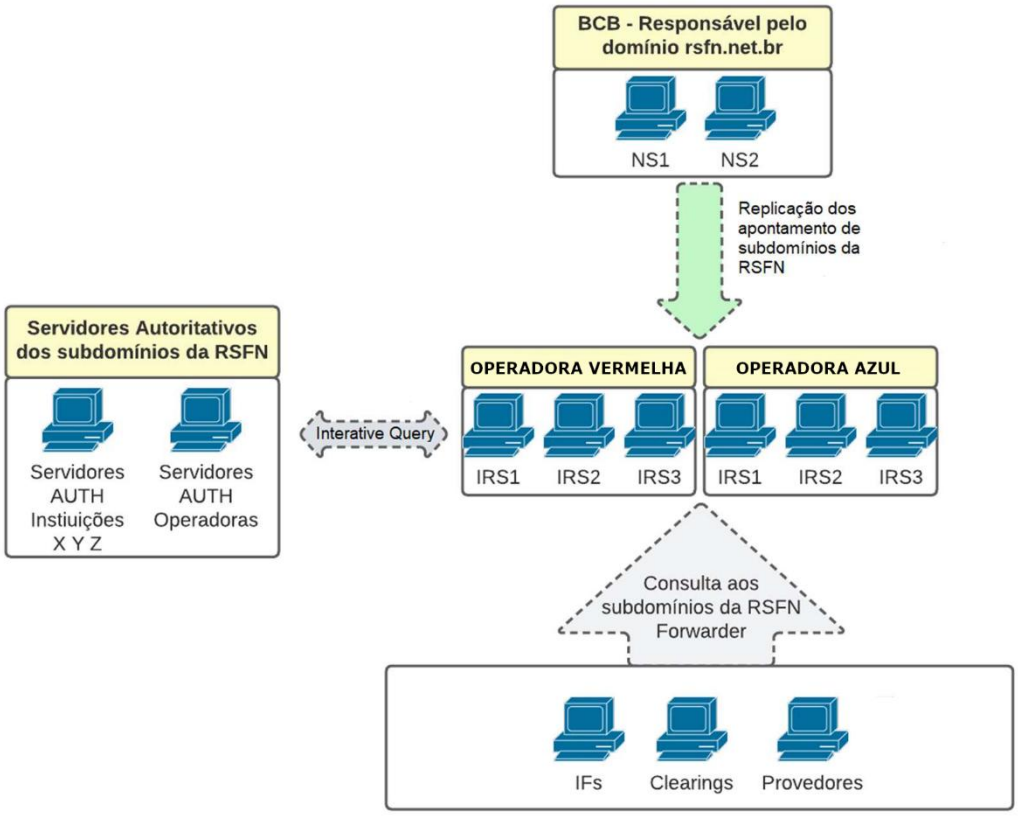


Figura 13 - Diagrama de consultas aos subdomínios na RSFN

A administração do domínio rsfn.net.br é realizada pelo BCB, onde estão localizados os servidores primários e secundários.

Quaisquer mudanças nas características dos subdomínios da RSFN são realizadas nos servidores do Banco Central.

Para prover balanceamento de carga e contingência do serviço de DNS, as configurações do domínio rsfn.net.br são replicadas para servidores secundários de DNS configurados como *Internal Root Servers* (IRS), mantidos pelas operadoras da RSFN. Os IRS, listados na Tabela 5, estão estrategicamente distribuídos nos segmentos de rede das operadoras em São Paulo (irs1), no Rio de Janeiro (irs2) e em Brasília (irs3).

Nome do servidor	Endereço IP	Operadora
irs1.att.rsfn.net.br	200.218.64.6	AZUL
irs1.ebtrtm.rsfn.net.br	200.218.64.134	VERMELHA
irs2.att.rsfn.net.br	200.218.64.38	AZUL
irs2.ebtrtm.rsfn.net.br	200.218.64.166	VERMELHA
irs3.att.rsfn.net.br	200.218.64.70	AZUL
irs3.ebtrtm.rsfn.net.br	200.218.64.198	VERMELHA

Tabela 5 - Lista de IRS

Cada subdomínio rsfn.net.br deverá possuir ao menos dois servidores com autoridade sobre sua respectiva zona de DNS, observando as seguintes diretrizes:

- os servidores devem estar configurados de forma que seja replicada imediatamente qualquer alteração do subdomínio para os servidores secundários;
- todos os participantes que utilizarem infraestrutura com sites no modelo Ativo/Passivo, deverão possuir ao menos um conjunto de servidores autoritativos (primário e secundário) em cada site.

6.1.2 Padronização de Nomes de Hosts

Os nomes de hosts utilizados na RSFN deverão seguir o padrão apresentado na Tabela 6.

host	Padrão a ser adotado
Roteador CPE OPERADORA VERMELHA	att-sub-domínio-localidade-cpe
Roteador CPE OPERADORA AZUL	ebtrtm-sub-domínio-localidade-cpe
HSRP	hsrp-sub-domínio-localidade-cpe
1º switch	sw01
2º switch	sw02
1º Servidor de DNS	ns1
2º Servidor de DNS	ns2
Servidor Produção MQ SPB	mqs01
1º Servidor Produção MQ multi-instance SPB02	mqs01a
2º Servidor Produção MQ multi-instance SPB02	mqs01b
Servidor Homologação MQ SPB	mqs02
1º Servidor Homologação MQ multi-instance SPB02	mqs02a
2º Servidor Homologação MQ multi-instance SPB02	mqs02b
Servidor MQ MES Produção	mqm01
Servidor MQ MES Homologação	mqm02
3ª Estação de trabalho	wks03
1º Firewall	fw01
2º Firewall	fw02

Tabela 6 - Padronização de nomes de hosts

6.1.3 Parâmetro de Temporização do Registro SOA

O temporizador TTL é o tempo de vida default para os registros do DNS de cada zona e indica quanto tempo um registro de outros domínios ficará armazenado no cache dos servidores de nomes. É obrigatório na RSFN o uso de TTL igual a ZERO para todos os hosts disponibilizados, incluindo servidores MQ, conforme modelo de configuração apresentado na Tabela 7.

Nome de domínio (FQDN)	TTL	Tipo	Classe	RData
mqsNN.sub-domínio.rsfn.net.br	0	A	IN	xxx.xxx.xxx.xxx
mqsNNa|b.sub-domínio.rsfn.net.br	0	A	IN	xxx.xxx.xxx.xxx
mqmNN.sub-domínio.rsfn.net.br	0	A	IN	xxx.xxx.xxx.xxx

Tabela 7 - Parâmetro de temporização de registro

6.1.4 DNS dos participantes e dos PSTI

O participante é responsável pela administração e pela manutenção de seus respectivos subdomínios.

O participante poderá escolher o nome de subdomínio a ser utilizado na RSFN, desde que não conflite com outro subdomínio ativo. Recomenda-se a padronização do nome utilizado na RSFN com o nome registrado no Registro.br ou instituição equivalente. Por exemplo: bcb.gov.br e bcb.rsfn.net.br.

Para resolução de nomes de outros subdomínios da RSFN, os participantes e os PSTI devem utilizar a configuração forwarder em seus servidores de DNS, observando as seguintes diretrizes:

- devem ser apontados todos os servidores IRS das operadoras listados na Tabela 5;
- participantes do grupo A devem configurar a diretiva forwarder tendo como primeiro servidor um IRS da operadora OPERADORA VERMELHA, como segundo um IRS da operadora OPERADORA AZUL e assim sucessivamente;
- participantes do grupo B devem configurar a diretiva forwarder tendo como primeiro servidor um IRS da operadora OPERADORA AZUL, como segundo um IRS da operadora OPERADORA VERMELHA e assim sucessivamente;
- respeitando as diretivas acima, recomenda-se ordenar os servidores forwarder de acordo com a latência, tomando como primeiro da lista o servidor de menor latência.

À exceção das Câmaras, os participantes da RSFN podem utilizar para resolução de nomes de forma autoritativa de seu subdomínio os servidores de uma das operadoras ou do PSTI contratado.

Participantes que possuem servidores de DNS próprios podem utilizá-los para outros domínios, por exemplo intranet/internet, desde que sejam tomadas todas as medidas de segurança garantindo a integridade e segmentação da RSFN.

Os registros de DNS para servidores MQ deverão obedecer adicionalmente à seção 7.2.1 - Padrão mandatório de endereços de hostnames.

6.2 Servidor de tempo (time server)

Está disponível um servidor de tempo no BCB que poderá ser utilizado pelos participantes da RSFN para o sincronismo de horário dos servidores MQ e demais servidores da RSFN através do protocolo NTP. Abaixo seguem descritos os dados necessários para acesso a este serviço:

- servidor: ntp.bcb.rsfn.net.br;
- porta de acesso: 123 (UDP).

6.3 Servidor Web da RSFN

O BCB disponibilizou na RSFN um servidor Web onde estão publicadas as informações referentes à RSFN. Esse serviço pode ser acessado através da rede pelo nome **www.rsfn.net.br**.

6.4 Servidor FTP

Para a RSFN, o serviço FTP no modo ativo utilizará as portas 20 (para transferência de dados) e 21 (para comandos). Já em modo passivo utilizará o range de portas 1110 a 1121.

Por exemplo, a solução VSFTP apresentará os seguintes parâmetros:

- pasv_enable=YES;
- pasv_min_port=1110;
- pasv_max_port=1121;
- port_enable=YES.

7 INFRAESTRUTURA DE MENSAGERIA

7.1 Diretrizes básicas

A mensageria é baseada em um *software* gerenciador de filas, o MQ. Recomenda-se utilizar a versão mais atual deste *software*; entretanto, isto não é requisito de funcionamento, sendo possível a comunicação entre diferentes versões. Não será permitida a utilização de outros aplicativos para transferência de mensagens, que não sejam de uso comum por todas as instituições participantes.

Não haverá conexões do MQ do tipo cliente-servidor entre os participantes da RSFN, todos deverão se conectar à rede usando o modo **servidor-servidor**. As conexões entre PSTI (aglomerados, conglomerados e provedores de contingência) e seus agregados podem ser do tipo cliente-servidor.

Para o tráfego de mensagens na RSFN, foram estabelecidos cinco domínios de sistemas: **SPB01**, **SPB02**, **MES01**, **MES02** e **MES03**.

Os domínios SPB01 e SPB02 dizem respeito ao tráfego de mensagens dos grupos de serviços relacionados ao Sistema de Pagamentos Brasileiro.

Os domínios de sistema da Mensageria Sisbacen (**MES01**, **MES02** e **MES03**) contêm os grupos de **mensagens não relacionadas a pagamentos**. Para o envio das mensagens nesses domínios, serão utilizados canais, filas, endereços (DNS) e portas específicas, ou seja, diferentes daquelas utilizadas pelo **SPB01** e pelo **SPB02**.

A permissão para tráfego das mensagens nos domínios dar-se-á conforme regulamentado no Catálogo de Serviços do SFN, para cada grupo de serviços.

Em todos os domínios de sistema, as instituições serão identificadas pelo CNPJ básico de oito posições ou, no caso dos participantes das mensagerias do SPB01 e do SPB02, pelo **ISPB**. O BCB será identificado por seu ISPB, ou seja, **00038166**.

O BCB usará um conjunto de filas (objetos MQ) para cada instituição, diferenciados de acordo com os domínios de sistema utilizado.

As instituições utilizarão os mesmos certificados digitais para os domínios SPB01 e SPB02, observando a separação entre os ambientes de homologação e de produção. Portanto, um certificado digital ativo para o domínio SPB01 estará ativo, automaticamente, no domínio SPB02. Não será possível ativar certificados distintos para os domínios SPB01 e SPB02 em um mesmo ambiente (de homologação ou de produção).

De forma análoga, as instituições utilizarão os mesmos certificados digitais para os domínios MES01, MES02 e MES03, observando a separação entre os ambientes de homologação e de produção. Portanto, um certificado digital ativo para o domínio MES01 estará ativo, automaticamente, nos domínios MES02 e MES03. Não será possível ativar certificados distintos para os domínios MES01, MES02 e MES03 em um mesmo ambiente (de homologação ou de produção).

Para o gerenciamento de certificados digitais, consulte o uso das mensagens do grupo de serviços **GEN** no Catálogo de Serviços do SFN.

7.2 Definições do MQ

Será ignorada a fila informada no campo *ReplyToQ* do *header* do MQ para as respostas geradas pelas aplicações. Será usada a fila de resposta padrão previamente definida.

A fila informada no campo *ReplyToQ* do *header* do MQ será usada apenas para as mensagens geradas automaticamente pelo *Queue Manager* (*reports* COA e COD). O gerenciador de filas informado no campo *ReplyToQMgr* deve ser informado no formato **QM.ISPBRemoto.seq[.X]**.

Não será permitida a gravação de mensagens nas filas de uma instituição definidas no BCB por outra entidade que não seja a própria, exceto na situação de contingência operada pelo BCB e autorizada pela instituição.

Serão aceitas para processamento apenas as mensagens contidas na(s) fila(s) da respectiva instituição que as gerou. Ou seja, o BCB processará apenas as mensagens cujo conteúdo seja da própria instituição que as emitiu, exceto na situação de contingência operada pelo BCB e autorizada pela instituição.

Não será utilizada a segmentação de mensagens no âmbito do MQ. A segmentação de mensagens, quando houver, ocorrerá da forma disposta no Catálogo de Serviços do SFN, no âmbito do *parser* XML.

Os ambientes de homologação e de produção deverão utilizar *queue managers* distintos, tanto nos domínios de sistema SPB quando nos domínios de sistema MES.

Todas as mensagens e os arquivos trafegarão na RSFN obrigatoriamente nas codificações previstas no Catálogo de Serviços do SFN. Caso necessário, a instituição deverá providenciar a conversão de código ao receber e enviar mensagens. Não poderá ser usada a conversão automática de código provida pelo *queue manager* porque a mensagem é cifrada. Logo, é necessário que ocorra o processo de decifragem antes da conversão de código.

O tamanho máximo de uma mensagem será 4 *MBytes*, incluindo o *header* do MQ, o *header* de segurança e a codificação do texto XML.

De acordo com o Artigo 27 do regulamento do STR, instituído pela Circular 3.488 de 18.03.2010, o COA (*Confirm on Arrival*) emitido pelo BCB é o protocolo de recebimento da mensagem.

Dessa forma, os campos importantes da mensagem COA (e COD, opcionalmente), emitida pelo BCB, que devem ser guardados pelos participantes para fins de comprovação de emissão são:

- MsgId (MQBYTE24);
- AccountingToken (MQBYTE32);
- ApplIdentityData (MQCHAR32);
- PutDate (MQCHAR8);
- PutTime (MQCHAR8).

Padrão de nomes para objetos MQ que será usado no ambiente do BCB, dos prestadores de serviços e das demais instituições participantes do SPB01, SPB02, MES01, MES02 e MES03:

Filas locais (na IF):

BC/Prestador **requisita** à IF	**QL.REQ.ISPBRemoto.ISPBLocal.seq[.X]**
BC/ Prestador **responde** à IF	**QL.RSP.ISPBRemoto.ISPBLocal.seq[.X]**
BC/ Prestador **reporta** à IF	**QL.REP.ISPBRemoto.ISPBLocal.seq[.X]**
BC/ Prestador envia mensagens de **suporte** à IF	**QL.SUP.ISPBRemoto.ISPBLocal.seq[.X]**

Tabela 8 - Filas locais (na IF)

Filas remotas (na IF):

IF **requisita** ao BC/ Prestador	**QR.REQ.ISPBLocal.ISPBRemoto.seq[.X]**
IF **responde** ao BC/ Prestador	**QR.RSP.ISPBLocal.ISPBRemoto.seq[.X]**

IF **reporta** ao BC/ Prestador	**QR.REP.ISPBLocal.ISPBRemoto.seq[.X]**
IF envia mensagens de **suporte** ao BC/ Prestador	**QR.SUP.ISPBLocal.ISPBRemoto.seq[.X]**

Tabela 9 - Filas remotas (na IF)

Filas locais (no BC/Prestador):

IF **requisita** ao BC/Prestador	**QL.REQ.ISPBRemoto.ISPBLocal.seq[.X]**
IF **responde** ao BC/Prestador	**QL.RSP.ISPBRemoto.ISPBLocal.seq[.X]**
IF **reporta** ao BC/Prestador	**QL.REP.ISPBRemoto.ISPBLocal.seq[.X]**
IF envia mensagens de **suporte** ao BC/Prestador	**QL.SUP.ISPBRemoto.ISPBLocal.seq[.X]**

Tabela 10 - Filas locais (no BC/Prestador)

Filas remotas (no BC/Prestador):

BC/Prestador **requisita** à IF	**QR.REQ.ISPBLocal.ISPBRemoto.seq[.X]**
BC/Prestador **responde** à IF	**QR.RSP.ISPBLocal.ISPBRemoto.seq[.X]**
BC/Prestador **reporta** à IF	**QR.REP.ISPBLocal.ISPBRemoto.seq[.X]**
BC/Prestador envia mensagens de **suporte** à IF	**QR.SUP.ISPBLocal.ISPBRemoto.seq[.X]**

Tabela 11 - Filas remotas (no BC/Prestador):

Filas de Transmissão: QM.ISPBRemoto.seq[.X]

Queue Manager Alias Name: QM.ISPBLocal.seq[.X]

- seq será igual a 01 para o domínio SPB01;
- seq será igual a 02 para o domínio MES01;
- seq será igual a 03 para o domínio MES02;
- seq será igual a 04 para o domínio MES03;
- seq será igual a 05 para o domínio SPB02; e
- .X é opcional, e X pode assumir valores entre A e Z, maiúsculos. Sua utilização, em cada domínio, dependerá de acordo prévio entre as partes.

Exemplos: no domínio MES01, a fila de requisição da instituição 99999999 no BCB poderá ser a QL.REQ.99999999.00038166.02 e o *queue manager* da instituição 99999999 poderá ser QM. 99999999.02. No domínio SPB02, a fila de requisição da instituição 99999999 na câmara 99999998, após acordo, poderá ser a QL.REQ.99999999.99999998.05 e o *queue manager* QM.99999999.05.A.

Canal sender: CISPBLocal.ISPBRemotoXn

Canal receiver: CISPBRemoto.ISPBLocalXn

- n será igual a 1 para o domínio SPB01;
- n será igual a 2 para o domínio MES01;
- n será igual a 3 para o domínio MES02;
- n será igual a 4 para o domínio MES03;
- n será igual a 5 para o domínio SPB02; e

- X pode assumir o valor "." (ponto) ou valores entre A e Z, maiúsculos. A utilização de valores diferentes de ".", em cada domínio, dependerá de acordo prévio entre as partes.

Exemplo: no domínio MES01, no *queue manager* da IF, o canal receptor (*receiver*) poderá ser C000038166. 99999999.2 (tráfego do BCB à IF 99999999) e o canal emissor (*sender*), C99999999.00038166.2 (tráfego da IF ao BCB). No domínio SPB02, o canal receptor poderá ser a C99999998.99999999A5 e o emissor C99999999.99999998A5.

7.2.1 Padrão mandatório de endereços de *hostnames*

Domínio SPB01:

- Ambiente Produção: mqs01.sub-domínio.rsfn.net.br
- Ambiente Homologação: mqs02.sub-domínio.rsfn.net.br
- Ambiente PPRO: mqs02.sub-domínio.rsfn.net.br

Domínio SPB02 *single-instance*:

- Ambiente Produção: mqs01.sub-domínio.rsfn.net.br
- Ambiente Homologação: mqs02.sub-domínio.rsfn.net.br
- Alternativamente, quando for necessário utilizar servidores distintos do SPB01, por motivo de segregação de tráfego, por exemplo, poderão ser adotados os nomes mqs03.sub-domínio.rsfn.net.br e mqs04.sub-domínio.rsfn.net.br, respectivamente, para produção e homologação.

Domínio SPB02 *multi-instance*:

- Ambiente Produção 1º servidor: mqs01a.sub-domínio.rsfn.net.br
- Ambiente Produção 2º servidor: mqs01b.sub-domínio.rsfn.net.br
- Ambiente Homologação 1º servidor: mqs02a.sub-domínio.rsfn.net.br
- Ambiente Homologação 2º servidor: mqs02b.sub-domínio.rsfn.net.br
- Alternativamente, quando for necessário utilizar servidores distintos do SPB01, por motivo de segregação de tráfego, por exemplo, poderão ser adotados os nomes mqs03a.sub-domínio.rsfn.net.br e mqs03b.sub-domínio.rsfn.net.br para produção e mqs04a.sub-domínio.rsfn.net.br e mqs04b.sub-domínio.rsfn.net.br para homologação.

Domínios MES (MES01, MES02 e MES03):

- Ambiente Produção: mqm01.sub-domínio.rsfn.net.br
- Ambiente Homologação: mqm02.sub-domínio.rsfn.net.br

Exemplos: O endereço MQ do BCB para o ambiente de produção dos domínios MES é o mqm01.bcb.rsfn.net.br, e o endereço de homologação é o mqm02.bcb.rsfn.net.br.

No domínio SPB01, o BCB utilizará a porta 1414 para o ambiente de produção. As instituições utilizarão apenas as portas 1414 a 1421. O BCB utilizará a porta 1514 para o ambiente de homologação e, as instituições, as portas 1514 a 1521. Para o ambiente PPRO, quando ativo, o BCB utilizará a porta 24430 e as instituições utilizarão as portas 24430 a 24437. O ambiente PPRO somente poderá ser configurado no domínio SPB01.

O BCB não oferecerá, aos participantes da RSFN, conexão para o domínio SPB02.

No domínio MES01, o BCB utilizará a porta 12422 para o ambiente de produção. As instituições utilizarão apenas as portas 12422 a 12429. O BCB utilizará a porta 12522 para o ambiente de homologação e, para as instituições as portas 12522 a 12529.

No domínio MES02, o BCB utilizará a porta 13422 para o ambiente de produção. As instituições utilizarão apenas as portas 13422 a 13429. O BCB utilizará a porta 13522 para o ambiente de homologação e, para as instituições as portas 13522 a 13529.

No domínio MES03, o BCB utilizará a porta 14422 para o ambiente de produção. As instituições utilizarão apenas as portas 14422 a 14429. O BCB utilizará a porta 14522 para o ambiente de homologação e, para as instituições as portas 14522 a 14529.

Domínio	Ambiente	Porta
SPB01	**Produção BCB**	**1414**
	Produção Instituição	1414 a 1421
	Homologação BCB	**1514**
	Homologação Instituição	1514 a 1521
	PPro BCB	**24430**
	PPro Instituição	24430 a 24437
SPB02	**Produção BCB**	**Não disponível**
	Produção Instituição	15422 a 15429
	Homologação BCB	**Não disponível**
	Homologação Instituição	15522 a 15529
MES01	**Produção BCB**	**12422**
	Produção Instituição	12422 a 12429
	Homologação BCB	**12522**
	Homologação Instituição	12522 a 12529
MES02	**Produção BCB**	**13422**
	Produção Instituição	13422 a 13429
	Homologação BCB	**13522**
	Homologação Instituição	13522 a 13529
MES03	**Produção BCB**	**14422**
	Produção Instituição	14422 a 14429
	Homologação BCB	**14522**
	Homologação Instituição	14522 a 14529

Tabela 12 - Domínios, ambientes e portas

Observações:

- **ISPBRemoto** é o ISPB ou o CNPJ base da instituição a qual pertence o *queue manager* remoto, com 8 dígitos;
- **ISPBLocal** é o ISPB ou o CNPJ base da instituição à qual pertence o *queue manager* local, com 8 dígitos;
- **sub-domínio** é a identificação DNS da instituição na RSFN;
- definir todos os objetos MQ usando letras MAIÚSCULAS;
- as filas de suporte são específicas para uso das equipes de suporte ao *queue manager* dos participantes do sistema;
- a diferenciação dos domínios MES baseia-se na porta TCP de conexão do MQ, além do endereço na RSFN;
- os canais emissores e receptores do BCB não necessariamente ficarão conectados todo o tempo, ocorrendo *timeout* e retorno do canal ao *status* de inatividade em caso de tráfego inexistente por determinado período de tempo. Para teste da conectividade, a IF deve enviar uma mensagem GEN0001.

Para se conectar à RSFN, cada instituição deverá definir um *Queue Manager Alias Name* da seguinte forma:

DEFINE QREMOTE (‘QM.ISPBLocal.seq[.X]’);

DESCR('QUEUE MANAGER ALIAS NAME') RNAME (' ');

RQMNAME ('nome real do queue manager da instituição');

XMITQ (' ')

REPLACE

Atenção:

Para os aglomerados e conglomerados que concentram mais de uma instituição num único *queue manager*, o padrão para o nome da fila de transmissão passa a ser QM.ISPBLocal.ISPBRemoto.seq[.X]. Além disso, para esses ambientes e para os que estão conectados a eles (BC e Prestadores), há a inclusão do conceito de *ReplyToQ alias* para permitir o retorno dos *reports* solicitados. O uso do *ReplyToQ alias* permite que as aplicações não precisem colocar o nome do *queue manager* no campo *ReplyToQMgr* do *header* do MQ e retira da aplicação a "decisão" sobre qual *ReplyToQmgr* apontar no MQMD para receber a resposta. Para isso, a aplicação informa o *alias* no *ReplyToQ* e deixa o *ReplyToQmgr* em branco, e deve ser definido o seguinte objeto no MQ para cada instituição à qual se está conectado:

DEFINE QREMOTE ('nome da reply-to-queue alias à escolha da instituição')

DESCR('REPLYTOQUEUE ALIAS NAME')

RNAME (' nome da fila local de report ou QL.REP.ISPBRemoto.ISPBLocal.seq[.X]')

RQMNAME ('QM.ISPBRemoto.seq[.X] ou QM.ISPBRemoto.ISPBLocal.seq[.X]')

XMITQ (' ')

REPLACE

A decisão do nome do RQMNAME é baseada no nome da fila de transmissão do *queue manager* remoto para o *queue manager* local. Ou seja, no ambiente do conglomerado ou aglomerado o RQMNAME é sempre **QM.ISPBRemoto.seq[.X]** e, nos ambientes aos quais o conglomerado ou aglomerado está conectado, é **QM.ISPBRemoto.ISPBLocal.seq[.X]**.

7.2.2 *HEADER* DO MQ (MQMD)

Alguns campos do *header* das mensagens que trafegam no MQ (MQMD) deverão ser formatados de acordo com o definido a seguir:

Report: ativar requisição dos *reports* do tipo COA (*Confirm on Arrival*), COD (*Confirm on Delivery*) e *Report Exception;*

MsgType: usar opção *request* para uma requisição, *reply* para resposta a uma requisição e *report* para um *report;*

Encoding: usar valor nativo da máquina onde está o MQ (opção *native* do MQ);

Persistence: usar opção *Persistence*;

Format: usar opção *NONE*;

CodedCharSetId: usar um dos listados abaixo: 37, 256, 273-275, 277-278, 280, 282, 284-285, 290, 297, 367, 420, 423-424, 437, 500, 813, 819, 833, 836, 838, 850-852, 855-858, 860-866, 869-871, 874-875, 880, 891, 895, 897, 903-905, 912, 915-916, 920, 923-924, 1004, 1009-1021, 1023, 1025-1027, 1040-1043, 1046-1047, 1051, 1088-1089, 1097, 1100-1107, 1114-1115, 1126, 1140, 1148, 1250-1256, 1275, 5348

ReplyToQ: informar o nome da fila, ou o *ReplyToQ alias* definido no ambiente da instituição, que receberá as mensagens geradas automaticamente pelo *Queue Manager*, tais como COA, COD, *Report Exceptions*.

ReplyToQMgr: informar o *queue manager alias name*, de acordo com o definido anteriormente (QM.**ISPBLocal**.seq[.X]) ou deixar em branco no caso de usar *ReplyToQ alias*.

7.2.3 Atributos para objetos do MQ

Atributos Comuns a Todas as Filas		
ATRIBUTO	***DEFAULT***	***CONSENSO***
ClusterName		na
ClusterNamelist		na
DefBind		na
DefPersistence	NO	YES
DefPriority	0	default
InhibitGet	ENABLED	default
InhibitPut	ENABLED	default
Qdesc		livre
QName		
QType		
Scope	QMGR	livre

Tabela 13 - Atributos Comuns a Todas as Filas

Atributos de Filas Locais		
ATRIBUTO	***DEFAULT***	
Archive		livre
BackoutRequeueQName		livre
BackoutThreshold		livre
CreationDate		livre
CreationTime		livre
CurrentQDepth		livre
DefinitionType	TEMPDYN	livre
DefInputOpenOption		livre
DistLists	NO	livre
HardenGetBackout	NO	HARDENED
IndexType	NONE	livre
InitiationQName		na
MaxMsgLength	4M	4M
MaxQDepth	5000	máximo
MsgDeliverySequence	PRIORITY	FIFO
OpenInputCount		livre
OpenOutputCount		livre
ProcessName		livre
QDepthHighEvent	DISABLED	livre
QDepthHighLimit	80 (%)	livre
QDepthLowEvent	DISABLED	livre
QDepthLowLimit	40(%)	livre
QDepthMaxEvent	ENABLED	livre

QServiceInterval	999999999	livre
QServiceIntervalEvent	NONE	livre
RetentionInterval	999999999	livre
Shareability		livre
StorageClass	DEFAULT'	livre
TriggerControl		livre
TriggerData		Livre
TriggerDepth	1	Livre
TriggerMsgPriority	0	Livre
TriggerType	FIRST	Livre
Usage	NORMAL	Livre

Tabela 14 - Atributos de Filas Locais

Atributos de Filas Remotas		
ATRIBUTO	**DEFAULT**	
RemoteQMgrName		
RemoteQName		
XmitQName		

Tabela 15 - Atributos de Filas Remotas

Atributos de Alias Queues		
ATRIBUTO	***DEFAULT***	
BaseQName		

Tabela 16 - Atributos de Alias Queues

Atributos de NameLists		
ATRIBUTO	***DEFAULT***	
AlterationDate		livre
AlterationTime		livre
NameCount		livre
NamelistDesc		livre
NamelistName		livre
Names		livre

Tabela 17 - Atributos de NameLists

Atributos de Processos		
ATRIBUTO	***DEFAULT***	
AlterationDate		livre
AlterationTime		livre
ApplId		livre
ApplType		livre
EnvData		livre
ProcessDesc		livre
ProcessName		livre
UserData		livre

Tabela 18 - Atributos de Processos

Atributos de Queue Managers		
ATRIBUTO	***DEFAULT***	
AuthorityEvent	DISABLED	livre
ChannelAutoDef	DISABLED	livre
ChannelAutoDefEvent	DISABLED	livre
ChannelAutoDefExit		livre
ClusterWorkloadData		na
ClusterWorkloadExit		na
ClusterWorkloadLength		na
CodedCharSetId		livre
CommandInputQName		livre
CommandLevel		na
DeadLetterQName		livre
DefXmitQName		livre
DistLists		livre
InhibitEvent	DISABLED	livre
LocalEvent	DISABLED	livre
MaxHandles	256	livre
MaxMsgLength	4 Mb	4Mb
MaxPriority	9	livre
MaxUncommittedMsgs	10000	livre
PerformanceEvent	DISABLED	livre
Platform		livre
QmgrDesc		livre
QmgrIdentifier		livre
QmgrName		padrão
RemoteEvent	DISABLED	livre
RepositoryName		livre
RepositoryNamelist	livre	
StartStopEvent	ENABLED	livre
SyncPoint	AVAILABLE	livre
TriggerInterval	999999999	livre

Tabela 19 - Atributos de Queue Managers

Atributos de Canais		
ATRIBUTO	***DEFAULT***	
Auto start (AUTOSTART)	DISABLED	NA
Batch interval (BATCHINT)	0	default
Batch size (BATCHSZ)	50*	default
Channel name (CHANNEL)		padrão
Channel type (CHLTYPE)		padrão
CICS profile name		livre
Cluster (CLUSTER)		

Cluster namelist (CLUSNL)		
Connection name (CONNAME)		DNS(PORTA)
Convert message (CONVERT)	NO	NO
Description (DESCR)		padrão
Disconnect interval (DISCINT)	6000	O
Heartbeat interval (HBINT)	300	default
Long retry count (LONGRTY)	999999999	livre
Long retry interval (LONGTMR)	1200	livre
LU 6.2 mode name (MODENAME)		na
LU 6.2 transaction program name (TPNAME)		na
Maximum message length (MAXMSGL)	4Mb	4Mb
Maximum transmission size		na
Message channel agent name (MCANAME)		na
Message channel agent type (MCATYPE)	PROCESS	livre
Message channel agent user ident(MCAUSER)		livre
Message exit name (MSGEXIT)		livre
Message exit user data (MSGDATA)		livre
Message-retry exit name (MREXIT)		livre
Message-retry exit user data (MRDATA)		livre
Message retry count (MRRTY)	10	livre
Message retry interval (MRTMR)	1000	livre
Nonpersistent message speed (NPMSPEED)	FAST	na
Network-connection priority (NETPRTY)		na
Password (PASSWORD)		na
PUT authority (PUTAUT)	DEFAULT	
Queue manager name (QMNAME)		padrão
Receive exit name (RCVEXIT)		livre
Receive exit user data (RCVDATA)		livre
Security exit name (SCYEXIT)		Livre
Security exit user data (SCYDATA)		Livre
Send exit name (SENDEXIT)		Livre
Send exit user data (SENDDATA)		Livre
Sequence number wrap (SEQWRAP)	999.999.999	99.999.999
Sequential delivery		Livre
Short retry count (SHORTRTY)	10	Default
Short retry interval (SHORTTMR)	60	default
Target system identifier		livre
Transmission queue name (XMITQ)		padrão
Transport type (TRPTYPE)		TCP

Tabela 20 - Atributos de Canais

* O valor do parâmetro *Batch size* (BATCHSZ) poderá ser definido entre 25 e 100, mediante acordo entre as partes.

7.3 Configuração do Servidor MQ - Opção ADOPTNEWMCA

Foi detectada uma limitação na configuração do MQ que, na ocorrência de falhas de comunicação, pode levar, eventualmente, a uma perda de conectividade entre servidores MQ, que só pode ser solucionada mediante comando STOP FORCE da conexão ou reinicialização do gerenciador de canais.

Para evitar tal falha, o suporte do fabricante do produto (IBM) recomendou a configuração de alguns parâmetros no MQ, com a utilização de atributos, que, por "default", não estão ativados.

Desta forma, considerando-se que tal alteração acarretará melhora na disponibilidade do serviço, deverá ser ativada, **obrigatoriamente**, a opção **ADOPTNEWMCA**.

Seguem, abaixo, exemplos com os parâmetros a serem alterados no *software*, para os sistemas operacionais mais utilizados.

Esclarecemos que eventuais dúvidas acerca dos procedimentos envolvidos na alteração deverão ser sanadas diretamente junto ao suporte do fabricante do produto.

Ativação da opção ADOPTNEWMCA do MQ no ambiente Windows:

1. No servidor MQ, abrir MQ Services;
2. Clicar com o botão direito do mouse sobre o Qmgr a ser modificado;
3. Selecionar Properties;
4. Selecionar a pasta Channels;
5. Marcar a opção ALL do parâmetro AdoptNewMCA;
6. Marcar a opção ALL do parâmetro AdoptNewMCACheck;
7. Manter o tempo default dessa opção (60 segundos).

Ativação da opção ADOPTNEWMCA do MQ no ambiente Unix:

Incluir as linhas abaixo no arquivo de configuração do *queue manager* (qm.ini):

CHANNELS:

AdoptNewMCACheck=ALL

AdoptNewMCATimeout=60

AdoptNewMCA=ALL

Ativação da opção ADOPTNEWMCA do MQ no ambiente z/OS:

Incluir os parâmetros abaixo na macro CSQ6CHIP do módulo de parâmetros do channel-initiator:

ADOPTCHK=ALL

ADOPTMCA=YES

Observação: se o MQ for OS/390 V2R1, esses parâmetros são adicionados via PTF que deve ser solicitada ao fabricante.

7.4 Configuração do MQ - BCB

Para que o BCB saiba referenciar corretamente os objetos MQ, o hostname e porta utilizados pela IF na RSFN, é necessário por parte da IF o preenchimento de cadastro conforme procedimento descrito a seguir.

Procedimento relativo à configuração do MQ no BCB:

1. Solicitar ao master Sisbacen de sua instituição a autorização para a transação associada ao domínio, a saber:

- Domínio MES01: SMES400
- Domínio MES02: SMES402
- Domínio MES03: SMES403
- Domínio SPB01: SMES401

2. Acessar o *site*: https://www9.bcb.gov.br/mensageria/mqconfig (Homologação) ou https://www3.bcb.gov.br/mensageria/mqconfig (Produção)
3. Escolher o domínio;
4. Definir os objetos MQ equivalentes na sua instituição, de acordo com os padrões estabelecidos neste manual;
5. Clicar em “Salvar informações”;
6. Observações:
7. No caso do domínio SPB01, é dada a possibilidade de criação de objetos perante o SELIC.

8 QUALIDADE DE SERVIÇO NA RSFN

A funcionalidade Qualidade de Serviço (QoS) na RSFN atribui parâmetros e largura de banda para diferenciar os serviços e garantir a performance da rede. Seis classes de serviço foram definidas, cuja regra geral de priorização e reserva de banda é dada na Tabela 21.

Nome	Marcação	Prioridade	Banda reservada participantes		Banda reservada BCB
			512 Kbps ou menos	1 Mbps ou mais	
Platina	AF41	Mais prioritário	14%	15%	60%
Ouro	AF31	Prioritário	19%	25%	N.A.*
Prata	AF21	Intermediário	13%	7%	7%
Bronze	AF11 e AF12	Menos Prioritário	25%	30%	10%
Infraestrutura	Padrão da operadora	Padrão da operadora	13%	7%	7%
Default	BE	Sem prioridade	13%	13%	13%

N.A. – não aplicável, pois o BCB utilizará enlaces dedicados para o PIX.

Tabela 21 - Configuração das marcações de Qualidade de Serviço na RSFN

O BCB, as câmaras e os prestadores de serviços de compensação e de liquidação poderão aplicar as regras de QoS da Tabela 22 para o conjunto de quatro circuitos que, distribuídos igualmente entre sites distintos, forem utilizados exclusivamente para o tráfego de somente uma das classes de negócio (Platina, Ouro, Prata ou Bronze) e os respectivos tráfegos de homologação e de transferência de arquivos.

Os dois provedores de telecomunicações da RSFN realizarão a marcação dos pacotes de acordo os critérios a seguir:

Nome	Marcação	Prioridade	Banda reservada	
			512 Kbps ou menos	1 Mbps ou mais
Bronze, Prata, Ouro ou Platina	AF11 e AF12, AF21, AF31 ou AF41	Prioritário	71%	77%
Infraestrutura	Padrão da operadora	Padrão da operadora	13%	7%
Default	BE	Sem prioridade	13%	13%

Tabela 22 - Configuração das marcações de Qualidade de Serviço na RSFN para circuitos dedicados

As marcações de pacotes deverão ser feitas de acordo com as recomendações do fabricante dos equipamentos utilizados pela rede, observando a Tabela 23.

A atribuição de classes de serviço usando portas e listas de acesso na configuração de QoS não foi implantada no InterAs em função de limitações técnicas da rede existentes na época da implantação do QoS e por conta da baixa utilização desses links.

Classe de Serviço	Porta(s) (*in/out*)	Aplicação/Domínio
PLATINA	**1414 a 1421 TCP**	**Mensageria de Produção – SPB01**
OURO	**16422 a 16429 TCP**	**Canal Primário de Mensagens do PIX - Produção**
PRATA	**14422 a 14429 TCP**	**Mensageria de Produção - MES03**
BRONZE	**12422 a 12429 TCP** **15422 a 15429 TCP**	**Mensageria de Produção - MES01 e SPB02**
INFRAESTRUTURA	**Serviços de infraestrutura**	**Monitoração e serviços de infraestrutura**
DEFAULT	**20 e 21 TCP** **1110 a 1121 TCP**	**FTP** **FTP – Passive Mode**
	1130 a 1141 TCP	**Transferência de arquivos do PIX**
	1514 a 1521 TCP	**Mensageria de Homologação - SPB01**
	12522 a 12529 TCP	**Mensageria de Homologação – MES01**
	13422 a 13429 TCP **13522 a 13529 TCP**	**Mensageria de Produção e Homologação – MES02**
	14522 a 14529 TCP	**Mensageria de Homologação – MES03**
	15522 a 15529 TCP	**Mensageria de Homologação - SPB02**
	16522 a 16529	**Canal Primário de Mensagens do PIX - Homologação**
	17422 a 17429	**Canal Secundário de Mensagens do PIX - Produção**
	17522 a 17529	**Canal Secundário de Mensagens do PIX - Homologação**
	Demais portas e aplicações da RSFN	

Tabela 23 - Configuração de Qualidade de Serviço na RSFN

9 GLOSSÁRIO

IOSMF - Instituição operadora de sistema do mercado financeiro, conforme definição dada pela Resolução BCB n° 304, de 20/3/2023.

Prestador de serviços – definido pelo Catálogo de Serviços do SFN, seção conceitos básicos.