

**RSFN**

**Rede do Sistema**  
**Financeiro Nacional**

***Manual de Redes do SFN***

Maio/2015

Versão 7.6.3

## ÍNDICE

<b>ÍNDICE .....</b>	<b>2</b>
<b>CONTROLE DE VERSÃO .....</b>	<b>5</b>
<b>VISÃO GERAL .....</b>	<b>6</b>
<b>ARQUITETURA DE REDE DE COMUNICAÇÃO PARA O SISTEMA FINANCEIRO .....</b>	<b>6</b>
Apresentação .....	6
RSFN - Rede do Sistema Financeiro Nacional .....	6
Sobre a Arquitetura .....	6
Atribuições e Responsabilidades do Subgrupo de Redes .....	7
Normas de utilização da RSFN .....	7
Recomendações .....	7
<b>CENTRAL DE ATENDIMENTO .....</b>	<b>8</b>
<b>PROCEDIMENTOS PARA ACESSO À RSFN .....</b>	<b>9</b>
Solicitação de conexão .....	9
Para solicitação das conexões as Entidades Solicitantes deverão: .....	9
Questionário: .....	10
Pré-requisito: .....	10
Política de encaminhamento do tráfego de entrada e saída de dados: .....	10
Testes de conectividade .....	11
Testes de contingência .....	12
<b>DESCRIÇÃO TÉCNICA .....</b>	<b>21</b>
Arquitetura de endereçamento IP .....	21
<b>ROTEAMENTO DA RSFN .....</b>	<b>26</b>
Roteamento para o Perfil A e B (Modelo 2) .....	26
Roteamento para o Perfil C (Modelo 1) .....	27
Roteamento para o Perfil D com roteadores da Entidade no barramento RSFN e NAT do 2º prefixo /28 (Modelo 6) .....	29
Roteamento para o Perfil D com <i>firewall</i> da Entidade no barramento RSFN (Modelo 4) .....	30
Roteamento para o Perfil D com <i>firewall</i> da Entidade no barramento RSFN (Modelo 5) .....	31
OBSERVAÇÃO IMPORTANTE RELATIVA AOS MODELOS 4 E 5 .....	31
<b>MODELOS DE TOPOLOGIA PARA CONEXÕES COM REDES INTERNAS .....</b>	<b>32</b>
<b>SERVIDOR DE TEMPO (TIME SERVER) .....</b>	<b>40</b>
<b>SERVIDOR WEB DA RSFN .....</b>	<b>40</b>
<b>SERVIDOR FTP .....</b>	<b>41</b>
<b>INFRA-ESTRUTURA DE MENSAGERIA .....</b>	<b>41</b>
Diretrizes básicas .....	41
Definições do MQseries .....	42
<b>CONFIGURAÇÃO DO SERVIDOR MQ - OPÇÃO ADOPTNEWMCA .....</b>	<b>51</b>
<b>CONFIGURAÇÃO DO MQ - BANCO CENTRAL .....</b>	<b>52</b>
<b>GERÊNCIA DE SEGUNDA NÍVEL DA RSFN .....</b>	<b>53</b>
Diretrizes básicas .....	53
<b>REQUISITOS PARA O MODELO OPERACIONAL DE PSTI .....</b>	<b>54</b>
Obrigações das Instituições Financeiras quando operam no modelo de PSTI: .....	54
Obrigações dos PSTIs: .....	54
Utilização de rede dedicada homologada pelo BACEN: .....	54
Gerência Integrada de Segundo Nível: .....	55
Infra-RSFN: .....	55
<b>QUALIDADE DE SERVIÇO NA RSFN .....</b>	<b>56</b>
Configuração atual de Qualidade de Serviço na RSFN .....	56
Nova configuração de Qualidade de Serviço na RSFN .....	57

<b>ANEXO I – CONFIGURAÇÃO DE DNS (DOMAIN NAME SYSTEM) .....</b>	<b>59</b>
INTRODUÇÃO .....	59
PREMISSAS BÁSICAS .....	60
DNS NA RSFN .....	61
Aplicações de DNS recomendadas .....	62
DNS em Servidores Unix .....	62
DNS em Servidores Windows .....	62
ARQUITETURA DE DNS DA RSFN .....	63
Sub-Domínios da RSFN .....	64
Delegando Direitos Para os Sub-Domínios .....	64
Incluindo ou Excluindo Domínios ou Sub-Domínios .....	65
Domínios Reversos da RSFN .....	65
Sub-Domínios Reversos da RSFN .....	67
Delegando Direitos Para os Sub-Domínios Reversos .....	67
Incluindo ou Excluindo Domínios ou Sub-Domínios Reversos .....	69
Sub-Domínios Reversos da RSFN .....	70
Servidores de DNS da RSFN .....	71
Servidor Primário dos Domínios Superiores – IRS (“ <i>Internal Root Server</i> ”) .....	71
Servidores Primários dos Sub-Domínios .....	72
Servidores Secundários dos Sub-Domínios .....	74
Registro dos Domínios Superiores nas Entidades Competentes .....	75
Registro dos Sub-Domínios das Entidades .....	76
Árvore de DNS da Parte Externa .....	76
Restrições sobre a Configuração do PNS e SNS dos Sub-Domínios .....	82
CONFIGURAÇÃO DOS <i>RESOLVERS</i> .....	82
PADRONIZAÇÃO DE NOMES DE <i>HOSTS</i> E INTERFACES .....	82
Padronização de Nomes de Usuários .....	83
IMPACTO DO TRÁFEGO DO DNS NA REDE .....	83
Localização dos Servidores .....	83
Parâmetros de Temporização do Registro SOA .....	84
Configuração dos <i>Resolvers</i> .....	84
<b>FERRAMENTAS DE DEPURAÇÃO DO DNS – <i>NSLOOKUP</i> .....</b>	<b>86</b>
INTRODUÇÃO .....	86
<b>DNS EM SERVIDORES DA MICROSOFT .....</b>	<b>88</b>
INTRODUÇÃO .....	88
CONFIGURAÇÃO DO DNS SERVER EM AMBIENTE WINDOWS 2000 .....	88
Criando um Domínio Reverso Primário .....	92
Criando um Domínio Direto Secundário .....	94
Criando um Domínio Reverso Secundário .....	95
Criando um Registro do Tipo A .....	95
Criando um Registro do Tipo PTR .....	96
Configurando os Servidores <i>Forwarders</i> .....	98
SERVIÇO DNS EM AMBIENTE WINDOWS NT 4.0 .....	99
Criando um Domínio Direto Primário .....	100
Criando um Domínio Reverso Primário .....	101
Criando um Domínio Reverso Secundário .....	102
Criando um Domínio Direto Secundário .....	104
Criando um Registro do Tipo A .....	104
Criando um Registro do Tipo PTR .....	105
Configurando os Servidores <i>Forwarders</i> .....	107

<i>Figura 1 – Modelo de conexão da rede RSFN</i>	12
<i>Figura 2 - Dois sites com interconexão pela rede interna</i>	14
<i>Figura 3 - Dois sites, porém com apenas dois CPE</i>	16
<i>Figura 4 - Conexão do Perfil D com roteamento iBGP</i>	17
<i>Figura 5 - Conexão direta do Perfil D com a célula de segurança</i>	19
<i>Figura 6 – Comunicação entre as entidades participantes da RSFN</i>	21
<i>Figura 7 - Perfis de conexão com a RSFN</i>	22
<i>Figura 8 - Serviço PSTI</i>	23
<i>Tabela 1 - Faixa de Endereços dos hosts TCP/IP com máscara /27</i>	24
<i>Tabela 2- Faixa de Endereços dos hosts TCP/IP com máscara /26</i>	24
<i>Tabela 3 - Faixa de Endereços dos hosts TCP/IP das IF com máscara /28</i>	25
<i>Tabela 4 - Faixa de Endereços dos hosts TCP/IP das IFs com máscara /27</i>	25
<i>Figura 9 - Topologia com dois sites, porém com apenas dois CPE</i>	26
<i>Figura 10 - Topologia com dois sites com interconexão pela rede interna</i>	27
<i>Figura 11 - Conexão do Perfil D com roteamento iBGP</i>	28
<i>Figura 12 -Topologia com dois sites, quatro roteadores da Entidade e NAT interno</i>	29
<i>Figura 13 - Conexão direta do Perfil D com a célula de segurança</i>	30
<i>Figura 14 - Topologia com dois domínios de broadcast</i>	31
<i>Figura 15 - Topologia de Acesso com Firewall</i>	32
<i>Figura 16 - Topologia de Acesso com Roteadores, Firewall e DMZ</i>	34
<i>Figura 17 - Topologia Redundante com Site de Contingência</i>	36
<i>Figura 18 - Topologia de Redundância Máxima Sem Site de Contingência</i>	38
<i>Figura 19 - Topologia de Redundância Máxima Com Site de Contingência</i>	39
<i>Tabela 5 – Domínios, ambientes e portas</i>	45
<i>Tabela 6 - Atributos Comuns a Todas as Filas</i>	47
<i>Tabela 7 - Atributos de Filas Locais</i>	48
<i>Tabela 8 - Atributos de Filas Remotas</i>	48
<i>Tabela 9 - Atributos de Alias Queues</i>	48
<i>Tabela 10 - Atributos de NameLists</i>	48
<i>Tabela 11 - Atributos de Processos</i>	49
<i>Tabela 12 - Atributos de Queue Managers</i>	49
<i>Tabela 13 - Atributos de Canais</i>	50
<i>Tabela 14 – Atual configuração de Qualidade de Serviço na RSFN</i>	57
<i>Tabela 15 – Nova configuração de Qualidade de Serviço na RSFN</i>	58

**CONTROLE DE VERSÃO**

Versão	Descrição das Modificações	Data da Modificação
7.6.3	- <b>Alteração Visão Geral – Normas de utilização da RSFN (p.7)</b>	<b>5 de Maio de 2015</b>
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 provedores 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 N° 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 MES	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 Banco Central no item “Diretrizes Básicas” da “Infraestrutura de Mensageria”.	02 de janeiro de 2004
4.0	- Adequação à Circular BACEN 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

## VISÃO GERAL

### ARQUITETURA DE REDE DE COMUNICAÇÃO PARA O SISTEMA FINANCEIRO

#### Apresentação

A *Arquitetura de Rede de Comunicação de Dados* entre o Banco Central do Brasil, as Instituições Financeiras e as Câmaras, foi projetada para suportar a implantação do novo Sistema de Pagamentos Brasileiro (SPB) e que deve estar preparada para agregar também outros serviços de comunicação entre instituições do sistema financeiro.

Para atingir os objetivos acima, o Subgrupo de Redes avaliou as diversas alternativas técnicas e soluções dos fornecedores e concessionárias, resultando na **RSFN**.

Este manual foi elaborado para a correta utilização desta rede, contendo informações técnicas e operacionais para as Instituições Financeiras se conectarem à **RSFN**, instituído pela Circular BACEN 3.629, de 19.02.2013.

#### RSFN - Rede do Sistema Financeiro Nacional

A **RSFN**, Rede do Sistema Financeiro Nacional, que utiliza atualmente a infraestrutura de comunicação das concessionárias Primesys e Embratel / RTM (que foram as qualificadas pelo Subgrupo de Redes), tem como finalidade suportar o tráfego entre as Instituições Financeiras participantes, o Banco Central do Brasil (BACEN) e as Câmaras de Liquidação (Câmaras). Baseada no protocolo TCP/IP, a rede foi implantada considerando a utilização de ferramentas/conceitos de Intranet que suportam as aplicações desenvolvidas para atender as necessidades do **SPB**, bem como agregar outros serviços de comunicação entre seus participantes.

#### Sobre a Arquitetura

Considerando-se que as operações dos sistemas serão processadas em regime de tempo real, esta arquitetura foi especificada partindo-se da premissa de que deverá ter alta disponibilidade, desempenho, segurança e contingência.

Baseado nas premissas acima, o Subgrupo de Redes estabeleceu critérios rigorosos nas suas especificações que, além de adotar as melhores tecnologias disponíveis atualmente, exigiu das concessionárias qualificadas a garantia de que a rede terá total aderência às nossas especificações e redundância em todos os seus segmentos: no seu backbone, nos seus entroncamentos e meios físicos, nos seus equipamentos, nos nós da rede e na sua última milha.

Estabeleceu também que, futuramente, essa rede deverá agregar novos serviços como Voz sobre IP, interconexão entre as instituições financeiras etc., sem a necessidade de se alterar a sua arquitetura com novos investimentos.

### Atribuições e Responsabilidades do Subgrupo de Redes

- Especificar a arquitetura da Rede.
- Especificar a Topologia da Rede.
- Especificar a Estrutura Física da Rede.
- Especificar normas e padrões para conexão IP entre as redes das concessionárias e as instituições participantes.
- Definir a melhor tecnologia, sob os aspectos evolutivos, tendências, segurança, contingências e custo / benefício.
- Especificar os pré-requisitos para os fornecedores e concessionárias apresentarem suas soluções e propostas.
- Negociar custos e propostas dos fornecedores e concessionárias.
- Avaliar, homologar e indicar os fornecedores e concessionárias para a elaboração da nova rede.
- Acompanhar, auditar e avaliar o processo de operacionalização da rede junto às concessionárias.

### Normas de utilização da RSFN

Todos os serviços a serem implementados na rede deverão ser homologados pelo Subgrupo de Redes, que definirá os padrões de endereçamento IP para cada tipo de serviço.

As configurações de roteamento da RSFN não permitem a comunicação indiscriminada entre os participantes. A conectividade na RSFN é regulada conforme abaixo:

- a. É permitido a todos os participantes da RSFN estabelecer comunicação direta com o Banco Central, com as câmaras, com os prestadores de serviços de compensação e de liquidação e com os seus respectivos Provedores de Serviços de Tecnologia da Informação – PSTIs.
- b. É permitido ao Banco Central, às câmaras e aos prestadores de serviços de compensação e de liquidação estabelecer comunicação direta com todos os participantes da RSFN.
- c. É permitido aos PSTIs estabelecer comunicação direta com o Banco Central e com os participantes da RSFN que utilizam o seu serviço.
- d. É vedado aos participantes da RSFN estabelecer comunicação direta entre si que não esteja prevista nos casos anteriores.
- e. É vedada a comunicação entre os dois sites de um mesmo participante via RSFN.

### Recomendações

Para a implementação da conexão com a RSFN, as seguintes recomendações são pertinentes:

- a) Atentar para as recomendações sobre segurança descritas no Capítulo **Modelos de Topologia para Conexões com Redes Internas**, deste documento;
- b) Escolha e implementação adequadas do Modelo de Topologia para Conexões com a Rede Interna da Entidade Participante;
- c) **É obrigatória a utilização do serviço de DNS (*Domain Name System*) e a configuração do parâmetro TTL (*Time to Live*) igual a ZERO para hosts disponibilizados na RSFN, ressaltamos que a contingência dos servidores de MQ, componente fundamental na estrutura dos domínios SPB01, MES01, MES02 e MES03, está baseada na utilização do serviço de DNS;**
- d) Observar as normas de endereçamento e do Serviço de DNS descritas no Capítulo **Arquitetura de Endereçamento IP** e **Anexo I**, deste documento;
- e) Execução de testes de funcionalidade e contingência da rede.

## **CENTRAL DE ATENDIMENTO**

O serviço de comunicação entre as Entidades Participantes da RSFN está sendo provido pelas concessionárias: Primesys e Embratel/RTM, que receberão as solicitações de conexão com a RSFN, informações e abertura de chamados técnicos referentes a problemas de conectividade encontrados pelas Entidades Participantes, através de suas Centrais de Atendimento pelos telefones 0800-7077288 e 0800-7077400, respectivamente.

Efetuada a conexão, poderá ser acessado o **Site Web da RSFN** no BACEN, através do endereço [www.rsfn.net.br](http://www.rsfn.net.br), onde estão disponíveis outros documentos relevantes, incluindo a lista de escalonamento para problemas recorrentes ou não-resolvidos.

## **PROCEDIMENTOS PARA ACESSO À RSFN**

### Solicitação de conexão

- a) Todos os participantes da RSFN deverão contratar obrigatoriamente pelo menos uma conexão com a Primesys e outra com a Embratel/RTM;
- b) As conexões serão instaladas pelas concessionárias nos endereços onde os Participantes indicarem, na modalidade Turn Key, ou seja, acesso local (par metálico, fibra óptica ou rádio) e roteador configurado;
- c) Em todas as conexões, as concessionárias fornecerão o Roteador devidamente homologado pelo Subgrupo de Redes, com o hardware, software e configuração necessária para suportar os serviços da RSFN;
- d) Essa rede deverá respeitar as especificações estabelecidas na RFP pelo Subgrupo de Redes e é de total conhecimento das concessionárias Primesys e Embratel / RTM;
- e) A não observância das especificações citadas no item anterior pelas concessionárias ou pelo Participante poderá comprometer a conectividade e segurança deste último, podendo não participar dos testes e implantação dos seus sistemas;
- f) Os roteadores serão de uso exclusivo para a RSFN e serão instalados e configurados pelas concessionárias conforme as regras de endereçamento IP definidos pelo Subgrupo de Redes.

### Para solicitação das conexões as Entidades Solicitantes deverão:

- a) Contatar as concessionárias, através das respectivas Centrais de Atendimento, que verificarão os dados na lista fornecida pelo Banco Central e encaminharão ao responsável administrativo do Solicitante o questionário abaixo listado, juntamente com outras informações que julgarem relevantes, o qual deverá ser preenchido e devolvido, por meio eletrônico, para as concessionárias;
- b) As concessionárias receberão as informações e as encaminharão para o Banco Central, por meio eletrônico, aos cuidados de [infra.rsfn@bcb.gov.br](mailto:infra.rsfn@bcb.gov.br);
- c) O Banco Central preencherá a planilha de cadastro contendo a faixa de endereços IP designada para utilização do Solicitante, que será enviada à caixa postal do responsável técnico do Solicitante e às duas concessionárias. Também será providenciado o cadastro do nome do subdomínio informado pelo Solicitante, eventual duplicidade de nomes de subdomínio será previamente comunicada e será negociado um novo nome entre o Banco Central e o Solicitante;
- d) Com a informação recebida, as concessionárias estarão autorizadas a incluir a Entidade Solicitante na RSFN e tomar as providências necessárias para liberação dos circuitos;
- e) Solicitar das concessionárias o contrato completo para aquisição da última milha e os seus serviços.

Questionário:

- 1) Em qual das categorias abaixo se enquadra o Solicitante?
  - a. Instituição Financeira;
  - b. Provedores de Serviços de Tecnologia da Informação - PSTI;
  - c. Câmaras ou Outros.
- 2) O Solicitante tem um *site backup* ou pretende implantá-lo no prazo máximo de um ano?
- 3) Se a resposta ao item 2 for positiva, definir qual será o perfil adotado para a comunicação entre os *sites*, dentre as opções sugeridas no Capítulo **Roteamento da RSFN** deste documento.
- 4) Qual o nome do Subdomínio pretendido pelo Solicitante (se já possuir um nome de domínio na Internet, recomenda-se utilizá-lo, este domínio terá obrigatoriamente a extensão .rsfn.net.br, p. ex., se o nome do domínio na Internet é **xyz.com.br**, sugere-se utilizar para a RSFN o nome **xyz.rsfn.net.br**).
- 5) Se o Solicitante for uma Instituição Financeira, utilizará a estrutura de Provedor PSTI? Qual será este provedor?
- 6) O Solicitante implantará o serviço de DNS próprio ou utilizará o serviço fornecido pela Concessionária? Caso queira utilizar o Serviço de DNS de uma das Concessionárias, deverá informar ao Banco Central os endereços IPs dos Servidores Autoritativos para o domínio do Solicitante.

Pré-requisito:

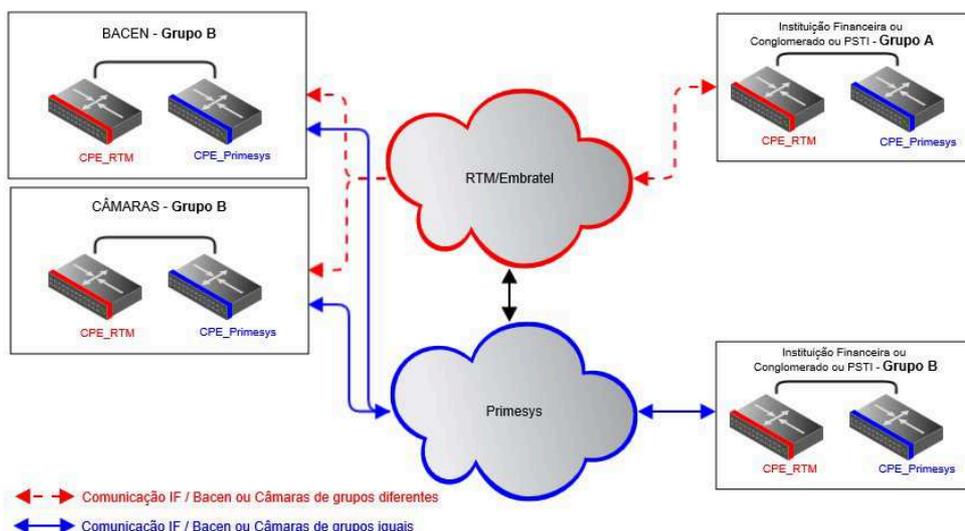
Conexão dos roteadores das duas concessionárias em barramento de rede local, conforme modelos sugeridos no Capítulo **Modelos de Topologia para Conexões com redes Internas** deste documento.

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

Segundo a definição do comitê gestor do grupo de redes da RSFN, 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 EBT/RTM e PRIMESYS) irão responder, sendo que um deles terá uma prioridade maior.

Para que uma concessionária não seja mais sobrecarregada que a outra, as Entidades serão divididas em dois grupos, em que um grupo preferencialmente terá como acesso ao backbone RSFN via o CPE Primesys e o outro terá acesso via o CPE EBT/RTM.

Na configuração proposta, a regra se resume em: o circuito Primesys terá preferência na comunicação entre entidades de mesmo grupo e o circuito EBT/RTM terá preferência na comunicação entre entidades de grupos diferentes. Desta forma, o fluxo de entrada de dados dependerá da origem e haverá balanceamento do tráfego entre as operadoras, conforme demonstra a figura abaixo:



### Testes de conectividade

A partir do recebimento da faixa de endereçamento IP da instituição, configurar uma estação com os parâmetros abaixo. Obs.: Caso a instituição opte por efetuar o teste através da sua rede local deve-se efetuar NAT.

- IP address do 10º host
- Subnetmask: fornecida na documentação
- Gateway: Endereço do HSRP

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

- Ping no endereço IP 200.218.66.5 (HSRP do BACEN)
- Se OK, retirar o cabo ou desligar o modem da Primesys e efetuar novamente o ping
- Se OK, reconectar o cabo ou ligar o modem Primesys e retirar o cabo ou desligar o modem da Embratel e efetuar novamente o ping
- Se OK, reconectar o cabo ou ligar o modem Embratel

Caso algum dos testes falhe, abrir chamado na Central de Atendimento da Concessionária e reportar o procedimento e a falha .

### Testes de contingência

Os testes de contingência e de backbone da RSFN consistem em validar as funcionalidades das redundâncias implementadas na rede pelas Concessionárias Primesys e Embratel/RTM. Serão realizados a critério do Banco Central.

A atual topologia da Rede e suas redundâncias de conexão estão exemplificadas na figura 1.

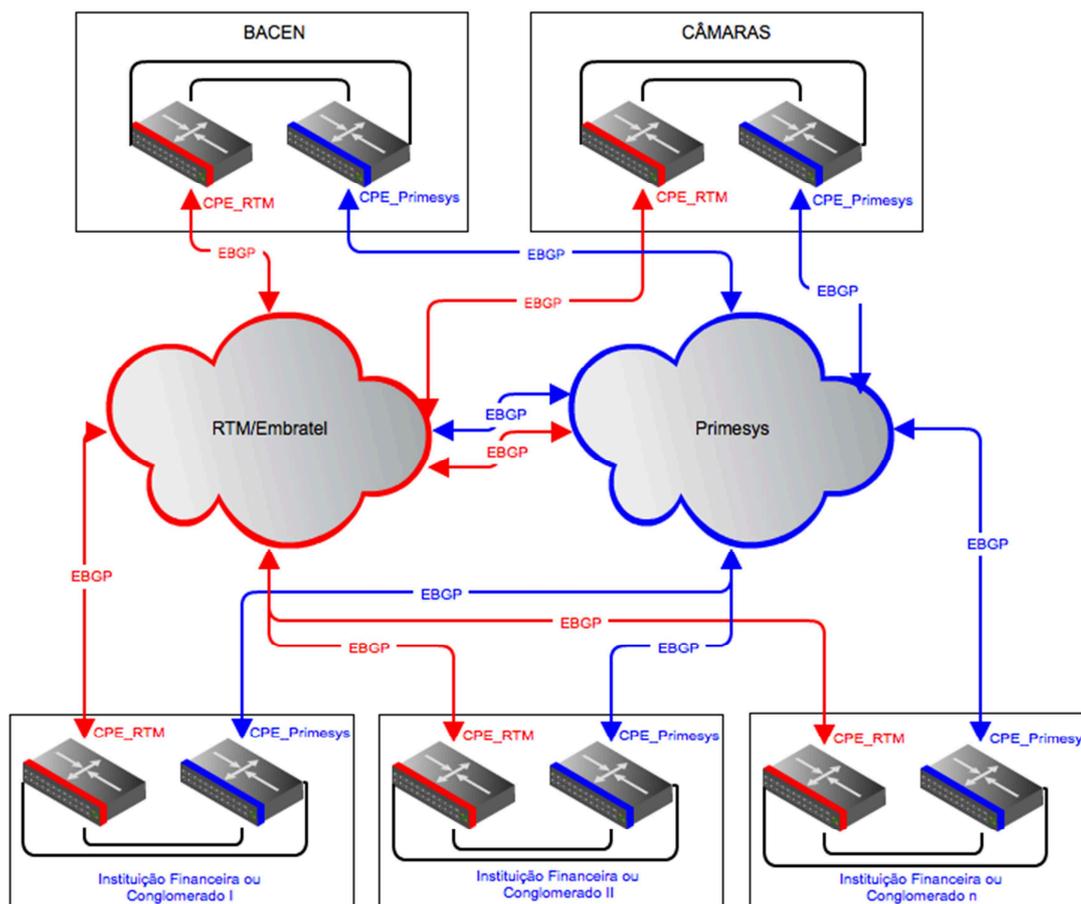


Figura 1 – Modelo de conexão da rede RSFN

Todas as Entidades possuem conexão com as duas nuvens: EBR/RTM e Primesys, o que deverá garantir a redundância de acesso a todos os serviços disponíveis na RSFN.

Durante a realização dos testes de contingência, serão simuladas situações de queda dessas conexões, a fim de validar as funcionalidades das redundâncias e medir os tempos de convergência na RSFN. Para tanto, foram definidos os procedimentos descritos a seguir:

Descrição dos procedimentos :

**1. Antes do início dos testes :**

a) Ping em 2 instituições do Grupo A

Deve-se efetuar, a partir de uma máquina (de preferência o DNS) com conexão à rede RSFN, comando “ping” utilizando o nome de, pelo menos, 100 pacotes no HSRP das instituições escolhidas .

Anotar o tempo de resposta médio na tabela .

b) Ping em 2 instituições do Grupo B

Deve-se efetuar, a partir de uma máquina (de preferência o DNS) com conexão à rede RSFN, comando “ping” utilizando o nome de, pelo menos, 100 pacotes no HSRP de uma das instituições escolhidas.

Anotar o tempo de resposta médio na tabela.

c) Traceroute para verificação dos “caminhos”

Efetuar traceroute utilizando os mesmos hosts.

Anexar os resultados na tabela.

**2. Durante a interrupção de cada dispositivo :**

a) Ping nas mesmas instituições do Grupo A

Deve-se efetuar, a partir de uma máquina (de preferência o DNS) com conexão à rede RSFN, comando “ping” (pelo nome) contínuo no HSRP das instituições escolhidas.

Anotar o tempo de resposta médio na tabela.

b) Ping nas mesmas instituições do Grupo B

Deve-se efetuar, a partir de uma máquina (de preferência o DNS) com conexão à rede RSFN, comando “ping” (pelo nome) contínuo no HSRP das instituições escolhidas .

Anotar o tempo de resposta médio na tabela.

c) Verificar qual dos hosts fica indisponível e qual o tempo de retorno

Anotar o host e o tempo de retorno.

d) Trace para verificação dos “caminhos”

Efetuar trace utilizando os mesmos hosts.

Anexar os resultados na tabela de testes.

**3. Retorno do dispositivo :**

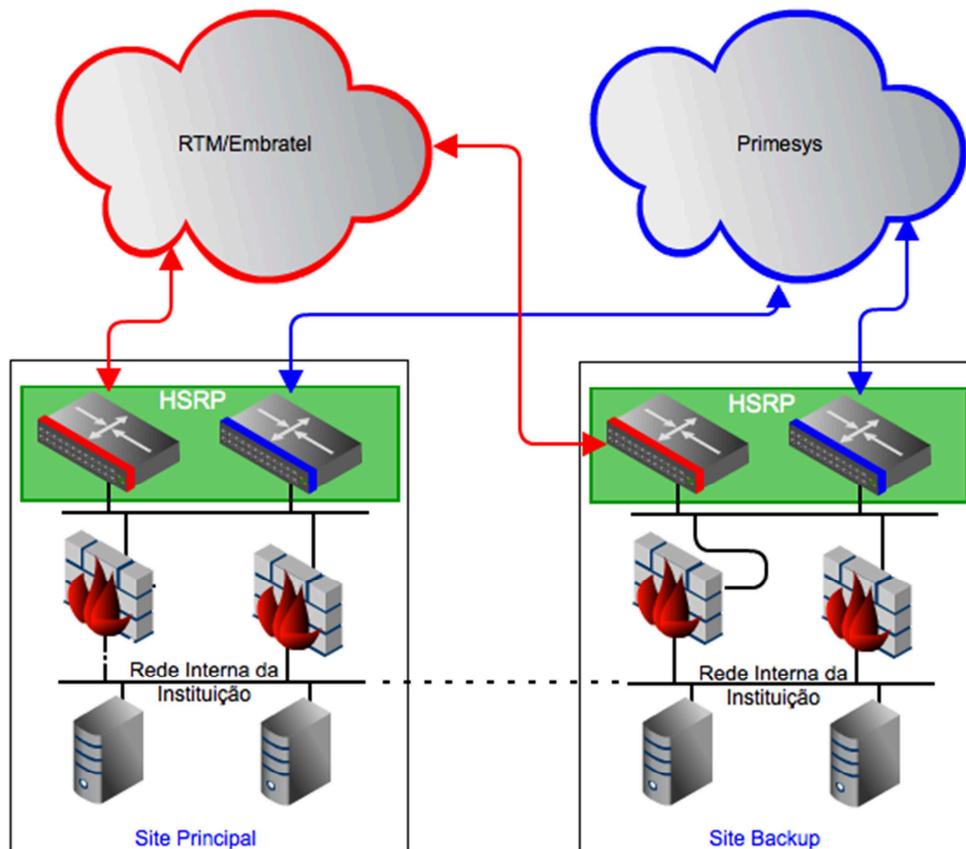
a) Verificar se ocorre indisponibilidade e qual o tempo de retorno.

Anotar o host e o tempo de retorno.

## Modelos de Topologia

### 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 2 - Dois sites com interconexão pela rede interna**

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

Testes :

- 1- Queda do circuito Primesys do *site principal*
- 2- Queda do circuito EBT do *site principal*
- 3- Queda do circuito Primesys do *site backup*
- 4- Queda do circuito EBT do *site backup*
- 5- Queda dos 2 circuitos do *site principal*
- 6- Queda dos 2 circuitos do *site principal* + Primesys *site backup*
- 7- Queda dos 2 circuitos do *site principal* + EBT *site backup*
- 8- Queda do roteador Primesys do *site principal*
- 9- Queda do roteador EBT do *site principal*
- 10- Queda do roteador Primesys do *site backup*
- 11- Queda do roteador EBT do *site backup*
- 12- Queda dos 2 roteadores do *site principal*
- 13- Queda dos 2 roteadores do *site principal* + Primesys *site backup*
- 14- Queda dos 2 roteadores do *site principal* + EBT *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*

MODELO 2:

Apenas um *site* com dois CPE de cada concessionária ou *site* Principal e *Backup* com apenas um CPE em cada.

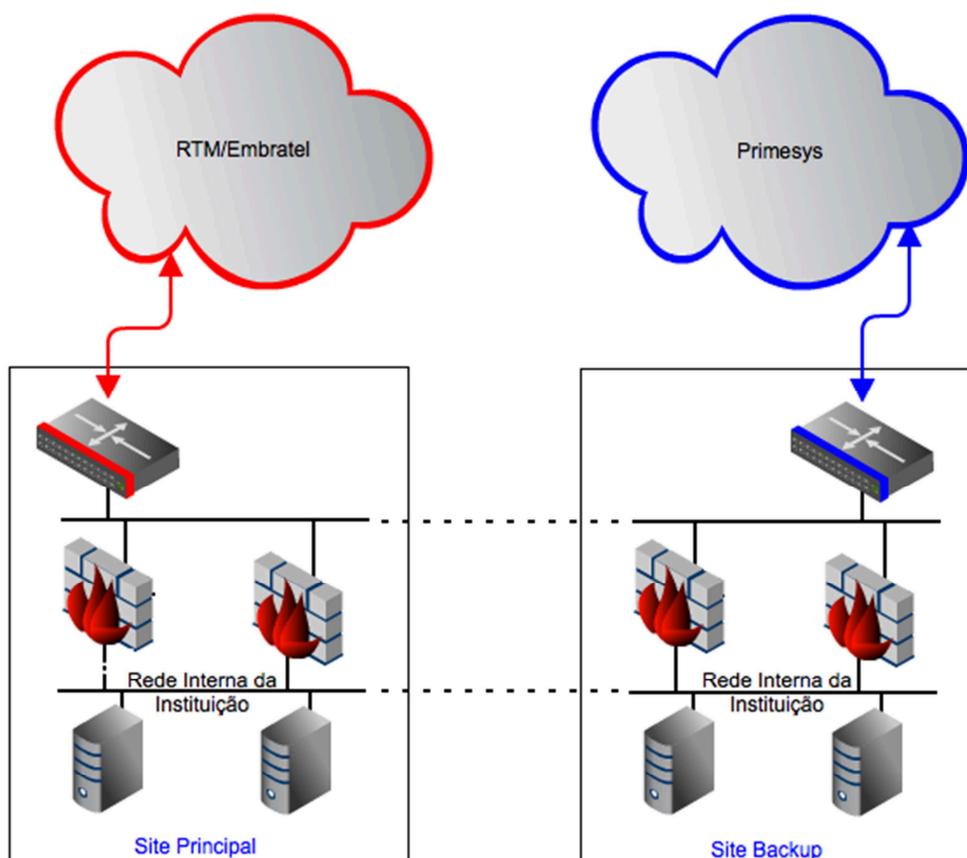


Figura 3 - Dois sites, porém com apenas dois CPE

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

Testes :

- 1- Queda do circuito Primesys do *site* principal
- 2- Queda do circuito EBT do *site backup*
- 3- Queda do roteador Primesys do *site* principal
- 4- Queda do roteador EBT do *site backup*
- 5- Queda do *firewall* do *site* principal
- 6- Queda do *firewall* do *site backup*

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).

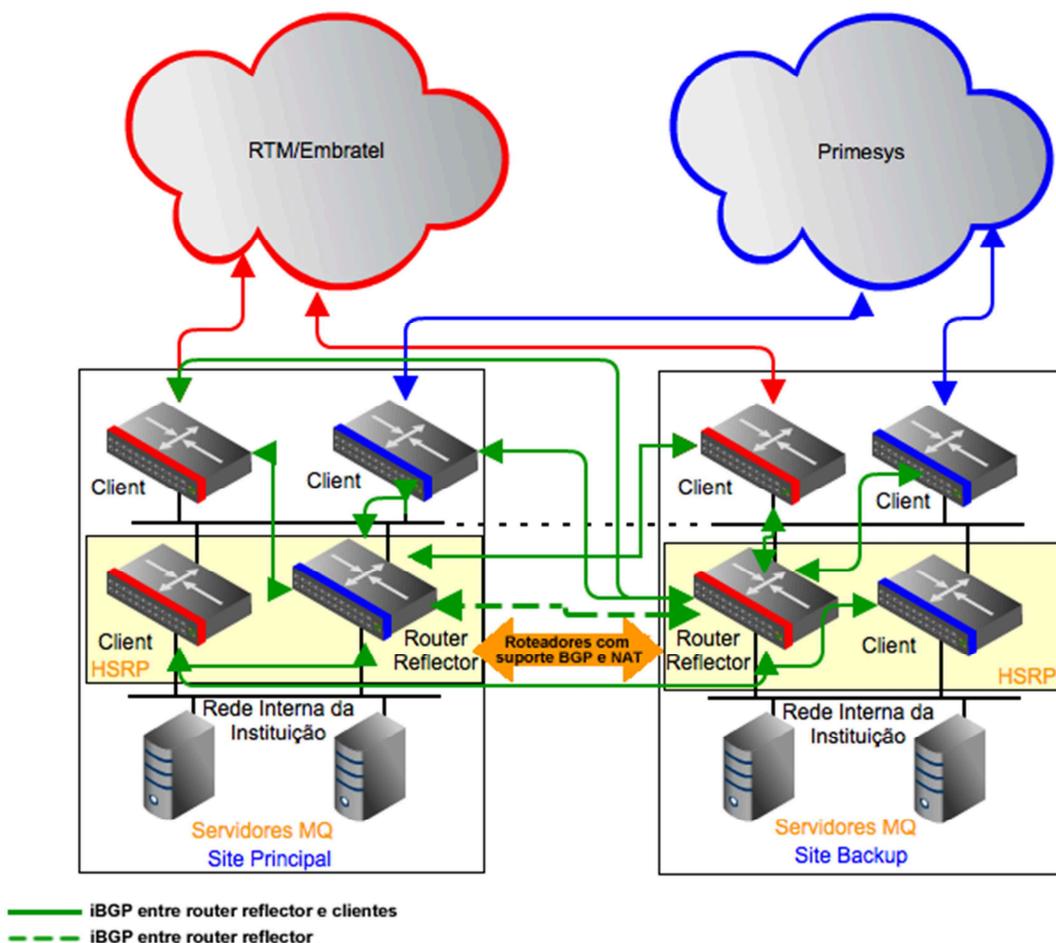


Figura 4 - Conexão do Perfil D com roteamento iBGP

Esse modelo pode ter como variantes

- 1-Apenas 2 CPE's e **n** roteadores BGP (onde **n** é um número entre 1 e 2) ; 2 em cada *site* 2-
- Sem *site backup* , com os **n** roteadores no mesmo *site*

Testes :

- 1- Queda do circuito Primesys do *site* principal
- 2- Queda do circuito EBT do *site* principal
- 3- Queda do circuito Primesys do *site backup*
- 4- Queda do circuito EBT do *site backup*
- 5- Queda dos 2 circuitos do *site* principal
- 6- Queda dos 2 circuitos do *site* principal + Primesys *site backup*
- 7- Queda dos 2 circuitos do *site* principal + EBT *site backup*
- 8- Queda do roteador Primesys do *site* principal
- 9- Queda do roteador EBT do *site* principal
- 10- Queda do roteador Primesys do *site backup*
- 11- Queda do roteador EBT do *site backup*
- 12- Queda dos 2 roteadores do *site* principal
- 13- Queda dos 2 roteadores do *site* principal + Primesys *site backup*
- 14- Queda dos 2 roteadores do *site* principal + EBT *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 roteador BGPs do *site* principal
- 20- Queda dos 2 roteador BGPs do *site* principal + Roteador BGP 1 *site backup*
- 21- Queda dos 2 roteador BGPs do *site* principal + Roteador BGP 2 *site backup*

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)

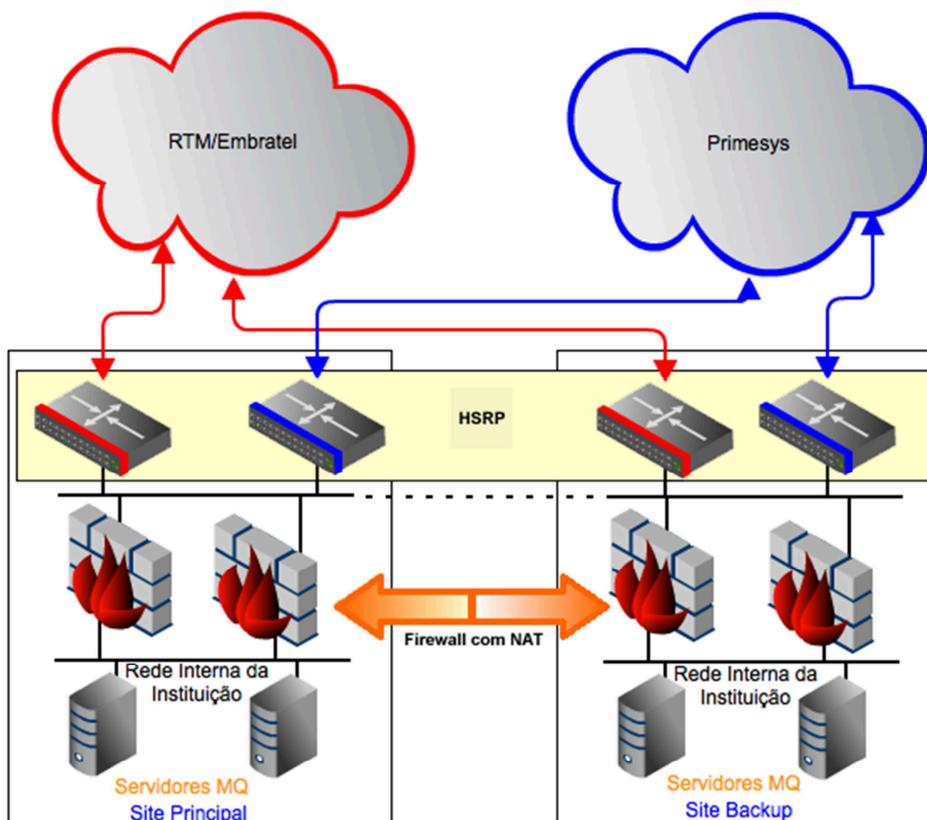


Figura 5 - Conexão direta do Perfil D com a célula de segurança

Testes :

- 1- Queda do circuito Primesys do *site principal*
- 2- Queda do circuito EBT do *site principal*
- 3- Queda do circuito Primesys do *site backup*
- 4- Queda do circuito EBT do *site backup*
- 5- Queda dos 2 circuitos do *site principal*
- 6- Queda dos 2 circuitos do *site principal* + Primesys *site backup*
- 7- Queda dos 2 circuitos do *site principal* + EBT *site backup*
- 8- Queda do roteador Primesys do *site principal*
- 9- Queda do roteador EBT do *site principal*
- 10- Queda do roteador Primesys do *site backup*
- 11- Queda do roteador EBT do *site backup*
- 12- Queda dos 2 roteadores do *site principal*
- 13- Queda dos 2 roteadores do *site principal* + Primesys *site backup*
- 14- Queda dos 2 roteadores do *site principal* + EBT *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*

## DESCRIÇÃO TÉCNICA

### Arquitetura de endereçamento IP

A RSFN recebeu do Comitê Gestor da Internet Brasil um prefixo /18 para ser distribuído entre as Entidades Participantes, a fim de evitar conflito com o endereçamento IP interno destas.

A topologia lógica da RSFN é composta de dois níveis hierárquicos: *core* e acesso. O *core* é composto pelas Concessionárias e o acesso pelas Entidades Participantes, que são: BACEN, Câmaras, Provedores PSTI e as Instituições Financeiras (IF).

O BACEN, as Câmaras e os Provedores PSTI deverão ter, no mínimo, dois *sites* e as IF poderão ter um ou mais *sites*.

Os conglomerados que englobam mais de uma Instituição Financeira, e possuem todos os serviços concentrados, serão vistos como um Provedor PSTI, de acordo com a norma vigente pelo Banco Central do Brasil.

A Figura 6 ilustra a comunicação entre as Entidades Participantes da RSFN:

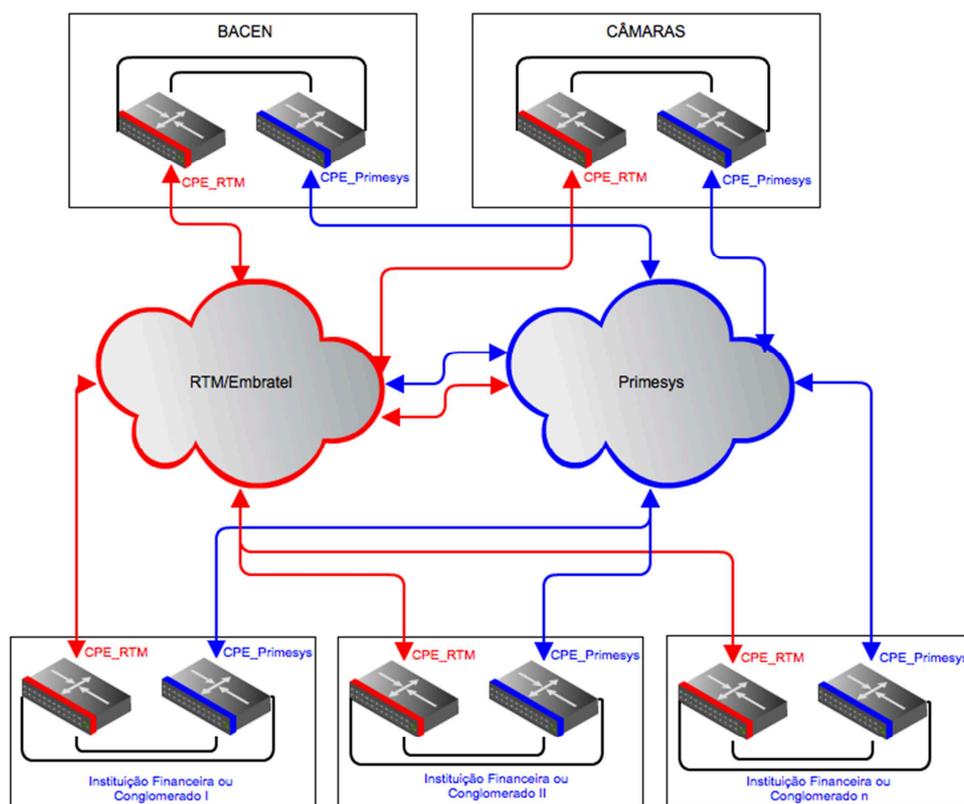
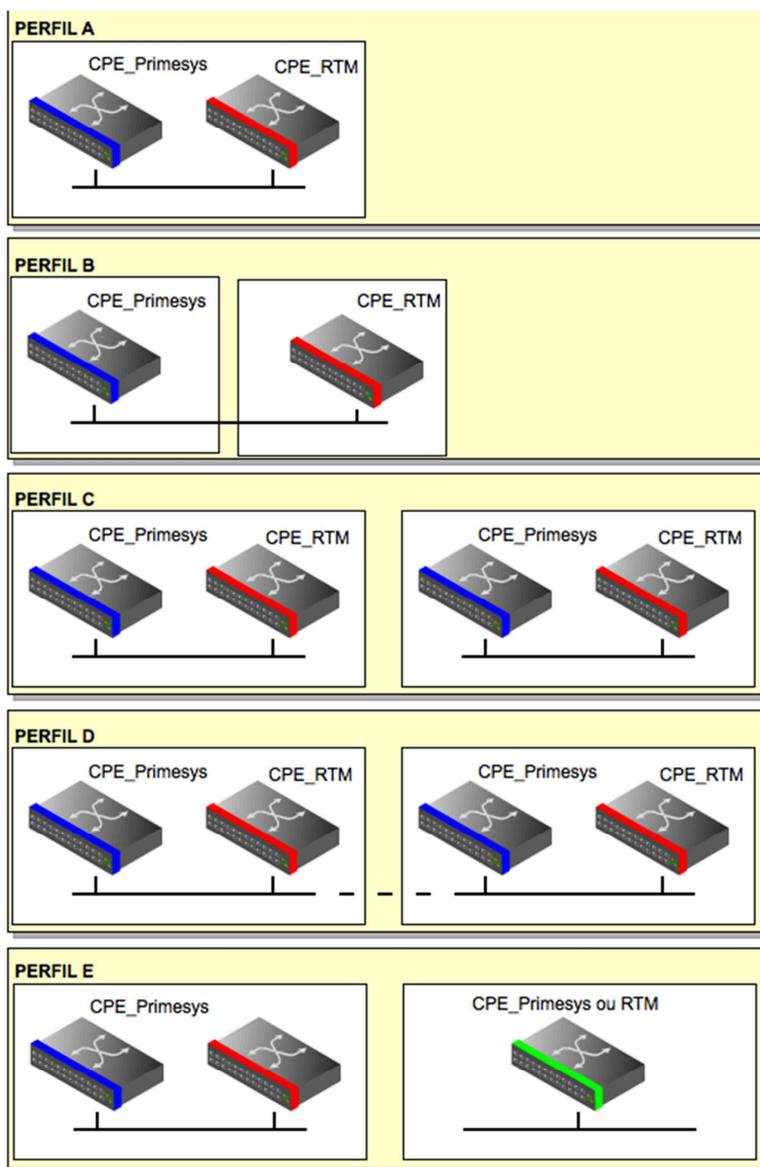


Figura 6 – Comunicação entre as entidades participantes da RSFN

O serviço de comunicação entre as Entidades Participantes da RSFN está sendo oferecido por duas concessionárias: Primesys e pela Embratel/RTM, através de um *backbone* com o serviço VPN/MPLS, garantindo um isolamento lógico da RSFN.

As Entidades Participantes deverão ter como conexão à RSFN um dos cinco perfis ilustrados na Figura 7.

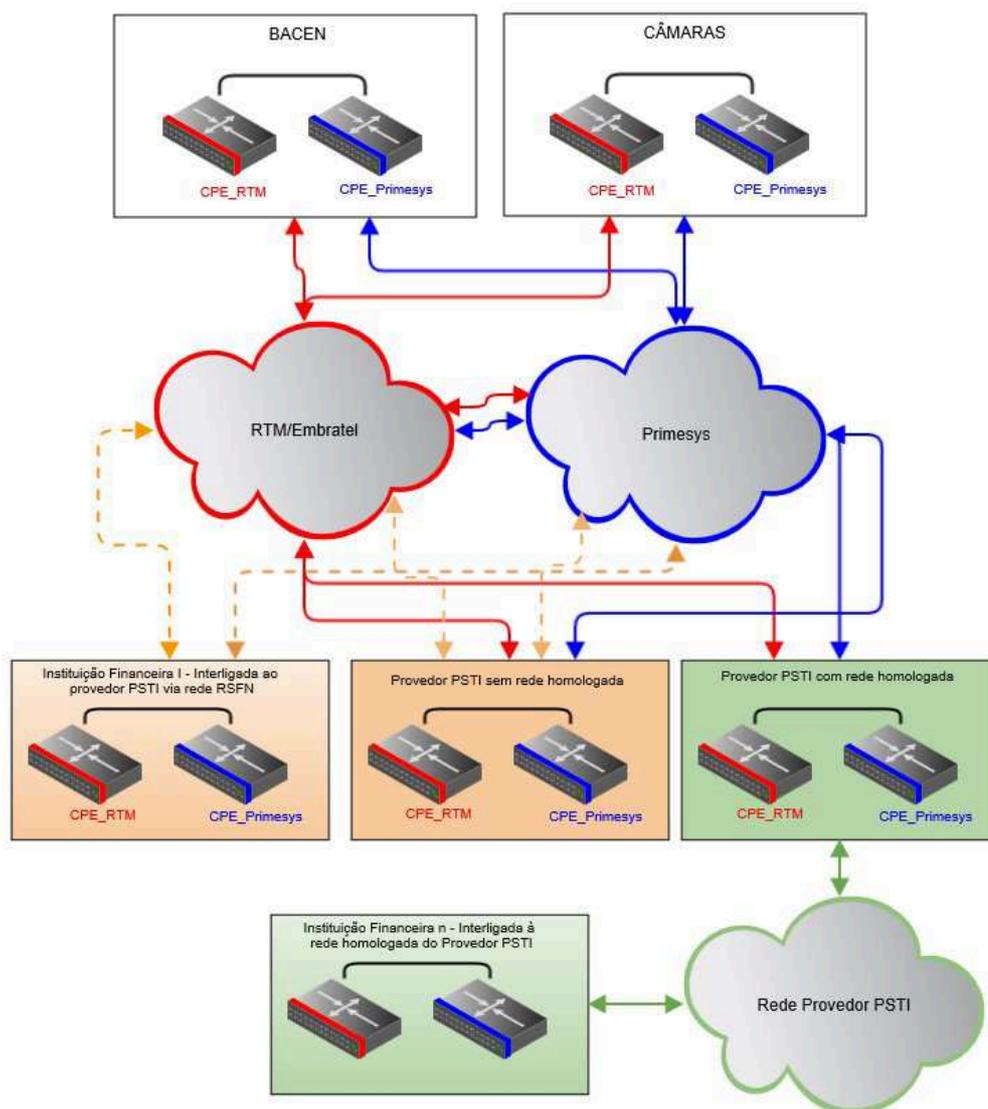


**Figura 7 - Perfis de conexão com a RSFN**

Caso o Participante adote os perfis A ou B, este receberá um prefixo /28 para a VLAN de conexão com a RSFN. Para os demais perfis receberá dois prefixos /28.

O BACEN, as Câmaras e os Provedores PSTI utilizarão o perfil C ou D recebendo dois prefixos /27.

O Provedor PSTI pode se comunicar apenas com o BACEN, as Câmaras e as IFs às quais ele presta serviço, conforme apresentado na Figura 8.



**Figura 8 - Serviço PSTI**

**Definição da Faixa de endereços dos Hosts de cada VLAN**

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.

**VLAN das Câmaras e dos Provedores PSTI**

A VLAN das Câmaras e dos Provedores PSTI possuem no máximo 30 hosts para cada prefixo /27. As faixas de hosts recomendadas para estas subredes estão ilustradas nas Tabela 1 e Tabela 2.

1º byte	2º byte	3º byte	4º byte	host	Tipo do host
X	X	X	xxx00001	1o.	Ethernet 0/0 CPE Primesys
X	X	X	xxx00010	2o.	Ethernet 0/0 CPE EBT/RTM
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 MQSeries
X	X	X	xxx01001	9o.	2o. Servidor MQSeries
X	X	X	xxx01010	10º.	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**

1º byte	2º byte	3º byte	4º byte	host	Tipo do host
X	X	X	Xx000001	1o.	Ethernet 0/0 CPE Primesys do <i>site principal</i>
X	X	X	Xx000010	2o.	Ethernet 0/0 CPE EBT/RTM do <i>site principal</i>
X	X	X	Xx000011	3o.	Ethernet 0/0 CPE Primesys do <i>site backup</i>
X	X	X	Xx000100	4o.	Ethernet 0/0 CPE EBT/RTM do <i>site backup</i>
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 MQSeries
X	X	X	Xx001001	9o.	2o. Servidor MQSeries
X	X	X	Xx001010	10o.	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**

**VLAN das IFs**

A VLAN das IF possuem no máximo 14 hosts para cada prefixo /28. As faixas de hosts recomendadas para estas subredes estão ilustradas nas Tabela 3 e Tabela 4.

1º byte	2º byte	3º byte	4º byte	host	Tipo do host
X	X	X	xxxx0001	1o.	Ethernet 0/0 CPE Primesys
X	X	X	xxxx0010	2o.	Ethernet 0/0 CPE EBT/RTM
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 MQSeries
X	X	X	xxxx1001	9o.	2o. Servidor MQSeries
X	X	X	xxxx1010	10º.	Reservado
X	X	X	...	...	Reservado
X	X	X	xxxx1101	13º.	Reservado
X	X	X	xxxx1110	14o.	<i>Firewall</i>

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

1º byte	2º byte	3º byte	4º byte	host	Tipo do host
X	X	X	xxx00001	1o.	Ethernet 0/0 CPE Primesys do <i>site principal</i>
X	X	X	xxx00010	2o.	Ethernet 0/0 CPE EBT/RTM do <i>site principal</i>
X	X	X	xxx00011	3o.	Ethernet 0/0 CPE Primesys do <i>site backup</i>
X	X	X	xxx00100	4o.	Ethernet 0/0 CPE EBT/RTM do <i>site backup</i>
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 MQSeries
X	X	X	xxx01001	9o.	2o. Servidor MQSeries
X	X	X	xxx01010	10º.	Reservado
X	X	X	...	...	...
X	X	X	xxx10111	22º.	Switch
X	X	X	...	...	...
X	X	X	xxx11010	26º.	<i>Firewall</i>
X	X	X	...	...	...
X	X	X	xxx11110	30o.	<i>Firewall</i>

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

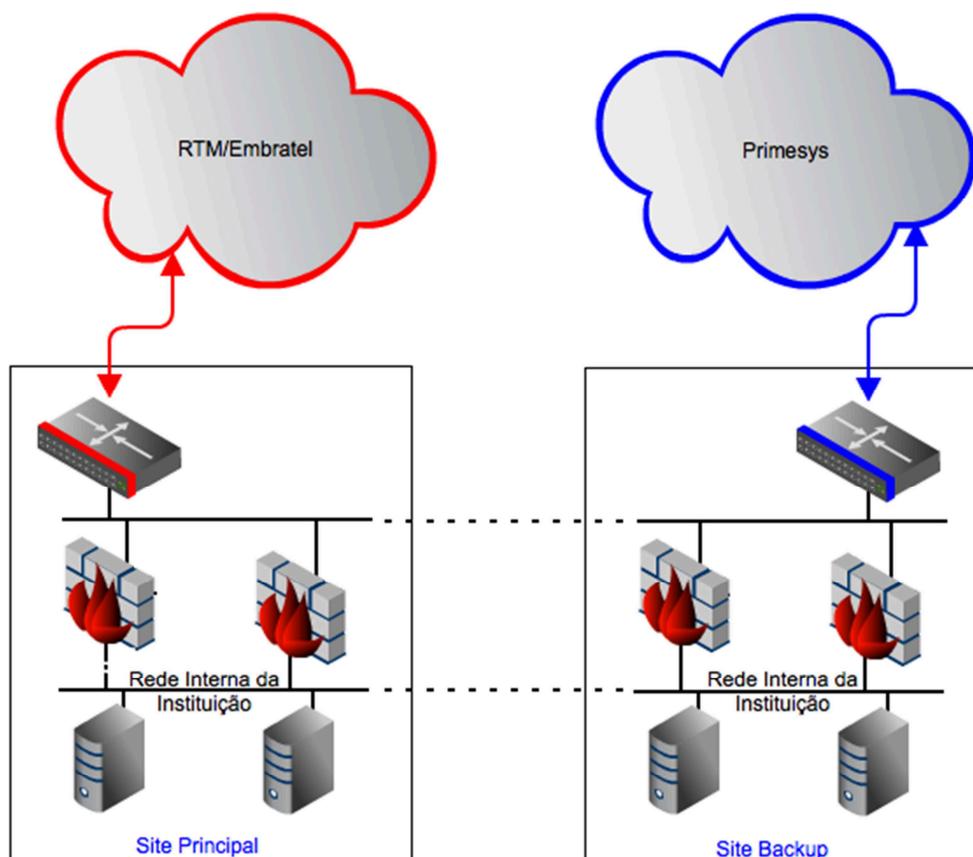
## ROTEAMENTO DA RSFN

As concessionárias garantem que as rotas das VPN das Entidades Participantes da RSFN não serão divulgadas para a Internet. A concessionária não deve interferir na Política de Roteamento das Entidades Participantes da RSFN.

O Subgrupo de Redes definiu que todo o tráfego das informações de entrada das Entidades Participantes não terá preferência entre os circuitos das duas concessionárias; o mesmo se aplica para todo o tráfego das informações de saída das Entidades Participantes, que não terão preferência entre os circuitos, dividindo o tráfego entre as duas concessionárias. Este controle é feito pelo protocolo de roteamento BGP responsável pelo roteamento dos pacotes entre os CPE e as concessionárias.

### Roteamento para o Perfil A e B (Modelo 2)

Apenas um *site* com dois CPE de cada concessionária ou *site* Principal e *Backup* com apenas um CPE em cada.



**Figura 9 - 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 CPEs e a célula de segurança não possui nenhum protocolo de roteamento dinâmico, sendo utilizado apenas roteamento estático.

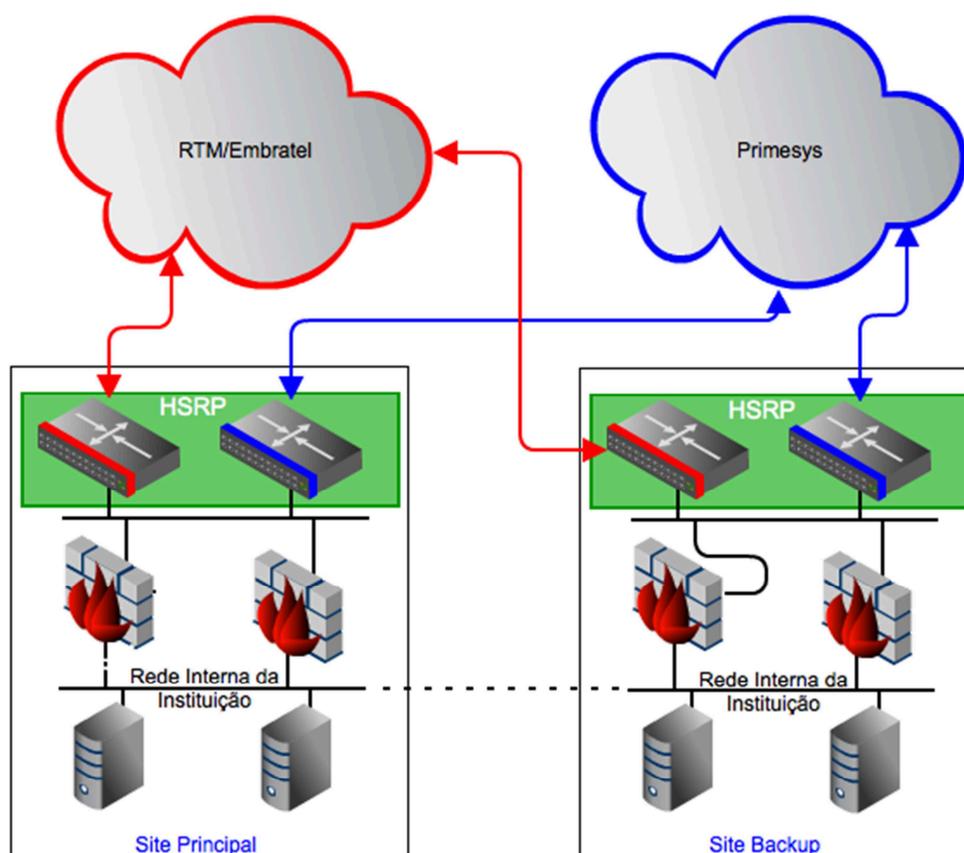
Como nesse segmento de rede local existem dois roteadores, será implementada a tecnologia HSRP. Desta forma, os *hosts* terão alternativas de acesso externo em caso de falha de um roteador, sem necessidade de configuração

manual.

Os dois roteadores possuirão alocação de endereços das interfaces Ethernet, porém 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.

### 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 10 - 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 consideradas duas Entidades, 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.

Roteamento para o Perfil D com roteadores da Entidade 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).

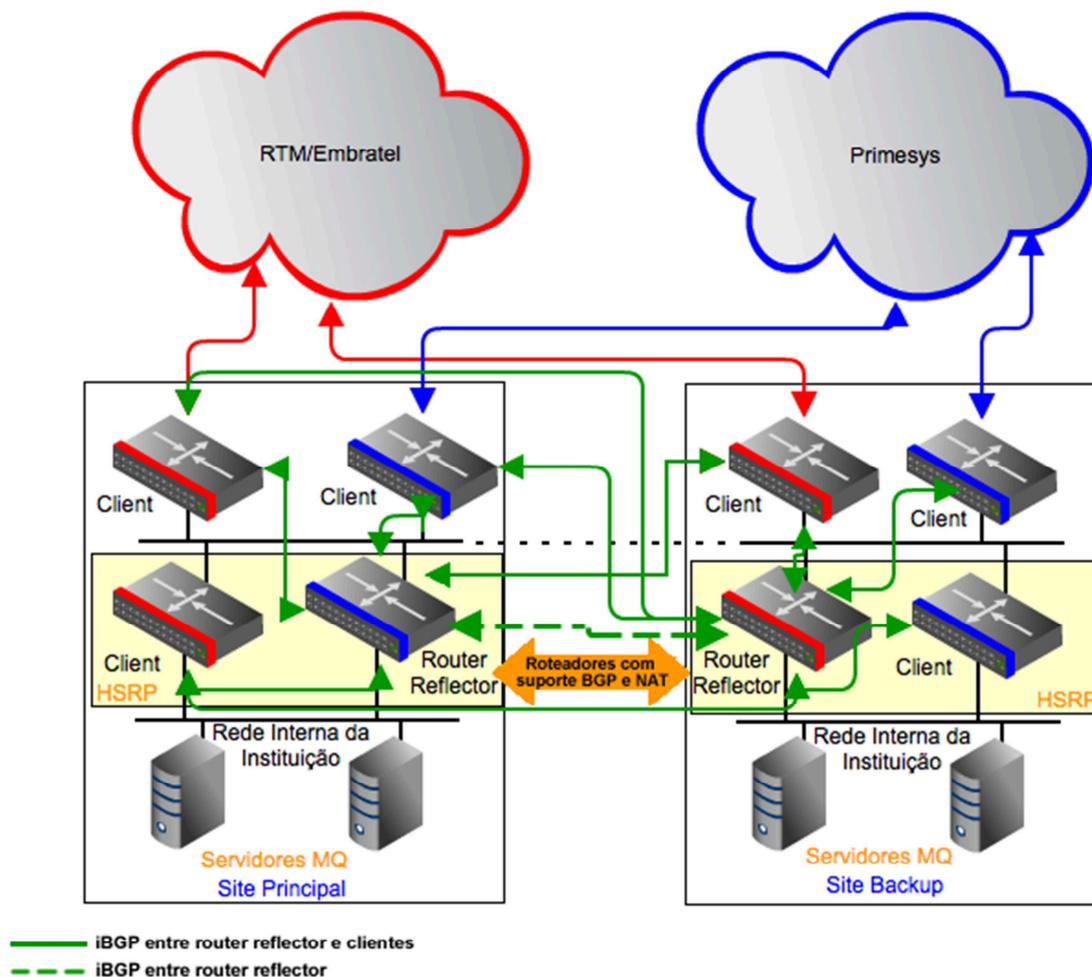


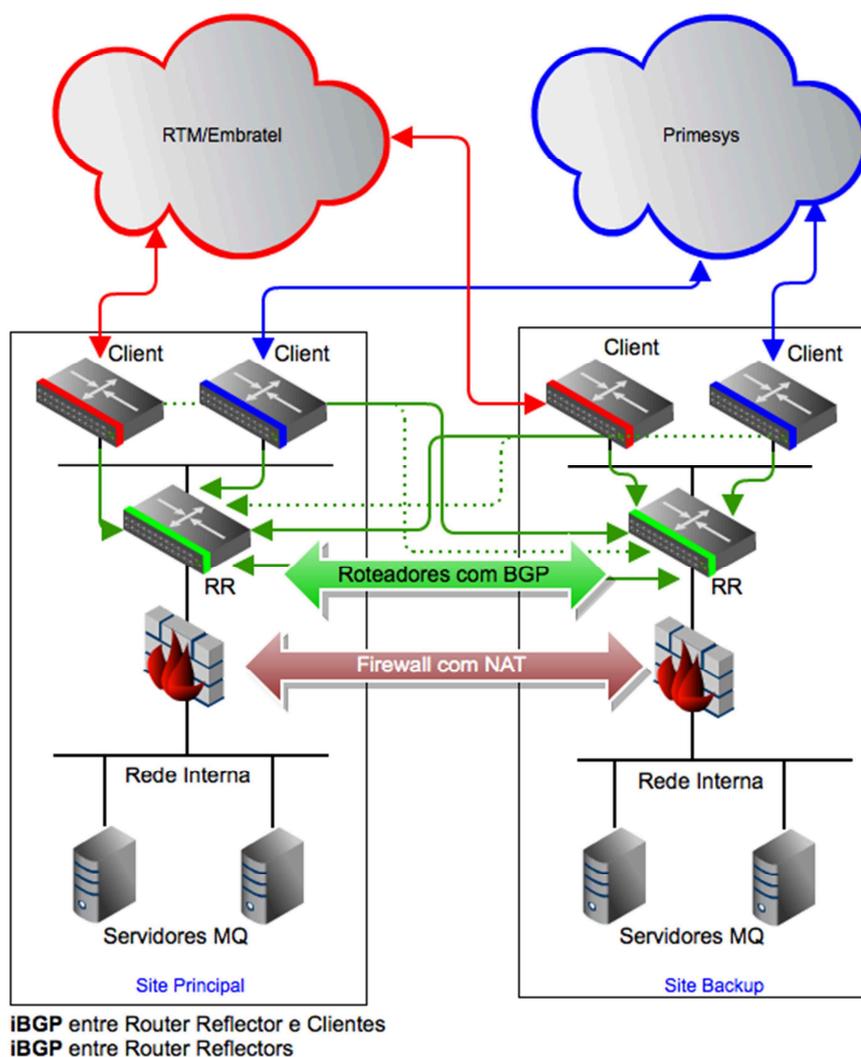
Figura 11 - Conexão do Perfil D com roteamento iBGP

Embora neste tipo de conexão as Entidades recebam dois blocos de endereçamento IP, para a RSFN será anunciado apenas um único prefixo (no caso de IF será o prefixo /27 e no caso de Câmara ou Provedor PSTI será o prefixo /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 concessionária 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 6 - Conexão do Perfil D com roteamento iBGP. Os roteadores das Entidades 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.

Roteamento para o Perfil D com roteadores da Entidade no barramento RSFN e NAT do 2º prefixo /28 (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) segmentando o prefixo /27 em dois prefixos /28 internamente 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 /28 a partir de roteadores internos para que os CPE possam alcançar os endereços deste prefixo a partir dos *route-reflectors*.



**Figura 12 -Topologia com dois sites, quatro roteadores da Entidade e NAT interno**

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).

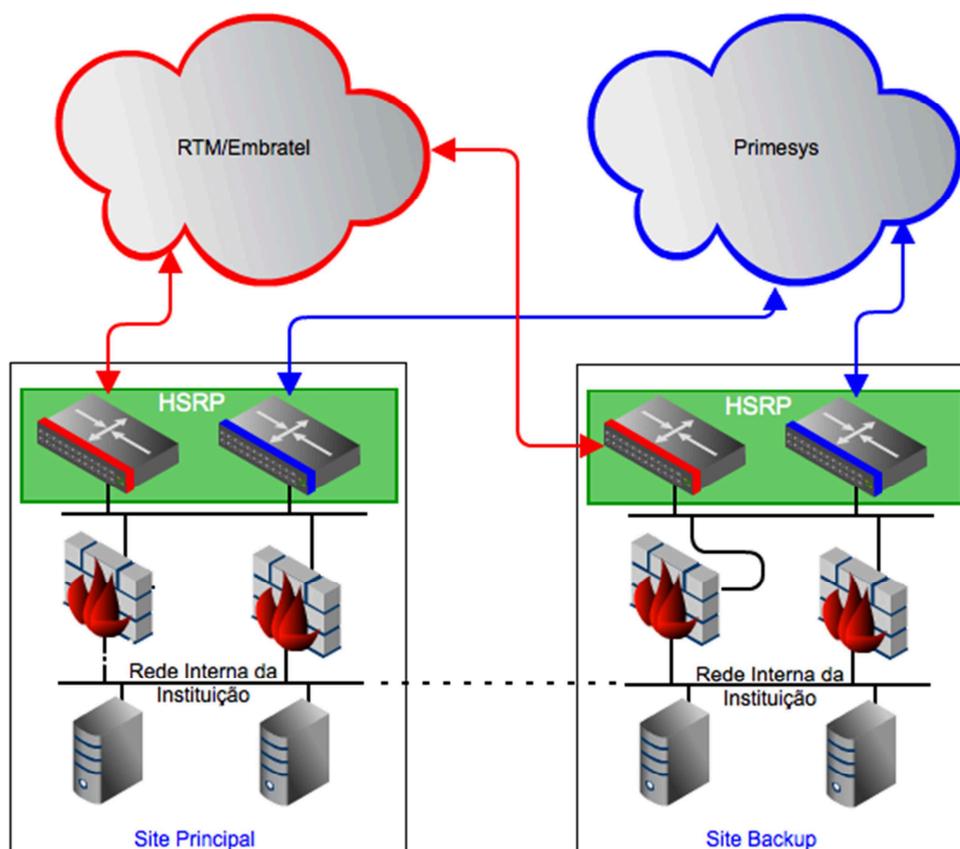
Para a RSFN, será anunciado apenas um único prefixo (no caso de IF será o prefixo /27 e no caso de Câmara/BACEN/Provedor PSTI será o prefixo /26) e o grupo (grupo A/B) será referente ao primeiro prefixo fornecido pelo BACEN (ou seja, se o primeiro prefixo for grupo A, o sumário será do grupo A).

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 concessionária 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 das Entidades 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 /28 e o *route-reflector* do *site* secundário o 14º. Apesar de, a partir dos CPE existirem dois caminhos para a o segundo prefixo /28, a opção de acesso será tomada para o vizinho (*neighbor*) com o menor endereço IP (*site* principal).

#### 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).**



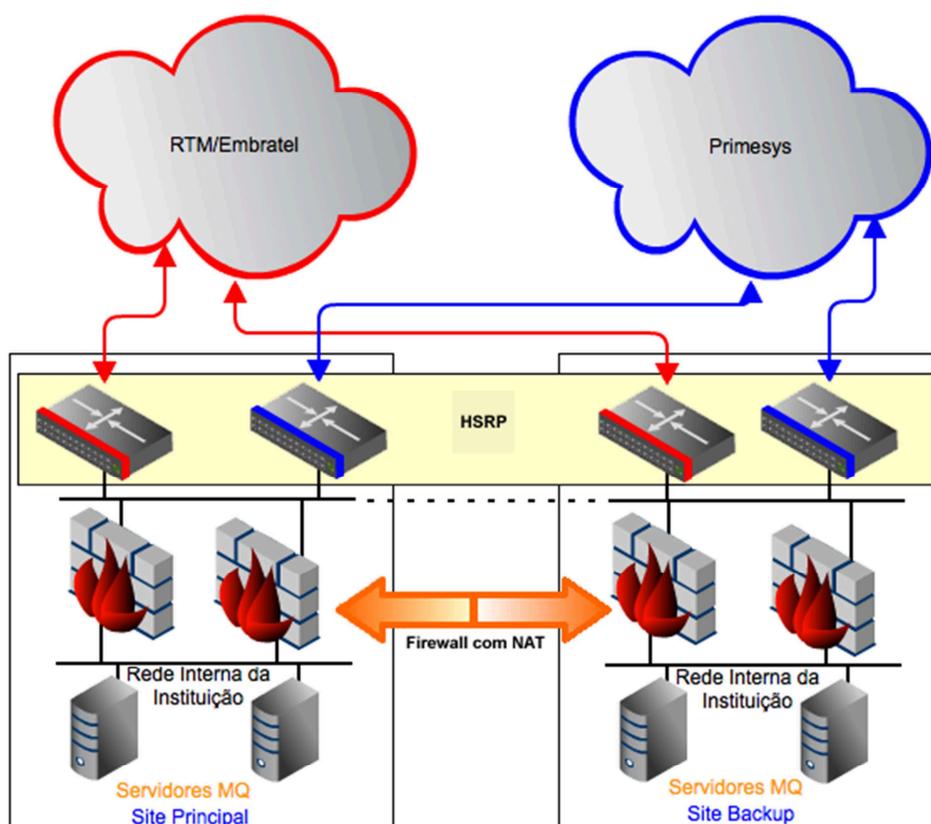
**Figura 13 - Conexão direta do Perfil D com a célula de segurança**

A diferença entre este modelo em relação ao anterior refere-se ao fato dos 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 este protocolo). Neste caso, deverá ser configurado HSRP envolvendo os 4 CPEs (dois de cada *site*). O anúncio do prefixo será /27 para as IF e /26 para as demais Entidades.

Roteamento para o Perfil D com *firewall* da Entidade no barramento RSFN (Modelo 5)

Similar ao modelo anterior, mas segmentando o prefixo /27 em dois prefixos /28 internamente 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. Desta forma não haverá necessidade de configurar uma tabela ARP estaticamente nos *firewall*, 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*.



**Figura 14 - Topologia com dois domínios de broadcast**

OBSERVAÇÃO IMPORTANTE RELATIVA AOS MODELOS 4 E 5

Tendo em vista o roteamento adotado na RSFN, os modelos 4 e 5 deverão 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*, nestes modelos, poderá causar perda de conectividade com a RSFN. As concessionárias devem ser consultadas para maiores detalhes sobre essa característica de tráfego.

## MODELOS DE TOPOLOGIA PARA CONEXÕES COM REDES INTERNAS

Foram apresentados alguns modelos de topologia para conectar o segmento da RSFN instalado em cada Entidade Participante com suas respectivas Intranets. Os modelos são:

- topologia de acesso com roteadores e *firewalls*;
- topologia de acesso com roteadores, *firewalls* e DMZ;
- topologia redundante com *site* de contingência;
- topologia de redundância máxima sem *site* de contingência;
- topologia de redundância máxima com *site* de contingência.

Os modelos levam em consideração os aspectos de segurança, unicidade de endereços IP, conversão de endereços IP utilizados nas redes internas e na RSFN, resolução de nomes via serviço de DNS, redundância e balanceamento de carga.

A escolha de um dos modelos indicados fica a cargo de cada Entidade, levando-se em conta a análise de custos X benefícios.

### Topologia de acesso com Firewall

Este modelo, considerado o modelo básico para a interligação entre o segmento da RSFN com a Intranet do Participante, é apresentado na Figura 15.

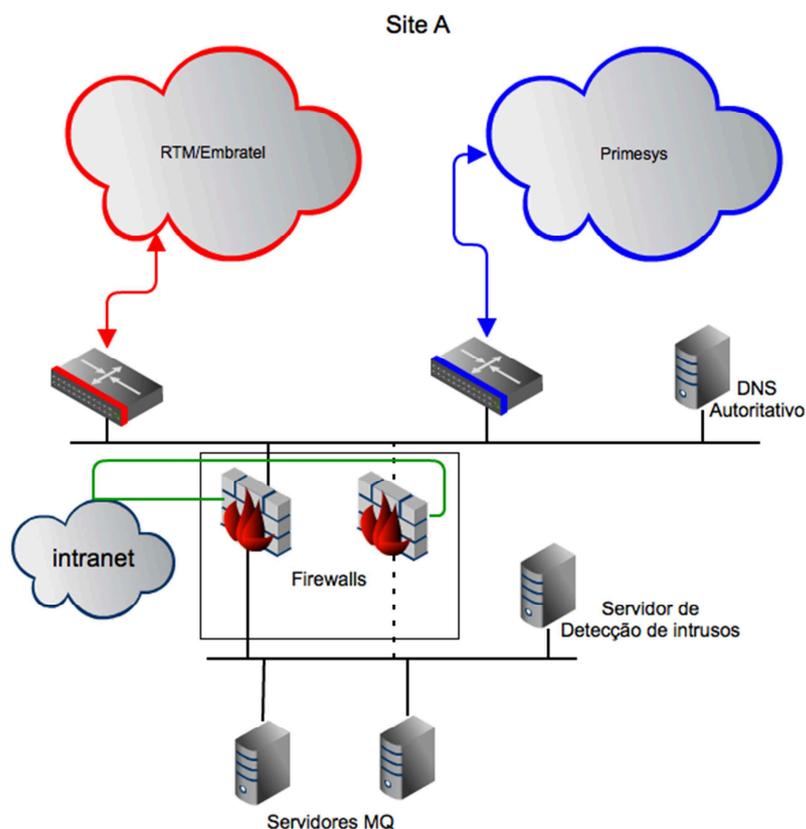


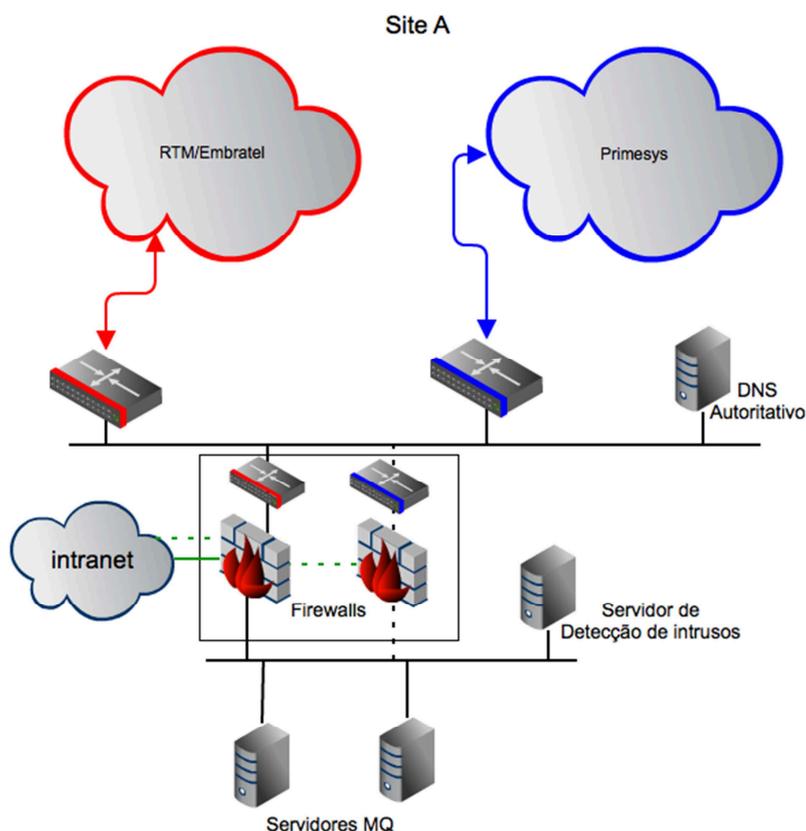
Figura 15 - Topologia de Acesso com Firewall

As seguintes observações são pertinentes:

- em hipótese alguma, o segmento da RSFN deve estar interligado ao segmento da Intranet sem a utilização de servidores de *Firewall* (servidores de *Firewall* especializados ou roteadores com função de *Firewall* ou que suportem a configuração de listas de acesso);
- para evitar que o *Firewall* seja ponto único de falha, a Entidade deve considerar a utilização de equipamentos redundantes;
- o balanceamento de carga entre os servidores de *Firewall* pode estar baseado em soluções de alta disponibilidade, mecanismos de *Failover* ou duplicação de tabelas e permissão de acesso em conjunto com protocolos de roteamento dinâmico;
- os servidores da RSFN podem estar fisicamente instalados em um segmento isolado ou podem fazer parte dos segmentos da Intranet da Entidade;
- os servidores de DNS da RSFN devem fazer parte do segmento da RSFN de cada Entidade, de forma a se evitar possíveis problemas de conversão de endereços;
- somente o segmento da RSFN deve utilizar endereços no padrão fornecido pela RSFN. Os demais segmentos de rede devem utilizar endereços da Intranet da Entidade;
- os servidores da RSFN serão configurados com endereços lógicos da RSFN no servidor de DNS de seu respectivo domínio. O servidor de *Firewall* deverá executar a conversão de endereços via NAT, no formato 1 para 1, ou seja, um endereço lógico da RSFN para cada endereço físico utilizado na Intranet;
- todas as estações de trabalho da Intranet que desejarem acessar serviços da RSFN, terão seus endereços da Intranet convertidos para um único endereço da RSFN. Esta conversão também deverá ser executada no servidor de *Firewall*, configurado com a função NAT;
- os roteadores da Intranet deverão ser configurados com rota específica para os endereços válidos na RSFN a serem fornecidos pelo Banco Central. Essas rotas deverão apontar para o servidor de *Firewall* utilizado na interligação da Intranet com a RSFN;
- Os servidores de *Firewall* deverão ser configurados com rota específica para o endereço do host **hsrp.sub-domínio.rsfnet.br**.

**Topologia de acesso com roteadores, Firewall e DMZ**

Este modelo é bastante similar ao anterior, diferenciando-se apenas pela utilização de roteadores internos para isolar o segmento da RSFN dos servidores de *Firewall*. A Figura 16 ilustra esta topologia.



**Figura 16 - Topologia de Acesso com Roteadores, Firewall e DMZ**

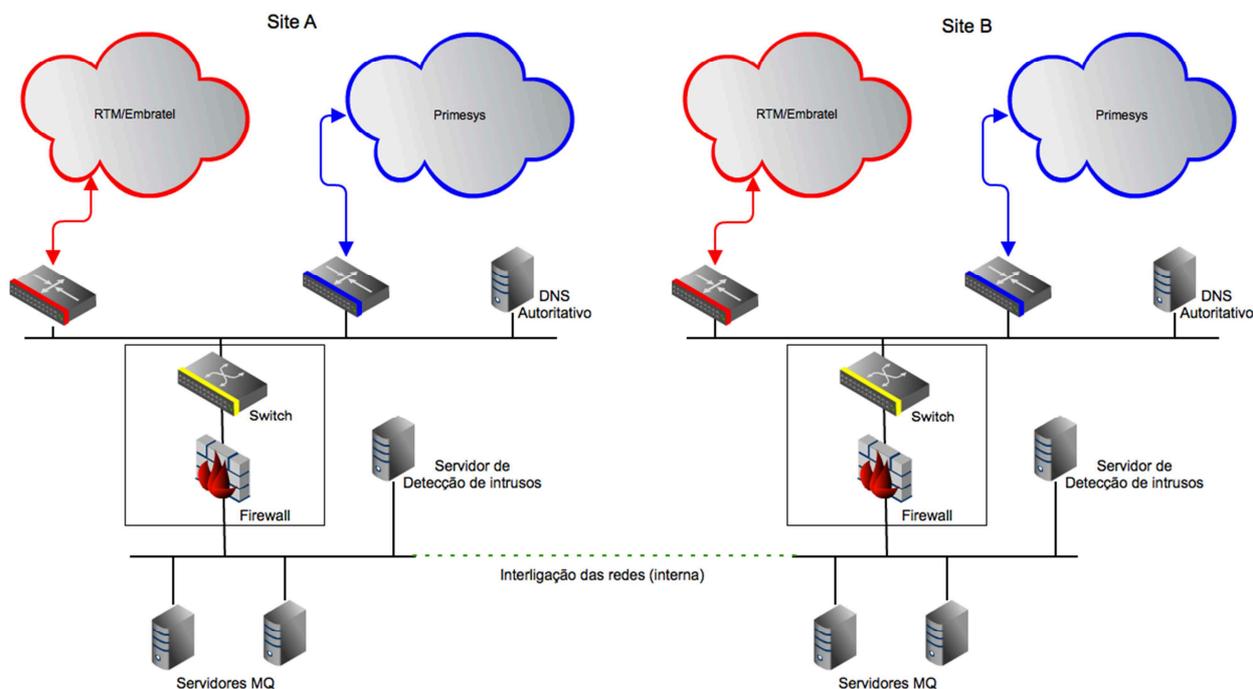
As seguintes observações são pertinentes:

- são utilizados roteadores internos entre o segmento da RSFN e os servidores de *Firewall*;
- em hipótese alguma, o segmento da rede RSFN deve estar interligado ao segmento da Intranet sem a utilização de servidores de *Firewall* (servidores de *Firewall* especializados ou roteadores com função de *Firewall* ou que suportem a configuração de listas de acesso);
- para evitar que o *Firewall* seja ponto único de falha, a Entidade deve considerar a utilização de equipamentos redundantes;
- o balanceamento de carga entre os servidores de *Firewall* pode estar baseado em soluções de alta disponibilidade, mecanismos de Failover ou duplicação de tabelas e permissão de acesso em conjunto com protocolos de roteamento dinâmico;
- os servidores da RSFN podem estar fisicamente instalados em um segmento isolado ou podem fazer parte dos segmentos da Intranet da Entidade;

- os servidores de DNS da RSFN devem fazer parte do segmento da RSFN de cada Entidade, de forma a evitar possíveis problemas de conversão de endereços;
- somente o segmento da RSFN deve utilizar endereços no padrão fornecido pela RSFN. Os demais segmentos de rede devem utilizar endereços da Intranet da Entidade;
- os servidores da RSFN serão configurados com endereços lógicos da RSFN no servidor de DNS de seu respectivo domínio. O servidor de *Firewall* deverá executar a conversão de endereços via NAT, no formato 1 para 1, ou seja, um endereço lógico da RSFN para cada endereço físico utilizado na Intranet;
- todas as estações de trabalho da Intranet que desejarem acessar serviços da RSFN, terão seus endereços da Intranet convertidos para um único endereço da RSFN. Esta conversão também deverá ser executada no servidor de *Firewall*, configurado com a função NAT;
- os roteadores da Intranet deverão ser configurados com rota específica para os endereços válidos na RSFN a ser fornecido pelo Banco Central. Estas rotas deverão apontar para o servidor de *Firewall* utilizado na interligação da Intranet com a RSFN;
- os servidores de *Firewall* deverão ser configurados com rota específica para o endereço do *host* **hsrp.sub-domínio.rsfn.net.br**.

### Topologia redundante com *site* de contingência

Neste modelo são utilizados dois *sites*: um principal e um de contingência, conforme ilustrado na Figura 17. Cabe à Entidade definir se os dois estarão ativos ou se o *site* de contingência somente será acionado em caso de falhas no *site* principal.



**Figura 17 - Topologia Redundante com *Site* de Contingência**

As seguintes observações são pertinentes:

- são utilizados *switches* de conteúdo com configuração de GLB (*Global Load Balance*) para realizar o balanceamento de carga entre os servidores que oferecem serviços para a RSFN;
- em hipótese alguma, o segmento da rede RSFN deve estar interligado ao segmento da Intranet sem a utilização de servidores de *Firewall* (servidores de *Firewall* especializados ou roteadores com função de *Firewall* ou que suportem a configuração de listas de acesso);
- para evitar que o *Firewall* seja ponto único de falha, a Entidade deve considerar a utilização de equipamentos redundantes, neste caso um em cada localidade;
- o balanceamento de carga entre os servidores de *Firewall* pode estar baseado em soluções de alta disponibilidade;
- a interligação entre os segmentos da rede interna pode ser executada utilizando-se diferentes tecnologias de LANs e MANs;
- os servidores da RSFN podem estar fisicamente instalados em um segmento isolado ou podem fazer parte dos segmentos da Intranet da Entidade;

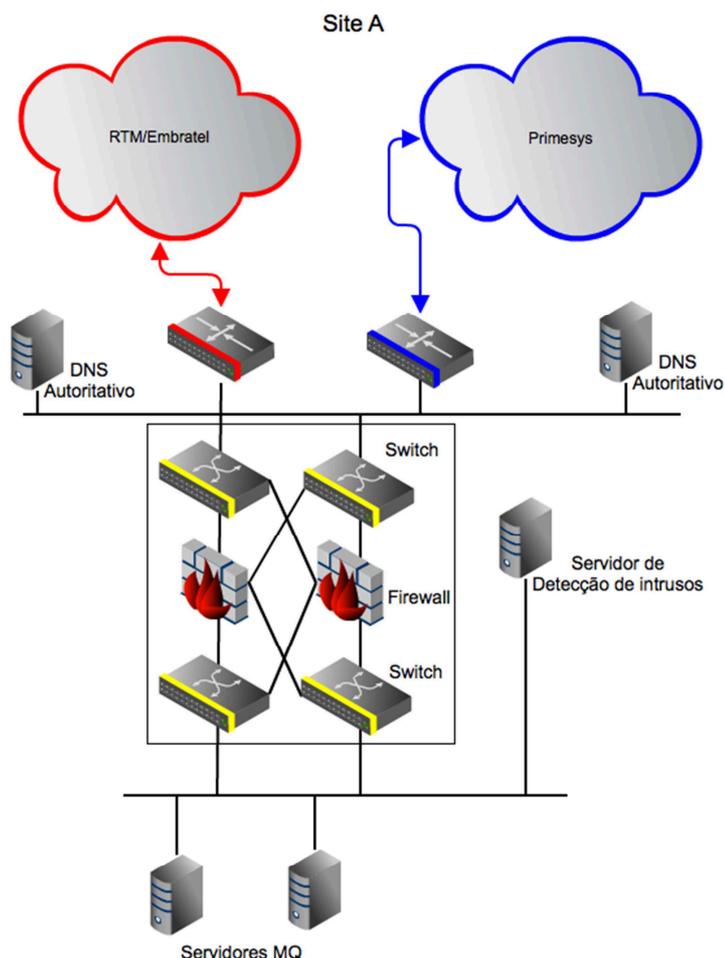
### **RSFN - Manual de Redes do SFN Versão 7.6.3**

---

- os servidores de DNS da RSFN devem fazer parte do segmento da RSFN de cada Entidade, de forma a se evitar possíveis problemas de conversão de endereços;
- somente o segmento da RSFN deve utilizar endereços no padrão fornecido pela RSFN. Os demais segmentos de rede devem utilizar endereços da Intranet da Entidade;
- os servidores da RSFN serão configurados com endereços lógicos da RSFN no servidor de DNS de seu respectivo domínio. O servidor de *Firewall* deverá executar a conversão de endereços via NAT, no formato 1 para 1, ou seja, um endereço lógico da RSFN para cada endereço físico utilizado na Intranet;
- todas as estações de trabalho da Intranet que desejarem acessar serviços da RSFN, terão seus endereços da Intranet convertidos para um único endereço da RSFN. Esta conversão também deverá ser executada no servidor de *Firewall*, configurado com a função NAT;
- os roteadores da Intranet deverão ser configurados com rota específica para os endereços válidos na RSFN a ser fornecido pelo Banco Central. Estas rotas deverão apontar para o servidor de *Firewall* utilizado na interligação da Intranet com a RSFN;
- os servidores de *Firewall* deverão ser configurados com rota específica para o endereço do host **hsrp.sub-domínio.rsfnet.br**.

### Topologia de redundância máxima sem *site* de contingência

Neste modelo a Entidade possui contingência de todos os equipamentos utilizados em um determinado *site* mas não possui *site* de contingência / *backup*. A Figura 18 ilustra este modelo:



**Figura 18 - Topologia de Redundância Máxima Sem *Site* de Contingência**

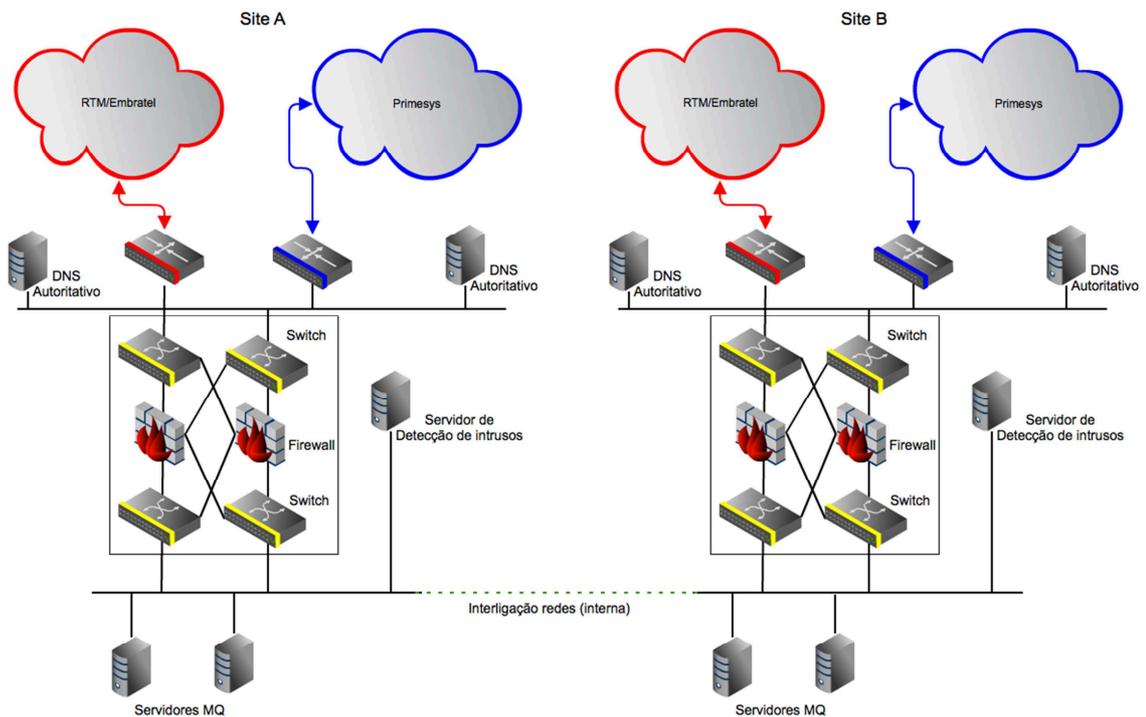
As seguintes observações são pertinentes:

- são utilizados switches de conteúdo com configuração de GLB (Global Load Balance) e FLB (*Firewall Load Balance*) para realizar o balanceamento de carga entre os servidores que oferecem serviços para a RSFN e entre os servidores de *Firewall*;
- em hipótese alguma, o segmento da rede RSFN deve estar interligado ao segmento da Intranet sem a utilização de servidores de *Firewall* (servidores de *Firewall* especializados ou roteadores com função de *Firewall* ou que suportem a configuração de listas de acesso);
- para evitar que o *Firewall* seja ponto único de falha, a Entidade deve considerar a utilização de equipamentos redundantes, neste caso um em cada localidade;
- os servidores de DNS da RSFN devem fazer parte do segmento da RSFN de cada Entidade, de forma a se evitar possíveis problemas de conversão de endereços;

- somente o segmento da RSFN deve utilizar endereços no padrão fornecido pela RSFN. Os demais segmentos de rede devem utilizar endereços da Intranet da Entidade;
- os servidores da RSFN serão configurados com endereços lógicos da RSFN no servidor de DNS de seu respectivo domínio. O servidor de *Firewall* deverá executar a conversão de endereços via NAT, no formato 1 para 1, ou seja, um endereço lógico da RSFN para cada endereço físico utilizado na Intranet;
- todas as estações de trabalho da Intranet que desejarem acessar serviços da RSFN, terão seus endereços da Intranet convertidos para um único endereço da RSFN. Essa conversão também deverá ser executada no servidor de *Firewall*, configurado com a função NAT;
- os roteadores da Intranet deverão ser configurados com rota específica para os endereços válidos na RSFN a ser fornecido pelo Banco Central. Essas rotas deverão apontar para o servidor de *Firewall* utilizado na interligação da Intranet com a RSFN;
- os servidores de *Firewall* deverão ser configurados com rota específica para o endereço do *host* **hsrp.sub-domínio.rsfnet.br**.

**Topologia de redundância máxima com site de contingência**

Neste modelo todos os equipamentos utilizados em um determinado *site* são contingenciados e existe contingência de *site*. Cabe à Entidade definir se os dois estarão ativos ou se o *site* de contingência somente será acionado em caso de falhas no principal. A Figura 19 ilustra esta topologia.



**Figura 19 - Topologia de Redundância Máxima Com Site de Contingência**

## **RSFN - Manual de Redes do SFN Versão 7.6.3**

---

As seguintes observações são pertinentes:

- são utilizados switches de conteúdo com configuração de GLB (*Global Load Balance*) e FLB (*Firewall Load Balance*) para realizar o balanceamento de carga entre os servidores que oferecem serviços para a RSFN e entre os servidores de *Firewall*;
- em hipótese alguma, o segmento da rede RSFN deve estar interligado ao segmento da Intranet sem a utilização de servidores de *Firewall* (servidores de *Firewall* especializados ou roteadores com função de *Firewall* ou que suportem a configuração de listas de acesso);
- interligação entre os segmentos da rede interna pode ser executada utilizando-se diferentes tecnologias de LANs e MANs;
- os servidores da RSFN podem estar fisicamente instalados em um segmento isolado ou pode fazer parte dos segmentos da Intranet da Entidade;
- os servidores de DNS da RSFN devem fazer parte do segmento da RSFN de cada Entidade, de forma a se evitar possíveis problemas de conversão de endereços;
- somente o segmento da RSFN deve utilizar endereços no padrão fornecido pela RSFN. Os demais segmentos de rede devem utilizar endereços da Intranet da Entidade;
- os servidores da RSFN serão configurados com endereços lógicos da RSFN no servidor de DNS de seu respectivo domínio. O servidor de *Firewall* deverá executar a conversão de endereços via NAT, no formato 1 para 1, ou seja, um endereço lógico da RSFN para cada endereço físico utilizado na Intranet;
- todas as estações de trabalho da Intranet que desejar acessar serviços da RSFN, terão seus endereços de Intranet convertidos para um único endereço da RSFN. Essa conversão também deverá ser executada no servidor de *Firewall*, configurado com a função NAT;
- os roteadores da Intranet deverão ser configurados com rota específica para os endereços válidos na RSFN a ser fornecido pelo Banco Central. Essas rotas deverão apontar para o servidor de *Firewall* utilizado na interligação da Intranet com a RSFN;
- os servidores de *Firewall* deverão ser configurados com rota específica para o endereço do *host* **hsrp.sub-domínio.rsfn.net.br**.

### **SERVIDOR DE TEMPO (*TIME SERVER*)**

Está disponível um servidor de tempo no BACEN que poderá ser utilizado pelos Participantes da RSFN para o sincronismo de horário dos servidores MQSeries 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**

Port de acesso: 123 (UDP)

### **SERVIDOR WEB DA RSFN**

O Banco Central 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](http://www.rsfn.net.br).

## SERVIDOR FTP

O serviço FTP no modo ativo utiliza a porta 20 – para transferência de dados – e a porta 21 – para comandos. Para a RSFN, o serviço FTP em modo passivo (Passive Mode) utilizará o range de portas 1110 a 1121.

Como exemplo, o arquivo de configuração, para a solução VSFTP, acrescentará os seguintes parâmetros:

- pasv\_enable=YES
- pasv\_min\_port=1110
- pasv\_max\_port=1121
- port\_enable=YES

## INFRA-ESTRUTURA DE MENSAGERIA

### Diretrizes básicas

A mensageria é baseada em um *software* gerenciador de filas, o MQSeries (ou simplesmente 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 MQSeries do tipo cliente-servidor entre os participantes da RSFN, todos deverão se conectar a rede usando o modo **servidor-servidor**. As conexões entre provedores 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 quatro domínios de sistemas: **SPB01, MES01, MES02 e MES03**.

O domínio SPB01 diz respeito ao tráfego de mensagens dos grupos de serviços do 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**.

A permissão para tráfego das mensagens nos domínios dar-se-á conforme regulamentado no volume 3 do Catálogo de Mensagens e de Arquivos da RSFN, 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 da Mensageria do SPB01, pelo **ISPB**. O Banco Central será identificado por seu ISPB, ou seja, **00038166**.

O BACEN 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 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 mensagens e arquivos da RSFN.

### Definições do MQseries

Será ignorada a fila informada no campo *ReplyToQ* do header do MQSeries 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**.

Não será permitida a gravação de mensagens nas filas de uma instituição definidas no BACEN por outra entidade que não seja a própria, exceto na situação de contingência operada pelo BACEN 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 BACEN processará apenas as mensagens cujo conteúdo seja da própria instituição que as emitiu, exceto na situação de contingência operada pelo BACEN e autorizada pela instituição.

Não será utilizada a segmentação de mensagens no âmbito do MQSeries. A segmentação de mensagens, quando houver, ocorrerá da forma disposta no Catálogo de Mensagens e Arquivos da RSFN, no âmbito do *parser* XML.

Os ambientes de homologação e de produção deverão utilizar *queue managers* distintos, tanto no domínio de sistema SPB quando nos domínios de sistema MES.

Todas as mensagens e arquivos trafegarão na RSFN obrigatoriamente em codificação **UNICODE UTF-16 BE**. A instalação que não o utiliza internamente deverá providenciar a conversão para código interno ao receber mensagens e o contrário ao 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 MQSeries, o header de segurança e a codificação do texto XML em UNICODE UTF-16 BE.

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 Banco Central é o protocolo de recebimento da mensagem. Dessa forma, os campos importantes da mensagem COA (e COD, opcionalmente), emitida pelo Banco Central, 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 MQSeries que será usado no ambiente do Banco Central, dos prestadores de serviços e das demais instituições participantes do SPB01, MES01, MES02 e MES03:

#### **Filas locais (na IF):**

BC/Prestador <b>requisita</b> à IF	<b>QL.REQ.ISPBRemoto.ISPBLocal.seq</b>
BC/ Prestador <b>responde</b> à IF	<b>QL.RSP.ISPBRemoto.ISPBLocal.seq</b>
BC/ Prestador <b>reporta</b> à IF	<b>QL.REP.ISPBRemoto.ISPBLocal.seq</b>
BC/ Prestador envia mensagens de <b>suporte</b> à IF	<b>QL.SUP.ISPBRemoto.ISPBLocal.seq</b>

**Filas remotas (na IF):**

IF <b>requisita</b> ao BC/ Prestador	<b>QR.REQ.ISPBLocal.ISPBRemoto.seq</b>
IF <b>responde</b> ao BC/ Prestador	<b>QR.RSP.ISPBLocal.ISPBRemoto.seq</b>
IF <b>reporta</b> ao BC/ Prestador	<b>REP.ISPBLocal.ISPBRemoto.seq</b>
IF envia mensagens de <b>suporte</b> ao BC/ Prestador	<b>QR.SUP.ISPBLocal.ISPBRemoto.seq</b>

**Filas locais (no BC/Prestador):**

IF <b>requisita</b> ao BC/Prestador	<b>QL.REQ.ISPBRemoto.ISPBLocal.seq</b>
IF <b>responde</b> ao BC/Prestador	<b>QL.RSP.ISPBRemoto.ISPBLocal.seq</b>
IF <b>reporta</b> ao BC/Prestador	<b>QL.REP.ISPBRemoto.ISPBLocal.seq</b>
IF envia mensagens de <b>suporte</b> ao BC/Prestador	<b>QL.SUP.ISPBRemoto.ISPBLocal.seq</b>

**Filas remotas (no BC/Prestador):**

BC/Prestador <b>requisita</b> à IF	<b>QR.REQ.ISPBLocal.ISPBRemoto.seq</b>
BC/Prestador <b>responde</b> à IF	<b>QR.RSP.ISPBLocal.ISPBRemoto.seq</b>
BC/Prestador <b>reporta</b> à IF	<b>QR.REP.ISPBLocal.ISPBRemoto.seq</b>
BC/Prestador envia mensagens de <b>suporte</b> à IF	<b>QR.SUP.ISPBLocal.ISPBRemoto.seq</b>

**Filas de Transmissão:**

**QM.ISPBRemoto.seq**

**Queue Manager Alias Name:**

**QM.ISPBLocal.seq**

- 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; e
- seq será igual a 04 para o domínio MES03.

Exemplo: no domínio MES01, a fila de requisição da instituição 99999999 no BACEN é a QL.REQ.99999999.00038166.02 e o *queue manager* da instituição 99999999 é QM. 99999999.02.

Canais

**Sender:** CISPBLocal.ISPBRemoto.n

**Receiver:** CISPBRemoto.ISPBLocal.n

- 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; e
- n será igual a 4 para o domínio MES03.

Exemplo: no domínio MES01, no *queue manager* da IF, temos o canal receptor (*receiver*) C000038166.99999999.2 (tráfego do BACEN à IF 99999999) e o canal emissor (*sender*) C99999999.00038166.2 (tráfego da IF ao BACEN).

Padrão mandatório de endereços de *hostnames*

**Ambiente Produção SPB01: mqs01.sub-domínio.rsfn.net.br**

**Ambiente Homologação SPB01: mqs02.sub-domínio.rsfn.net.br**

**Ambiente PPRO SPB01: mqs02.sub-domínio.rsfn.net.br**

**Ambiente Produção MES: mqm01.sub-domínio.rsfn.net.br**

**Ambiente Homologação MES: mqm02.sub-domínio.rsfn.net.br**

Exemplo: o endereço do MQSeries do Banco Central 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 Banco Central utilizará a porta 1414 para o ambiente de produção. As instituições utilizarão apenas as portas 1414 a 1421. O Banco Central utilizará a porta 1514 para o ambiente de homologação e, as instituições, as portas 1514 a 1521. Para o ambiente PPRO, o Banco Central utilizará a porta 24430 e as instituições utilizarão as portas 24430 a 24437. O ambiente PPRO somente está configurado no domínio SPB01.

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

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

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

Domínio	Ambiente	Porta
SPB01	<b>Produção Bacen</b>	<b>1414</b>
	Produção Instituição	1414 a 1421
	<b>Homologação Bacen</b>	<b>1514</b>
	Homologação Instituição	1514 a 1521
	<b>PPro Bacen</b>	<b>24430</b>
	PPro Instituição	24430 a 24437
MES01	<b>Produção Bacen</b>	<b>12422</b>
	Produção Instituição	12422 a 12429
	<b>Homologação Bacen</b>	<b>12522</b>
	Homologação Instituição	12522 a 12529
MES02	<b>Produção Bacen</b>	<b>13422</b>
	Produção Instituição	13422 a 13429
	<b>Homologação Bacen</b>	<b>13522</b>
	Homologação Instituição	13522 a 13529
MES03	<b>Produção Bacen</b>	<b>14422</b>
	Produção Instituição	14422 a 14429
	<b>Homologação Bacen</b>	<b>14522</b>
	Homologação Instituição	14522 a 14529

**Tabela 5 – Domínios, ambientes e portas**

**Observações:**

- 1) **ISPBRemoto** é o ISPB ou o CNPJ base da instituição a qual pertence o *queue manager* remoto, com 8 dígitos;
- 2) **ISPBLocal** é o ISPB ou o CNPJ base da instituição à qual pertence o *queue manager* local, com 8 dígitos;
- 3) **Sub-domínio** é a identificação DNS da instituição na RSFN;
- 4) Definir todos os objetos MQ usando letras MAIÚSCULAS;
- 5) As filas de suporte são específicas para uso das equipes de suporte ao *queue manager* dos participantes do sistema;
- 6) A diferenciação dos domínios MES baseia-se na porta TCP de conexão do MQSeries, além do endereço na RSFN;
- 7) Nos domínios MES, diferentemente do SPB01, os canais emissores e receptores do BACEN 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')
  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**

### RSFN - Manual de Redes do SFN Versão 7.6.3

**QM.ISPBLocal.ISPBRemoto.seq.** 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')
RQMNAME ('QM.ISPBRemoto.seq ou QM.ISPBRemoto.ISPBLocal.seq')
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.**, e nos ambientes aos quais o conglomerado ou aglomerado está conectado, é **QM.ISPBRemoto.ISPBLocal.seq.**

#### HEADER DO MQSERIES (MQMD)

Alguns campos do *header* das mensagens que trafegam no MQSeries (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) ou deixar em branco no caso de usar ReplyToQ alias.

**ATRIBUTOS PARA OBJETOS DO MQSERIES**

<b>Atributos Comuns a Todas as Filas</b>		
<b>ATRIBUTO</b>	<b>DEFAULT</b>	<b>CONSENSO</b>
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 6 - Atributos Comuns a Todas as Filas**

<b>Atributos de Filas Locais</b>		
<b>ATRIBUTO</b>	<b>DEFAULT</b>	
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

**RSFN - Manual de Redes do SFN Versão 7.6.3**

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 7 - Atributos de Filas Locais**

<b>Atributos de Filas Remotas</b>		
<b>ATRIBUTO</b>	<b>DEFAULT</b>	
RemoteQMgrName		
RemoteQName		
XmitQName		

**Tabela 8 - Atributos de Filas Remotas**

<b>Atributos de Alias Queues</b>		
<b>ATRIBUTO</b>	<b>DEFAULT</b>	
BaseQName		

**Tabela 9 - Atributos de Alias Queues**

<b>Atributos de NameLists</b>		
<b>ATRIBUTO</b>	<b>DEFAULT</b>	
AlterationDate		livre
AlterationTime		livre
NameCount		livre
NamelistDesc		livre
NamelistName		livre
Names		livre

**Tabela 10 - Atributos de NameLists**

<b>Atributos de Processos</b>		
<b>ATRIBUTO</b>	<b>DEFAULT</b>	
AlterationDate		livre
AlterationTime		livre
ApplId		livre
ApplType		livre
EnvData		livre
ProcessDesc		livre
ProcessName		livre
UserData		livre

**Tabela 11 - Atributos de Processos**

<b>Atributos de Queue Managers</b>		
<b>ATRIBUTO</b>	<b>DEFAULT</b>	
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 12 - Atributos de Queue Managers**

<b>Atributos de Canais</b>		
<b>ATRIBUTO</b>	<b>DEFAULT</b>	
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 13 - Atributos de Canais**

## **CONFIGURAÇÃO DO SERVIDOR MQ - OPÇÃO ADOPTNEWMCA**

Foi detectada uma limitação na configuração do MQSeries 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 MQSeries no ambiente Windows:***

1. No servidor MQseries, abrir *MQseries 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 MQSeries 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 MQSeries no ambiente z/OS:***

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

```
ADOPTCHK=ALL  
ADOPTMCA=YES
```

Observação: no MQSeries for OS/390 V2R1, esses parâmetros são adicionados via PTF que deve ser solicitada ao fabricante.

## **CONFIGURAÇÃO DO MQ - BANCO CENTRAL**

Para que o Banco Central 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 MQSeries no Banco Central:

1. Solicitar ao master Sisbacen de sua instituição a autorização para a transação associada ao domínio, a saber:
  - a) Domínio MES01: SMES400
  - b) Domínio MES02: SMES402
  - c) Domínio MES03: SMES403
  - d) 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”;

Observações:

- No caso do domínio SPB01, é dada a possibilidade de criação de objetos perante o SELIC.

## **GERÊNCIA DE SEGUNDA NÍVEL DA RSFN**

### Diretrizes básicas

A gerência de segundo nível da Rede do Sistema Financeiro Nacional tem como finalidades principais:

- a) administração e controle de todo o tráfego de mensagens, arquivos e demais serviços autorizados pelo Banco Central;
- b) controle centralizado dos serviços prestados pelas operadoras; e
- c) assessoramento à Coordenação do Subgrupo de Redes nas questões relacionadas ao funcionamento da RSFN.

Este serviço será prestado por empresa contratada para este fim pelos signatários do "Instrumento de Acordo Operacional", firmado com as provedoras de telecomunicações da RSFN, que deverá ter a concordância do Banco Central.

Cabe à prestadora de serviços:

- a) cumprir os procedimentos descritos no Manual Operacional de Gerência de Segundo Nível;
- b) seguir as diretrizes estabelecidas pelo Banco Central;
- c) preparação de relatórios específicos sobre a RSFN solicitados pela Coordenação do Subgrupo de Redes; e encaminhamento de relatórios gerenciais periódicos à Coordenação do Subgrupo de Redes sobre a utilização da RSFN.

Também fazem parte dos serviços de gerenciamento de Segundo Nível as atividades abaixo relacionadas:

- acompanhar as atividades de configuração e falhas da RSFN, com funções de planejamento, monitoração, execução e documentação;
- garantir a manutenção e atualização da arquitetura da RSFN, seus critérios de configuração e o cumprimento dos acordos de níveis de serviços estabelecidos nos contratos entre os participantes e as provedoras;
- acompanhar o desempenho da rede até o nó de entrada dos participantes da RSFN;
- acompanhar e auditar o funcionamento da RSFN e o cumprimento dos níveis de atendimento dos provedores;
- acompanhar e auditar todo o tráfego dos participantes, comunicando ao Banco Central eventuais desvios na utilização da RSFN;
- auxiliar na solução de chamados 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;
- planejar a implantação de novos serviços.

As atividades desempenhadas pela Gerência de Segundo Nível serão executadas no período das 7 às 22 horas, de segunda-feira à sexta-feira, exceto quando não houver movimentação no Sistema de Transferência de Reservas do Banco Central.

Todos os participantes da Rede do Sistema Financeiro Nacional - RSFN devem assinar o termo de adesão do Contrato de Prestação de Serviços de Gerência de Segundo Nível.

A equipe da gerência de segundo nível estará tecnicamente ligada à Coordenação do Subgrupo de Redes, a quem devem ser encaminhados todos os pedidos de relatórios e informações referentes à RSFN.

## **REQUISITOS PARA O MODELO OPERACIONAL DE PSTI**

Tendo como objetivo manter o mesmo nível de controle e eficiência dos sistemas de pagamento que utilizam a RSFN, alguns requisitos devem ser atendidos por cada um dos envolvidos na operação e manutenção do sistema quando utilizado o modelo operacional de Prestador de Serviço de Tecnologia da Informação – PSTI, em complemento ao definido na CIRCULAR Nº 3.629, DE 19 DE FEVEREIRO DE 2013:

Obrigações das Instituições Financeiras quando operam no modelo de PSTI:

- Solicitação de subdomínio DNS para a RSFN: Esta solicitação servirá aos operadores do suporte à RSFN como controle das instituições usuárias do PSTI;
- Solicitação de configuração do subdomínio da RSFN nos root-servers do Banco Central do Brasil: Devem ser indicados na solicitação os servidores DNS do provedor como autoritativos para o subdomínio;
- Prestar informações ao DEINF quando solicitado.

Obrigações dos PSTIs:

- Configuração dos canais MQS no Banco Central do Brasil utilizando o subdomínio específico da instituição, e não o subdomínio do PSTI;
- Fornecer mensalmente para a Gerência de Segundo Nível da RSFN, relação com todas as instituições interligadas ao provedor, com detalhamento quanto: instituições ativas, 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, informações como o ISPB, subdomínio da RSFN e informações de contato técnico, bem como outros dados que poderão ser acrescidos em um segundo momento;
- Fornecer telefone de contato técnico do provedor PSTI, tanto para seus clientes quanto para a Gerência de Segundo Nível, para o suporte às aplicações do SPB, que tenha atendimento capacitado a verificar a conectividade dos canais do STR, em ambos os sentidos, bem como para as demais ferramentas fornecidas aos seus clientes como parte do serviço prestado;
- Fornecer caderno de testes/homologação, e verificação em caso de problemas, da solução completa de mensageria desde o cliente até o Banco Central do Brasil;
- Fornecer ao Banco Central do Brasil e Gerência Integrada de 2º Nível da RSFN, o modelo adotado de segurança na comunicação entre o cliente e o provedor PSTI;
- Possuir centro de gerenciamento de rede que realize atividades compatíveis com as realizadas pela Gerência de Segundo Nível, tanto quanto à avaliação do desempenho de rede, quanto na resolução de problemas complexos que necessitem da articulação entre diversos envolvidos;
- Fornecer à Gerência de Segundo Nível documento com plano de testes de aceitação a serem realizados nos acessos no momento da ativação. Os procedimentos apresentados neste documento devem substituir os atualmente executados para os acessos ativados na RSFN de acordo com as definições do Manual Técnico [1];

Utilização de rede dedicada homologada pelo BACEN:

- Somente por meio da RSFN ou de rede dedicada, homologada pelo Banco Central do Brasil é permitida a troca de informações entre o PSTI e as instituições detentoras de conta Reservas Bancárias que dele se utilizam e entre o PSTI e os demais participantes do STR;
- A troca de informações entre o PSTI e os demais participantes do STR deve ocorrer por meio da RSFN;

Gerência Integrada de Segundo Nível:

- Controle das instituições usuárias do serviço do PSTI através das configurações do serviço de DNS, e de relatório mensal fornecido pelo provedor;
- Suporte ao cliente do PSTI indiretamente, na verificação de problemas relacionados aos acessos do provedor à RSFN, como ponto de contato para o suporte próprio PSTI e/ou Provedor da rede homologada;
- Gerenciamento do desempenho de rede apenas para o PSTI, por não ser possível identificar comunicações individuais dentro do tráfego nos circuitos do PSTI na RSFN;
- Suporte ao Banco Central do Brasil para a verificação de falhas de conectividade de canal do STR até os servidores do PSTI;
- Realização de auditoria “in-loco” para verificação da infra-estrutura do PSTI e da infra-estrutura de acesso da operadora.

Infra-RSFN:

- Alocação de subdomínio da RSFN para a instituição solicitante;
- Encaminhamento de solicitações de configuração e suporte aos serviços de DNS à Gerência de Segundo Nível da RSFN.

## QUALIDADE DE SERVIÇO NA RSFN

### Configuração atual de 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. Três classes de serviço foram definidas: INFRA-ESTRUTURA, SPB-MENSAGERIA e *DEFAULT*.

A classe de SPB-MENSAGERIA, com 65% da banda total de cada *link* podendo, por determinação do Banco Central do Brasil, atingir até 95%, é a classe missão crítica para a RSFN. Deve ter os seguintes parâmetros:

- a) tempo de resposta (*one-way trip time*) entre as portas de acesso dos CPEs de duas entidades quaisquer, apurado mensalmente com 4 medidas a cada hora entre 7 e 21 horas a cada dia (com largura de banda otimizada, sem congestionamento): inferior a 120 ms a cada média horária;
- b) taxa média diária de perda de pacotes (*round-trip*) no backbone, apurado mensalmente: inferior a 1% ao dia.

A classe de INFRA-ESTRUTURA, com 5% da banda total de cada link provê uma banda mínima para o tráfego de roteamento e divulgação de rotas BGP e outras aplicações de controle de rede, como gerenciamento SNMP, sincronismo de relógio através do protocolo NTP, informações de domínio DNS e acessos telnet. Essa garantia de banda é necessária porque o tráfego desses protocolos não é beneficiado pelo mecanismo interno de *PAK\_PRIORITY* dos roteadores da Cisco.

A classe *DEFAULT* é usada para a transferência de arquivos através de FTP e demais serviços expressamente autorizados pelo Banco Central do Brasil que venham a utilizar a RSFN. Essa classe é a típica classe *Best Effort*, na qual não há garantia de banda mínima.

As marcações de pacotes deverão ser feitas de acordo com as recomendações do fabricante dos equipamentos utilizados pela rede. A atribuição de classes de serviço usando portas e access list 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*.

Os dois provedores de telecomunicações da RSFN adotarão o padrão de classe de serviço definido abaixo:

**RSFN - Manual de Redes do SFN Versão 7.6.3**

Classe de Serviço	Largura de banda	Lista	Serviço/ Porta (in/out)	Aplicação
INFRA-ESTRUTURA	5%	102 102 102 102 102 102	Telnet/TCP BGP/TCP NTP/UDP DOMAIN/UDP SNMP/UDP Tacacs/TCP	Telnet/TCP Infra-estrutura
SPB-MENSAGERIA	65%	101	BC: 1414 IF/Prestador: 1414 a 1421 /TCP	Mensageria SPB (SPB01)
DEFAULT	30%		FTP/TCP e UDP	FTP
			BC: 12422 IF/Prestador: 12422 a 12429 /TCP	Mensageria Sisbacen (MES01)
			IF/Prestador: 13422 a 13429 /TCP	Mensageria Sisbacen (MES02)
			BC: 14422 IF/Prestador: 14422 a 14429 /TCP	Mensageria Sisbacen (MES03)

**Tabela 14 – Atual configuração de Qualidade de Serviço na RSFN**

Nova configuração de Qualidade de Serviço na RSFN

O Subgrupo de Redes decidiu, em reunião ocorrida no dia 30 de outubro de 2013, que a configuração atual de QoS será alterada para tratar adequadamente os novos serviços que trafegam na RSFN. O projeto de migração para a nova configuração de QoS encontra-se em andamento. Após a conclusão da migração, a configuração de QoS será a representada na tabela abaixo:

Classe de Serviço	Largura de banda	Lista	Serviço/ Porta	Aplicação
INFRA-ESTRUTURA	5%	104 104 104 104 104 104	Telnet/TCP BGP/TCP NTP/UDP DOMAIN/UDP SNMP/UDP Tacacs/TCP	Telnet DNS NTP Gerência
SPB01 – Mensageria	60%	102	<b>BC Produção: 1414</b> IF/Prestador Produção: 1414 a 1421/TCP	Mensageria Produção: SPB01
MES01 - Mensageria	20%	103	<b>BC Produção: 12422</b> IF/Prestador Produção: 12422 a 12429/TCP	Mensageria Produção: MES01
MES03 - Mensageria	1%	101	<b>BC Produção: 14422</b> IF/Prestador Produção: 14422 a 14429/TCP	Mensageria Produção: MES03

**RSFN - Manual de Redes do SFN Versão 7.6.3**

<i>DEFAULT</i>	14%		<p align="center"><b>SPB01</b>  <b>BC Homologação: 1514</b>                      IF/Prestador Homologação: 1514 a 1521  <b>BC PPRO: 24430</b>                      IF/Prestador PPRO: 24430 a 24437</p> <p align="center"><b>MES01</b>  <b>BC Homologação: 12522</b>                      IF/Prestador Homologação: 12522 a 12529</p> <p align="center"><b>MES02</b>  <b>BC Produção: 13422</b>  <b>BC Homologação: 13522</b>                      IF/Prestador Produção: 13422 a 13429                      IF/Prestador Homologação: 13522 a 13529</p> <p align="center"><b>MES03</b>  <b>BC Homologação: 14522</b>                      IF/Prestador Homologação: 14522 a 14529</p> <p align="center"><b>FTP (TCP) – 20 e 21</b>  <b>FTP (TCP) – PASSV – 1110 a 1121</b></p>	<p><b>Mensageria Produção: MES02</b></p> <p><b>Mensageria Homologação: SPB01 MES01 MES02 MES03</b></p> <p><b>Mensageria PPRO: SPB01</b></p> <p><b>Sisbacen FTP</b></p> <p><b>Outros Serviços</b></p>
----------------	-----	--	---	--

**Tabela 15 – Nova configuração de Qualidade de Serviço na RSFN**

## **ANEXO I – CONFIGURAÇÃO DE DNS (DOMAIN NAME SYSTEM)**

### INTRODUÇÃO

A RSFN (Rede do Sistema Financeiro Nacional) permitirá a comunicação direta entre o Banco Central do Brasil e as instituições autorizadas nos termos dos artigos 1º e 28 do regulamento anexo à Circular nº 3.629, de 19 de fevereiro de 2013.

Baseada no protocolo TCP/IP, esta rede foi implantada considerando a utilização de ferramentas/conceitos de Intranet (aplicações cliente-servidor com interface Web e correio eletrônico, por exemplo). Estas características tornam a utilização do DNS obrigatória.

Por ser tratar de um projeto lógico (não amarrado a características físicas da rede), o projeto de Arquitetura de DNS atende tanto a topologia inicial do *Backbone* da RSFN, conforme os itens listados a seguir, bem como poderá ser facilmente escalado para atender novas Entidades que se conectarão a rede posteriormente.

O Comitê Gestor da Internet no Brasil reservou um prefixo 0/18 para a RSFN;

foram registrados na Internet domínios de nível superior e domínio reverso, de modo a permitir a futura integração da RSFN com a Internet;

2 provedores de serviços de telecomunicações (Primesys e o consórcio formado pelas empresas EMBRATEL e RTM, denominado EBT/RTM, os quais fornecem serviços de VPN/MPLS para garantir a privacidade dos dados que trafegam nesta rede).

Este Anexo, tem por objetivo apresentar a Arquitetura de DNS recomendada para a RSFN. Os seguintes itens são cobertos:

- apresentação da arquitetura de DNS da RSFN;
- apresentação do modelo de configuração do serviço de DNS nesta rede;
- sugestão de regras para nomeação de domínios, sub-domínios e *hosts* desta rede, além da metodologia para registros dos mesmos;
- sugestão de padrão de nomes para usuários dos serviços de correio eletrônico via SMTP;
- procedimentos para integração dos serviços de DNS necessários para atender a Intranet de cada Entidade, sua conexão com a Internet e sua conexão com a RSFN.

Ao final deste, são apresentados conceitos técnicos do DNS, os quais serão úteis para o completo entendimento deste projeto, além dos passos que deverão ser seguidos para se configurar o DNS em servidores Windows com a aplicação de DNS da Microsoft, uma vez que o corpo do relatório terá como base a configuração do DNS em servidores Unix e utilização da aplicação *Bind*.

## PREMISSAS BÁSICAS

Premissas básicas contempladas na elaboração do Projeto de Arquitetura de DNS da RSFN:

- domínios de DNS registrados junto à Fapesp ou qualquer outro órgão internacional, para acesso à Internet:
  - serão considerados os seguintes domínios diretos: **rsfn.net.br** e seguinte domínio reverso: **64.218.200.in-addr.arpa**;
  - cada Entidade escolherá o nome a ser utilizado em seu próprio sub-domínio, respeitando-se as regras de unicidade do mesmo. Recomenda-se a adoção de um nome já utilizado e registrado na conexão à Internet. Será definido um órgão responsável pela administração dos registros e nomeação dos sub-domínios;
- servidores de DNS (primários e secundários) responsáveis pelos domínios anteriores:
  - cada uma das concessionárias dos serviços de telecomunicações (Primesys e EBT/RTM) terá três segmentos de rede (sendo um em São Paulo, um no Rio de Janeiro e um em Brasília) que farão parte da VPN da RSFN. Estes segmentos abrigarão os servidores de DNS configurados como *internal root servers* para os domínios anteriores. Cada concessionária providenciará um servidor *internal root server* para cada segmento. Estes servidores apontarão os servidores de DNS para cada um dos sub-domínios da rede;
- sub-domínios da rede RSFN. Para facilitar a administração da rede, foi criado um sub-domínio direto e um sub-domínio reverso para cada Entidade Participante conectada à rede. Cada Entidade ficará responsável por administrar seus respectivos sub-domínios. Exemplos dos sub-domínios:
  - Primesys **att.rsfn.net.br**
  - EBT/RTM **ebtrtm.rsfn.net.br**
- terceirização da administração dos sub-domínios de DNS:
  - As Entidades ligadas à RSFN poderão terceirizar com as concessionárias a administração do serviço de DNS. Neste caso, as concessionárias utilizarão servidores de DNS autoritativos, servidores estes também localizados nos segmentos de rede que farão parte da VPN da RSFN, e que obrigatoriamente estarão em máquinas diferentes dos servidores de DNS configurados como *internal root servers*. Os servidores autoritativos serão configurados com informações específicas do domínio da entidade que solicitar este serviço;
- tipo de servidores que abrigarão os serviços de DNS:
  - embora não seja obrigatória sua utilização, é recomendada a adoção de servidores de DNS baseados em sistema operacional Unix e uso da aplicação *Bind* 8.x ou 9.x. Todas as configurações utilizarão este padrão como modelo.
- interligação com a Internet:
  - foi registrado o domínio de nível superior (direto e reverso) na Internet;
- interligação com as redes internas das Entidades:
  - Provavelmente, Entidades que fazem (ou farão) parte da RSFN, utilizarão o DNS. Tais servidores resolvem nomes das Intranets destas empresas e da Internet. Como alternativa, para conexão à rede RSFN, podem ser aproveitados os mesmos servidores utilizados atualmente, tornando-os autoritativos para seus respectivos domínios (sub-domínio.rsfn.net.br) e configurando-os para apontarem para os servidores de *root* da Internet ou para os servidores internos de *root* da RSFN conforme necessário. A Entidade pode optar também pela utilização de servidores de DNS específicos para a rede RSFN;
- tipo de servidores que abrigarão os serviços de DNS nas Intranets das empresas:
  - devem ser mantidos os mesmos servidores de DNS utilizados atualmente;

- padrões de nomes de *hosts* (servidores, roteadores, *hubs*, *switches*, etc.) utilizados na RSFN:
  - foi sugerida uma regra de formação de nomes de *hosts* utilizados na RSFN;
- os nomes dos servidores MQ deverão obedecer o seguinte padrão:
  - SPB01: mqsNN.sub-domínio.rsfn.net.br, onde NN varia de 01 a 02. Este padrão é utilizado para todos os servidores MQ, sendo o 01 destinado ao servidor de produção e o 02 ao servidor de homologação e ao servidor PPRO;
  - MES01, MES02 e MES03: mqmNN.sub-domínio.rsfn.net.br, onde NN varia de 01 a 02. Este padrão é utilizado para todos os servidores MQ, sendo o 01 destinado ao servidor de produção e o 02 ao servidor de homologação.

### DNS NA RSFN

O DNS (*Domain Name System*) é um banco de dados distribuído que contém informações sobre os *hosts* de uma rede TCP/IP, permitindo a utilização de nomes ao invés de endereços IP, quer seja pelos usuários da rede quer seja pelas aplicações residentes nos diversos *hosts* desta rede (Recomenda-se a leitura do Anexo I para mais informações sobre o DNS).

Como qualquer outra aplicação TCP/IP, o DNS é mais uma aplicação que utiliza a arquitetura cliente-servidor. Nesta arquitetura, a parte cliente (*resolver*) faz requisições específicas (*queries* de DNS) para a parte servidora (*name server*) quando necessita resolver nomes através do DNS.

### DNS X BIND

Freqüentemente, ocorre uma grande confusão entre o que vem a ser o DNS (*Domain Name System*) e o que vem a ser o BIND (*Berkeley Internet Name Domain*).

A primeira implementação do DNS foi chamada *Jeeves*, e foi escrita por *Paul Mockapetris*. Uma implementação posterior foi chamada de BIND, e foi escrita por *Kevin Dunlap* para o sistema operacional UNIX 4.3BSD de Berkeley.

Desde então, o BIND é a versão mais popular e a mais completa implementação de DNS, encontrando-se portada para a maioria dos sistemas operacionais existentes (Unix, VMS, NT, Windows 2000). Mesmo implementações proprietárias de DNS fazem referência à versão do BIND à qual são compatíveis.

Atualmente o BIND apresenta três linhas de versões:

BIND 4.x

BIND 8.x

BIND 9.x

A linha 4.x utiliza arquivos de configuração de DNS com formatos diferentes das demais linhas. Até a versão 4.8.3, o grupo *Computer Systems Research Group* da universidade de Berkeley na Califórnia era responsável pela manutenção do BIND. As versões 4.9 e 4.9.1 foram liberadas pela *Digital Equipment Corporation*. A versão 4.9.2 foi patrocinada por *Vixie Enterprises*, e a partir da versão 4.9.3, a responsabilidade de manutenção e desenvolvimento do BIND passou a ser do *Internet Software Consortium* (ISC).

Em Maio de 1997, o ISC liberou a primeira versão do BIND-8. O desenvolvimento da versão BIND-4 foi completamente interrompido, com exceção da liberação de alguns *patches* para assuntos relacionados à segurança. A partir de agora, nenhuma nova função deverá ser adicionada ao BIND-4. Portanto, é natural que as novas implementações passem a utilizar pelo menos o BIND-8.

As principais características existentes nas versões do BIND 8 e 9 são:

- suporte a atualizações dinâmicas de DNS - *DNS Dynamic Updates*, descrita na RFC 2136;
- permite que os servidores primários notifiquem os secundários das mudanças ocorridas, de forma a diminuir o tempo de convergência da rede - *DNS Notify*, descrita na RFC 1996;
- o arquivo de carga do serviço de DNS utiliza sintaxe diferente da adotada no *Bind 4*;
- permite o registro (*logging*) de certas atividades relacionadas ao DNS;
- permite o controle de acesso baseado no endereço IP - *ACL Access Control List* para *queries*, *zone transfers* e *updates*; tal controle pode inclusive ser definido para uma zona específica;

- possui mecanismo de suporte a transferência incremental de zona;
- suporta até 16 milhões de zonas por servidor.

As principais diferenças existentes entre as linhas do BIND 9.x e BIND 8.x são apresentadas a seguir:

- suporte a banco de dados para maior flexibilidade na gerência e manutenção das informações de nomes;
- suporte a mecanismos de segurança para transferência e requisições seguras mais abrangentes;
- suporte e melhor aproveitamento de ambientes multiprocessados;
- suporte a mecanismos de auditoria e controle;
- suporte a características específicas do IPV6.

### Aplicações de DNS recomendadas

O projeto de DNS da RSFN recomenda como base para este serviço a utilização da linha BIND 8.x, em virtude dos seguintes motivos:

- a linha BIND 8.x é a linha mais utilizada atualmente em grandes redes que utilizam o TCP/IP como protocolo de comunicação. Desta forma é natural que esta seja a aplicação de DNS mais estável e adequada para uso nestas redes;
- a rede da RSFN utilizará vários servidores de DNS em ambientes Microsoft (Windows NT 4.0 e Windows 2000), dificultando a padronização dos serviços em torno da linha *Bind* 9;
- o formato de configuração dos arquivos de DNS na linha BIND 9.x é idêntico ao utilizado na linha BIND 8.x, o que permite a migração sem qualquer alteração significativa no projeto.

### DNS em Servidores Unix

O BIND 8.2.3 é a aplicação de DNS recomendada para todos os servidores Unix da RSFN que ofertarão o serviço de resolução de nomes DNS. As plataformas Unix normalmente já incluem uma versão do BIND em seu conjunto de aplicações TCP/IP. No entanto, a versão desta aplicação depende do momento de aquisição da máquina.

Para utilizar a versão mais recente do BIND, os arquivos necessários poderão ser encontrados no *site* [www.isc.org](http://www.isc.org), via Web ou no *site* [ftp.isc.org/isc/bind](ftp://ftp.isc.org/isc/bind), comprimidos (gz) e em formato "tar". Eles deverão ser descomprimidos, extraídos do formato "tar" e compilados seguindo as orientações contidas no pacote.

A atualização da versão do BIND poderá ser feita sempre que necessário utilizando os *sites* referenciados acima. O ISC vem cada vez mais facilitando o processo de atualização das versões do BIND, atualizações estas cada vez mais motivadas por acréscimos de funções de segurança no aplicativo.

### DNS em Servidores Windows

A Microsoft disponibiliza junto com o pacote Windows 2000 uma versão proprietária e similar à linha BIND 8.x. e junto com o pacote Windows NT 4.0 uma versão proprietária e similar à linha BIND 4.x.

A principal característica das aplicações de DNS providas pela Microsoft, para uso em servidores Windows 2000 e Windows NT 4.0, é a utilização de uma interface gráfica que tem por objetivo facilitar a administração da base de dados do DNS. A Microsoft entende também que redes que necessitem de resolução de nomes TCP/IP via DNS e nomes NetBIOS via WINS, podem ter ganhos se utilizar sua aplicação de DNS. Como a rede RSFN não utilizará o protocolo NetBIOS, a vantagem pela utilização do DNS da Microsoft restringe-se ao uso de interfaces gráficas para a administração dos serviços.

Desta forma, para unificar a solução recomenda-se a adoção da aplicação BIND 8.2.3 também para os servidores Windows 2000 e Windows NT 4.0. Estas aplicações também podem ser obtidas no *site* do ISC. As aplicações de DNS proprietárias da Microsoft devem ser consideradas como segunda opção, embora tenham funcionado corretamente no piloto da rede.

## ARQUITETURA DE DNS DA RSFN

### Domínios Superiores da RSFN

O primeiro ponto a ser definido em uma arquitetura de DNS são os domínios de nível superior da rede. No caso específico da RSFN, estes domínios foram definidos contemplando a integração total desta rede com a Internet. Além de definir os nomes dos domínios superiores, é fundamental a definição da Entidade responsável por sua administração e os servidores de DNS que são utilizados para armazenar as informações relativas a cada domínio. Na rede da RSFN, a administração dos domínios superiores será realizada pelo BACEN. Para prover balanceamento de carga e contingência da rede, servidores secundários serão estrategicamente espalhados nos segmentos de redes das concessionárias.

A Tabela 1 apresenta os domínios superiores da RSFN, as entidades responsáveis por sua administração e seus respectivos servidores de DNS, os quais serão denominados servidores internos de *root* para a RSFN (*Internal Root Servers – IRS*). A partir destes domínios serão delegados os respectivos direitos para cada sub-domínio desta rede.

Sempre que houver a necessidade da criação de outros domínios superiores para a RSFN, os mesmos terão que ser registrados nos servidores internos de *root* desta rede.

<b>Domínio</b>	<b>Administração do Domínio</b>	<b>Servidores de Nomes</b>
rsfn.net.br	Bacen – Servidor Primário Bacen – Servidor Secundário Bacen – Servidor Secundário	ns1.bcb.rsfn.net.br ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br

Tabela 1 - Domínios de Níveis Superiores da RSFN

### Sub-Domínios da RSFN

Os sub-domínios foram criados para identificar cada uma das Entidades Participantes da VPN da RSFN. Cada Entidade é responsável por administrar seus respectivos sub-domínios.

Cada Entidade escolherá o nome a ser utilizado em seu próprio sub-domínio, respeitando-se as regras de unicidade do mesmo. Recomenda-se adoção de um nome já utilizado e registrado na conexão à Internet.

A Tabela 2 apresenta exemplos de nomes de sub-domínios desta rede.

<b>rsfn.net.Br Nome Completo</b>	<b>rsfn.net.br Nome Abreviado</b>
Banco Central do Brasil	bcb.rsfn.net.br
<a href="#">Bolsa de Valores &amp; Futuros</a>	bmf.rsfn.net.br
Companhia Brasileira de Liquidação e Custódia	cblc.rsfn.net.br
Câmara de Custódia e Liquidação	cetip.rsfn.net.br
Sistema Especial de Liquidação e Custódia	selic.rsfn.net.br
Bank Boston	bkb.rsfn.net.br
Banco Merrill Lynch	ml.rsfn.net.br
Banco Sudameris	sudameris.rsfn.net.br
Deutsche Bank	db.rsfn.net.br
Telmex	att.rsfn.net.br
Embratel	ebtrtm.rsfn.net.br

Tabela 2 - Sub-Domínios da RSFN

### Delegando Direitos Para os Sub-Domínios

O servidor primário da zona **rsfn.net.br** é quem tem o direito de criar e delegar direitos para seus sub-domínios. Esta delegação ocorre através da configuração de registros do tipo NS (*Name Servers*), atrelados a registros do tipo A (*Address*) para cada um dos sub-domínios criados (*glue records*).

A seguir segue um trecho para exemplificar a configuração para delegação de direitos para os sub-domínios de **rsfn.net.br**, os quais deverão estar totalmente compatíveis com a tabela de endereços IP fornecida para cada Entidade.

```
@ IN SOA ns1.bcb.rsfn.net.br. spb_registro.bcb.gov.br. (  
2001081401 ; Número de Série  
28800 ; refresh  
3600 ; retry  
604800 ; expire  
86400 ; default_ttl  
)  
;  
; Servidores de nomes deste domínio  
;  
IN NS ns1.bcb.rsfn.net.br.  
IN NS ns2.bcb.rsfn.net.br.  
IN NS irs1.att.rsfn.net.br.  
IN NS irs2.att.rsfn.net.br.  
IN NS irs3.att.rsfn.net.br.  
IN NS irs1.ebtrtm.rsfn.net.br.  
IN NS irs2.ebtrtm.rsfn.net.br.  
IN NS irs3.ebtrtm.rsfn.net.br.  
;  
; Delegação de Direitos para Clerings/Bacen (4 linhas p/ cada sub-domínio)
```

```
;  
; bcb.rsfn.net.br. IN NS ns1.bcb.rsfn.net.br.  
; bcb.rsfn.net.br. IN NS ns2.bcb.rsfn.net.br.  
; ns1.bacenbsa.rsfn.net.br. IN A 200.218.66.6  
; ns2.bacenbsa.rsfn.net.br. IN A 200.218.66.7  
  
; selic.rsfn.net.br. IN NS ns1.selic.rsfn.net.br.  
; selic.rsfn.net.br. IN NS ns2.selic.rsfn.net.br.  
; ns1.selic.rsfn.net.br. IN A 200.218.66.38  
; ns2.selic.rsfn.net.br. IN A 200.218.66.39  
  
; clearing1.rsfn.net.br. IN NS ns1.clearing1.rsfn.net.br.  
; clearing1.rsfn.net.br. IN NS ns2.clearing1.rsfn.net.br.  
; ns1.clearing1.rsfn.net.br. IN A 200.218.66.70  
; ns2.clearing1.rsfn.net.br. IN A 200.218.66.71  
;  
; Delegação de Direitos para IFs (4 linhas p/ cada sub-domínio)  
;  
; if1.rsfn.net.br. IN NS ns1.if1.rsfn.net.br.  
; if1.rsfn.net.br. IN NS ns2.if1.rsfn.net.br.  
; ns1.if1.rsfn.net.br. IN A 200.218.80.6  
; ns2.if1.rsfn.net.br. IN A 200.218.80.7  
;  
; Delegação de Direitos para SPs (6 linhas p/ cada sub-domínio)  
;  
; att.rsfn.net.br. IN NS irs1.att.rsfn.net.br.  
; att.rsfn.net.br. IN NS irs2.att.rsfn.net.br.  
; att.rsfn.net.br. IN NS irs3.att.rsfn.net.br.  
; irs1.att.rsfn.net.br. IN A 200.218.64.6  
; irs2.att.rsfn.net.br. IN A 200.218.64.38  
; irs3.att.rsfn.net.br. IN A 200.218.64.70  
  
; ebtrtm.rsfn.net.br. IN NS irs1.ebtrtm.rsfn.net.br.  
; ebtrtm.rsfn.net.br. IN NS irs2.ebtrtm.rsfn.net.br.  
; ebtrtm.rsfn.net.br. IN NS irs3.ebtrtm.rsfn.net.br.  
; irs1.ebtrtm.rsfn.net.br. IN A 200.218.64.134  
; irs2.ebtrtm.rsfn.net.br. IN A 200.218.64.166  
; irs3.ebtrtm.rsfn.net.br. IN A 200.218.64.198
```

### Incluindo ou Excluindo Domínios ou Sub-Domínios

A RSFN pode a qualquer momento incluir ou excluir domínios ou sub-domínios de DNS em sua rede, desde que respeite as regras definidas neste manual:

- ter um *Primary Name Server* – PNS e no mínimo um *Secondary Name Server* – SNS para cada zona;
- preparar os arquivos de configuração de forma a tornar operacional o novo domínio, tanto no PNS como no SNS;
- registrar os domínios e seus respectivos servidores nos órgãos competentes;
- considerar os tempos de convergência necessários para que a rede tome conhecimento das modificações realizadas.

### Domínios Reversos da RSFN

Além dos domínios e sub-domínios diretos descritos anteriormente, a RSFN possui domínios reversos para permitir a resolução de nomes de *hosts* de DNS a partir de um dado endereço IP. Esta técnica de resolução tem sido largamente utilizada tanto para permitir funções de gerenciamento de rede como para controlar o acesso a aplicações específicas da rede.

### RSFN - Manual de Redes do SFN Versão 7.6.3

Definidos de maneira análoga a utilizada para os domínios reversos, os domínios diretos também apresentam sub-domínios para cada Entidade Participante da rede e também foi contemplada a integração total desta rede com a Internet. Portanto, tais domínios possuem os mesmos nomes de domínios que são utilizados e registrados na rede mundial, formados a partir do bloco CIDR reservado para esta rede: 200.218.64.0/18.

Na rede da RSFN, a administração dos domínios reversos superiores será também realizada pelo BACEN. Para prover balanceamento de carga e contingência da rede, servidores secundários serão estrategicamente espalhados nos segmentos de redes das concessionárias.

A Tabela 3 apresenta os domínios superiores da RSFN, as entidades responsáveis por sua administração e seus respectivos servidores de DNS, os quais serão denominados servidores internos de *root* para a RSFN (*Internal Root Servers – IRS*). A partir destes domínios foram delegados os respectivos direitos para cada sub-domínio reverso desta rede. Sempre que houver a necessidade da criação de outros domínios superiores para a RSFN, os mesmos terão que ser registrados nos servidores internos de *root* desta rede.

Domínio	Administração do Domínio	Servidores de Nomes
64.218.200.in-addr.arpa	Bacen – Servidor Primário Bacen – Servidor Secundário Bacen – Servidor Secundário	ns1.bcb.rsfn.net.br ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br
66.218.200.in-addr.arpa	Bacen – Servidor Primário Bacen – Servidor Secundário Bacen – Servidor Secundário	ns1.bcb.rsfn.net.br ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br
67.218.200.in-addr.arpa	Bacen – Servidor Primário Bacen – Servidor Secundário Bacen – Servidor Secundário	ns1.bcb.rsfn.net.br ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br
80.218.200.in-addr.arpa	Bacen – Servidor Primário Bacen – Servidor Secundário Bacen – Servidor Secundário	ns1.bcb.rsfn.net.br ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br
.	Bacen – Servidor Primário Bacen – Servidor Secundário Bacen – Servidor Secundário	ns1.bcb.rsfn.net.br ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br
95.218.200.in-addr.arpa	Bacen – Servidor Primário Bacen – Servidor Secundário Bacen – Servidor Secundário Bacen – Servidor Secundário	ns1.bcb.rsfn.net.br ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br

### RSFN - Manual de Redes do SFN Versão 7.6.3

	Bacen – Servidor Secundário	irs3.att.rsfn.net.br
	Bacen – Servidor Secundário	irs1.ebtrtm.rsfn.net.br
	Bacen – Servidor Secundário	irs2.ebtrtm.rsfn.net.br
	Bacen – Servidor Secundário	irs3.ebtrtm.rsfn.net.br

Tabela 3 - Domínios Superiores Reversos da RSFN

#### Sub-Domínios Reversos da RSFN

Os sub-domínios reversos da RSFN refletem exatamente as faixas de endereços IP definidas para cada Entidade Participante desta rede. Estes sub-domínios foram criados para identificar cada uma das Entidades Participantes da VPN da RSFN.

Cada Entidade é responsável por administrar seus respectivos sub-domínios. O nome do sub-domínio é derivado da faixa de endereços IP reservada para cada Entidade.

A Tabela 4 apresenta exemplos de nomes:

Entidade	Exemplo de Nomes de Domínios Reversos da RSFN
Bacen BSA	0-31.66.218.200.in-addr.arpa
Bacen RJO (Selic)	32-63.66.218.200.in-addr.arpa
Clearing1	64-95.66.218.200.in-addr.arpa
Clearing2	96-127.66.218.200.in-addr.arpa
Clearing3	128-159.66.218.200.in-addr.arpa
Clearing4	160-191.66.218.200.in-addr.arpa
IF1	0-15.80.218.200.in-addr.arpa
IF2	16-31.80.218.200.in-addr.arpa
IF3	32-47.80.218.200.in-addr.arpa
IF4	48-63.80.218.200.in-addr.arpa
IF5	64-79.80.218.200.in-addr.arpa
Primesys	0-127.64.218.200.in-addr.arpa
EBT/RTM	128-255.64.218.200.in-addr.arpa

Tabela 4 - Exemplo de Sub-Domínios Reversos da RSFN

#### Delegando Direitos Para os Sub-Domínios Reversos

O servidor primário das zonas **64.218.200.in-addr.arpa** até **95.218.200.in-addr.arpa** é quem tem o direito de criar e delegar direitos para seus sub-domínios. Esta delegação ocorre através da configuração de registros do tipo NS (*Name Servers*), atrelados a registros do tipo A (*Address*) para cada um dos sub-domínios criados.

Adicionalmente, como são utilizadas zonas com endereços quebrados (14 ou 30 endereços válidos), os responsáveis por cada zona de endereçamento reverso tem que criar um registro CNAME para cada endereço disponível de cada Entidade Participante da rede.

A seguir é apresentado o exemplo da configuração para delegação de direitos para o sub-domínio de **66.218.200.in-addr.arpa**, o qual deverá estar totalmente compatível com a tabela de endereços IP fornecida para cada Entidade da RSFN.

```
66.218.200.in-addr.arpa. IN SOA ns1.bcb.rsfn.net.br. spb_registro.bcb.gov.br. (
2001081401 ; Número de Série
28800 ; refresh
3600 ; retry
604800 ; expire
86400 ; default_ttl
)
;
; Servidores de nomes deste domínio
;
IN NS ns1.bcb.rsfn.net.br.
```

### RSFN - Manual de Redes do SFN Versão 7.6.3

---

```
IN NS ns2.bcb.rsfn.net.br.
IN NS irs1.att.rsfn.net.br.
IN NS irs2.att.rsfn.net.br.
IN NS irs3.att.rsfn.net.br.
IN NS irs1.ebtrtm.rsfn.net.br.
IN NS irs2.ebtrtm.rsfn.net.br.
IN NS irs3.ebtrtm.rsfn.net.br.
;
; Delegação de Direitos para Clerings/Bacen (2 linhas p/ cada sub-domínio)
;
0-31.66.218.200.in-addr.arpa. IN NS ns1.bcb.rsfn.net.br.
0-31.66.218.200.in-addr.arpa. IN NS ns2.bcb.rsfn.net.br.

32-63.66.218.200.in-addr.arpa. IN NS ns1.selic.rsfn.net.br.
32-63.66.218.200.in-addr.arpa. IN NS ns2.selic.rsfn.net.br.

64-95.66.218.200.in-addr.arpa. IN NS ns1.clearing1.rsfn.net.br.
64-95.66.218.200.in-addr.arpa. IN NS ns2.clearing1.rsfn.net.br.

96-127.66.218.200.in-addr.arpa. IN NS ns1.clearing2.rsfn.net.br.
96-127.66.218.200.in-addr.arpa. IN NS ns2.clearing2.rsfn.net.br.

128-159.66.218.200.in-addr.arpa. IN NS ns1.clearing3.rsfn.net.br.
128-159.66.218.200.in-addr.arpa. IN NS ns2.clearing3.rsfn.net.br.

160-191.66.218.200.in-addr.arpa. IN NS ns1.clearing4.rsfn.net.br.
160-191.66.218.200.in-addr.arpa. IN NS ns2.clearing4.rsfn.net.br.
;
; CNAME para hosts de bacenbsa (1 linha p/ cada endereço válido)
;
1 IN CNAME 1.0-31.66.218.200.in-addr.arpa.
2 IN CNAME 2.0-31.66.218.200.in-addr.arpa.
.
.
.
29 IN CNAME 29.0-31.66.218.200.in-addr.arpa.
30 IN CNAME 30.0-31.66.218.200.in-addr.arpa.
;
; CNAME para hosts de bacenrjo (1 linha p/ cada endereço válido)
;
33 IN CNAME 33.32-63.66.218.200.in-addr.arpa.
34 IN CNAME 34.32-63.66.218.200.in-addr.arpa.
.
.
.
61 IN CNAME 61.32-63.66.218.200.in-addr.arpa.
62 IN CNAME 62.32-63.66.218.200.in-addr.arpa.
;
; CNAME para hosts de Clearing1 (1 linha p/ cada endereço válido)
;
65 IN CNAME 65.64-95.66.218.200.in-addr.arpa.
66 IN CNAME 65.64-95.66.218.200.in-addr.arpa.
.
.
.
93 IN CNAME 93.64-95.66.218.200.in-addr.arpa.
94 IN CNAME 94.64-95.66.218.200.in-addr.arpa.
;
; CNAME para hosts de Clearing2 (1 linha p/ cada endereço válido)
;
```

### **RSFN - Manual de Redes do SFN Versão 7.6.3**

---

```
97 IN CNAME 97.96-127.66.218.200.in-addr.arpa.
98 IN CNAME 98.96-127.66.218.200.in-addr.arpa.
.
.
.
125 IN CNAME 125.96-127.66.218.200.in-addr.arpa.
126 IN CNAME 126.96-127.66.218.200.in-addr.arpa.
;
; CNAME para hosts de Clearing3 (1 linha p/ cada endereço válido)
;
129 IN CNAME 129.128-159.66.218.200.in-addr.arpa.
130 IN CNAME 130.128-159.66.218.200.in-addr.arpa.
.
.
.
157 IN CNAME 157.128-159.66.218.200.in-addr.arpa.
158 IN CNAME 158.128-159.66.218.200.in-addr.arpa.
;
; CNAME para hosts de Clearing4 (1 linha p/ cada endereço válido)
;
161 IN CNAME 161.160-191.66.218.200.in-addr.arpa.
162 IN CNAME 162.160-191.66.218.200.in-addr.arpa.
.
.
.
189 IN CNAME 189.160-191.66.218.200.in-addr.arpa.
190 IN CNAME 190.160-191.66.218.200.in-addr.arpa.
```

#### Incluindo ou Excluindo Domínios ou Sub-Domínios Reversos

A RSFN pode a qualquer momento incluir ou excluir domínios ou sub-domínios reversos de DNS em sua rede, desde que respeite as regras definidas neste manual:

- ter um *Primary Name Server* – PNS e no mínimo um *Secondary Name Server* – SNS para cada zona;
- preparar os arquivos de configuração de forma a tornar operacional o novo domínio, tanto no PNS como no SNS;
- registrar os domínios e seus respectivos servidores nos órgãos competentes;
- considerar os tempos de convergência necessários para que a rede tome conhecimento das modificações realizadas.

Sub-Domínios Reversos da RSFN

As árvores de DNS utilizadas na RSFN estão apresentadas nas Figura 1 e Figura 2:

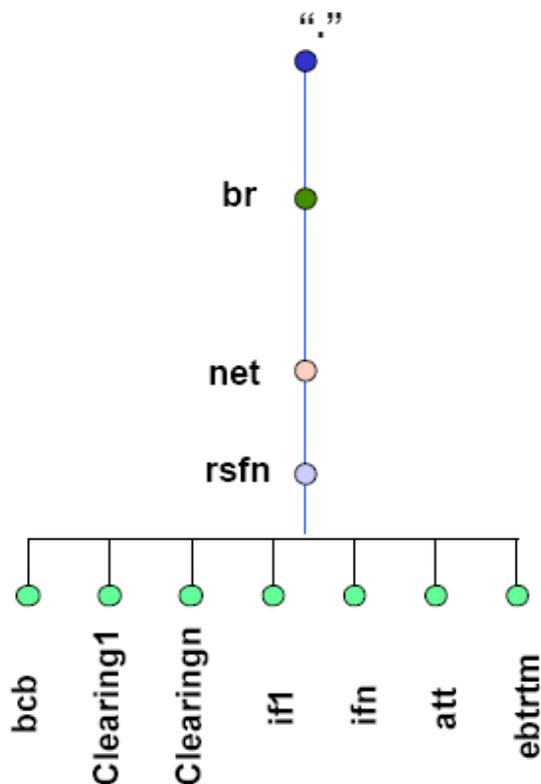


Figura 1 - Árvore de DNS da RSFN

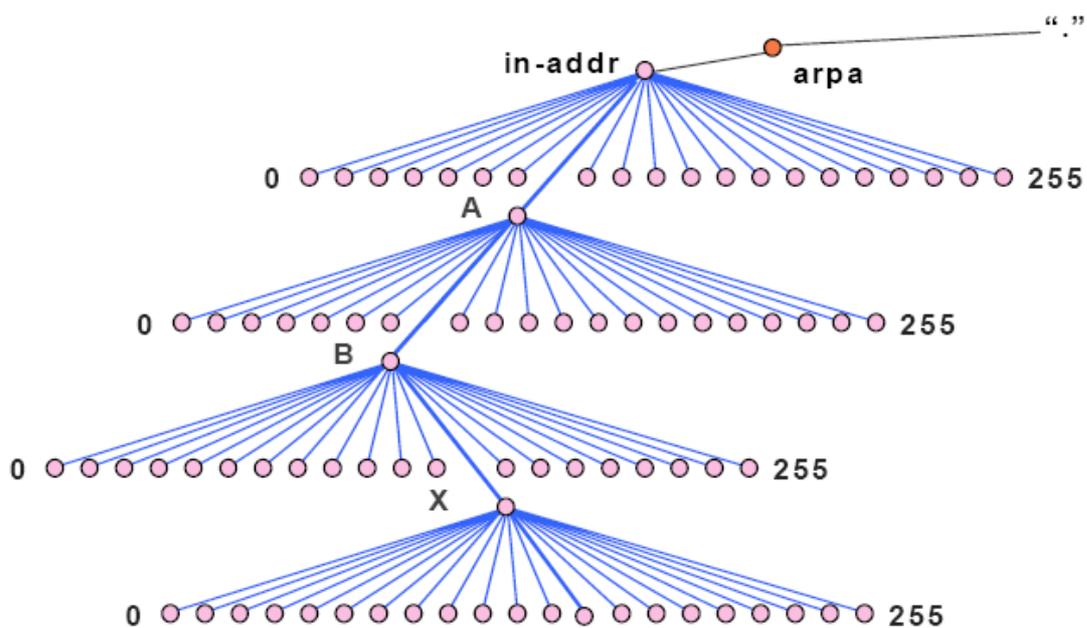


Figura 2 – Árvore de DNS Reverso da RSFN

### Servidores de DNS da RSFN

Cada domínio ou sub-domínio da RSFN possui um servidor primário de nomes com autoridade sobre sua respectiva zona. Todas as alterações nos bancos de dados do DNS são feitas nestes servidores.

Para resolver problemas de contingência, divisão de carga e performance da rede, cada domínio terá pelo menos um servidor secundário de nomes. Estes servidores manterão uma réplica dos bancos de dados dos servidores primários, e periodicamente e automaticamente contatarão os servidores primários para atualização dos seus bancos de dados.

Desde que todas as versões de DNS utilizadas na rede suportem a função DNS *Notify* (RFC 1996), os servidores primários podem enviar imediatamente após qualquer mudança no banco de dados do DNS, uma notificação para os servidores secundários solicitando que estes iniciem o processo de *Zone Transfer*, diminuindo o tempo de convergência das modificações de DNS na rede.

### Servidor Primário dos Domínios Superiores – IRS (“Internal Root Server”)

Os servidores primários de nomes (PNS) dos domínios superiores da RSFN estão apresentados na Tabela 5:

Domínio Superior	Servidor Primário (PNS)	Entidade Responsável
rsfn.net.br	ns1.bcb.rsfn.net.br	Bacen
64.218.200.in-addr.arpa	ns1.bcb.rsfn.net.br	Bacen
66.218.200.in-addr.arpa	ns1.bcb.rsfn.net.br	Bacen
67.218.200.in-addr.arpa	ns1.bcb.rsfn.net.br	Bacen
80.218.200.in-addr.arpa até	ns1.bcb.rsfn.net.br	Bacen
95.218.200.in-addr.arpa	ns1.bcb.rsfn.net.br	Bacen

Tabela 5 - Servidores PNS dos Domínios Superiores da RSFN

Vale lembrar que uma mesma máquina pode ser configurada como servidor primário de nomes para vários domínios, como servidor secundário de nomes para vários domínios e mesmo como servidor primário para alguns domínios e secundário para outros.

Para resolver nomes de *hosts* da Internet, este servidor deve ser configurado para utilizar os servidores de *root* da Internet.

### Servidores Secundários dos Domínios Superiores – IRS (“Internals Root Servers”)

Os servidores secundários de nomes (SNS) dos domínios superiores da RSFN estão apresentados na Tabela 6:

Domínio Superior	Servidor Primário (PNS)	Entidade Responsável
rsfn.net.br	ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Bacen Primesys Primesys Primesys EBT/RTM EBT/RTM EBT/RTM
64.218.200.in-addr.arpa	ns2.bcb.rsfn.net.br irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Bacen Primesys Primesys Primesys EBT/RTM EBT/RTM EBT/RTM

**RSFN - Manual de Redes do SFN Versão 7.6.3**

66.218.200. in-addr.arpa	ns2.bcb.rsfn.net.br  irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Bacen  Primesys Primesys Primesys EBT/RTM EBT/RTM EBT/RTM
67.218.200. in-addr.arpa	ns2.bcb.rsfn.net.br  irs1.att.rsfn.net.br irs2.att.rsfn.net.br irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Bacen  Primesys Primesys Primesys EBT/RTM EBT/RTM EBT/RTM
80.218.200. in-addr.arpa Até 95.218.200. in-addr.arpa	ns2.bcb.rsfn.net.br  irs1.att.rsfn.net.br irs2.att.rsfn.net.br  irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Bacen  Primesys Primesys  Primesys EBT/RTM EBT/RTM EBT/RTM
64.218.200. in-addr.arpa	irs2.att.rsfn.net.br  irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Primesys  Primesys EBT/RTM EBT/RTM EBT/RTM
66.218.200. in-addr.arpa	irs2.att.rsfn.net.br  irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Primesys  Primesys EBT/RTM EBT/RTM EBT/RTM
67.218.200. in-addr.arpa	irs2.att.rsfn.net.br  irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Primesys  Primesys EBT/RTM EBT/RTM EBT/RTM
80.218.200. in-addr.arpa até 95.218.200. in-addr.arpa	irs2.att.rsfn.net.br  irs3.att.rsfn.net.br irs1.ebtrtm.rsfn.net.br  irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	Primesys  Primesys EBT/RTM  EBT/RTM EBT/RTM

Tabela 6 - Servidores SNS dos Domínios Superiores da RSFN

**Servidores Primários dos Sub-Domínios**

Cada sub-domínio da RSFN terá seu próprio servidor primário de nomes (PNS). Estes servidores estarão localizados no segmento da RSFN de cada Entidade participante da rede, a qual será responsável pela administração do mesmo. Em situações especiais, uma determinada Entidade pode terceirizar a tarefa de administração de seus sub-domínios com um dos provedores de serviços da rede.

## RSFN - Manual de Redes do SFN Versão 7.6.3

A Tabela 7 apresenta exemplo de servidores primários para os sub-domínios diretos da RSFN:

Sub-Domínio Direto da RSFN	Servidor Primário (PNS)	Entidade Responsável
bcf.rsfn.net.br	ns1.bcf.rsfn.net.br	Bacen
clearing1.rsfn.net.br	ns1.clearing1.rsfn.net.br	Clearing1
clearing2.rsfn.net.br	ns1.clearing2.rsfn.net.br	Primesys (*opcional)
Provedornx21.rsfn.net.br	ns1.Provedornx21.rsfn.net.br	Provedor nx2 1
if1.rsfn.net.br	ns1.if1.rsfn.net.br	IF1
if2.rsfn.net.br	ns1.if2.rsfn.net.br	EBT/RTM (*opcional)
att.rsfn.net.br	irs1.att.rsfn.net.br	Primesys
ebtrtm.rsfn.net.br	irs1.ebtrtm.rsfn.net.br	EBT/RTM

Tabela 7 - Servidores PNS dos Sub-Domínios Diretos da RSFN

A Tabela 8 apresenta exemplo de servidores primários para os sub-domínios reversos da RSFN:

Sub-Domínio Reverso da RSFN	Servidor Primário (PNS)	Entidade Responsável
0-31.66.218.200.in-addr.arpa	ns1.bcf.rsfn.net.br	Bacen
64-95.66.218.200.in-addr.arpa	ns1.clearing1.rsfn.net.br	Clearing1
96.127.66.218.200.in-addr.arpa	ns1.clearing2.rsfn.net.br	Primesys (*opcional)
128.159.67.218.200.in-addr.arpa	ns1.Provedornx21.rsfn.net.br	Provedor nx2 1
0-15.80.218.200.in-addr.arpa	ns1.if1.rsfn.net.br	IF1
16-31.80.218.200.in-addr.arpa	ns1.if2.rsfn.net.br	EBT/RTM (*opcional)
0-127.64.218.200.in-addr.arpa	irs1.att.rsfn.net.br	Primesys
128-255.64.218.200.in-addr.arpa	irs1.ebtrtm.rsfn.net.br	EBT/RTM

Tabela 8 - Servidores PNS dos Sub-Domínios Reversos da RSFN

No entanto, para que os servidores anteriores sejam capazes de resolver endereços reversos de zonas parciais de DNS, uma vez que a RSFN utiliza sub-redes com endereços de “Classe C” particionados (16 ou 32 endereços), os servidores de DNS das instituições conectadas a esta rede terão que ser configurados como servidores secundários dos domínios reversos correspondentes à “Classe C” cheia da qual faz parte sua faixa de endereços.

A Tabela 9 apresenta a configuração adicional como SNS para que os servidores primários para os sub-domínios reversos da RSFN sejam capazes de resolver endereços reversos:

Sub-Domínio Reverso da RSFN	Servidor Primário (PNS)	Entidade Responsável
66.218.200.in-addr.arpa	ns1.bcf.rsfn.net.br	Bacen
66.218.200.in-addr.arpa	ns1.clearing1.rsfn.net.br	Clearing1
66.218.200.in-addr.arpa	ns1.clearing2.rsfn.net.br	Primesys (*opcional)
67.218.200.in-addr.arpa	ns1.Provedornx21.rsfn.net.br	Provedor nx2 1
80.218.200.in-addr.arpa	ns1.if1.rsfn.net.br	IF1
80.218.200.in-addr.arpa	ns1.if2.rsfn.net.br	EBT/RTM (*opcional)
64.218.200.in-addr.arpa	irs1.att.rsfn.net.br	Primesys
64.218.200.in-addr.arpa	irs1.ebtrtm.rsfn.net.br	EBT/RTM

Tabela 9 - Servidores SNS dos Sub-Domínios de “Classe C” Completos da RSFN

Para resolver nomes de *hosts* de outros sub-domínios diretos ou reversos da RSFN, uma das seguintes alternativas terá que ser utilizada:

- opção A – RSFN não conectada à Internet e Entidade utiliza um servidor de DNS dedicado para a RSFN. Basta configurar o servidor de DNS da Entidade para enviar requisições para outros domínios através da diretiva *forwarder*. Esta diretiva deve apontar para todos os 6 servidores internos de *root* apresentados anteriormente;
- opção B – RSFN não conectada à Internet e Entidade utiliza um servidor de DNS compartilhado para a RSFN, Intranet e conexão com a Internet. Neste caso a diretiva *forwarder* genérica não funcionará, caso contrário, o servidor não mais será capaz de resolver nomes de *hosts* da Internet. Neste caso, será necessário criar uma zona com *type forward* para os demais “Endereços cheios de Classe C da RSFN”, além da própria zona “rsfn.net.br”. Esta configuração é conhecida como *forward específico*;
- opção C – RSFN conectada à Internet – configuração idêntica a utilizada na opção B;

## RSFN - Manual de Redes do SFN Versão 7.6.3

nas três opções anteriores, a seguinte regra de configuração deve ser utilizada: instituições do Grupo A devem ser configuradas tendo como primeiro servidor de *forwarder* um servidor da Primesys e como segundo servidor de *forwarder* um servidor da EBT/RTM. Por sua vez, instituições do grupo B devem ser configuradas com a ordem contrária.

Problemas com as opções B e C: a solução de DNS da Microsoft não suporta opção de *forward* para uma zona específica, exigindo o uso da aplicação BIND.

### Servidores Secundários dos Sub-Domínios

Cada sub-domínio da RSFN deverá ter pelo menos um servidor secundário (SNS). Estes servidores estarão localizados no segmento da RSFN de cada Entidade Participante da rede, a qual será responsável pela administração do mesmo. Em situações especiais, uma determinada Entidade pode terceirizar a tarefa de administração de seus sub-domínios com um dos provedores de serviços da rede.

A Tabela 10 apresenta exemplo de servidores secundários para os sub-domínios diretos da RSFN:

Sub-Domínio Direto da RSFN	Servidor Secundário (SNS)	Entidade Responsável
bcf.rsfn.net.br	ns2.bcf.rsfn.net.br	Bacen
clearing1.rsfn.net.br	ns2.clearing1.rsfn.net.br	Clearing1
clearing2.rsfn.net.br	ns2.clearing2.rsfn.net.br	Primesys (*opcional)
Provedornx21.rsfn.net.br	ns2.Provedornx21.rsfn.net.br	Provedor nx2 1
if1.rsfn.net.Br	ns2.if1.rsfn.net.br	IF1
if2.rsfn.net.br	ns2.if2.rsfn.net.br	EBT/RTM (*opcional)
att.rsfn.net.br	irs2.att.rsfn.net.br irs3.att.rsfn.net.br	Primesys
ebtrtm.rsfn.net.br	irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	EBT/RTM

Tabela 10 - Servidores SNS dos Sub-Domínios Diretos da RSFN

A Tabela 11 apresenta exemplo de servidores secundários para os sub-domínios reversos da RSFN:

Sub-Domínio Reverso da RSFN	Servidor Secundário (SNS)	Entidade Responsável
0-31.66.218.200.in-addr.arpa	ns2.bcf.rsfn.net.br	Bacen
64-95.66.218.200.in-addr.arpa	ns2.clearing1.rsfn.net.br	Clearing1
96.127.66.218.200.in-addr.arpa	ns2.clearing2.rsfn.net.br	Primesys (*opcional)
128-159.67.218.200.in-addr.arpa	ns2.Provedornx21.rsfn.net.br	Provedor nx2 1
0-15.80.218.200.in-addr.arpa	ns2.if1.rsfn.net.br	IF1
16-31.80.218.200.in-addr.arpa	ns2.if2.rsfn.net.br	EBT/RTM (*opcional)
0-127.64.218.200.in-addr.arpa	irs2.att.rsfn.net.br irs3.att.rsfn.net.br	Primesys
128.255.64.218.200.in-addr.arpa	irs2.ebtrtm.rsfn.net.br irs3.ebtrtm.rsfn.net.br	EBT/RTM

Tabela 11 - Servidores SNS dos Sub-Domínios Reversos da RSFN

No entanto, para que os servidores anteriores sejam capazes de resolver endereços reversos de zonas parciais de DNS, uma vez que a RSFN utiliza sub-redes com endereços de “Classe C” particionados (16 ou 32 endereços), os servidores de DNS das instituições conectadas a esta rede terão que ser configurados como servidores secundários dos domínios reversos correspondentes à “Classe C” cheia da qual faz parte sua faixa de endereços.

A Tabela 12 apresenta a configuração adicional como SNS para que os servidores primários para os sub-domínios reversos da RSFN sejam capazes de resolver endereços reversos:

Sub-Domínio Reverso da RSFN	Servidor Secundário (SNS)	Entidade Responsável
66.218.200.in-addr.arpa	ns2.bcf.rsfn.net.br	Bacen
66.218.200.in-addr.arpa	ns2.clearing1.rsfn.net.br	Clearing1
66.218.200.in-addr.arpa	ns2.clearing2.rsfn.net.br	Primesys (*opcional)
67.218.200.in-addr.arpa	ns2.Provedornx21.rsfn.net.br	Provedor nx2 1

### RSFN - Manual de Redes do SFN Versão 7.6.3

80.218.200.in-addr.arpa	ns2.if1.rsfn.net.br	IF1
80.218.200.in-addr.arpa	ns2.if2.rsfn.net.br	EBT/RTM (*opcional)
64.218.200.in-addr.arpa	irs2.att.rsfn.net.br	Primesys
	irs3.att.rsfn.net.br	
64.218.200.in-addr.arpa	irs2.ebtrtm.rsfn.net.br	EBT/RTM
	irs3.ebtrtm.rsfn.net.br	

Tabela 12 - Servidores SNS dos Sub-Domínios de “Classe C” Completos da RSFN

Para resolver nomes de *hosts* de outros sub-domínios diretos ou reversos da RSFN, uma das seguintes alternativas terá que ser utilizada:

- opção A – RSFN não conectada à Internet e Entidade utiliza um servidor de DNS dedicado para a RSFN. Basta configurar o servidor de DNS da Entidade para enviar requisições para outros domínios através da diretiva *forwarder*. Esta diretiva deve apontar para todos os 6 servidores internos de *root* apresentados anteriormente;
- opção B – RSFN não conectada à Internet e Entidade utiliza um servidor de DNS compartilhado para a RSFN, Intranet e conexão com a Internet. Neste caso a diretiva *forwarder* genérica não funcionará, caso contrário, o servidor não mais será capaz de resolver nomes de *hosts* da Internet. Neste caso, será necessário criar uma zona com *type forward* para os demais “Endereços cheios de Classe C da RSFN”, além da própria zona “rsfn.net.br”. Esta configuração é conhecida como *forward específico*;
- opção C – RSFN conectada à Internet – configuração idêntica a utilizada na opção B.

nas três opções anteriores, a seguinte regra de configuração deve ser utilizada: instituições do Grupo A devem ser configuradas tendo como primeiro servidor de *forwarder* um servidor da Primesys e como segundo servidor de *forwarder* um servidor da EBT/RTM. Por sua vez, instituições do grupo B devem ser configuradas com a ordem contrária.

Problemas com as opções B e C: a solução de DNS da Microsoft não suporta opção de *Forward* para uma zona específica, exigindo o uso da aplicação BIND.

### Registro dos Domínios Superiores nas Entidades Competentes

Para que a comunidade Internet saiba quem são os servidores de nomes dos domínios existentes na RSFN, todos estes servidores (primários e secundários) têm que estar definidos nos domínios de níveis superiores relacionados com a solução (**net.br**).

A administração dos domínios brasileiros (**.br**) é realizada pela FAPESP, e existem algumas restrições para registros de domínios no formato **net.br**.

O registro dos diferentes domínios superiores externos da RSFN é feito através da página <http://registro.br>. Após o correto preenchimento dos dados cadastrais referentes aos domínios, será efetuado um teste automático de transferência de zona entre os servidores informados. Caso a resposta dos servidores esteja dentro das normas que **net.br** regem o serviço de DNS, serão gerados registros deste domínio nos arquivos de zonas do domínio conforme o exemplo abaixo:

```

;
; Trechos do Arquivo de Zona do Domínio NET.BR.
; Este arquivo é administrado pela FAPESP. A RSFN não tem
; qualquer controle sobre ele.
; Os nomes e endereços utilizados para servidores de DNS devem ser
; considerados como exemplos.
; O exemplo considera que o PNS da Zona NET.BR. é o servidor ns.dns.br
;
net.br. INSOA ns.dns.br. root.ns.dns.br. (
2001050101 ; Número de Série (yyyymmddss)
8h ; Refresh após 8 horas
1h ; Retry após 1 hora
1w ; Expire após 1 semana
1d ) ; TTL de 1 dia
;
; PNS e SNS do domínio net.br.
```

```
;  
IN NS ns.dns.br.  
IN NS ns1.dns.br.  
IN NS ns2.dns.br.  
;  
; Delegação de Direitos Para os domínios administrados pela RSFN  
; Para a documentação, será listado apenas o domínio  
; rsfn.net.br  
;  
rsfn.net.br. IN NS ns1.bacen.com.br.  
ns1.bacen.com.br. IN A 200.30.30.5  
rsfn.net.br. IN NS ns2.bacen.com.br.  
ns2.bacen.com.br. IN A 200.30.30.6  
;  
; Fim do arquivo  
;
```

### Registro dos Sub-Domínios das Entidades

Os sub-domínios da RSFN indicando as Entidades Participantes não precisam ser registrados na FAPESP. A própria regra de delegação de direitos do DNS se encarregará de permitir a resolução de nomes de hosts dos sub-domínios.

#### Incluindo ou Excluindo Domínios Superiores Externos

A RSFN pode a qualquer momento incluir ou excluir domínios superiores, desde que respeite as regras definidas neste relatório:

- o ter um *Primary Name Server* – PNS e no mínimo um *Secondary Name Server* – SNS para cada zona com endereços válidos na Internet;
- o preparar os arquivos de configuração de forma a tornar operacional o novo domínio, tanto no PNS com no SNS;
- o registrar os domínios externos e seus respectivos servidores nos órgãos competentes;
- o considerar os tempos de convergência necessários para que a Internet tome conhecimento das modificações realizadas.

### Árvore de DNS da Parte Externa

As árvores de DNS dos domínios superiores externos da RSFN apresentam uma estrutura similar à anterior.

#### Configuração do PNS dos Sub-Domínios – ns1.bcb.rsfn.net.br

Este capítulo apresenta o modelo de configuração para os servidores PNS dos sub-domínios das Entidades.

```
Arquivo /etc/named.conf  
options {  
directory "/var/named";  
recursion yes;  
notify yes;  
allow-query { any; };  
allow-transfer { any; };  
query-source address * port 53;  
listen-on port 53 { any; };  
};  
  
zone "bcb.rsfn.net.br" {  
type master;  
file "db.bacen";  
  
};
```

```
zone "0-31.66.218.200.in-addr.arpa" {
type master;
file "db.200.218.66.0-31";
};

zone "66.218.200.in-addr.arpa" {
type slave;
masters { 200.218.64.6; 200.218.64.134; };
file "db.200.218.66";
};

zone "rsfn.net.br" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};

zone "64.218.200.in-addr.arpa" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};

zone "67.218.200.in-addr.arpa" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};

zone "80.218.200.in-addr.arpa" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};

/* Configurar todas as zonas reversas até 95.218.200.in-addr.arpa */

zone "95.218.200.in-addr.arpa" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};

zone "0.0.127.in-addr.arpa" {
type master;
file "named.rev";
};

zone "localhost" {
type master;
file "named.local";
};

zone "0.in-addr.arpa" {
type master;
file "db.0";
};

zone "255.in-addr.arpa" {
type master;
```

```
file "db.255";
};

zone "." {
type hint;
file "named.ca";
};

Arquivo /var/named/db.bacen.net
@ IN SOA ns1.bcb.rsfnet.br. root.ns1.bcb.rsfnet.br. (
2001050101 ; Número de Série
8h ; Refresh após 8 horas
1h ; Retry após 1 hora
1w ; Expire após 1 semana
1d ) ; TTL de 1 dia
;
; Servidores de nomes deste domínio
;
IN NS ns1.bcb.rsfnet.br.
IN NS ns2.bcb.rsfnet.br.
;
; Definição dos hosts do domínio.
;
att-bacen-bsa-cpe IN A 200.218.66.1
ebtrtm-bacen-bsa-cpe IN A 200.218.66.2
hsrp-bacen-bsa-cpe IN A 200.218.66.3
sw1 IN A 200.218.66.4
sw2 IN A 200.218.66.5
ns1 IN A 200.218.66.6
ns2 IN A 200.218.66.7
mqs01 0 IN A 200.218.66.8
mqs02 0 IN A 200.218.66.9
mqm01 0 IN A 200.218.66.14
mqm02 0 IN A 200.218.66.15

/var/named/db.200.218.66.0-31
@ IN SOA ns1.bcb.rsfnet.br. root.ns1.bcb.rsfnet.br. (
2001050101 ; Número de Série
8h ; Refresh após 8 horas
1h ; Retry após 1 hora
1w ; Expire após 1 semana
1d ) ; TTL de 1 dia
;
; Servidores de nomes deste domínio
;
IN NS ns1.bcb.rsfnet.br.
IN NS ns2.bcb.rsfnet.br.
;
; Definição dos hosts do domínio.
;
1 IN PTR att-bacen-bsa-cpe.bcb.rsfnet.br
2 IN PTR ebtrtm-bacen-bsa-cpe.bcb.rsfnet.br
3 IN PTR hsrp-bacen-bsa-cpe.bcb.rsfnet.br
4 IN PTR sw1.bcb.rsfnet.br
5 IN PTR sw2.bcb.rsfnet.br
6 IN PTR ns1.bcb.rsfnet.br
7 IN PTR ns2.bcb.rsfnet.br
8 IN PTR mqs01.bcb.rsfnet.br
9 IN PTR mqs02.bcb.rsfnet.br
14 IN PTR mqm01.bcb.rsfnet.br
```

15 INPTR mqm02.bcb.rsfn.net.br

/var/named/db.200.218.66

Este arquivo será atualizado automaticamente.

Arquivo /var/named/named.local

```
@ IN SOA ns1.bcb.rsfn.net.br. root.ns1.bcb.rsfn.net.br. (
2001050101 ; Número de Série
8h ; Refresh após 8 horas
1h ; Retry após 1 hora
1w ; Expire após 1 semana
1d ) ; TTL de 1 dia
;
; Servidores de nomes deste domínio
;
IN NS ns1.bcb.rsfn.net.br.
IN NS ns2.bcb.rsfn.net.br.
;
; Servidor local
;
localhost. IN A 127.0.0.1
```

Arquivo /var/named/db.127

```
@ IN SOA ns1.bcb.rsfn.net.br. root.ns1.bcb.rsfn.net.br. (
2001050101 ; Número de Série
8h ; Refresh após 8 horas
1h ; Retry após 1 hora
1w ; Expire após 1 semana
1d ) ; TTL de 1 dia
;
; Servidores de nomes deste domínio
;
IN NS ns1.bcb.rsfn.net.br.
IN NS ns2.bcb.rsfn.net.br.
;
; Servidor local
;
1 IN PTR localhost.
```

Arquivo /var/named/db.255

```
@ IN SOA ns1.bcb.rsfn.net.br. root.ns1.bcb.rsfn.net.br. (
2001050101 ; Número de Série
8h ; Refresh após 8 horas
1h ; Retry após 1 hora
1w ; Expire após 1 semana
1d ) ; TTL de 1 dia
;
; Servidores de nomes deste domínio
;
IN NS ns1.bcb.rsfn.net.br.
IN NS ns2.bcb.rsfn.net.br.
```

Arquivo /var/named/db.0

```
@ IN SOA ns1.bcb.rsfn.net.br. root.ns1.bcb.rsfn.net.br. (
2001050101 ; Número de Série
8h ; Refresh após 8 horas
1h ; Retry após 1 hora
1w ; Expire após 1 semana
1d ) ; TTL de 1 dia
;
```

```
; Servidores de nomes deste domínio
;
IN NS ns1.bcb.rsfnet.br.
IN NS ns2.bcb.rsfnet.br.
```

Arquivo /var/named/named.ca

Este arquivo será idêntico ao arquivo named.ca apresentados anteriormente.

Configuração do SNS dos Sub-Domínios – ns2.bcb.rsfnet.br

Este capítulo apresenta o modelo de configuração para os servidores SNS dos sub-domínios das Entidades.

Arquivo /etc/named.conf

```
options {
directory "/var/named";
recursion yes;
notify yes;
allow-query { any; };
allow-transfer { any; };
query-source address * port 53;
listen-on port 53 { any; };
};

zone "bcb.rsfnet.br" {
type slave;
masters { 200.218.66.1; };
file "db.bacen";
};

zone "0-31.66.218.200.in-addr.arpa" {
type slave;
masters { 200.218.66.1; };
file "db.200.218.66.0-31";
};

zone "66.218.200.in-addr.arpa" {
type slave;
masters { 200.218.64.6; 200.218.64.134; };
file "db.200.218.66";
};

zone "rsfnet.br" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};

zone "64.218.200.in-addr.arpa" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};

zone "67.218.200.in-addr.arpa" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};

zone "80.218.200.in-addr.arpa" {
type forward;
```

```
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};
```

*/\* Configurar todas as zonas reversas até 95.218.200.in-addr.arpa \*/*

```
zone "95.218.200.in-addr.arpa" {
type forward;
forward only;
forwarders { 200.218.64.6; 200.218.64.134; };
};
```

```
zone "0.0.127.in-addr.arpa" {
type master;
file "named.rev";
};
```

```
zone "localhost" {
type master;
file "named.local";
};
```

```
zone "0.in-addr.arpa" {
type master;
file "db.0";
};
```

```
zone "255.in-addr.arpa" {
type master;
file "db.255";
};
```

```
zone "." {
type hint;
file "named.ca";
};
```

Arquivo /var/named/db.bacen.net  
Este arquivo será atualizado automaticamente.

/var/named/db.200.218.66.0-31  
Este arquivo será atualizado automaticamente.

/var/named/db.200.218.66  
Este arquivo será atualizado automaticamente.

Arquivo /var/named/named.local  
Este arquivo será idêntico ao arquivo do PNS para este sub-domínio.

Arquivo /var/named/db.127  
Este arquivo será idêntico ao arquivo do PNS para este sub-domínio.

Arquivo /var/named/db.255  
Este arquivo será idêntico ao arquivo do PNS para este sub-domínio.

Arquivo /var/named/db.0  
Este arquivo será idêntico ao arquivo do PNS para este sub-domínio.

Arquivo /var/named/named.ca  
Este arquivo será idêntico ao arquivo named.ca apresentados anteriormente.

### Restrições sobre a Configuração do PNS e SNS dos Sub-Domínios

Caso a Entidade conectada a RSFN opte pela utilização da aplicação de DNS da Microsoft, não será possível utilizar o conceito de zona com *type forward*, para executar operações de *forward* específico por zona.

Se a Entidade estiver utilizando um servidor de DNS dedicado para a RSFN, poderá configurar o servidor para utilizar o conceito de *forward* genérico, que repassará qualquer requisição de *hosts* de outras zonas para os servidores especificados. No entanto, esta opção não funcionará caso a Entidade queira compartilhar o servidor de DNS da RSFN para também resolver nomes de *hosts* da rede interna e da Internet.

### CONFIGURAÇÃO DOS RESOLVERS

Para que as diversas estações da rede possam utilizar o DNS, estas foram configuradas como *resolvers*.

O resolver realiza as seguintes atividades:

- pergunta ao servidor de nomes qual o endereço IP do nome desejado;
- interpreta a resposta (informações solicitadas ou erro de comunicação);
- repassa as informações para a aplicação que solicitou.

Os *resolvers* possuem somente um arquivo de configuração de DNS, normalmente denominado **resolv.cfg** ou **resolv.conf** (verificar o sistema operacional do *host*). Este arquivo identifica o nome do domínio ao qual pertence o *host* e os endereços de até três servidores de nomes deste domínio. Os servidores de nomes definidos neste arquivo podem ser tanto primário como secundário. Os clientes de DNS não fazem qualquer restrição a isto. Os clientes de DNS deverão ser configurados da seguinte forma:

- o primeiro servidor de nomes da lista deve estar na mesma rede do *host* em questão;
- o segundo servidor de nomes da lista também deve pertencer ao sub-domínio respectivo, podendo ou não estar na mesma sub-rede.

O exemplo a seguir mostra a configuração de um *resolver* do sub-domínio **bcb.rsfnet.br**.

```
domain bcb.rsfnet.br
nameserver 200.218.66.6 ;endereço do primeiro servidor de DNS
nameserver 200.218.66.7 ;endereço do segundo servidor de DNS
```

### PADRONIZAÇÃO DE NOMES DE HOSTS E INTERFACES

O padrão de nomes de *hosts* utilizados da RSFN é apresentado na tabela seguinte. A qualquer momento o Grupo de Redes da RSFN poderá optar pela alteração deste padrão.

<b>Tipo de host</b>	<b>Tipo de host</b>
Roteador CPE Telmex	att-sub-domínio-localidade-cpe
Roteador CPE EBTRTM	ebtrtm-sub-domínio-localidade-cpe
HSRP	hsrp-sub-domínio-localidade-cpe
1º <i>switch</i>	sw01
2º <i>switch</i>	sw02
1º Servidor de DNS	ns1
2º Servidor de DNS	ns2
1º Servidor MQSeries SPB Produção	mqs01
1º Servidor MQSeries SPB Homologação	mqs02
1º Servidor MQSeries MES Produção	mqm01
2º Servidor MQSeries MES Homologação	mqm02
3ª Estação de trabalho	wks03
1º <i>Firewall</i>	fw01
2º <i>Firewall</i>	fw02

Tabela 13 - Padronização de *host*

### Padronização de Nomes de Usuários

Outra padronização importante num projeto de DNS é a de nomes de usuários. Foi proposto que seja utilizado o padrão recomendado pela WEMA (*Worldwide Electronic Messaging Association*) para facilitar a conversão de nomes entre os diferentes sistemas de correio eletrônico.

Tal padrão prioriza a identificação do usuário através de três variáveis até se formar um nome único na empresa: Primeiro Nome, Sobrenome e Iniciais dos nomes do meio.

Por exemplo, o usuário José Roberto Teixeira poderia ter seu nome de usuário definido da seguinte forma:

Primeiro Nome José  
Sobrenome Teixeira  
Iniciais Intermediárias R  
Nome de usuário Jose.Teixeira@bacen.rsfn.net.br ou  
Jose.R.Teixeira@bacen.rsfn.net.br

Uma outra alternativa seria:

Primeiro Nome José  
Sobrenome Teixeira  
Nome do Meio Roberto  
Nome do usuário Jose.Roberto.Teixeira@bacen.rsfn.net.br

### IMPACTO DO TRÁFEGO DO DNS NA REDE

O DNS deve ser encarado como uma ferramenta de auxílio ao uso e administração da rede, e não pode, em hipótese alguma, comprometer a eficiência da rede, através da geração de tráfego excessivo na rede.

Para garantir que o tráfego de DNS não influenciará negativamente a performance da rede, os seguintes pontos devem ser cuidadosamente observados:

- localização dos servidores de DNS;
- configuração dos parâmetros de temporização do registro SOA;
- configuração dos *Resolvers*;
- tamanho dos arquivos de cada zona.

### Localização dos Servidores

Conforme dito no decorrer deste manual, os servidores de nomes são os responsáveis por armazenar informações sobre uma determinada região do *address space* do DNS (Zona). Quando os *resolvers* (clientes do DNS) precisarem resolver nomes de um determinado *host* da rede corporativa, perguntarão a estes servidores.

Caso os servidores sejam concentrados somente em algumas localidades, a maioria das requisições dos *resolvers* atravessaria os circuitos seriais de baixa velocidade, o que implicaria em problemas de performance nestes circuitos, normalmente já superutilizados com o tráfego da rede.

Para resolver esta questão, o projeto definiu a utilização de pelo menos um servidor de nomes (primário ou secundário) em cada localidade remota interligada à RSFN por meio de circuitos seriais de telecomunicações (circuitos de WAN). Desta forma, este servidor responderá localmente por todas as requisições para resolução de nomes originadas pelos *resolvers* de sua rede local. Naturalmente, quando este servidor receber requisições para nomes de *hosts* localizados fora de sua zona, estas requisições serão repassadas para os servidores Mestres RSFN. No entanto, como os servidores de nomes utilizam técnicas de *cache*, tais requisições implicam em tráfego consideravelmente menor quando comparado com todas as requisições dos clientes, não prejudicando de forma alguma a operação da rede RSFN.

### Parâmetros de Temporização do Registro SOA

O registro SOA contém parâmetros de temporização que definem o modo de comunicação entre os diferentes servidores de nomes de uma rede corporativa.

O parâmetro *refresh* indica a frequência em que o servidor secundário de nomes (SNS) verifica a acurácia dos seus dados junto ao servidor primário (PNS). Este valor deve ser definido para o período máximo que o cliente considere adequado para que o SNS permaneça com os dados desatualizados. Um valor entre 2 e 12 horas é recomendado para a maior parte das configurações.

Considerando que a maioria das modificações na rede devam ser executadas fora do horário de produção (normalmente no período noturno), entende-se que a definição deste parâmetro para 8 horas concentrará todas as operações de *Zone Transfer* no período noturno, e em situações normais, tal transferência de zona ocorrerá no máximo uma única vez a cada dia.

As versões mais recentes do BIND permitem que o PNS automaticamente notifique os secundários sobre modificações verificadas em seu banco de dados de DNS. Desta forma, os servidores secundários poderão iniciar as operações de *Zone Transfer* imediatamente, diminuindo o tempo de convergência da rede enquanto pode aumentar o tráfego entre operações de transferências de zonas.

Outro parâmetro que afeta a comunicação entre servidores de DNS é o parâmetro *retry*. Em caso de falha na comunicação entre o SNS e o PNS, o SNS tentará novamente estabelecer a conexão com o PNS após a expiração deste temporizador. Este valor é tipicamente configurado como uma fração do intervalo de *refresh*. No caso da RSFN, recomenda-se que seja utilizado uma hora.

O temporizador mais importante para a rede RSFN será sem dúvida o **TTL**. Este parâmetro 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. Deve ser definido conforme a frequência de modificações no banco de dados do DNS. Valores entre 1 e 5 dias normalmente atendem às necessidades das diferentes redes. Vale lembrar que este valor pode ser definido especificamente para um determinado registro. A configuração deve definir este valor para 1 dia.

Na prática, o parâmetro **TTL** é quem fará com que a utilização de um servidor de nomes em cada segmento de rede separado por circuitos seriais gere um tráfego muito menor do que somente a utilização de *resolvers* nestes segmentos.

### Configuração dos Resolvers

A configuração do *resolver* (arquivo **resolv.conf** ou **resolv.cfg**) permite que sejam especificados até três servidores de nomes através da diretiva (*nameserver*). O *resolver* questionará estes servidores, na ordem listada neste arquivo, até receber uma resposta ou até que o intervalo de *timeout* se expire.

Na rede RSFN, cada *resolver* será configurado com dois ou três servidores de nomes, o primeiro estando obrigatoriamente na mesma sub-rede do cliente. Caso a sub-rede do cliente tenha pelo menos dois servidores de nomes, o segundo servidor do cliente também estará na rede local, e o terceiro remoto (na rede do concentrador regional mais próximo). Se existir somente um servidor de nomes na sub-rede, o servidor de nomes localizado no concentrador regional mais próximo será o segundo servidor do cliente.

Com mais do que um servidor de nomes configurado no cliente, o comportamento deste ocorrerá da seguinte forma:

- *resolver* iniciará o processo de resolução de nomes questionando o primeiro servidor de nomes de sua lista (servidor local), com um *timeout* de 5 segundos. Se o período de *timeout* expirar ou se o cliente receber uma mensagem de erro indicando que o processo servidor de nomes não está ativo no primeiro servidor, o *resolver* então questionará o próximo servidor da lista, também com um *timeout* de 5 segundos. Após questionar todos os servidores listados, se o *resolver* não receber nenhuma resposta dentro deste intervalo de tempo, os períodos de *timeout* serão sucessivamente aumentados para 10, 20 e

40 segundos, sendo que em cada ciclo, o questionamento a cada um dos servidores de nomes será devidamente repetido.

Portanto, em situações normais, os *resolvers* da RSFN sempre terão suas requisições resolvidas por servidores de nomes localizados no mesmo segmento de rede local, e com a ajuda do mecanismo de *cache* destes servidores e do correto dimensionamento dos parâmetros **TTL** dos *hosts* mais utilizados, pode-se garantir que o DNS praticamente não irá utilizar os circuitos seriais de baixa velocidade para a resolução de nomes de *hosts* na rede da RSFN.

## FERRAMENTAS DE DEPURAÇÃO DO DNS – *NSLOOKUP*

### INTRODUÇÃO

A RSFN necessita de uma ferramenta eficiente para se certificar do correto funcionamento de seu DNS e para auxiliá-lo na depuração de problemas de interoperabilidade com outras redes.

Neste capítulo serão apresentados alguns comandos normalmente utilizados pelo *nslookup*, por ser esta ferramenta distribuída sem custos adicionais com o *Bind* e com várias outras aplicações de DNS, tornando-a uma ferramenta padrão para análise da funcionalidade do DNS.

O *nslookup* pode ser iniciado de forma interativa ou não interativa. A forma não interativa normalmente é utilizada quando se deseja uma única resposta. A forma interativa tem preferência quando se necessita verificar o comportamento do DNS para diversas questões.

#### ACESSO NÃO INTERATIVO

Para se iniciar uma sessão não interativa, o usuário deve teclar *nslookup* seguido pelo **nome a ser resolvido**, no *prompt* do servidor Unix.

```
% nslookup mqs01.bcb.rsfnet.br
Default Server: ns1.bcb.rsfnet.br
Address: 200.218.66.6
```

```
Name: mqs01.bcb.rsfnet.br
Address: 200.218.66.8
```

#### ACESSO INTERATIVO

Para se iniciar uma sessão interativa, o usuário deve simplesmente teclar *nslookup* no *prompt* do servidor Unix.

```
% nslookup
Default Server: ns1.bcb.rsfnet.br
Address: 200.218.66.6
```

O servidor *default* será o primeiro servidor configurado com a diretiva *nameserver* no arquivo **resolv.conf**. Somente este servidor será utilizado para a resolução das *queries* descritas nesta sessão interativa. Vale lembrar que todos os nomes que não terminem com o ponto, terão acrescido o nome de domínio ou as listas de pesquisa (*search*), também definidas no arquivo **resolv.conf**.

#### Solicitando Ajuda

O *nslookup* possui um *help* próprio que pode ser acionado sempre que houver dúvidas sobre os comandos suportados:

```
% nslookup
Default Server: ns1.bcb.rsfnet.br
Address: 200.218.66.6
```

```
> ? ou help
```

#### Resolução Direta de Nomes e Endereços

Uma das maiores utilizações do *nslookup* é encontrar o endereço IP de um determinado nome ou o nome a partir de um determinado endereço. Estes tipos de *queries* devem ser utilizados sempre que um novo *host* for incluído no DNS, de forma que o administrador possa se certificar do correto funcionamento do DNS para este *host*.

```
% nslookup
Default Server: ns1.bcb.rsfnet.br
Address: 200.218.66.6
```

```
> mqs01.bcb.rsfnet.br
Default Server: ns1.bcb.rsfnet.br
Address: 200.218.66.6
```

```
Name: mqs01.bcb.rsfn.net.br
Address: 200.218.66.8
```

```
> 200.218.66.8
Default Server: ns1.bcb.rsfn.net.br
Address: 200.218.66.6
```

```
Name: mqs01.bcb.rsfn.net.br
Address: 200.218.66.8
```

#### Chaveando Para Outros Servidores de DNS

Às vezes é necessário chavear para um outro servidor de DNS a partir do *nslookup*, para que seja observado o comportamento deste novo servidor. A partir deste ponto, o servidor ns2 passará a responder as *queries* desta sessão interativa.

```
% nslookup
Default Server: ns1.bcb.rsfn.net.br
Address: 200.218.66.6
```

```
> server ns1.santos.rsfn.net.br
Default Server: ns1.santos.rsfn.net.br
Address: 200.218.80.6
```

#### Habilitando *Debug* Para Análise das *Queries*

Em caso de análise de problemas de resolução de nomes via DNS, podem ser habilitadas funções de *debug* para que o *nslookup* mostre as *queries* executadas e suas respectivas respostas. A opção *debug*, mostra somente as respostas de cada *query*, enquanto que a opção **d2** mostras as *queries* e suas respostas.

```
% nslookup
Default Server: ns1.bcb.rsfn.net.br
Address: 200.218.66.6
```

```
> set debug
> set d2
> set nodebug
```

#### *Zone Transfer*

*Nslookup* pode ser usado para transferir o arquivo completo de uma zona através do comando **ls**.

```
% nslookup
Default Server: ns1.bcb.rsfn.net.br
Address: 200.218.66.6
```

```
ls -d rsfn.net.br
```

## DNS EM SERVIDORES DA MICROSOFT

### INTRODUÇÃO

Conforme mencionado anteriormente, as aplicações de DNS proprietárias da Microsoft devem ser consideradas como segunda opção para o serviço de DNS da RSFN. Recomenda-se prioritariamente a utilização da aplicação BIND 8.2.3, tanto para servidores Unix como para servidores Microsoft (Windows NT 4.0 e Windows 2000).

Para as instituições que optarem pela utilização da aplicação de DNS da Microsoft, este capítulo descreve os procedimentos para configuração deste serviço nos servidores Windows 2000 e Windows NT 4.0, através da ferramenta *DNS Manager*. Vale ressaltar que a aplicação de DNS da Microsoft funcionou corretamente no piloto da rede.

Partindo do princípio que o serviço de DNS está devidamente instalado no servidor, serão descritas as instruções necessárias para a criação de domínios diretos, domínios reversos, registro do tipo A, registros do tipo PTR e a configuração para utilização de *forwarders*. Todos os nomes e endereços IP utilizados nas telas de exemplo são aleatórios e devem ser utilizados apenas para orientação.

### CONFIGURAÇÃO DO DNS SERVER EM AMBIENTE WINDOWS 2000

Para iniciar a ferramenta *DNS Manager*, clique em *Start/Programs/Settings/Control Panel/Administrative Tools/DNS Manager*. Na tela inicial do *DNS Manager*, clique em DNS para apresentar os servidores cadastrados.

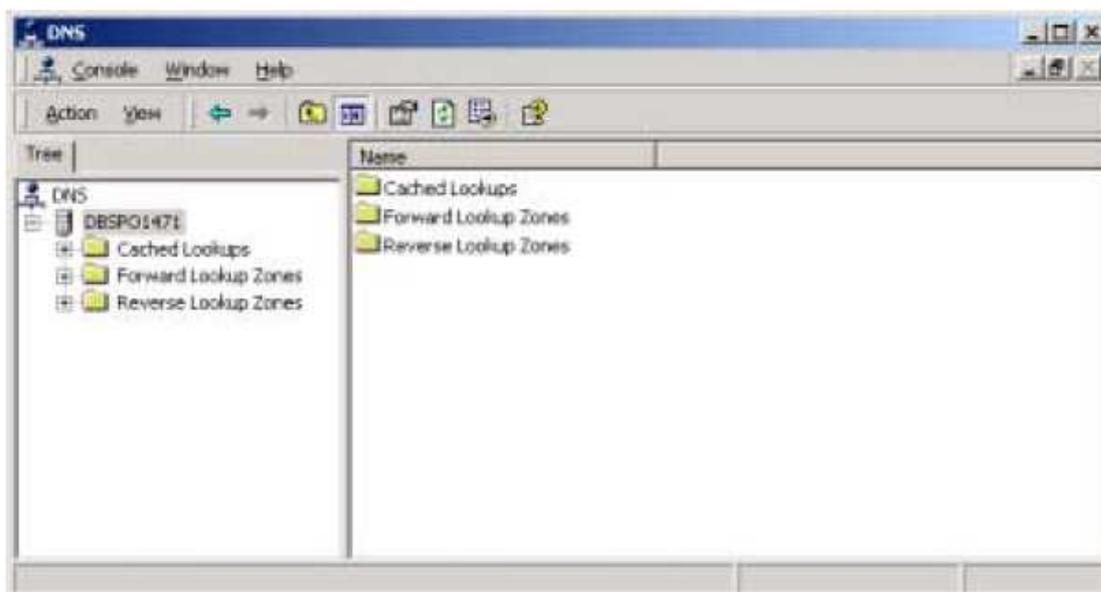


Figura 3 - Tela Inicial do DNS Manager em Servidores Windows 2000

Para adicionar um novo servidor, clique com o botão da direita do mouse em DNS e selecione a opção *New Server*. Cadastre o nome ou o endereço IP do novo servidores de DNS na janela *Add New Server*.



Figura 4 - Adicionando um Novo Servidor de DNS – Windows 2000

#### Criando um Domínio Direto Primário

Para cadastrar um domínio direto, clique com o botão direito do mouse na opção *Forward Lookup Zones* que está abaixo do servidor criado, e selecione *New Zone*.

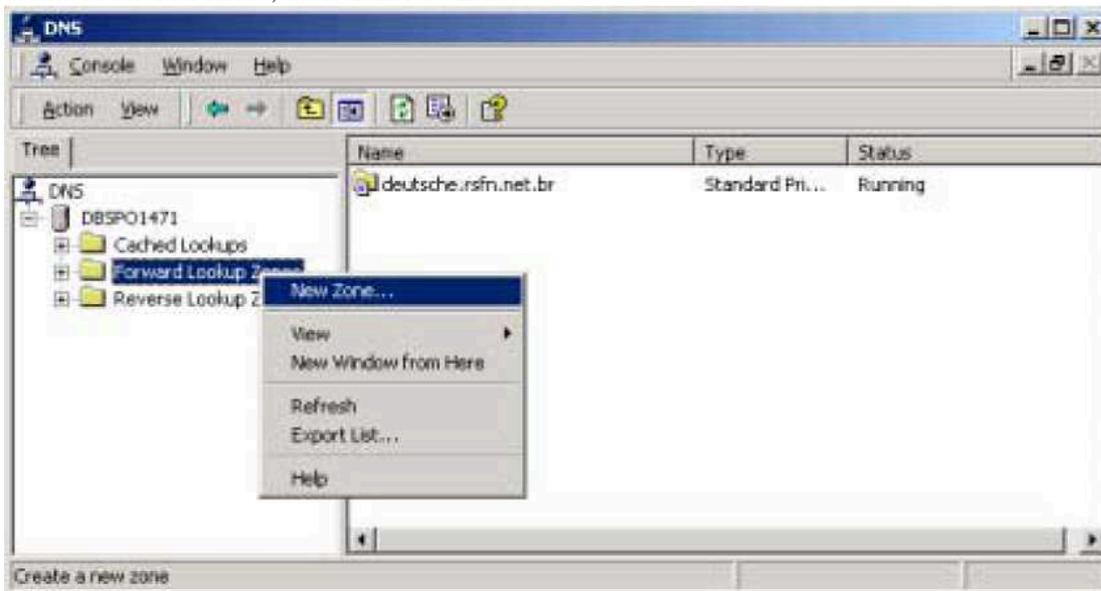


Figura 5 - Criando um Domínio Direto Primário – Windows 2000

Neste momento será iniciado um *Wizard* que coordenará todo o processo de criação do domínio. Clicando no botão *Next*, será solicitado o tipo de zona que se deseja criar. Clique na opção *Standard Primary* e em *Next* para continuar.

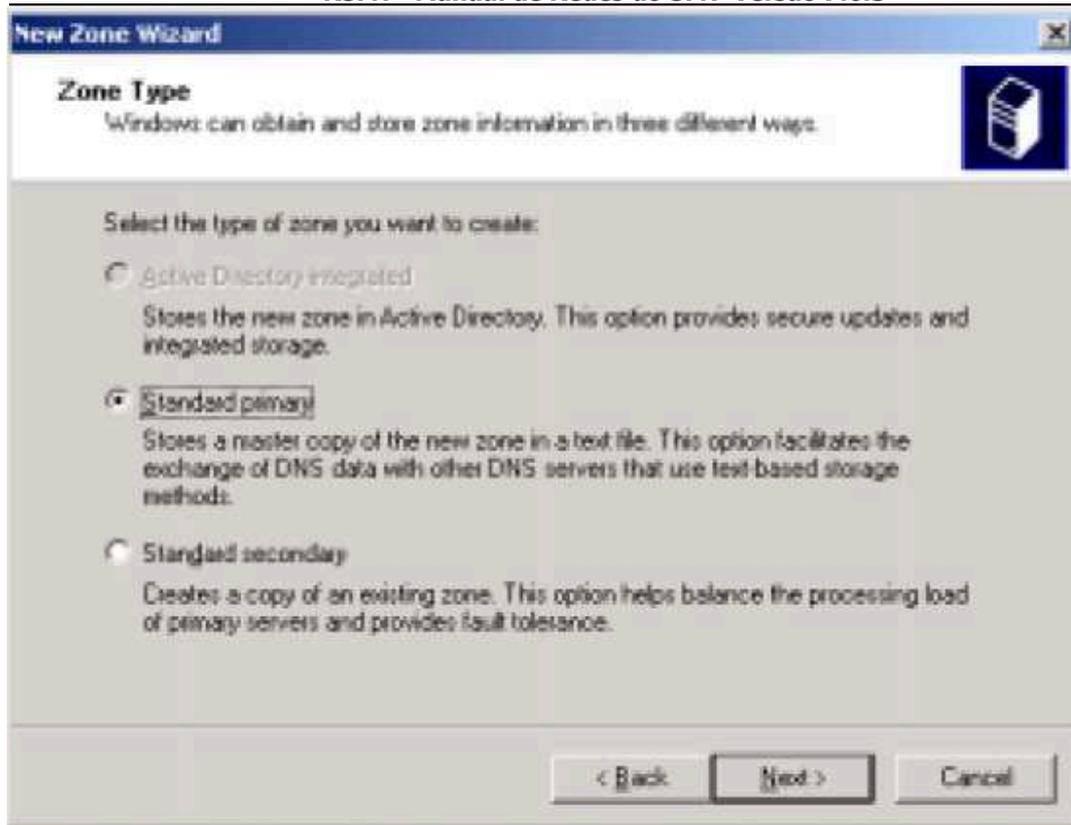


Figura 6 - Definindo o Tipo de Zona de DNS – Windows 2000

No campo *Name*, preencha com o nome do domínio a ser criado e clique em *Next* para continuar.

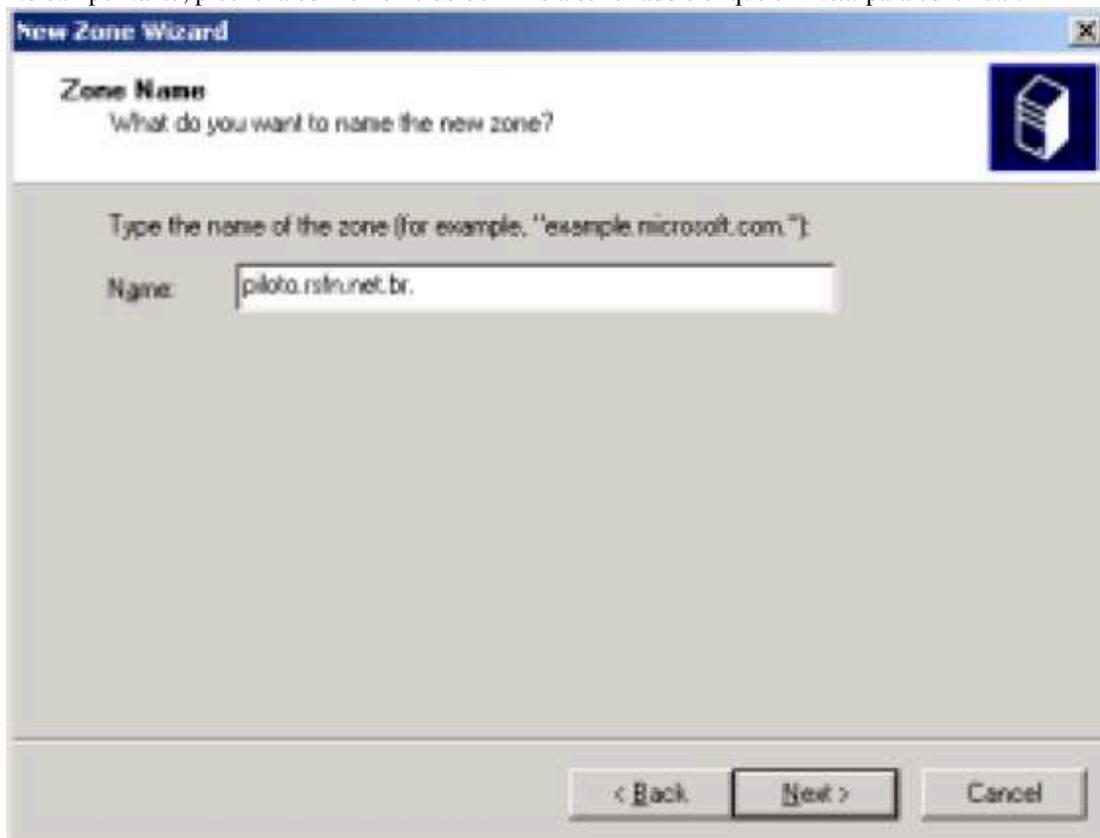


Figura 7 - Definindo o Nome de Zona de DNS – Windows 2000

Será apresentada uma tela para a confirmação do arquivo da zona que está sendo criada. É recomendável que se o utilize o mesmo nome da zona para o arquivo que está sendo criado através da opção *Create a new file with this file name*. Nesta mesma tela, tem-se a possibilidade de escolher um arquivo já existente. Após a definição do nome do arquivo, clique na opção *Next*.

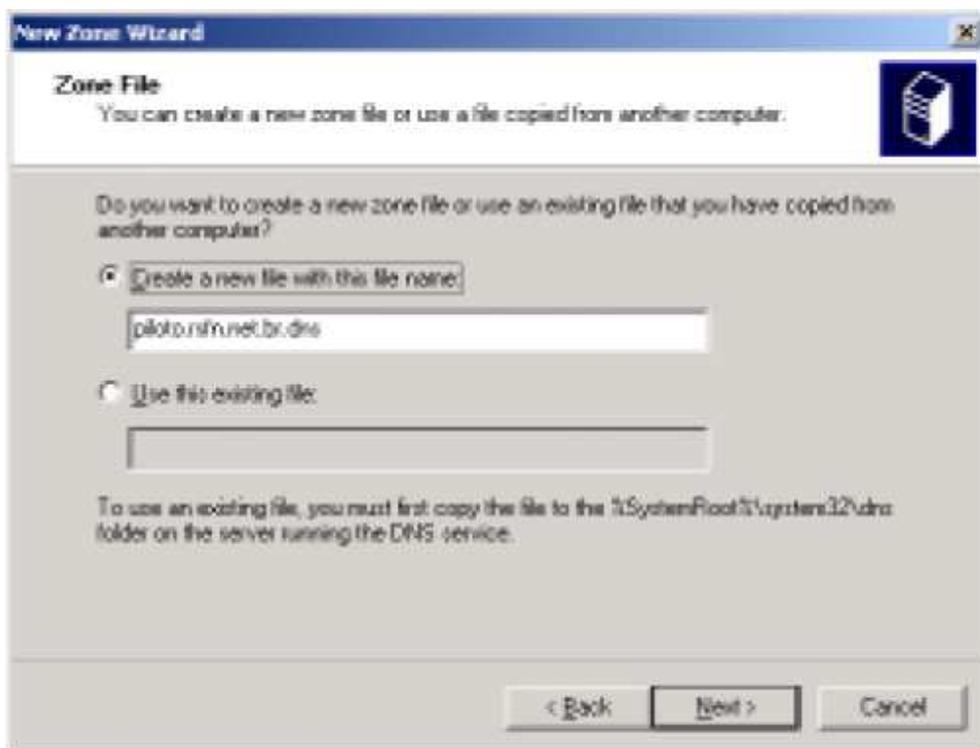


Figura 8 - Definindo o Nome do Arquivo de Zona do DNS – Windows 2000

A última tela do *Wizard* solicita uma confirmação dos dados fornecidos para a criação do novo domínio. Clique na opção *Finish* para confirmar e finalizar a criação do domínio direto primário.



Figura 9 - Criando um Domínio Direto Primário – Confirmação – Windows 2000

### Criando um Domínio Reverso Primário

Para cadastrar um domínio reverso, clique com o botão direito do mouse na opção *Reverse Lookup Zones* que está abaixo do servidor criado, e selecione *New Zone*.

Na tela *Zone Type* selecione a opção *Standard Primary*.

Na tela *Reverse Lookup Zone*, existem duas opções para o preenchimento do nome do domínio reverso. Na primeira opção, *Network ID*, deve ser cadastrado o endereço de rede do domínio reverso que está sendo criado. Na segunda opção, o campo

*Reverse lookup zone name* deve ser preenchido com o endereço da rede no formato invertido, adicionando-se o padrão *in-addr.arpa*. Para a criação de domínios reversos de sub-redes de endereços Classe C, que serão utilizados na RSFN, a segunda opção deve ser utilizada.

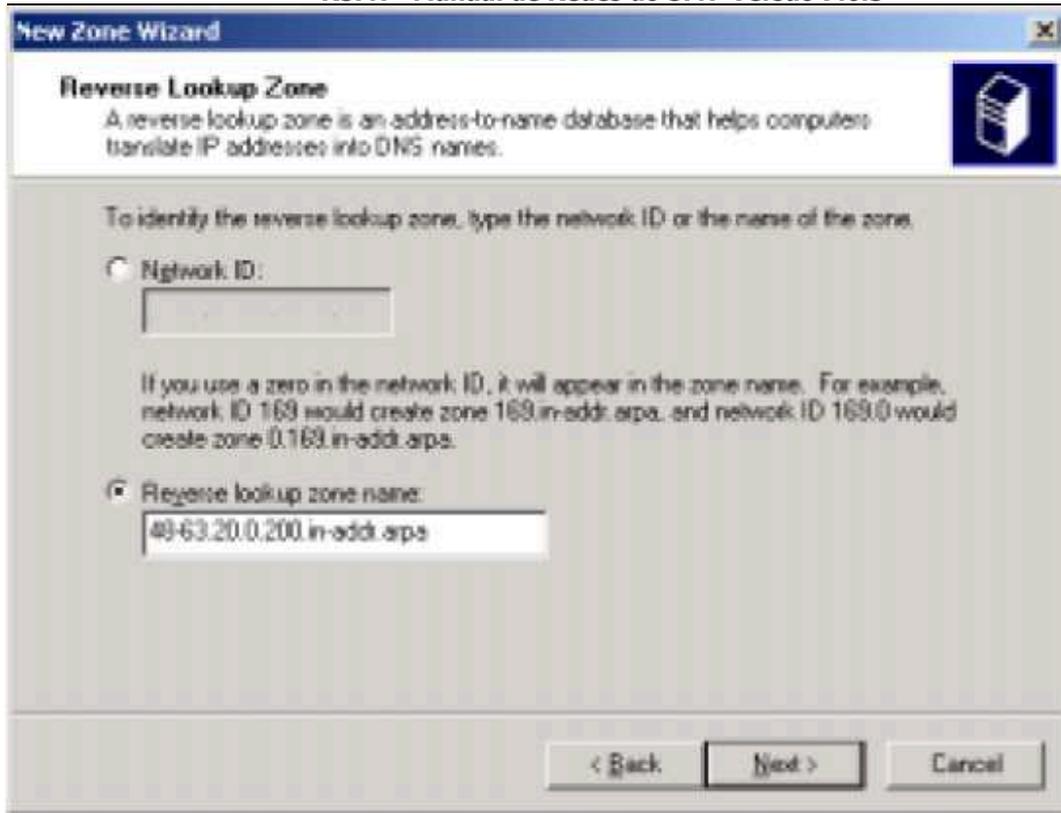


Figura 10 - Criando um Domínio Reverso Primário – Windows 2000

Clicando no botão *Next*, será apresentada uma tela para a confirmação do arquivo do domínio que está sendo criado. É recomendável que se utilize o mesmo nome do domínio, através da opção *Create a new file with this file name*, para identificar o arquivo que está sendo criado. Nesta mesma tela, tem-se a possibilidade de escolher um arquivo já existente, através da opção *Use this existing file*.

A última tela do *Wizard* solicita uma confirmação dos dados fornecidos para a criação do novo domínio reverso. Clique na opção *Finish* para confirmar e finalizar a criação do domínio reverso primário.



Figura 11 - Criando um Domínio Reverso Primário – Tela de Confirmação – Windows 2000

#### Criando um Domínio Direto Secundário

Para cadastrar um domínio direto secundário, clique com o botão direito do mouse na opção *Forward Lookup Zones* que está abaixo do servidor criado, e selecione *New Zone*. Na tela *Zone Type*, selecione a opção *Standard Secondary*.

Na tela *Zone Name*, preencha o campo *Name* com o nome do domínio a ser criado, e no campo *Server*, o endereço IP do servidor que está sendo configurado. Clicando no botão *Next*, será apresentada a tela para a confirmação do arquivo do domínio que está sendo criado.

Após a confirmação do nome do arquivo do domínio, digite o endereço IP do servidor *Master* do domínio secundário no campo *IP Master(s)* e clique no botão *Add* para adicioná-lo. Este campo permite que vários servidores *Masters* sejam cadastrados.

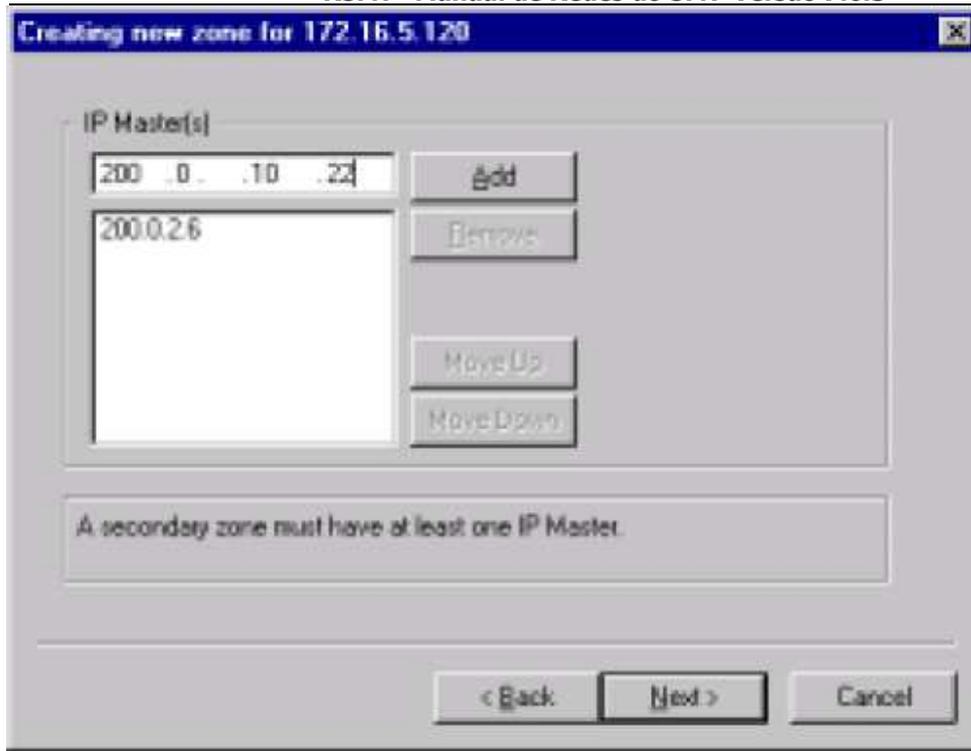


Figura 12 - Definindo os Servidores Masters do Domínio Direto Secundário- Windows 2000

A última tela do *Wizard* solicita a confirmação dos dados fornecidos para a criação do novo domínio. Clique na opção *Finish* para confirmar e finalizar a criação do domínio direto secundário.

### Criando um Domínio Reverso Secundário

Para cadastrar um domínio reverso secundário, clique com o botão direito do mouse na opção *Reverse Lookup Zones*, que está abaixo do servidor criado, e selecione *New Zone*. Na tela *Zone Type*, selecione a opção *Standard Secondary*.

Na tela *Reverse Lookup Zone*, existem duas opções para o preenchimento do nome do domínio reverso. Na primeira opção, *Network ID*, deve ser cadastrado o endereço da rede para a qual o domínio reverso está sendo criado. Na segunda opção, o campo *Reverse lookup zone name* deve ser preenchido com o endereço da rede no formato invertido, adicionando-se o padrão *in-addr.arpa*. Para a criação de domínios reversos de sub-redes de endereçamento Classe C, que serão utilizados na rede RSFN, a segunda opção deve ser utilizada.

Clicando no botão *Next*, será apresentada a tela para a confirmação do arquivo do domínio que está sendo criado. É recomendável que se utilize o nome do domínio, através da opção *Create a new file with this file name*, para identificar o arquivo que está sendo criado. Nesta mesma tela, tem-se a possibilidade de escolher um arquivo já existente, através da opção *Use this existing file*.

A última tela do *Wizard* solicita uma confirmação dos dados fornecidos para a criação do novo domínio reverso. Clique na opção *Finish* para confirmar e finalizar a criação do domínio reverso primário.

### Criando um Registro do Tipo A

Selecione o domínio direto no qual será criado o novo registro com o botão direito do mouse e escolha a opção *New Host*.

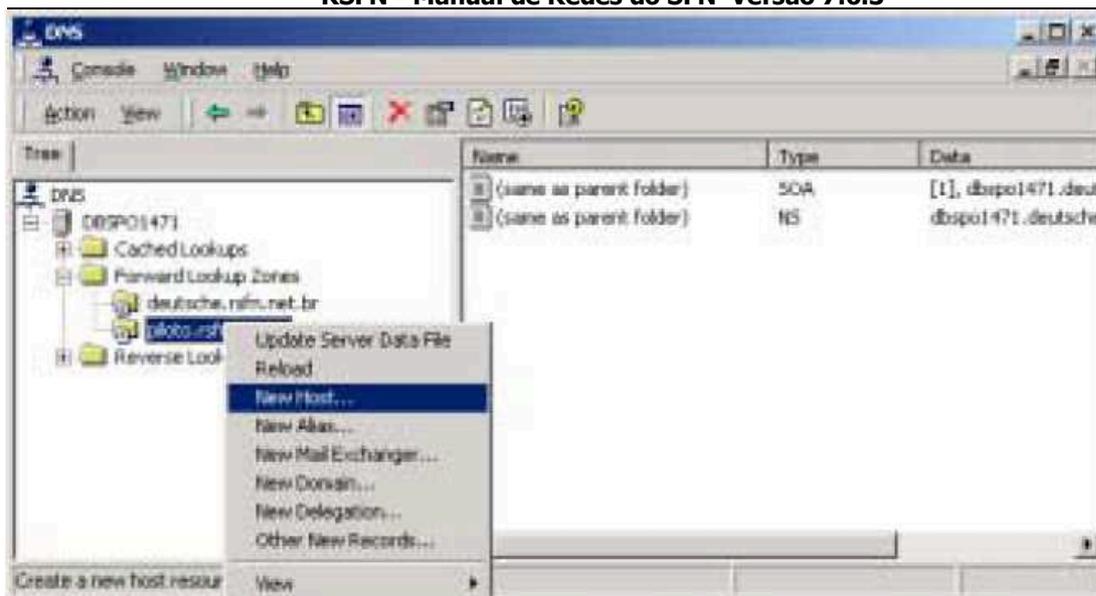


Figura 13 - Criando um Registro do Tipo A – Windows 2000

Na tela *New Host*, preencha os campos *Name* e *IP address*. Selecionando-se o item *Create associated pointer (PTR) record*, um registro PTR associado ao endereço IP do *host* será criado no domínio reverso correspondente. Para domínios reversos de sub-redes de endereçamento Classe C, este item não funciona corretamente e não deve ser marcado. A criação de registros PTR para endereços IP que fazem parte de uma sub-rede de endereçamento Classe C deve ser feita separadamente e será explicada posteriormente. Clique no botão *Add Host* para adicionar o registro.

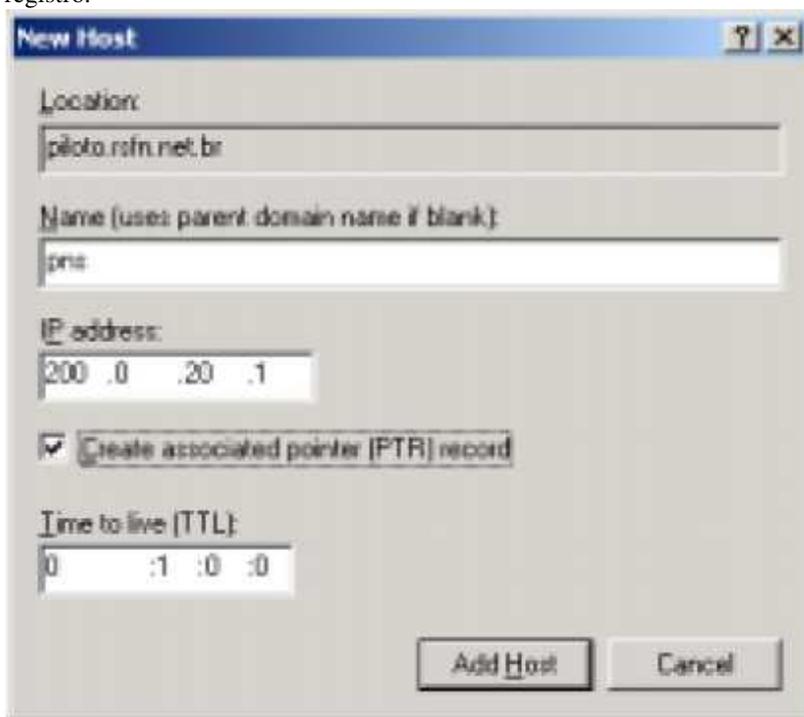


Figura 14 - Definindo as Características do Registro do Tipo A – Windows 2000

### Criando um Registro do Tipo PTR

Selecione o domínio reverso no qual será criado o novo registro com o botão da direita do mouse e escolha a opção *New Pointer*.

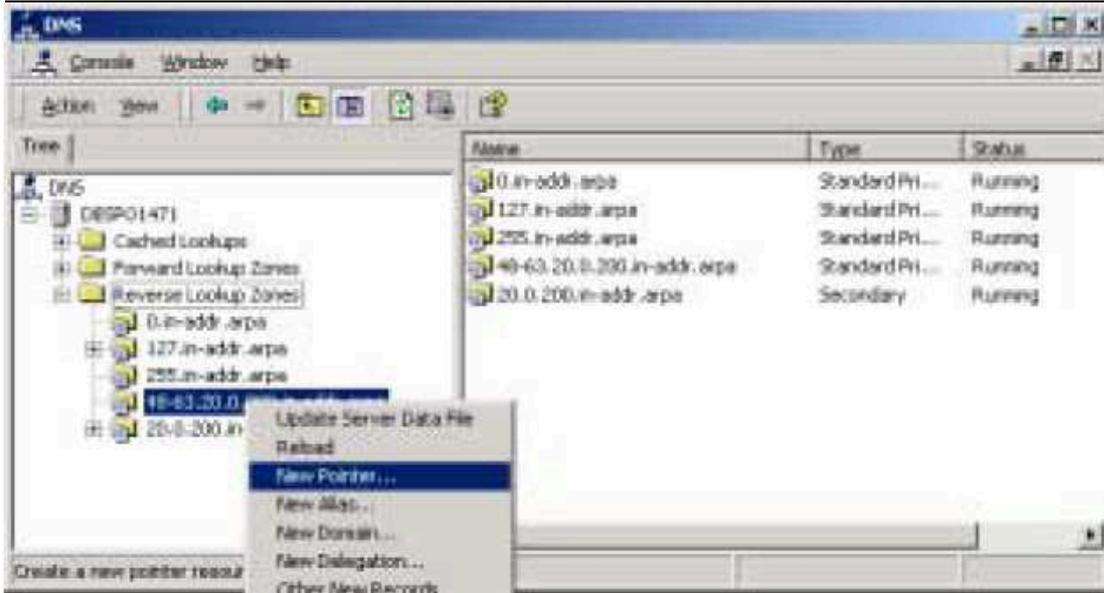


Figura 15 - Criando um Registro do Tipo PTR – Windows 2000

Na tela *New resource record*, cadastre no campo *Host IP number* o último octeto do endereço IP e no campo *Host Name* preencha com o nome completo (nome do *host* + domínio) do servidor. Clique em OK para finalizar a criação do registro PTR.

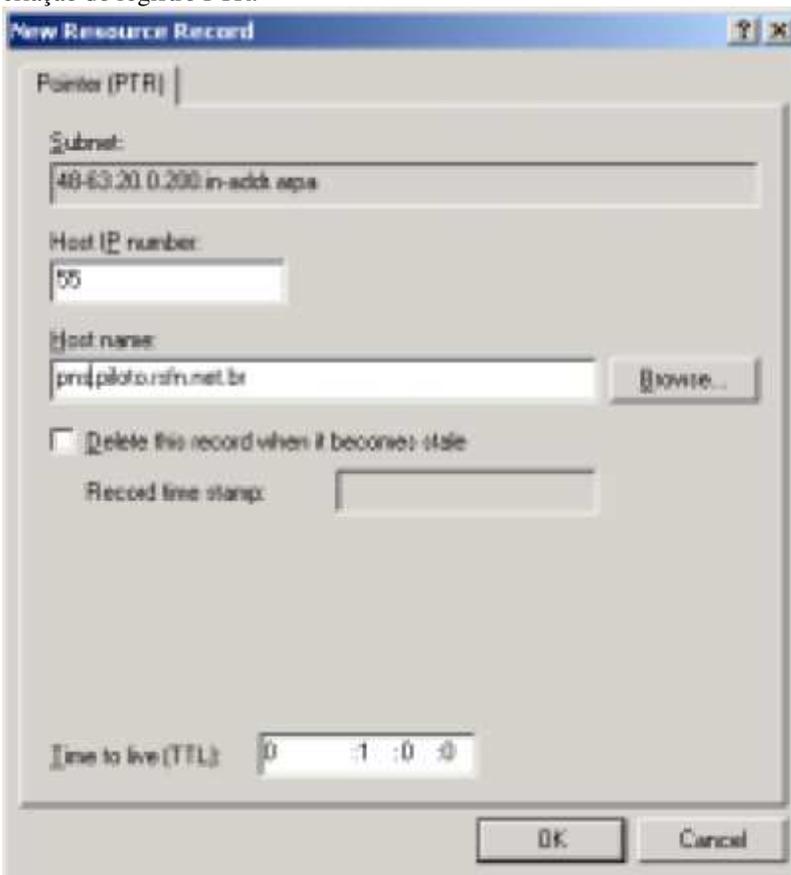


Figura 16 - Definindo as Características do Registro do Tipo PTR – Windows 2000

### Configurando os Servidores *Forwarders*

Conforme mencionado anteriormente, o DNS da Microsoft não permite a utilização da opção *Forward* para um domínio específico. Para contornar esta limitação, devem ser cadastrados os servidores genéricos de *forward*, que serão consultados quando uma *query* não for resolvida localmente.

Para cadastrar um *Forwarder* através do *DNS Manager*, selecione o servidor de DNS que está sendo utilizado na lista de servidores disponíveis com o botão da direita do mouse e escolha a opção *Properties*.

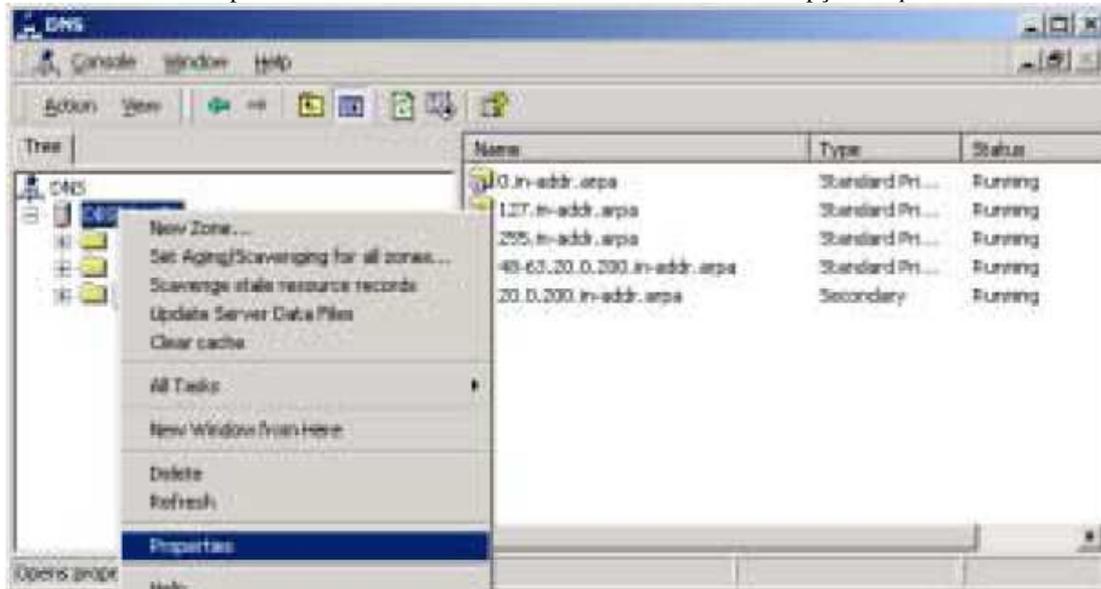


Figura 17 - Definindo as Configurações de Servidores de *Forward* Genéricos – Windows 2000

Na tela apresentada, selecione a pasta *Forwarders*. Clique no item *Enable Forwarders* para ativar a sua utilização e cadastre no campo *IP address* o endereço IP do servidor que será utilizado como *Forwarder*. Clique no botão *Add* para efetivar o cadastramento e no botão *OK* para fechar a tela.



Figura 18 - Definindo as Configurações de Servidores de *Forward* Genéricos – Windows 2000

#### SERVIÇO DNS EM AMBIENTE WINDOWS NT 4.0

Para iniciar a ferramenta *DNS Manager*, clique em *Start/Programs/Administrative Tools/DNS Manager*. Na tela inicial do *DNS Manager*, clique no ícone *Server List* para apresentar os servidores cadastrados.



Figura 19 - Tela Inicial do *DNS Manager* em Servidores Windows NT 4.0

Para adicionar um novo servidor, clique com o botão da direita do mouse no ícone *Server List* e selecione a opção *New Server*. Cadastre o nome ou o endereço IP do novo servidor de DNS na janela *Add New Server*.



Figura 20 - Adicionando Servidores de DNS em Servidores Windows NT 4.0

### Criando um Domínio Direto Primário

Para cadastrar um domínio direto, clique com o botão direito do mouse no servidor que foi criado e selecione *New Zone*.

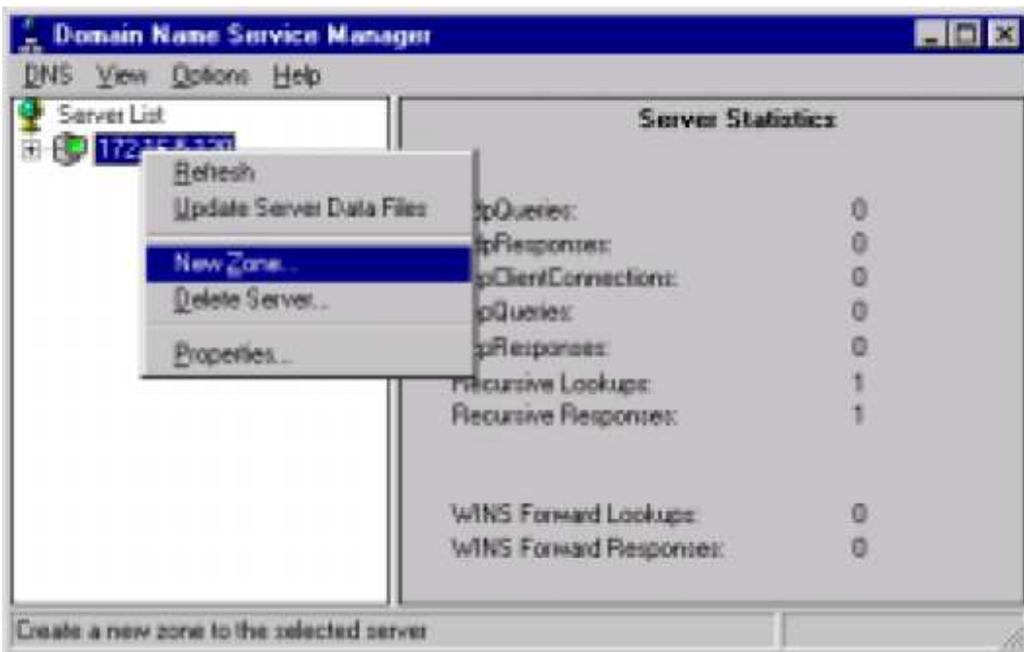


Figura 21 - Criando Nova Zona de DNS em Servidores Windows NT 4.0

Na tela *Zone Type* selecione a opção *Primary* e clique no botão *Next*.



Figura 22 - Definindo a Nova Zona de DNS como Primária - Servidores Windows NT 4.0

Na tela *Zone Info*, preencha o campo *Zone Name* com o nome do domínio a ser criado e pressione *Tab* para que o campo *Zone File* seja preenchido automaticamente. Clique em *Next* para finalizar a criação do domínio direto.



Figura 23 - Definindo a Nova Zona de DNS como Primária - Servidores Windows NT 4.0

### Criando um Domínio Reverso Primário

Para cadastrar um domínio reverso, clique com o botão direito do mouse no servidor que foi criado e selecione *New Zone*. Na tela *Zone Type* selecione a opção *Primary* e clique no botão *Next*. A tela *Zone Info* será apresentada,

preencha o campo *Zone Name* com o nome do domínio a ser criado e pressione *Tab* para que o campo *Zone File* seja preenchido automaticamente. Clique em *Next* para finalizar a criação do domínio direto.

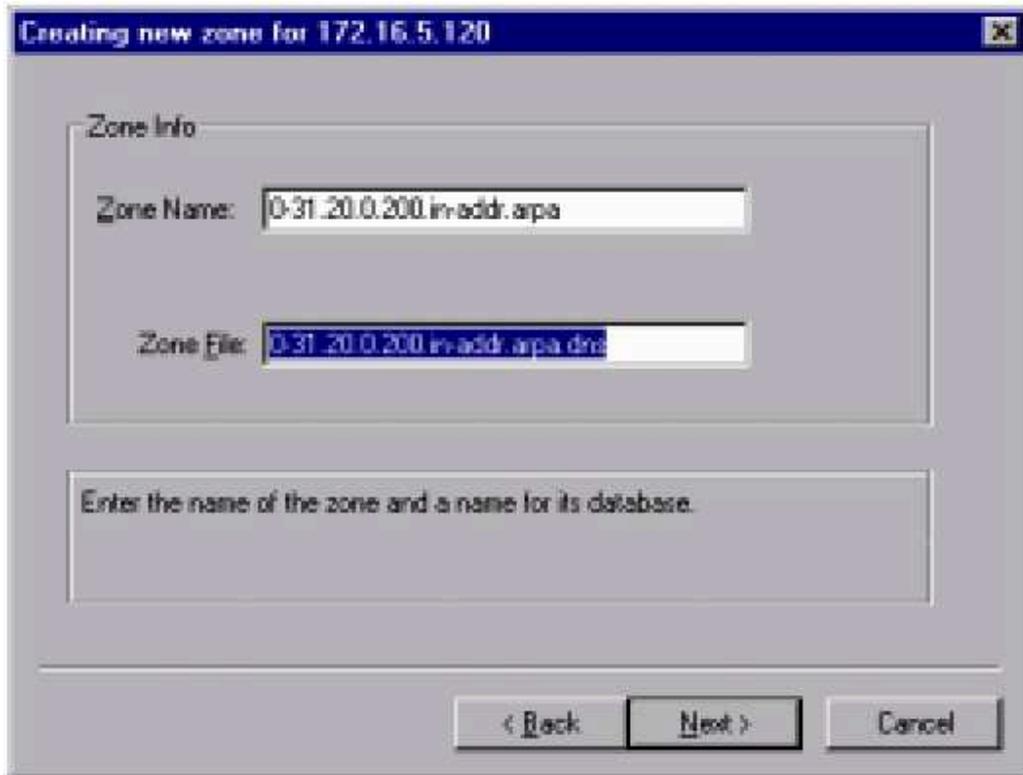


Figura 24 - Definindo a Nova Zona Reversa de DNS - Servidores Windows NT 4.0

#### Criando um Domínio Reverso Secundário

Para cadastrar um domínio reverso, clique com o botão direito do mouse no servidor que foi criado e selecione *New Zone*. Na tela *Zone Type*, selecione a opção *Secondary* e preencha o campo *Zone* com o endereço do domínio reverso a ser criado, em formato invertido, mais o padrão in-addr.arpa, e no campo *Server*, preencha com o endereço IP do servidor que está sendo configurado.

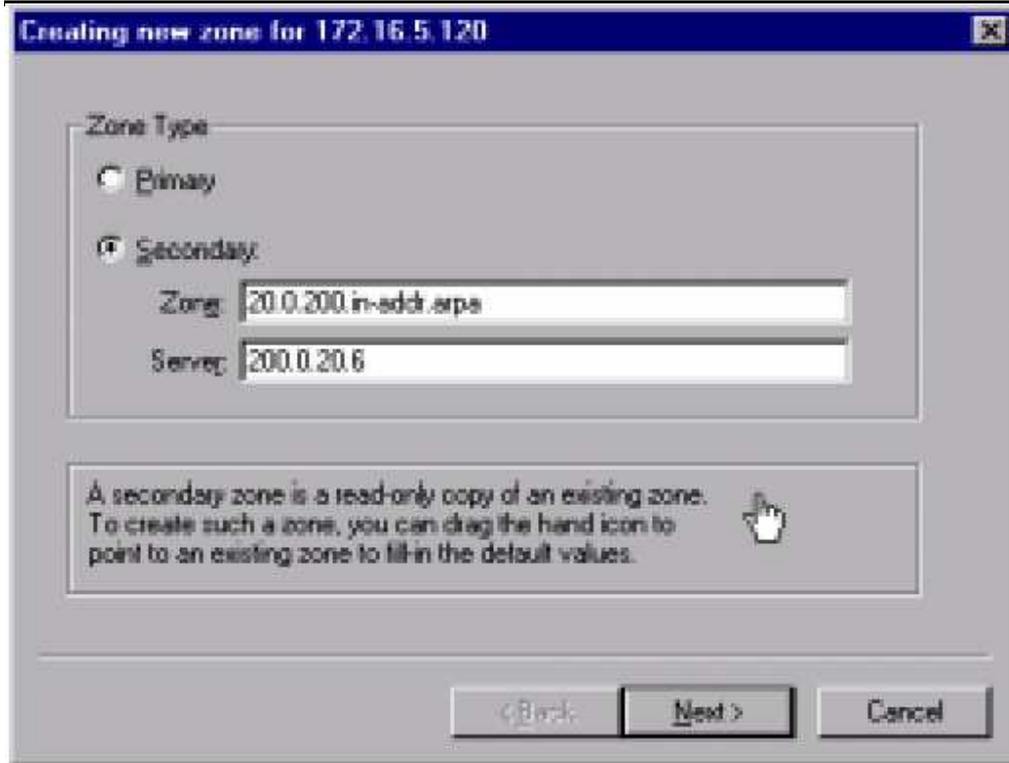


Figura 25 - Definindo uma Zona Reversa Secundária de DNS - Servidores Windows NT 4.0

Clicando no botão *Next*, será apresentada a tela *Zone Info*. Preencha o campo *Zone Name* com o nome do domínio a ser criado e pressione *Tab* para que o campo *Zone File* seja preenchido automaticamente.

Após a confirmação do nome do arquivo do domínio, digite o endereço IP do servidor *Master* do domínio secundário no campo *IP Master(s)* e clique no botão *Add* para adicioná-lo. Este campo permite que vários servidores *Masters* sejam cadastrados. Clique em *Next* para finalizar a criação do domínio reverso secundário.

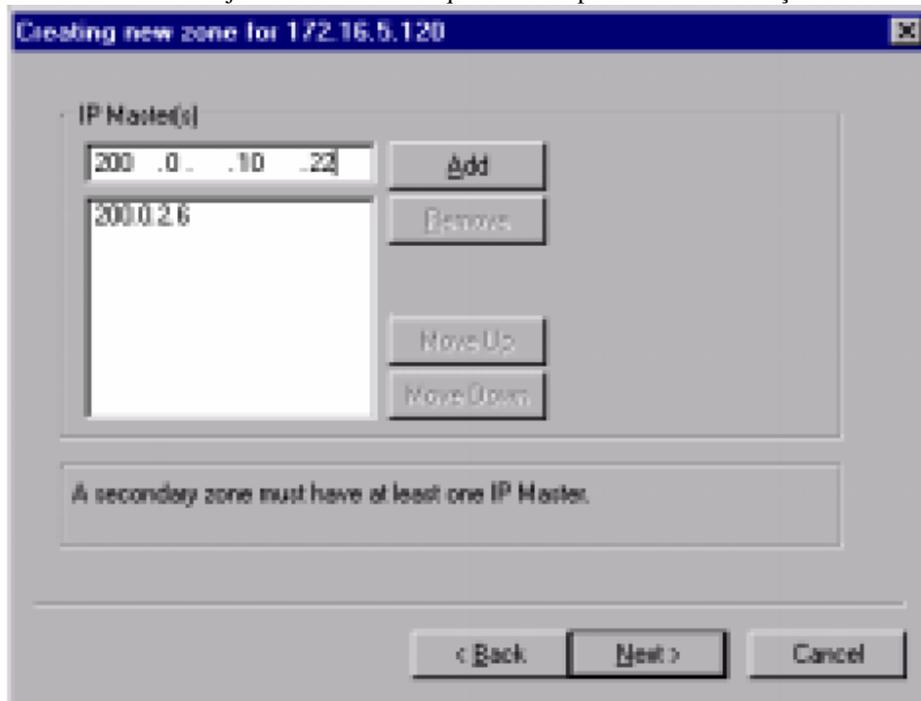


Figura 26 - Configuração dos Servidores *Masters* da Zona Reversa Secundária de DNS

### Criando um Domínio Direto Secundário

Para cadastrar um domínio direto secundário, clique com o botão direito do mouse no servidor que foi criado e selecione *New Zone*. Na tela *Zone Type*, selecione a opção *Secondary*, preencha o campo *Zone* com o nome do domínio direto, e o campo *Server* com o endereço IP do servidor que está sendo configurado.

Clicando no botão *Next*, será apresentada a tela *Zone Info*. Preencha o campo *Zone Name* com o nome do domínio a ser criado e pressione *Tab* para que o campo *Zone File* seja preenchido automaticamente.

Após a confirmação do nome do arquivo do domínio, digite o endereço IP do servidor *Master* do domínio secundário no campo *IP Master(s)* e clique no botão *Add* para adicioná-lo. Este campo permite que vários servidores *Masters* sejam cadastrados. Clique em *Next* para finalizar a criação do domínio direto secundário.

### Criando um Registro do Tipo A

Selecione o domínio direto no qual será criado o novo registro com o botão da direita do mouse e escolha a opção *New Host*.

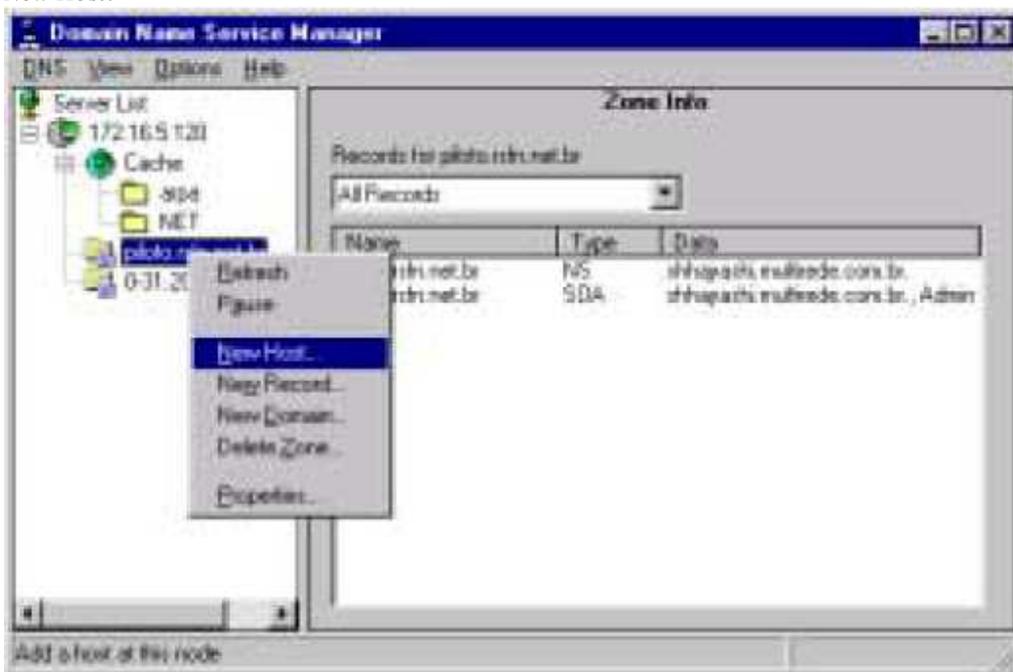
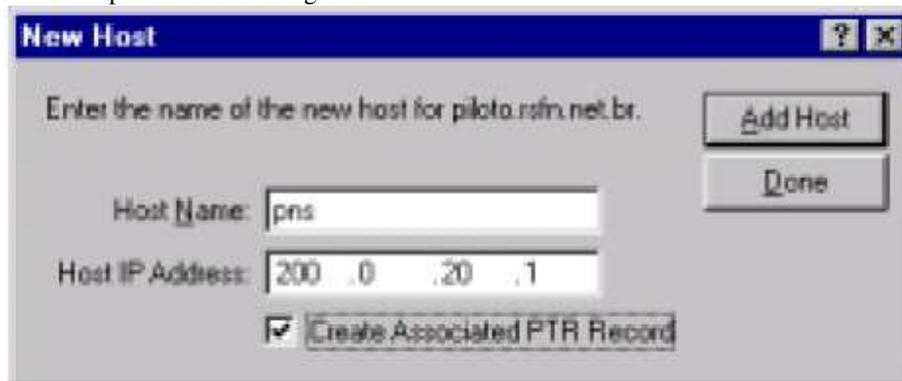


Figura 27 - Criando um Registro do Tipo A – Windows NT 4.0

Na tela *New Host*, preencha os campos *Host Name* e *Host IP address*. Selecionando-se o item *Create associated pointer (PTR) record*, um registro PTR associado ao endereço IP do host será criado no domínio reverso correspondente. Para domínios reversos de sub-redes de endereçamento Classe C, este item não funciona corretamente e não deve ser marcado. A criação de registros PTR para endereços IP que fazem parte de uma sub-rede de endereçamento Classe C deve ser feita separadamente e será explicada posteriormente. Clique no botão *Add Host* para adicionar o registro.



### Criando um Registro do Tipo PTR

A criação de registros PTR de uma sub-rede de endereço Classe C, através do utilitário *DNS Manager* de servidores Windows NT 4.0, não funciona corretamente. Neste caso, a criação destes registros deve ser feita de forma manual, ou seja, editando-se o arquivo de configuração do domínio reverso correspondente. Para isso, é necessário que o serviço de DNS esteja parado.

Para finalizar o serviço de DNS, clique em *Start/Settings/Control Panel/Services*, selecione o serviço *Microsoft DNS Server*, e clique no botão *Stop*. Os arquivos de configuração encontram-se no diretório *c:\winnt\system32\dns*. E possuem a extensão *.dns*. Utilize o *notepad* ou qualquer ferramenta de edição de arquivos texto para editá-los. Um exemplo de um arquivo de configuração de um domínio reverso está descrito a seguir:

```
@ IN SOA ns1.bcb.rsfn.net.br. spb_registro.bcb.rsfn.net.br. (
2001040901 ; Número de Série
8h ; Refresh após 8 horas
1h ; Retry após 1 hora
1w ; Expire após 1 semana
1d ) ; TTL de 1 dia
;
; Servidores de nomes deste domínio
;
IN NS ns1.bcb.rsfn.net.br.
IN NS ns2.bcb.rsfn.net.br.
;
; Equipamentos alocados neste dominio
;
1 IN PTR att-bacen-bsa-cpe.bcb.rsfn.net.br.
2 IN PTR ebtrtm-bacen-bsa-cpe.bcb.rsfn.net.br.
3 IN PTR hsrp-bacen-bsa-cpe.bcb.rsfn.net.br.
6 IN PTR pns.bcb.rsfn.net.br.
```

Após a inclusão dos registros PTR no arquivo de configuração, reinicie o serviço de DNS. Os registros PTR cadastrados manualmente deverão aparecer no *DNS Manager*.

Caso o registro PTR a ser criado não pertença a uma sub-rede de endereçamento Classe C, a ferramenta *DNS Manager* poderá ser utilizada. Dessa forma, selecione o domínio reverso no qual será criado o novo registro com o botão da direita do mouse e escolha a opção *New Pointer*.

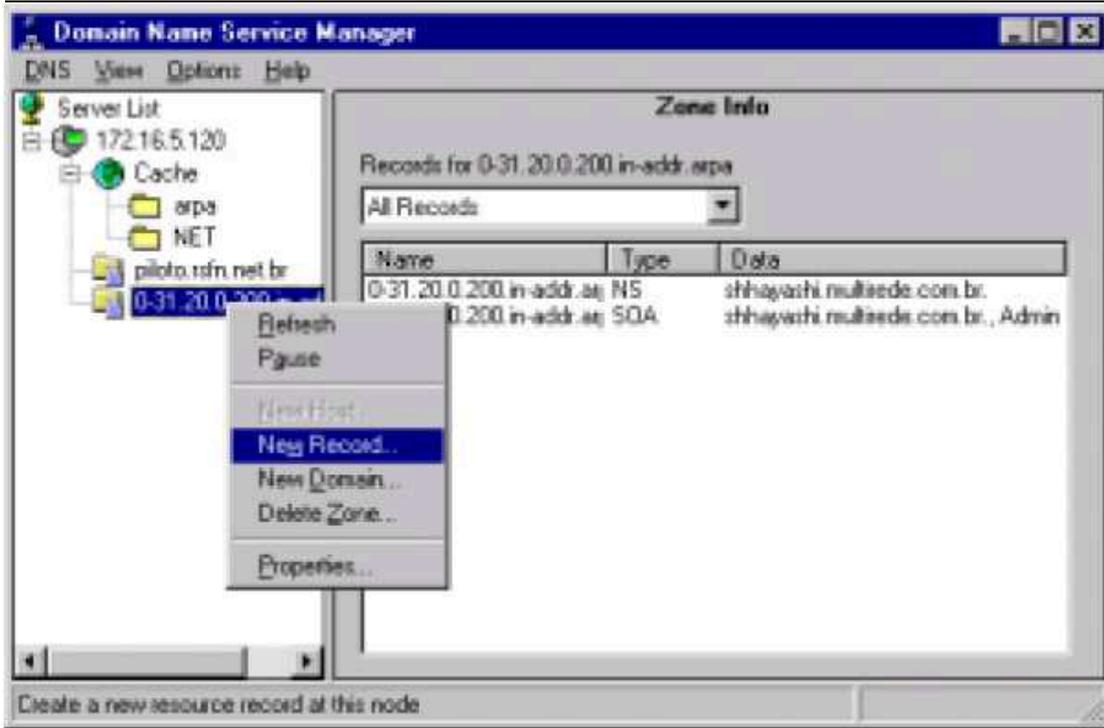


Figura 29 - Criando um Registro do Tipo PTR – Windows NT 4.0

Na tela *New resource Record*, selecione *PTR Record* na janela *Record Type*, cadastre no campo *IP Address* o endereço IP, e no campo *Host DNS Name*, preencha com o nome completo (nome do *host* + domínio) do servidor. Clique em *OK* para finalizar a criação do registro PTR.



Figura 30 - Definindo as Características do Tipo PTR – Windows NT 4.0

Configurando os Servidores *Forwarders*

Conforme mencionado anteriormente, o DNS da Microsoft não permite a utilização da opção *Forward* para um domínio específico. Para contornar esta limitação, devem ser cadastrados os servidores genéricos de *forward*, que serão consultados quando uma *query* não for resolvida localmente.

Para cadastrar um *Forwarder* através do *DNS Manager*, selecione o servidor de DNS que está sendo utilizado na lista de servidores disponíveis com o botão da direita do mouse e escolha a opção *Properties*.



Figura 31 - Configuração de Servidores de *Forwarders* – Windows NT 4.0

Na tela apresentada, selecione a pasta *Forwarders*. Clique no item *Use Forwarders* para ativar a sua utilização e cadastre o endereço IP do servidor que será utilizado como *Forwarder*. Clique no botão *Add* para efetivar o cadastramento e no botão *OK* para fechar a tela.



Figura 32 - Configuração de Servidores de *Forwarders* – Windows NT 4.0