Digitel

MANUAL DE INSTALAÇÃO E OPERAÇÃO

NetRouter 2G

205.1660.02-0

2007 - DIGITEL S.A. INDÚSTRIA ELETRÔNICA
Rua Dr. João Inácio, 1165
Bairro: Navegantes
CEP 90230-181 • Porto Alegre/RS • Brasil
Fone: (51) 3337.1999
Fax: (51) 3337.1923
http://www.digitel.com.br
E-mail: info@digitel.com.br

Este manual foi desenvolvido por:
SCIENTIFIC LINGUAGEM LTDA.
Fone: (51) 3388.5000
http://www.scientific.com.br
vendas@scientific.com.br

Projeto gráfico:
CONTEXTO MARKETING EDITORIAL LTDA.
Fone/Fax: (51) 3395.2515 / 3395.2404
E-mail: contexto@contextomkt.com.br

- É imprescindível a leitura atenta das informações gerais e das instruções de instalação constantes no manual antes de operar o produto.
- Para limpar o produto, desligue-o da alimentação. Não use produtos de limpeza líquidos, em pasta, aerossol ou abrasivos. Use um pano seco ou levemente umedecido e nunca deixe que líquidos ou materiais caiam sobre ou dentro do produto.
- Não exponha o produto à chuva nem às variações de temperatura ou umidade além das especificadas pelo manual.
- Sempre verifique se as conexões físicas estão perfeitamente encaixadas (conectores, plugues, cabos e acessórios) e tenha certeza de que estão de acordo com os itens que descrevem características técnicas, conexões e instalação do produto no manual. Somente efetue conexões físicas de produtos, periféricos ou acessórios quando o sistema estiver desligado.
- Alguns produtos da Digitel podem ser inseridos em gabinetes e bastidores sem a necessidade de desligar a fonte de alimentação. Neste caso, siga a orientação descrita no item Instalação do produto.
- No caso de produtos que são ligados à rede elétrica, nunca sobrecarregue as tomadas. Caso necessite usar extensão, utilize fios e tomadas compatíveis com a capacidade especificada.
- Não substitua peças do produto por outras não originais. Em caso de dúvida, procure sempre orientação no Centro de Assistência Técnica Digitel mais próximo.
- Tome todas as medidas de proteção antiestática e contra descargas elétricas, inclusive a instalação de aterramento, uso de filtros de energia ou estabilizadores de tensão e nobreaks.
- Os gabinetes devem ser instalados em uma superfície plana e firme. As frestas e aberturas não devem ser bloqueadas ou cobertas, pois servem para ventilação e evitam o superaquecimento. Garanta uma área livre de no mínimo 3,5 cm sobre o gabinete. Nunca empilhe os gabinetes.
- No caso de produtos Digitel que permitam empilhamento, verifique a descrição desse procedimento no item do manual que descreve a sua instalação.
- A Digitel se reserva o direito de alterar as especificações contidas neste documento sem notificação prévia.

Para informações sobre garantia e assistência técnica, consulte a seção no final deste manual.

• Índice

• Apresentação 8
• Descrição do produto 17
PRINCIPAIS CARACTERÍSTICAS 17
Roteamento IP 17
IP Masquerade 17
Implementação de servidores virtuais (Redirect) 17
Firewall 17
VPN 17
DHCP Server 18
Protocolo de interconexão: PPP 18
Protocolo de interconexão: HDLC-Cisco 18
Protocolo de interconexão: Frame Relay 18
Operação chaveada por demanda 18
Múltiplas interfaces 18
Monitoração dos sinais da interface 18
Controle de segurança 19
Armazenamento de configuração 19
Atualização de firmware 19
Autoteste e boot-up 19
Porta Console 19
Serviço Telnet 19
Serviço SSH 19
Gerenciamento SNMP 20
Dip-switch e modo de segurança (modelo NR-2G 4200) 20
Slots de expansão com hot-swap (modelo NR-2G 4200) 20
Expansão de memória interna (modelo NR-2G 4200) 20
• Instalação e configuração inicial 21
REQUISITOS PARA INSTALAÇÃO E CONFIGURAÇÃO INICIAL 21
CONEXÃO DA PORTA LAN0 21
CONEXÃO DA PORTA CONSOLE 21
MONTAGEM DO NETROUTER 2G 4200 22
INSTALAÇÃO DO MÓDULO 1X WAN (NR-2G-MW1-800.0923.00-7) 23
INSTALAÇÃO DOS MÓDULOS FXS (NR-2G-MV4/FXS-800.0924.00-3) E FXO (NR-2G-MV4/FXO-800.0935.00-5) 23
Inserção e retirada de módulos de voz 23
Integração de módulos ao NR-2G 4200 24
Ordenação das interfaces de voz no NR-2G 4200 25
Instalação de módulos adquiridos em separado 25
Instalação de software 25
CONFIGURAÇÃO DOS MÓDULOS DE VOZ FXS E FXO 26
Sintaxe dos nomes de extenções 26
Sintaxe básica da línguagem 27
RECONFIGURAÇÃO DOS ENDEREÇOS IP (OPCIONAL) 34
CONFIGURAÇÃO INICIAL VIA WEBCONFIG 34
CONFIGURAÇÃO INICIAL VIA CLI 35
• Painéis 36
PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 3200 36
PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 3250 37
PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 3260 38
PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 3280 39
PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 4200 40
Composição dos leds e conectores dos modelos NetRouter 2G - Série 3200 42
Indicador ST 42
Indicador LAN 42
Indicador AUX 42
Indicadores TD e RD 42
Indicadores WTD e WRD 42
Conector AUX 42
Conector WAN multiinterface 43
Dip-switch (modelo NR-2G 4200) 43
Chaves R0 e R1 (modelo NR-2G 4200) 44
Indicadores S0 e S1 (modelo NR-2G 4200) 44
Alimentação (modelo NR-2G 4200) 45
Alimentação (modelo NR-2G 3200) 45

- Cabos 46

CABO LAN CROSS (CB-LAN/X-NR) 46
CABO CONSOLE RJ (CB-CONS/AUX-NR) 46
ADAPTADOR TERMINAL DB9 (AD-RJ/TERM/DB9-NR) 47
ADAPTADOR TERMINAL DB25 (AD-RJ/TERM/DB25-NR) 48
ADAPTADOR MODEM DB25 (AD-RJ/MODEM/DB25-NR) 48
CABO PARA INTERFACE V.24/V.28 - RS232 (CB-V24-NR) 49
CABO PARA INTERFACE V.11/V.36 (CB-V36-NR) 50
CABO PARA INTERFACE V.35/MRAC34 (CB-V35-NR) 51
CABO PARA INTERFACE V.35/PADRÃO TELEBRÁS (CB-V35/PT-NR) 52
CABO PARA INTERFACE V.35/ISO2110 (CB-V35/ISO-NR) 53
CABO PARA INTERFACE V.35/NEWBRIDGE (CB-V35/NB-NR) 54
ADAPTADOR PARA INTERFACE G.703 (CB-G703-NR) 55

- Operação 56

INICIALIZAÇÃO E REINICIALIZAÇÃO DO EQUIPAMENTO 56
NR2GBOOT E OS MODOS DE OPERAÇÃO 56
MODO DE SEGURANÇA 56
Recuperando a configuração do roteador 58
Recuperando a versão de firmware 58
Limpando configuração do roteador 59
MODO DE OPERAÇÃO NORMAL 59
CONFIGURAÇÃO VIA WEBCONFIG 59
CONFIGURAÇÃO VIA CLI (TELNET/CONSOLE/SSH) 63

- Guia da CLI - Command Line Interface 64

INTRODUÇÃO A CLI 64
Acessando um equipamento via CLI 64
Categorias de comando 64
MODIFICANDO O USUÁRIO E A SENHA 68
MODIFICANDO O HOSTNAME DO EQUIPAMENTO 69
EXPORTANDO E IMPORTANDO ARQUIVOS DE CONFIGURAÇÃO 69
ATUALIZAÇÃO DE SOFTWARE 70
Atualização do sistema operacional 71
Atualização do BOOTLOADER e SOFTWARE 72
CONFIGURANDO ENDEREÇO ETHERNET 73
CONFIGURANDO ENDEREÇO ETHERNET VIRTUAL 74
CONFIGURANDO VLAN (802.1Q) 74
PROTOCOLO FRAME RELAY 74
PROTOCOLO PPP 76
PROTOCOLO PPP ASSÍNCRONO 77
PROTOCOLO HDLC 79
PROTOCOLO X25 79
CONFIGURAÇÃO PARA INTERFACE UNNUMBERED 80
ADICIONANDO ROTAS ESTÁTICAS 80
PROTOCOLOS DE ROTEAMENTO DINÂMICO 82
RIP (Routing Information Protocol) 82
OSPF (Open Shortest Path First) 83
NAT (NETWORK ADDRESS TRANSLATOR) 84
Introdução 84
Configurando NAT MASQUERADE 84
Configurando NAT REDIRECT 84
Configurando NAT 1:1 85
Configurando NAT EXCLUSION 85
Configurando NAT POOL 86
HABILITANDO O SNMP - SIMPLE NETWORK MANAGMENT PROTOCOL 86
IP TUNNELING 87
GRE (Generic Routing Encapsulation) 87
PPTP (Point-to-Point Tunneling Protocol) 88
L2TP (Layer 2 Transport Protocol) 89

IPSEC - SECURE IP OVER THE INTERNET 90
Introdução 90
Protocolos do IPSEC 91
DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) 94
DHCP Server 95
DHCP Reservation 96
DHCP Relay 96
CONFIGURAÇÃO DE PROTOCOLO BRIDGE 97
QUALIDADE DE SERVIÇO (QOS) 98
Controle de tráfego 98
Disciplinas de serviço 98
FIREWALL 101
Introdução 101
Politicas 101
Cadeias (chains) 101
Especificando inversão 102
Especificando fragmentos 103
Parâmetros de configuração 103
SISTEMAS DE AUTENTICAÇÃO 105
Introdução 105
RADIUS 106
TACAS 107
ESTATÍSTICAS DE INTERFACE 107
WAN (todos os protocolos - interface HDLC) 107
WAN (protocolo HDLC - Cisco) 109
WAN (protocolo FRAME RELAY - interface HDLC) 109
WAN (protocolo FRAME RELAY - interface PVC) 109
WAN (protocolo X25 - interface HDLC) 109
LAN (todos os protocolos - interface ETH) 109
SYSLOG 110
Facility 111
Priority (Level) 111
VRRP (VIRTUAL ROUTER REDUNDANCY PROTOCOL) 112
Definições 112
Configuração 113
PROTOCOLO CRTP 114
PROTOCOLO NTP 115
LISTA COMPLETA DE COMANDOS 118
Configuração de Sistema - SYSTEM 118
Configuração de Ethernet/LAN 119
Configuração de Interface WAN 120
Configuração de Rotas Estáticas - ROUTES 123
Configuração de Linha Backup - BACKUP 123
Configuração de Roteamento Dinâmico - RIP 123
Configuração de Roteamento Dinâmico - OSPF 124
Configuração de Roteamento dinâmico Avançado - ZEBRA 125
Configuração de NAT 125
Configuração de Túneis - GRE 126
Configuração de VPN - PPTP 126
Configuração de VPN - L2TP 126
Configuração de VPN - IPSEC 127
Configuração de Protocolo DHCP 128
Configuração de Protocolo SNMP 129
Configuração de Protocolo IPX 129
Configuração de Protocolo BRIDGE 129
Configuração de Firewall 130
Configuração de Qualidade de serviço IP - QOS 132

Configuração de Protocolo VRRP 133
Configuração de IP Accounting 133
Configuração da Tabela ARP 133
Configuração de PPPoE (PPP over Ethernet) 134
Configuração de Interface LoopBack 134
Configuração de XOT (X25 over TCP) 134

- Atualização de software 135

ATUALIZAÇÃO DO SISTEMA OPERACIONAL 135
ATUALIZAÇÃO DO BOOTLOADER (NR2GBoot) 135

- Especificações 137

- Aplicações 144

ESCRITÓRIOS REMOTOS 144
BACKBONE REGIONAL 145
ACESSO À INTERNET 145
INTERCONEXÃO VIA INTERNET - EXTRANET 146
INTERNETWORKING SOBRE REDE FRAME RELAY 147
APLICAÇÕES COM ROTEADORES GPRS, EDGE E CDMA 148
Aplicação Típica 148
Roteador GPRS como Backup de outro Roteador 149
Máquina X.25 sobre GSM/GPRS 149
Roteador GPRS com Dial Backup 150
GSM/GPRS como Backup de porta WAN Serial 151
GSM/GPRS como Backup de acesso Ethernet 151

- Assistência técnica e garantia 154

• Apresentação

A segunda geração de roteadores da Digitel, NetRouter 2G, consiste de uma família de roteadores de acesso de altíssima performance, destinados principalmente ao mercado corporativo, atendendo qualquer porte de empresa ou rede. Com um razoável conjunto de características, como interfaces, protocolos e serviços, atendem a um grande número de utilizações, aplicáveis nas mais variadas redes de comunicação de dados disponíveis na atualidade. Os novos modelos, a seguir apresentados, demonstram a evolução da linha de roteadores e são o resultado da manutenção do objetivo de possuir uma linha própria, garantido pelo continuo investimento da Digitel no desenvolvimento e na fabricação de produtos IP.

Desenvolvida para atender aplicações de roteadores do tipo CPE (acesso), a família NetRouter 2G é composta por diversos modelos, atendendo as mais variadas combinações de interfaces WAN e LAN utilizadas no mercado. Através de seu modelo modular, NR-2G 4200, oferece inclusive solução convergente de voz e dados com os módulos VoIP. Mas a grande novidade fica por conta dos modelos de roteadores com opção de interfaces WAN/ Wireless, podendo ser utilizados em aplicações com redes celulares GSM (GPRS ou EDGE) e CDMA.

A família NetRouter 2G apresenta, entre outras inovações, uma arquitetura de hardware de alta performance, baseada em processadores Power PC RISC de 32 bits, permitindo desempenho superior a modelos similares do mercado, com capacidade de trabalhar na porta WAN em velocidades de até 5 Mbps, na porta LAN até 100 Mbps e suportar a criptografia 3DES (chave de 168 bits) ou AES (chave de 256 bits) sem a necessidade de hardware adicional.

Com sistema operacional próprio, desenvolvido pela Digitel e baseado em Linux embarcado, incorpora as últimas novidades em facilidades e protocolos do ambiente de redes, como Firewall, controle de tráfego (QoS) e VPN/IP de última geração (IPSec/3DES/AES). A utilização de um sistema operacional aberto permite uma rápida incorporação de novidades tecnológicas que venham a surgir no mercado.

A família NR-2G é basicamente subdividida em duas arquiteturas e portes de produto: os modelos 3200 e o modelo 4200. Os modelos de prefixo 3200 apresentam diversas opções com diferentes combinações fixas de interfaces LAN, WAN/Serial, WAN/Wireless e WAN/Auxiliar. O 4200 é um modelo único, de arquitetura modular, que já traz em sua unidade básica duas interfaces LAN, duas portas WAN/Serial e dois slots (posições) para instalação de módulos opcionais, como o acréscimo de interfaces de voz ou expansão do número de portas WAN/Serial.

Após o consagrado sucesso nos roteadores de primeira geração da Digitel, é mantido o conceito de facilidade e simplificação na configuração e supervisão do roteador através de uma interface web browser. Incorpora também uma interface avançada para configuração, diagnóstico e manutenção, a partir de linhas de comando (CLI), que podem ser executados diretamente na porta console do roteador ou através de um acesso Telnet ou SSH (Telnet Seguro - criptografado).

Neste momento, a família NetRouter 2G é composta por três séries.

- Série NR-2G 4200 é composta por um único modelo, modular, que já traz em sua unidade básica duas interfaces LAN, duas portas WAN/Serial e dois slots (posições) para instalação de módulos opcionais, como módulos com interface de voz ou expansão do número de portas WAN/Serial.
- Série NR-2G 3200, composta por diversos modelos de roteadores convencionais, com diferentes combinações de interfaces LAN, WAN/Serial e WAN/Auxiliar.
- Série NR-2G 3250 GPRS, composta por diversos modelos de roteadores GPRS, com diferentes combinações de interfaces LAN, WAN/Serial e WAN/Auxiliar, mas sempre com uma interface WAN/Wireless para redes celulares GSM, somente na tecnologia GPRS.
- Série NR-2G 3260 EDGE, composto por diversos modelos de roteadores EDGE, com diferentes combinações de interfaces LAN, WAN/Serial e WAN/Auxiliar, mas sempre com uma interface WAN/Wireless para redes celulares GSM, suportando as tecnnologias GPRS e EDGE; e
- Série NR-2G 3280 CDMA, composta por diversos modelos de roteadores CDMA, com diferentes combinações de interfaces LAN, WAN/Serial e WAN/Auxiliar, mas sempre com uma interface WAN/Wireless para redes celulares CDMA.

Os modelos que seguem a arquitetura 3200 possuem combinações fixas de interfaces e são imutáveis, pois não são modulares. Embora suportem e tratem o tráfego de voz sobre IP (VoIP), não possuem a interface física de voz, podendo ser utilizados com gateways de voz externos. Para soluções em que seja necessária total integração, é indicado o modelo 4200, que, com a instalação de módulos de voz, incorpora a funcionalidade de gateways de voz internos.

O quadro-resumo a seguir apresenta as interfaces suportadas por cada modelo da família NetRouter 2G:

Modelo NR-2G	LAN 10/100	WAN Serial Mbps	WAN Auxiliar	WAN Wireless	GPRS EDGE CDMA	Console	Memória Flash/RAM MB	Slots p/ Módulos Adicionais
4200	2	2	-	-		1	32/128[1]	2
3201	1	1	1[2]	-		1	08/16	-
3211	1	1	-	-		1	16/32	-
3212	1	1	1	-		1	16/32	-
3214	2	1	1	-		1	16/32	-
3218	2	2	1	-		1	16/32	-
3238	2	2	1	-		1	16/64	-
3251	1	-	-	1	GPRS	1	16/32	-
3252	1	-	1	1	GPRS	1	16/32	-
3254	2	-	1	1	GPRS	1	16/32	-
3258	2	1	1	1	GPRS	1	16/32	-
3261	1	-	-	1	EDGE	1	16/32	-
3262	1	-	1	1	EDGE	1	16/32	-
3264	2	-	1	1	EDGE	1	16/32	-
3268	2	1	1	1	EDGE	1	16/32	-
3281	1	-	-	1	CDMA	1	16/32	-
3282	1	-	1	1	CDMA	1	16/32	-
3284	2	-	1	1	CDMA	1	16/32	-
3288	2	1	1	1	CDMA	1	16/32	-

Tabela 1. Modelos da família NetRouter 2G

[1] Limite de memória RAM reconhecida pelo equipamento. Capacidade padrão de fábrica é 32MB.

[2] Interface com montagem opcional.

A seguir, uma breve descrição das interfaces utilizadas pelos diferentes modelos da família NetRouter 2G:

- LAN: a interface LAN de todos os modelos opera a 10 ou 100 Mbps, autosense, half ou full duplex. Todos os modelos possuem pelo menos uma interface LAN e alguns possuem uma segunda interface LAN (não é HUB ou Switch);
- WAN/Serial: é uma porta WAN serial com opção de múltiplas interfaces (MI), suportando velocidades até 5 Mbps e operando com os protocolos PPP síncrono ou assíncrono, HDLC-Cisco, Frame Relay ou X.25, no modos dedicado, ou com o protocolo PPP assíncrono no modo discado (*dial on demand* e *dial backup*). Dependendo do modelo, essa interface pode não existir, ou pode ter até duas portas WAN/Serial. A definição da interface elétrica (V.24/V.28 (RS-232), V36, V.35 e G.703) é dada pelo cabo serial utilizado, onde também é feita a compatibilização mecânica da interface desejada (observar pinagem específica para cabo Digitel);
- WAN/Auxiliar: é uma interface auxiliar do tipo RS-232 (V.24/V.28), que suporta velocidades até 115,2 kbps e opera com o protocolo PPP assíncrono, nos modos dedicado ou discado (*dial on demand e dial backup*). O modem (DCE) não faz parte do equipamento (deve ser um modem externo), podendo ser modem analógico (V.90), terminal ISDN ou modem celular externo. Nem todos os modelos possuem porta WAN/Auxiliar;
- WAN/Wireless: é uma interface área para acesso a redes de operadoras celulares CDMA (tecnologia 1xRTT) ou GSM (tecnologia GPRS ou EDGE). Utiliza um módulo modem integrado ao equipamento (modem interno). Quando for utilizado um dos modelos para operação com rede celular GSM (GPRS ou EDGE), deve ser instalado o SIM Card devidamente habilitado pela operadora em questão. O modelo EDGE suporta tecnologia para acesso a redes GPRS e EDGE.

- Console: todos os modelos possuem uma interface RS-232 (V.24/V28), que suporta velocidades até 230,4 kbps e possui duas funcionalidades definidas por configuração:

  • interface física dedicada a configuração e supervisão da unidade (TTY), ou seja, a porta console propriamente dita (função *default*); e

  • interface WAN Auxiliar para operação em modo discado (*dial on demand e dial backup*) com protocolo PPP assíncrono, comandada por configuração.

O cabo adaptador, ligado ao conector correspondente no painel traseiro do equipamento, irá configurar a porta serial de acordo com o tipo de interface elétrica selecionada. Os cabos de adaptação de interface das portas WAN devem ser solicitados separadamente, conforme a tabela abaixo.

Cabo WAN interface V.24/V.28 (RS-232)	CB-V24-NR	código 810.0293
Cabo WAN interface V.36	CB-V36-NR	código 810.0290
Cabo WAN interface V.35 padrão MRAC34	CB-V35-NR	código 810.0289
Cabo WAN interface V.35 padrão TELEBRAS	CB-V35/PT-NR	código 810.0291
Cabo WAN interface V.35 padrão ISO 2110	CB-V35/ISO-NR	código 810.0297
Cabo WAN interface V.35 padrão Newbridge	CB-V35/NB-NR	código 810.0323
Cabo WAN interface G.703 2 Mbps	CB-G703-NR	código 810.0349

Os roteadores NR-2G já saem de fábrica com um MAC Address individualizado, com ID Company privado da Digitel, registrado no IEEE (*Institute of Electrical and Electronics Engineers*). O software já é carregado na fábrica, mas o usuário pode realizar atualizações em campo quando necessário (o site da Digitel possui sempre a versão mais atualizada).

Todos os modelos possuem opção de alimentação AC ou DC. Originalmente, é disponibilizada a opção de alimentação AC, enquanto que a opção de alimentação DC deve ser feita na ocasião da colocação do pedido de compra. Se não for definida a opção de alimentação por ocasião do pedido, o equipamento será fornecido com alimentação AC.

O conjunto de características implementadas na família NetRouter 2G é suficiente para atender desde as necessidades básicas de *internetworking* com roteadores de acesso até aplicações mais complexas, sempre garantindo uma excelente relação custo benefício. A seguir, destacamos algumas das principais características:

- porta WAN/Serial, síncrona ou assíncrona, com múltiplas interfaces (RS-232, V.36, V.35 e G.703/2 Mbps), para velocidades até 5 Mbps;
- protocolo Frame Relay, sem limite de DLCIs, nos modos ANSI, ITU, ou sem LMI;
- roteamento estático ou dinâmico (BGP4, OSPF, RIP ou RIP2);
- segunda interface LAN, em alguns modelos, para soluções de redes mais seguras;
- possibilidade de configuração de vários endereços IP por interface LAN;
- servidor DHCP para o fornecimento de endereço IP e default gateway;
- DHCP Relay para aplicações que tenham um servidor DHCP centralizado;
- compartilhamento de endereços IP através de NAT;
- firewall do tipo *statefull inspection* com filtros de datagramas por endereços IP de origem ou destino e intervalos de portas TCP (sockets) ou UDP (de destino) e lista de acesso (*access list)*;
- protocolos PPTP, L2TP e GRE para tunelamento (VPN) (o PPTP não é suportado pelo modelo 3201);
- IPSec para redes VPN seguras, inclusive com criptografia 3DES (chave de 168 bits) e AES (chave de até 256 bits) (menos no modelo 3201);
- Suporte a priorização de pacotes, limitação de banda, balanceamento de carga e controle de congestionamento, através de ferramentas de QoS;
- acionamento de discagem por demanda (*dial on demand*);
- acionamento de discagem por contingência ou sobrecarga do link principal - *dial backup*, nos modelos com mais de uma porta WAN;
- acionamento de acesso *wireless* como contingência ou sobrecarga do link principal - *backup* sobre GPRS, (modelos *wireless*);

- solução de alta disponibilidade com um segundo gateway redundante, através do protocolo VRRP(menos no modelo 3201);
- suporte a aplicações com virtual LAN (VLAN), IEEE 802.1q;
- configuração por linha de comando (CLI) por Console, Telnet e SSHv2;
- configuração simplificada através de web-browser;
- suporta gerenciamento centralizado através de SNMP MIB2 padrão e MIBs proprietárias;
- três níveis de usuário e autenticação em servidor externo via TACACS, TACACS+ (AAA) e/ou RADIUS;
- *download/upload* de arquivo de configuração;
- atualização de software via TFTP ou FTP (menos no modelo 3201);
- log de eventos interno ou destinado a elemento externo na rede; e
- compatibilidade com roteadores de terceiros.

A família NetRouter 2G foi desenvolvida para trabalhar nas mais variadas aplicações, bem como em:

- conexões de escritórios remotos à matriz (*remote office* ou SOHO);
- acesso a redes Frame Relay ou X.25, públicas ou privadas;
- acesso corporativo à Internet ou ISPs (*Internet Service Providers*);
- *internetworking* sobre redes IP ou Internet, com a possibilidade de formação de redes VPN/IP criptografadas (IPSec/3DES ou AES);
- acesso dedicado ou comutado (*dial on demand*), inclusive ISDN/RDSI (através de adaptador externo);
- acesso a redes GSM/GPRS com modem integrado (Série 3250);
- aplicação com contingência, tipo *dial backup*;
- soluções de voz e dados, com gateway de voz (VoIP) integrado (modelo 4200);
- soluções de firewall (*statefull inspection)*, inclusive com opção de segunda interface LAN (DMZ).

Mais adiante, são apresentadas, com mais detalhes, algumas dessas aplicações. A figura a seguir ilustra apenas alguns exemplos de aplicações básicas com os modelos da família NetRouter 2G:

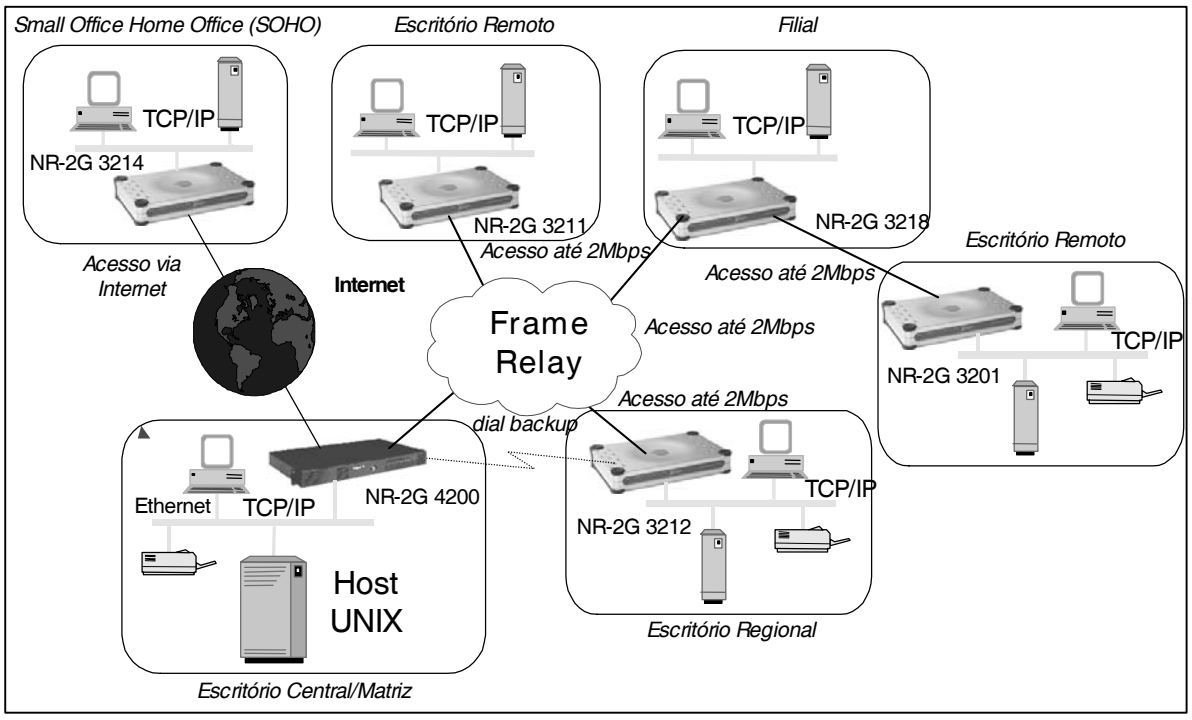


Figura 1. Algumas aplicações com a família NetRouter 2G

Série NetRouter 2G 3200

Quando abrir a embalagem, você encontrará :

1) NetRouter 2G 3200;
2) Fonte de alimentação AC ou 3) DC;
4) Cabo CONSOLE RJ45 (CB-CONS/AUX-NR, código Digitel 690.4025);
5) Adaptador TERMINAL DB9 (AD-RJ/TERM/DB9-NR, código Digitel 690.4022);
6) CD com documentação técnica e comercial

1)

2)

3)

4)

5)

6)

Série NetRouter 2G 3250 GPRS

Quando abrir a embalagem, você encontrará :

1) NetRouter 2G 3250 GPRS;
2) Fonte de alimentação AC ou 3) DC;
4) Cabo CONSOLE RJ45 (CB-CONS/AUX-NR, código Digitel 690.4025);
5) Adaptador TERMINAL DB9 (AD-RJ/TERM/DB9-NR, código Digitel 690.4022);
6) CD com documentação técnica e comercial;
7) Antena Dual Band GSM (código Digitel 690.2172).

1)

2)

5)

4)

3)

7)

6)

Série NetRouter 2G 3260 EDGE

Quando abrir a embalagem, você encontrará :

1) NetRouter 2G 3260 EDGE;
2) Fonte de alimentação AC ou 3) DC;
4) Cabo CONSOLE RJ45 (CB-CONS/AUX-NR, código Digitel 690.4025);
5) Adaptador TERMINAL DB9 (AD-RJ/TERM/DB9-NR, código Digitel 690.4022);
6) CD com documentação técnica e comercial;
7) Antena Quadri Band GSM (código Digitel 690.2310).

1)

2)

5)

4)

3)

7)

6)

Série NetRouter 2G 3280 CDMA

Quando abrir a embalagem, você encontrará :

1) NetRouter 2G 3280 CDMA;
2) Fonte de alimentação AC ou 3) DC;
4) Cabo CONSOLE RJ45 (CB-CONS/AUX-NR, código Digitel 690.4025);
5) Adaptador TERMINAL DB9 (AD-RJ/TERM/DB9-NR, código Digitel 690.4022);
6) CD com documentação técnica e comercial;
7) Antena CDMA (código Digitel 690.7045).

1)

2)

5)

4)

3)

7)

6)

Série NetRouter 2G 4200

Quando abrir a embalagem, você encontrará:

1) NetRouter 2G 4200;
2) Cabo CROSS, LAN categoria 5, crossover (CB-LAN/X-NR, código Digitel 690.1938);
3) Cabo CONSOLE RJ45 (CB-CONS/AUX-NR, código Digitel 690.4025);
4) Adaptador TERMINAL DB9 (AD-RJ/TERM/DB9-NR, código Digitel 690.4022);
5) Adaptador TERMINAL DB25 (AD-RJ/TERM/DB25-NR, código Digitel 690.4023);
6) CD com documentação técnica e comercial;

- Fonte de alimentação (AC ou DC) embutida;
- Cordão de alimentação (apenas no modelo AC);
- Kit para fixação em bastidor de 19" (já montado na unidade);

1)

2)

6)

5)

4)

3)

PRINCIPAIS CARACTERÍSTICAS

Roteamento IP

O NetRouter 2G suporta roteamento IP através de tabela de roteamento estático, programável pelo usuário, e roteamento dinâmico, utilizando os protocolos RIP, RIP2, OSPF ou BGP.

IP Masquerade

O NetRouter 2G possibilita o compartilhamento de um único endereço IP válido para várias estações na mesma sub-rede. Essa característica é chamada de IP Masquerade ou NAT/PAT (Network Address Translation with Port Address Translation) e permite que toda a rede se conecte à Internet utilizando apenas um endereço IP, fornecido, dinâmica ou estaticamente, pelo seu provedor de acesso.

Implementação de servidores virtuais (Redirect)

O NetRouter 2G permite mapear serviços de rede de forma a manter um único ponto de controle, limitando o número de conexões e timeouts de conexões ociosas e não consumindo recursos de servidores, cujo tempo de resposta é valioso. Os servidores virtuais facilitam o remapeamento em caso de queda e a manutenção de um servidor, sem que seja preciso reconfigurar todas as estações de clientes. Utilizando o Redirect em conjunto com o IP Masquerade, é possível disponibilizar serviços para a Internet mesmo quando estes forem oferecidos por servidores utilizando IP reservados.

Firewall

O NetRouter 2G possui um mecanismo de firewall sofisticado e poderoso, permitindo a criação de um conjunto de regras que proporcionam segurança ao usuário sem prejudicar a acessibilidade.

Permite a criação de regras contendo diversas formas de escolha de tráfego, tais como:

- por interface;
- pacote IP, TCP e UDP;
- tráfego de origem, destino e saída;
- estado de conexão (connection tracking);
- limite de tráfego;
- endereço MAC;
- tipo de serviço TOS;
- fragmento de pacote;
- por tempo (dia e hora de tráfego válido);
- estado de conexão (SPI).

Além disso, o firewall dispõe de outros recursos importantes, tais como a criação de DMZs e o monitoramento de tráfego (LOG).

VPN

O NetRouter 2G oferece o protocolo IPSEC, que, através de autenticação e criptografia, permite o estabelecimento de túneis seguros através de redes inseguras e, conseqüentemente, a criação de VPNs (Virtual Private Networks). A implementação utiliza para criptografia, os algoritmos 3DES (TripleDES) ou AES executados por hardware exclusivo, e para a autenticação de pacotes, os algoritmos MD5 ou SHA. Além do IPSEC e quando a criptografia do canal não é uma prioridade, o NetRouter 2G também oferece os protocolos L2TP, PPTP e GRE, que permite encapsular enlaces PPP através de túneis GRE.

DHCP Server

O NetRouter 2G possui um servidor DHCP que permite que máquinas remotas obtenham dinamicamente endereços IP, servidores DNS, WINS e Gateways. É possível definir ranges de endereços e endereços IP específicos com base no endereço MAC do cliente.

Protocolo de interconexão: PPP

As portas WAN podem ser configuradas para o protocolo PPP, operando em modo de transferência assíncrono ou síncrono HDLC (RFC1662). No modo síncrono HDLC, velocidades de até 5 Mbps são suportadas. No modo assíncrono, as velocidades suportadas são de, no máximo, 230 kbps por porta. No modo assíncrono, o usuário pode programar como será negociada a maior parte das opções do protocolo PPP, bem como suporte à criação rápida de scripts de conexão para modens cobre, GPRS ou scripts customizados.

Protocolo de interconexão: HDLC-Cisco

As portas WAN também podem ser configuradas para o protocolo HDLC-Cisco no caso de conexão a equipamentos que utilizam esse protocolo. A transferência é síncrona, e as velocidades suportadas vão até 5 Mbps.

Protocolo de interconexão: Frame Relay

As portas WAN podem, alternativamente, ser configuradas para o protocolo Frame Relay no caso de conexão a redes públicas ou privadas que utilizam esse protocolo. A transferência é síncrona, sendo que velocidades de até 5 Mbps são suportadas.

O usuário pode programar vários circuitos virtuais permanentes (PVC - Permanent Virtual Circuits) nas portas WAN. O NetRouter 2G não impõe limite quanto ao número de PVCs, sendo o mesmo determinado pela norma e, principalmente, pelo dimensionamento definido pela aplicação. A compatibilidade do protocolo de controle do enlace (LMI - Link Management Interface) pode ser programada para as normas ANSI, ITU-T ou nenhuma.

Operação chaveada por demanda

Com o protocolo PPP em modo assíncrono, as portas WAN podem operar com o enlace em modo permanente (normal) ou chaveado por demanda (discado). No modo permanente, a porta local estabelece o enlace com a ponta remota quando o equipamento é ligado, e não o desativa enquanto o NetRouter 2G estiver ligado. No modo chaveado por demanda, o enlace com a ponta remota somente é ativado quando existirem dados a serem enviados pela porta local. Neste modo, o enlace poderá ser desativado caso não existam dados sendo transferidos pela interface.

Múltiplas interfaces

As portas WAN oferecem quatro tipos de interfaces (V.24/V.28, V.35, V.36 e G.703), selecionadas automaticamente pelo cabo ou adaptador ligado ao conector de cada porta.

Monitoração dos sinais da interface

O equipamento permite a monitoração dos sinais de atividade das portas LAN (LAN0 nos modelos 3201, 3211, 3212, 3251, 3252, 3261, 3281 e 3282; LAN0 e LAN1 nos modelos 3214, 3218, 3254, 3258, 3264, 3268, 3284 e 3288.

Os sinais de transmissão (TD) e recepção (RD) das portas WAN são indicados através de leds no painel frontal nos modelos 3201, 3211, 3214, 3218, 3258, 3268 e 3288. Nos modelos 3212, 3214, 3218, 3252, 3254, 3262, 3264, 3268, 3282, 3284 e 3288, a monitoração dos sinais de atividade da porta auxiliar (WAN auxiliar) é feita através do led AUX.

Os sinais de transmissão (WTD) e recepção (WRD) da porta wireless GSM (GPRS/EDGE) e CDMA é feita através dos leds no painel frontal nas séries NR-2G 3250, NR-2G 3260 e NR-2G 3280.

Controle de segurança

O sistema de segurança suporta múltiplos usuários e os categoriza em três níveis de acesso. O sistema de segurança está disponível via CLI (Telnet/Console/SSH). Os três níveis de acesso são:

- Operator: possui permissão para ver as configurações e estatísticas.
- Moderator: possui permissão para visualizar configurações, estatísticas e operações de sistema (gerenciamento de usuários, atualização de software, ajuste de data/hora, etc.).
- Administrator: controle total sobre a configuração e a visualização de configurações e estatísticas.

Armazenamento de configuração

A configuração é armazenada em memória não-volátil, sendo carregada automaticamente sempre que o equipamento é ligado. Com o CLI, é possível armazenar a configuração do NR-2G em arquivo, em formato de script de comandos. Essa configuração é restaurada através do próprio CLI. Através do WebConfig, é possível armazenar a configuração do NR-2G em arquivo, sendo necessário apenas copiar e colar a configuração (em formato de script CLI) em um arquivo texto. O próprio WebConfig permite a restauração da configuração salva.

Atualização de firmware

O firmware do NetRouter 2G está armazenado em memória flash, permitindo a atualização do equipamento em campo através dos protocolos TFTP e FTP. Caso ocorra um problema de comunicação durante a transferência de um novo firmware, um conjunto mínimo de funções garantirá o acesso via porta Console, onde será possível realizar uma atualização local, também através do protocolo TFTP.

Autoteste e boot-up

Ao ser ligado, o NetRouter 2G realiza um autoteste. Caso seja detectada alguma falha, o indicador de status (ST), no painel frontal, exibirá a cor vermelha.

Se nenhum erro ocorrer, o equipamento completará o processo de inicialização (boot-up) do sistema operacional Linux, e o indicador ST passa à cor laranja. Esse processo dura cerca de 20 segundos, e depois o equipamento entra em operação normal. O indicador ST fica permanentemente ligado na cor verde.

Porta Console

A porta Console do NetRouter 2G é assíncrona e pode ser usada para a monitoração do estado do equipamento (modo normal) ou para sua configuração inicial (modo de segurança), utilizando um terminal TTY qualquer ou um aplicativo de terminal existente em qualquer estação de trabalho que disponha de uma porta serial assíncrona RS-232. No modo normal, permite a operação avançada através de linhas de comando (CLI).

Serviço Telnet

Durante a operação normal (indicador ST ligado na cor verde), o NetRouter 2G disponibiliza um serviço Telnet através da rede IP, que permite o acesso ao CLI e, conseqüentemente, às configurações e estatísticas do equipamento no modo de operação avançada.

Serviço SSH

Segurança é importante em qualquer lugar, ainda mais em se tratando de equipamentos de acesso. Nesse sentido, o NR-2G provê acesso seguro via SSHv2, propiciando confiabilidade e segurança no acesso a configuração.

Gerenciamento SNMP

O NetRouter 2G incorpora um agente SNMP (RFC1157) com suporte a MIB I (RFC1156), MIB II (RFC1213) e MIBs proprietárias permitindo a consulta e a configuração de diversos parâmetros de roteamento, QoS, Interfaces, bem como a coleta de estatísticas sobre a operação do roteador. O agente SNMP garante segurança adicional ao estabelecer que apenas as estações cadastradas como gerenciadoras poderão acessá-lo.

Os eventos importantes ocorridos no equipamento serão relatados a todos os gerentes cadastrados através de mensagens de trap, conforme especificado pela RFC1215.

Dip-switch e modo de segurança (modelo NR-2G 4200)

O painel traseiro do NR-2G 4200 apresenta uma dip-switch com quatro chaves, que permitem colocar o roteador em diferentes estados de operação (modo normal ou automático, modo de segurança ou modo de manutenção).

No modo de segurança, o NR-2G 4200 inicia com uma configuração mínima conhecida, permitindo a comunicação com o EasyConfig em caso de configuração inadequada. Através da porta Console, é possível configurar ou visualizar estatísticas, bem como realizar a atualização do firmware do equipamento localmente, utilizando o protocolo TFTP.

Slots de expansão com hot-swap (modelo NR-2G 4200)

O NetRouter 2G 4200 dispõe de dois slots para instalação de novos módulos de hardware, que permitem a expansão do número e do tipo de interfaces do equipamento, além do acréscimo de facilidades futuramente oferecidas. A colocação ou substituição desses módulos poderá ser feita pelo próprio usuário, com o equipamento ligado, seguindo fielmente as instruções que acompanham o módulo de expansão adquirido.

Expansão de memória interna (modelo NR-2G 4200)

O NetRouter 2G 4200 sai de fábrica com um pente de memória RAM dinâmica síncrona (SDRAM) com capacidade para armazenar 32 MB de informação, permitindo uma operação confiável em situações de alto tráfego. Com vistas à utilização de facilidades futuras, é possível substituir esta memória por outra de 128MB.

ATENÇÃO!
A substituição da memória interna do NetRouter 2G 4200 somente deve ser efetuada pela Assistência Técnica da Digitel.

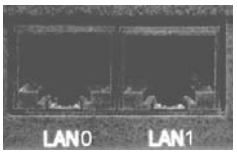
Antes de proceder à instalação do NetRouter 2G, certifique-se de que o equipamento não sofreu danos mecânicos durante o transporte, tais como arranhões, amassados, peças quebradas ou soltas, etc. Se algum problema for detectado durante a inspeção, notifique a companhia transportadora e o Centro de Assistência Técnica Digitel, que providenciará a substituição ou o conserto do equipamento.

REQUISITOS PARA INSTALAÇÃO E CONFIGURAÇÃO INICIAL

Para que a configuração inicial do NetRouter 2G seja possível, é necessária uma estação de trabalho que esteja rodando a pilha de protocolos TCP/IP, com suporte para conexões de rede local (LAN), ou seja, pode ser uma estação Unix, Windows ou outra. A rede local será utilizada para a comunicação via Telnet, SSH ou WebConfig com o NetRouter 2G.

É adequado, ainda, o uso de um terminal ASCII com interface serial assíncrona, ou de um programa de emulação de terminal instalado numa estação de trabalho com interface serial assíncrona padrão V.24 (RS-232).

CONEXÃO DA PORTA LAN0



A porta LAN0 do NetRouter 2G está inicialmente habilitada e configurada com um endereço de IP específico (ipaddr=192.168.1.254; netmask=255.255.255.0; gatewayip=192.168.1.1), permitindo a comunicação com a estação de trabalho em que o EasyConfig foi instalado ou SSH através da rede local.

Conecte a porta LAN0 do NetRouter 2G a um equipamento de LAN (hub ou switch) através de um cabo UTP direto (sem função crossover).

Alternativamente, a porta LAN0 poderá ser ligada diretamente a uma porta LAN da estação de trabalho, utilizando o cabo CROSS fornecido com o equipamento (CB-LAN/X-NR). O cabo de LAN CROSS, que implementa a função crossover, apresenta a seguinte pinagem:

Função	Pinos RJ45	Pinos RJ45	Função
TD+	1	3	RD+
TD-	2	6	RD-
RD+	3	1	TD+
RD-	6	2	TD-

CONEXÃO DA PORTA CONSOLE

A porta Console do NetRouter 2G é uma porta serial assíncrona com pinagem padrão ETD V.24 (RS-232). Ela permite a monitoração do funcionamento do roteador através de um terminal assíncrono ASCII ou VT100, ou através de um programa que emule um desses terminais.

Para utilizar a porta Console, conecte à mesma uma das extremidades do cabo CONSOLE que acompanha o equipamento. A outra extremidade deverá ser ligada a um dos adaptadores fornecidos com o NetRouter 2G, dependendo do tipo de equipamento que será utilizado.

Para conexão direta a um terminal ou estação de trabalho com uma porta serial e conector DB9 macho, utilize o adaptador TERMINAL com conector DB9 fêmea. Para conexão direta a um terminal ou estação de trabalho com uma porta serial e conector DB25 macho, utilize o adaptador TERMINAL com conector DB25 fêmea. Finalmente, para conexão a um terminal ou estação remota através de modens, utilize o adaptador MODEM, que apresenta um conector DB25 macho.

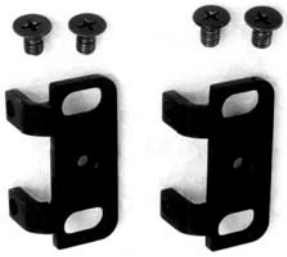
A pinagem desses cabos serão apresentadas no capítulo Cabos.

Por fim, configure o terminal assíncrono ou o programa de emulação de terminal na estação de trabalho com os seguintes parâmetros:

Velocidade	57600 bps
Largura do caractere	8 bits
Bits de parada	1 bit
Paridade	nenhuma
Controle de fluxo	nenhum

MONTAGEM DO NETROUTER 2G 4200

O NetRouter 2G 4200 pode ser montado sobre uma mesa ou fixado em um bastidor (rack) de 19". No caso de montagem em bastidor, os dois suportes de fixação laterais que acompanham o equipamento devem ser utilizados. Os suportes de fixação saem de fábrica presos nas laterais do NetRouter 2G. Caso o equipamento seja montado sobre uma mesa (desktop), os suportes podem ser retirados e guardados para futuras utilizações.



Suporte de fixação

Montagem

INSTALAÇÃO DO MÓDULO 1 x WAN (NR-2G-MW1-800.0923.00-7)

Este módulo permite a instalação de uma interface WAN adicional, oferecendo as mesmas funcionalidades das WAN0 e WAN1 fixas. O módulo 1 x WAN pode ser instalado em qualquer slot do equipamento, seguindo estritamente as recomendações de instalação descritas no item Instalação do módulo 1 x WAN (800.0923.00-7).

Para a instalação ou substituição do módulo NR-2G-MW1, faz-se necessário desligar o equipamento. Com o equipamento desligado, retire a “tampa cega” ou módulo a substituir e, depois, insira o módulo NR-2G-MW1 desejado.

A retirada de um módulo se dá pelo afrouxamento dos parafusos de fixação do mesmo e pela extração do módulo utilizando os parafusos como puxadores. A inserção de um módulo se dá pelo seu correto posicionamento nas corrediças laterais do slot correspondente. Após seu posicionamento, os módulos devem ser completamente

> IMPORTANTE!
> Os módulos WAN não devem ser retirados ou inseridos com o equipamento ligado.

inseridos até que se dê o alinhamento com o painel traseiro e, então, parafusados.

Ao ligar o equipamento, os módulos inseridos serão automaticamente reconhecidos; entretanto, caberá ao usuário proceder à configuração dos módulos instalados ou intercambiados com relação aos slots. Esta configuração para os módulos NR-2G-MW1 se dá nos mesmos moldes da configuração realizada para as portas WAN0 e WAN1 fixas. Em caso de substituição de um módulo NR-2G-MW1 por outro previamente configurado, não há necessidade de proceder à reconfiguração da porta WAN associada.

A numeração das portas WAN presentes nos slots segue a ordenação crescente da esquerda para a direita, sendo a interface mais à esquerda nomeada como WAN2. Assim, se houver apenas um módulo NR-2G-MW1 instalado em slot, este módulo corresponderá à interface WAN2, seja qual for o slot onde esteja instalado. Se houver dois módulos NR-2G-MW1 instalados, aquele mais à esquerda será a WAN2, e aquele mais à direita será a WAN3.

INSTALAÇÃO DOS MÓDULOS FXS (NR-2G-MV4/FXS-800.0924.00-3) E FXO (NR-2G-MV4/FXO-800.0935.00-5)

Os módulos FXS e FXO do NetRouter 2G 4200 permitem incluir a funcionalidade de voz sobre o IP no roteador. O módulo FXS possibilita a ligação de aparelhos telefônicos ao NetRouter, e o módulo FXO permite a ligação com linhas telefônicas.

Dependendo do tipo de fornecimento dos módulos VoIP (conjuntamente com o NetRouter 4200 ou separadamente), alteram-se as necessidades de instalação, entre elas a necessidade ou não de instalar o software de suporte a VoIP. Para detalhes a respeito da instalação de software, veja o item *Instalação de software*. A seguir serão apresentados tópicos comuns aos dois casos e cujo conhecimento é de fundamental importância para o usuário dos módulos VoIP.

Inserção e retirada de módulos de voz

Os módulos de expansão de voz do NetRouter 2G contam com a característica hot-swap, que lhes permite, dentro de um procedimento padronizado, serem retirados e inseridos sem prejuízo de funcionamento das outras interfaces.

Para que um módulo possa ser retirado ou inserido, é necessário que o sistema operacional seja avisado e disponha de tempo para desligar as interfaces afetadas. Este aviso é realizado ao se acionar a chave de substituição de módulos para o slot requerido.

Enquanto um módulo estiver ativo, o sistema operacional mantém iluminado o indicador correspondente ao slot onde o módulo se encontra. Nessa condição, os módulos não podem ser retirados, sob pena de interrupção nos serviços do roteador (pode até mesmo advir algum tipo de pane elétrica não-recuperável). Portanto, recomenda-se que os procedimentos de inserção e retirada sejam estritamente seguidos.

Para a retirada de um módulo, deve-se sinalizar esta intenção pressionando a chave de substituição correspondente àquele módulo. Se o módulo não possuir nenhuma interface ocupada por um aplicativo em execução, o sistema operacional irá iniciar um procedimento de liberação, sinalizado pelo indicador luminoso piscando. Quando o sistema operacional tiver completado o procedimento de liberação do módulo, o indicador será desligado, e o módulo poderá, então, ser retirado sem riscos.

Indicações dos LED de substituição de módulos

Condição do LED	Estado das interfaces	Retirada e inserção
Apagado	Inoperante	Permitida
Piscando	Mudando	Não permitida
Aceso	Operante	Não permitida

Se o módulo que se deseja retirar possui interfaces em uso, a solicitação de retirada do módulo será negada pelo sistema operacional. Neste caso, o estado do LED correspondente ao módulo não irá mudar, permanecendo aceso. Na Console, o sistema informará a impossibilidade de liberação do módulo pela mensagem (módulo 0, no caso):

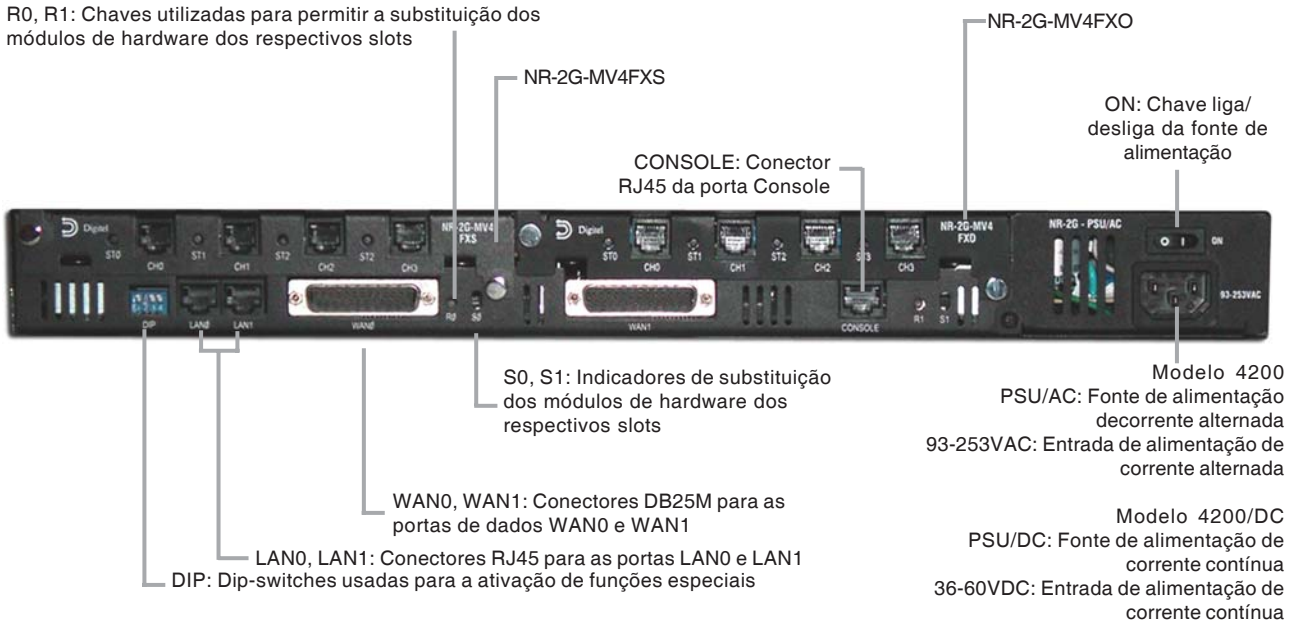
```
>FAILED removing module #0!
```

Integração de módulos ao NR-2G 4200

O NetRouter 2G 4200 possui dois slots para a instalação de módulos que permitem a expansão das funcionalidades do equipamento, identificados como slot0 e slot1.

A figura a seguir apresenta o painel traseiro do NetRouter 2G 4200 e identifica detalhes importantes com relação aos slots de expansão. Visto por trás, o slot0 fica à esquerda, e o slot1 fica ao centro, ao lado da fonte de alimentação.

Cada slot possui uma chave e um indicador luminoso utilizados quando da adição ou substituição de módulos. A chave correspondente ao slot0 é identificada no painel como R0, e o indicador, como S0; eles ficam posicionados sob a abertura do slot0. Da mesma forma, a chave R1 e indicador S1 correspondem ao slot1 e ficam localizados sob a abertura deste no painel traseiro.



O painel frontal possui um indicador luminoso para cada um dos slots, e a função destes indicadores é reportar a atividade ou o status do módulo instalado no respectivo slot.

O indicador de status do módulo instalado no slot0 é marcado como S0 e ocupa a penúltima posição mais à esquerda dentre os indicadores luminosos; o indicador S1, associado ao módulo instalado no slot1, ocupa a última posição mais à esquerda. Caso existam slots não-ocupados, seus respectivos indicadores permanecerão apagados.

Ordenação das interfaces de voz no NR-2G 4200

O NetRouter 2G 4200 adota, para interfaces disponíveis através de módulos de expansão, um esquema de numeração diferenciado por tipo de interface. Para o caso dos módulos de expansão VoIP, as interfaces são identificadas por uma numeração fixa. São previstas até quatro interfaces de voz por módulo de expansão. As interfaces instaladas no slot 0 serão numeradas de 0 a 3, da esquerda para a direita (vistas do painel traseiro), e aquelas instaladas no slot 1 serão numeradas de 4 a 7. Esta numeração é fixa, independentemente de se ter um ou dois slots ocupados por interfaces de voz.

Instalação de módulos adquiridos em separado

Módulos de expansão comprados em separado necessitam ser inseridos em um slot vago para que possam ser instalados. O procedimento de instalação de módulos novos deve partir da verificação da existência do software de suporte VoIP instalado no NetRouter 2G 4200.

Toda a modificação funcional que se deseje implantar no NetRouter 2G deverá ser efetuada por meio da interface de linha da Console. Esta interface proporciona o acesso a todas as características VoIP configuráveis do NetRouter 2G 4200 por meio de comandos. Todos os comandos CLI de VoIP estão disponíveis na seção *Sintaxe básica da linguagem*.

Para verificar se existe suporte em software instalado no NetRouter 2G 4200, utilize o comando **show**. Caso exista suporte, a palavra “VoIP” aparecerá.

Instalação de software

A utilização das características VoIP do NR2G 4200 requer a presença dos módulos com as interfaces adequadas e a instalação do software de suporte às facilidades de voz. Ao ser adquirido com módulos VoIP, o NetRouter 2G 4200 já contará com este suporte instalado em fábrica; no caso de aquisição dos módulos em separado, o software de VoIP será fornecido junto com os módulos, e sua instalação é facilmente realizada pelo usuário.

Para a instalação do software de VoIP, é necessário que o arquivo contendo o software esteja disponível em um servidor de ftp do cliente. Além disso, é necessário que seu endereço na rede IP seja conhecido. A instalação solicitará um nome de usuário e uma senha. Eis os comandos necessários à instalação:

```
SET SYSTEM UPGRADE
SERVER <IP do servidor ftp>
USER <usuário>
PASS <senha>
INSTALL voip1.0.tgz
```

As seguintes mensagens aparecerão na Console:

```
Download voip package... done
Installing voip package... done
```

Após estes passos, o sistema deverá ser reinicializado:

```
SET SYSTEM RESTART
```

CONFIGURAÇÃO DOS MÓDULOS DE VOZ FXS E FXO

As funcionalidades de voz do NetRouter 2G 4200 somente estarão disponíveis a partir da instalação e configuração do software de suporte VoIP. Para detalhes sobre a instalação, consulte o item *Instalação de software*.

Plano de discagem

A configuração do software de suporte a VoIP irá determinar as condições de uso das interfaces de telefonia, dos protocolos e das funcionalidades adicionais de PBX. Permitirá, sobretudo, programar o tratamento que o NetRouter 2G 4200 deverá dispensar aos eventos de telefonia e seus interesses. Eventos de telefonia são as chamadas dirigidas a ele com origem na rede pública ou na Internet, bem como chamadas iniciadas nos telefones ligados ao próprio NetRouter 2G 4200. O interesse de um evento de telefonia é o recurso oferecido pelo NetRouter 2G 4200 que este evento busca acessar. O tratamento oferecido aos eventos é o modo pelo qual se oferecerá o acesso aos recursos telefonia e de Internet disponíveis através do NetRouter 2G 4200, como o redirecionamento de chamadas e o acesso aos ramais internos.

evento	
invite	chamada entrando pela Internet
ringing	chamada entrando pela rede pública
hangup	chamada originada no equipamento

Esta programação do tratamento dos eventos é chamada de plano de discagem. O plano de discagem é formado por unidades de tratamento, denominados contextos. Os contextos são responsáveis por manter as descrições dos tratamentos dados aos eventos de telefonia.

O plano de discagem é formado por, no mínimo, um contexto: o contexto padrão ou default. Outros contextos podem ser criados além do default e poderão, de alguma forma, relacionar-se com este. A existência de vários contextos em um plano de discagem permite o tratamento seletivo aos diferentes eventos de telefonia e o agrupamento de eventos segundo interesses específicos.

Os contextos são construídos como listas de tratamento de extensões, onde as extensões são códigos atribuídos aos interesses oferecidos pelo NetRouter 2G 4200. Se uma ligação tem interesse em um ramal local, a extensão poderá ser o número deste ramal. Se um evento tem interesse em acessar um número ou mesmo uma faixa de números de telefones na rede pública, então a extensão se refere a este número ou faixa de números.

O tratamento de um interesse pode requerer uma série de passos. Por esse motivo, os contextos poderão ter várias linhas de tratamento referentes a uma mesma extensão. A diferença entre essas linhas destinadas à mesma extensão é um número de ordem, que estabelece a ordem em que os tratamentos devem ocorrer. Esse número de ordem aparece nos comandos como prioridade (em inglês: priority).

Sintaxe dos nomes de extensões

Nomes de extensões podem ser números, letras ou combinações de ambos. Se uma extensão possui o prefixo "_", a mesma é interpretada como uma máscara, e não como um código. Em máscaras, alguns caracteres têm significado especial:

X - qualquer dígito de 0-9

N - qualquer dígito de 2-9

[1235-9] - qualquer dígito entre os colchetes (neste exemplo, 1, 2, 3, 5, 6, 7, 8 ou 9)

"." - curinga, ou seja, vale qualquer seqüência restante (exemplo: "_9011." equivale a qualquer seqüência iniciando com 9011, inclusive 9011)

Por exemplo, o ramal _NXXXXXXX equivale a discagens normais de oito dígitos, enquanto _1NXXNXXXXXXX representa um código de área mais um número de telefone precedido de um dígito 1.

Sintaxe básica da linguagem

Comandos gerais (manutenção)

SET VOIP RELOAD
Recarrega os parâmetros VoIP sem parar as aplicações.
Para a versão XXX do "NetRouter VoIP Suite" este comando irá parar as aplicações em execução e reiniciá-las com os novos parâmetros.
SET VOIP UP
Inicia todas as aplicações relacionadas com VoIP.
SET VOIP DOWN
Imediatamente pára todas as aplicações VoIP.
SET VOIP PURGEALL
Pára imediatamente todas as aplicações VoIP e retorna todos os parâmetros aos seus valores default.
SET VOIP PURGE
Retorna todos os parâmetros do módulo VoIP aos seus valores default.

Comandos VoIP

SET VOIP LOG Configura os parâmetros de registro de eventos.
DEBUG Configura se mensagens serão enviadas para a lista de mensagens de depuração.
ON Envia as mensagens de depuração para o registro de depuração.
OFF Não envia mensagens para o registro de depuração.
CONSOLE Configura os tipos de mensagens que serão enviadas para a Console.
NOTICE Envia mensagens de aviso para a Console do sistema.
WARNING Envia mensagens de alerta para a Console do sistema.
ERROR Envia mensagens de erro para a Console do sistema.
DEBUG Envia mensagens de depuração para a Console do sistema.
PURGE Não envia mensagens para a Console do sistema.
MESSAGES Configura os tipos de mensagens que serão enviadas para a lista normal de mensagens.
NOTICE Envia mensagens de aviso para a lista normal de mensagens.
WARNING Envia mensagens de alerta para a lista normal de mensagens.
ERROR Envia mensagens de erro para a lista normal de mensagens.
DEBUG Envia mensagens de depuração para a lista normal de mensagens.
PURGE Não envia mensagens para a lista normal de mensagens
SHOW VOIP LOG Mostra as mensagens registradas nas listas de mensagens.
DEBUG-LOGGED Mostra as mensagens registradas na lista de mensagens de depuração.
MESSAGES-LOGGED Mostra as mensagens registradas na lista normal de mensagens.
SET VOIP Modifica ou cria o plano de discagem.
CONTEXT Configura um novo contexto de discagem no plano de discagem.
PURGE Exclui todo um contexto.
INCLUDE <nome do contexto incluído>
Inclui um contexto em outro.
PURGE Exclui um contexto de outro.
EXTEN <nome do contexto> <número da extensão>
Cria uma linha de tratamento para uma extensão em um contexto. O tratamento de uma extensão em um contexto deverá ter as seguintes associações:
Extensão => <número discado> <prioridade> <aplicação> (<parâmetros>)
PURGE Exclui do contexto todas as linhas referentes a este extensão.
COPYTO [<Nome do contexto>] <Nome da extensão> Copia a extensão correspondente (com todas as prioridades) para outra extensão (opcionalmente de outro contexto).
<número de prioridade>
Configura a prioridade de execução da aplicação.
PURGE Retira a aplicação associada à extensão.
COPYTO[[<Nome do contexto>]<Nome da extensão>]<Número da prioridade> Copia a prioridade correspondente para outra prioridade

(opcionalmente de outra extensão e de outro contexto).

TYPE Configura o tipo de aplicação a ser executada quando o número do extensão for discado.
ANSWER ou **BUSY** ou **CONGESTION** ou **HANGUP** ou **RINGING** ou **GOTO** ou **VOICEMAIL** ou **WAIT** ou **VOICEMAILMAIN** ou **DIAL** ou **DATETIME** ou **ECHO** ou **MILLIWATT DIGITTIMEOUT** ou **RESPONSETIMEOUT** ou **BACKGROUND** ou **PLAYBACK**

A aplicação não terá parâmetro caso **TYPE** seja:
ANSWER ou **BUSY** ou **CONGESTION** ou **HANGUP** ou **RINGING** ou **DATETIME** ou **ECHO** ou **MILLIWATT**.

A seguir são apresentadas as opções para aplicações que exigem parâmetros.

Caso **TYPE=GOTO**
O tratamento é interrompido e continuado em outro contexto (ou no mesmo), em uma outra extensão ou em uma outra prioridade.

CONTEXT<nome de contexto> ou **NONE**
Nome do contexto onde continuar o tratamento.
EXTENSION <número de extensão> ou **NONE**
Número do ramal onde continuar o tratamento.
PRIORITY<número de prioridade>
Número da prioridade onde continuar a execução.

Caso **TYPE=WAIT** Faz com que o tratamento espere o número indicado de segundos.
TIME<tempo em segundos>

Caso **TYPE=DIGITTIMEOUT** Configura o tempo máximo que o sistema espera pelo próximo dígito em uma discagem.
TIME<tempo em segundos>

Caso **TYPE=RESPONSETIMEOUT** Configura o tempo máximo que o sistema espera pelo início de uma discagem.
TIME<tempo em segundos>

Caso **TYPE=BACKGROUND** Configura uma mensagem de áudio para ser executada em background.

FILE<nome de arquivo sem extensão>

Caso **TYPE=PLAYBACK** Configura uma mensagem de áudio para ser executada, provocando uma pausa na execução do tratamento.
FILE<nome de arquivo sem extensão>

Caso **TYPE=DIAL**
CHANNEL SIP OU **PHONE** Configura os parâmetros relacionados à chamada que deve ser relacionada a esta prioridade.

TIMEOUT<Tempo em segundos> OU **NONE**
Tempo máximo de espera por uma resposta dos destinatários.

CALLEE<Identificação de destinatário>
Identifica os vários (possíveis) destinatários de uma mesma extensão. Cada destinatário pode usar um dispositivo ou protocolo específico para realizar a chamada. Quando a extensão tiver apenas um destinatário (caso mais comum), apenas a identificação "0" deve ser usada.

PURGE Exclui todos os destinatários configurados (exceto o referente à identificação "0", que não pode ser removido).

DIALTO <Identificação da extensão> OU **NONE**
Número, alias ou identificação do usuário a ser contactado. A macro "${EXTEN}" também pode ser utilizada para formar o valor do campo DIALTO, com base na exten-
s ã o
atual. Para obter maiores informações, consulte o item Usando macros no plano de discagem.

CHANNEL **SIP** OU **PHONE** OU **H323** Tipo de canal a ser usado na discagem.

Se CHANNEL = H323:

HOSTIP <Endereço IP> OU **NONE**

Define o endereço IP do terminal ou gateway H.323 destino. Deve ser **NONE** se houver um HOSTNAME definido.

HOSTNAME <Host name> OU **NONE**
Define o nome do terminal ou gateway H.323 destino. Deve ser NONE se houver um HOSTNAME definido.

PORT <Número da porta> OU **NONE**
Define o número da porta que deve ser acessada na negociação com o equipamento destino. O número 1720 será usado caso o campo tenha valor NONE.

Se CHANNEL = SIP:

HOSTIP <Endereço IP> OU **NONE**
Define o endereço IP do agente ou proxy SIP destino. Deve ser **NONE** se houver um HOSTNAME definido.

HOSTNAME <Host name> OU **NONE**
Define o nome do agente ou proxy SIP destino. Deve ser NONE se houver um HOSTNAME definido.

PORT <Número da porta> OU **NONE**
Define o número da porta que deve ser acessada na negociação com o equipamento destino. O número 5060 será usado caso o campo tenha valor NONE.

Se CHANNEL = PHONE:

DEVICE <Número do dispositivo> [0..7] ou uma macro que seja traduzida em algum desses dígitos.

Dispositivos de telefonia (phone) para o qual discar. Cada dispositivo corresponde a um canal dos módulos de expansão VoIP, onde o canal 0 é o CH0 do módulo inserido no slot 0 e o canal 4 é o CH0 do módulo do slot 1.

SET VOIP COUNTRY Configura os tons de discagem conforme o país. Na versão atual, o NR2G só permite o uso do padrão brasileiro de tons de discagem. Em caso de outras necessidades, consulte o suporte da Digitel.

SET VOIP RTP Configura a faixa de portas UDP usadas pelo protocolo RTP e parâmetros relacionados ao buffer de de-jitter do protocolo SIP.

STARTPORT<porta inicial>	Configura a porta inicial da faixa de portas rtp.
ENDPORT<porta final>	Configura a porta final da faixa de portas rtp.
JBUFFER YES OU **NO**	Habilita ou desabilita o buffer de de-jitter.
MAXJBUFFER <Buffer máximo>	Configura a máxima profundidade do buffer (em milissegundos, limitado a 3000).
PREFJBUFFER<Buffer Ref>	Configura a profundidade preferencial de operação do buffer (em milissegundos, limitado a 1000). Uma vez excedido este nível, o mesmo funcionará com um nível mínimo.
DROPRATE <Drop rate>	Configura a taxa máxima aceitável de perda de pacotes. Uma taxa de perda maior que este valor força o buffer a se readaptar (0 a 99).

SHOW VOIP

ALLDIALPLAN	Mostra o plano de discagem completo.
DIALPLAN <Nome do contexto>	Mostra o plano de discagem de um contexto específico.
CHANNELS	Mostra os canais utilizados no momento.

SOUND

FILES [<Subdiretório>]

Mostra todos os arquivos no repositório de sons ou, opcionalmente, em algum subdiretório.

Comandos relacionados com os canais de telefonia

SET PHONE
Configura os parâmetros do canal phone.

VOCODER

ULAW ALLOW OU **DISALLOW**	Permite ou inibe o uso do codificador -Law.
G723-1 ALLOW|DISALLOW	Permite ou inibe o uso do codificador G.723.1.
G729 ALLOW|DISALLOW	Permite ou inibe o uso do codificador G.729A.

MODE DIALTONE ou **IMMEDIATE**
Seleciona o modo de operação para um canal phone.
DIALTONE Oferece o tom de discar e espera até que seja discada uma extensão válida.
IMMEDIATE Desvia o tratamento para a extensão start do contexto especificado.

ECHOCANCEL OFF ou **LOW** ou **MEDIUM** ou **HIGH**
Configura o cancelador de eco a ser utilizado em todos os canais phone.

VAD YES ou **NO**	Liga ou desliga o Voice Activity Detection (VAD) a ser utilizado em todos os canais phone.
RECLEVEL [0..200]	Configura o volume geral de gravação a ser utilizado em todos os canais phone (100 é o valor default).
PLAYLEVEL [0..200]	Configura o volume geral de reprodução a ser utilizado em todos os canais phone (100 é o valor default).

CONTEXT<nome de contexto>	Configura o contexto default a ser utilizado em todos os canais phone.
PHONE<número>	Configura parâmetros específicos para um determinado canal phone.

ENABLE YES ou **NO**	Habilita ou desabilita o canal correspondente
RECLEVEL [0..200]	Configura o volume de gravação para o canal.
PLAYLEVEL [0..200]	Configura o volume de reprodução para o canal, onde 100 é o valor default.

CONTEXT<nome de contexto>	Configura o contexto para o canal.
MODE DIALTONE ou **IMMEDIATE**	Seleciona o modo de operação para este canal phone.
DIALTONE	Oferece o tom de discar e espera até que seja discada uma extensão válida.
IMMEDIATE	Desvia o tratamento para a extensão start do contexto especificado.

DIALTIMEOUT [0..45] <em segundos>
Configura o tempo máximo de reprodução do tom de discar quando o modo da porta for DIALTONE (default = 7; 0 = sem limitação).

HANGUP	Corta uma ligação em curso em um canal especificado.
PURGE	Retorna a configuração phone aos seus valores default.

Comandos relacionados com o protocolo SIP

SET SIP Configura parâmetros dos canais SIP.
VOCODER
ULAW

ALLOW	Permite que o vocoder ULAW seja negociado quando do estabelecimento de uma chamada SIP.
DISALLOW	Impede o vocoder ULAW de ser negociado quando do estabelecimento de uma chamada SIP.

G723-1 ALLOW ou **DISALLOW**
Permite ou impede o vocoder G723-1 de ser negociado quando do estabelecimento de uma chamada SIP.

G729A ALLOW ou **DISALLOW**

Permite ou impede o vocoder G729A de ser negociado quando do estabelecimento de uma chamada SIP.

ORDER <Seqüência de preferência de vocoders>
Configura a ordem de preferência dos vocoders para as chamadas SIP.

Exemplo:
SET SIP VOCODER ORDER G729A ULAW Define a ordem para todos os vocoders permitidos.

PORT<número de porta> Configura a porta por onde escutar chamadas SIP (default = 5060).

ADDRESS<endereço IP> Configura o endereço IP em que o sistema aceitará chamadas entrantes (0.0.0.0 = usa todos os endereços locais).

VALIDIP<endereço IP externo>
Configura um endereço externo para o qual reportar mensagens SIP se o equipamento estiver por trás de um NAT.

REGISTER<número de identificação do registro>
USER <nome de usuário>
(NO-)PASS <senha>
HOST <nome de hospedeiro>
(NO-)EXTENSION<código de extensão>
PURGE
Remove a informação de registro de um hospedeiro SIP.

TOS LOWDELAY ou **THROUGHPUT** ou **RELIABILITY** ou **MINCOST** ou **NONE**
Configura o tipo de serviço (também conhecido como campo DSCP) dos pacotes IP. Os valores aceitáveis são: **LOWDELAY, THROUGHPUT, RELIABILITY, MINCOST e NONE**.

ENTITY<número de identificação da entidade>
Cria ou modifica uma configuração SIP.

NAME <nome de entidade> Configura o nome da entidade.
TYPE FRIEND ou **USER** ou **PEER** Configura o comportamento permitido a esta entidade.
FRIEND Entidade que pode tanto realizar ou receber chamadas.
USER Apenas realiza chamadas.
PEER Apenas recebe chamadas.
USER<nome de usuário> Configura o usuário que irá se conectar a esta entidade.
(NO-)PASS<senha> Configura o segredo compartilhado utilizado para registros de autenticação.
HOST <endereço IP> ou **<endereço de hospedeiro>** ou **DYNAMIC**
Configura o endereço da entidade. É aceito como parâmetro um nome que possa ser resolvido, um endereço IP ou a palavra-chave DYNAMIC.
NAT YES ou **NO** Configura a habilidade desta entidade em lidar com network translated adresses (NAT).
(NO-)DEFAULTIP<endereço IP default>
Configura o endereço IP default para hospedeiros declarados como dynamic. Este endereço será utilizado quando o cliente não houver se registrado ainda.
CANREINVITE YES ou **NO**
Configura a opção de comunicar ao servidor que nunca se deve enviar um reinvite para o cliente. Geralmente usado para entidades ATA da Cisco.
(NO-)CONTEXT<nome de contexto> ou **NONE**
Configura o contexto default para este cliente.
DTMF INBAND ou **OOBAND** ou **INFO**
Seleciona como os dígitos DTMF serão enviados pela rede de pacotes.
INBAND: DTMF É enviado como áudio.
OOBAND: DTMF É enviado out-of-band, utilizando a RFC2833 (default).
INFO: DTMF É enviado out-of-band, utilizando mensagens INFO.
(NO-)QUALIFY<tempo máximo>
Configura o tempo máximo, em mili segundos, para que o cliente responda.
(NO-)FROMUSER <nome de usuário>
Configura o nome do usuário a ser inserido no campo from em lugar da identificação do chamador (caller ID).

PURGE Exclui toda a seção de um “peer”.
PURGE Retorna a configuração SIP aos seus parâmetros default.

SHOW SIP
PEERS Mostra todos os clientes SIP registrados.
CHANNELS Mostra os canais correntemente em uso por clientes SIP.

Comandos relacionados no protocolo H.323

SET H323
ADDRESS <Endereço IP> Configura o endereço IP em que o sistema aceitará chamadas entrantes (0.0.0.0 = usa todos os endereços locais).
LISTENPORT <Número da porta> Configura a porta TCP em que o sistema aceitará chamadas H.323 (padrão = 1720).
CONNECTPORT <Número da porta> Configura a porta TCP que o sistema usará como padrão na hora de iniciar chamadas. Usado apenas quando não é usado **gatekeeper**.
TCPSTART <Número da porta> Configura o início da faixa de portas TCP a serem usadas pelo H.323.
TCPEND <Port number> Configura o fim da faixa de portas TCP a serem usadas pelo H.323.
FASTSTART YES OU **NO** Configura o método de início das chamadas H.323.
TUNNELLING YES OU **NO** Configura a opção de utilizar tunelamento H.245 em chamadas H.323.
H245INSETUP YES OU **NO** Configura a opção do uso de adiantamento das mensagens H.245 no estabelecimento da chamada.
DTMFINBAND YES OU **NO** Configura a opção de detecção de DTMF na banda de áudio (padrão do Netmeeting).
JITTERMIN [20..1000] Configura a mínima profundidade do buffer de de-jitter (em milissegundos).
JITTERMAX [20..1000] Configura a máxima profundidade do buffer de de-jitter (em milissegundos).
TOS LOWDELAY OU **THROUGHPUT** OU **RELIABILITY** OU **MINCOST** OU **NONE**
Configura o campo ToS do pacotes IP. Valores possíveis: LOWDELAY (baixo atraso), THROUGHPUT (alta vazão), RELIABILITY (alta confiabilidade), MINCOST (mínimo custo) e NONE.
MAXCONNECTIONS <Número de conexões> OU **NONE**
Configura o número máximo de chamadas H.323 simultâneas (entrada e saída).
MAXBANDWIDTH <Largura de banda> OU **NONE**
Configura o limite de largura de banda. Valor usado para informar o gatekeeper.
GATEKEEPER DISABLE OU **DISCOVER** OU **<Nome do host>** OU **<Endereço IP>** OU **GKID:<Id>** Configura a opção de uso do gatekeeper. Valores possíveis: DISABLE (não utiliza gatekeeper), DISCOVER (procura um gatekeeper na rede), um nome de host válido, um endereço IP ou a identificação do gatekeeper (usado principalmente quando existe mais de um na rede).
(NO-)GKPASSWORD <Senha> Configura a senha usada com o gatekeeper.
GKTIMEOUT [0...10000] OU **NONE**
Configura o tempo limite para registro no gatekeeper (em segundos).
INPUTMODE Q931 OU **STRING** OU **TONE** OU **RFC2833**
Configura o modo de transmissão das entradas de usuário (tipicamente dígitos) para as chamadas H.323. Valores possíveis: Q931 (informação de teclado Q.931), STRING (string H.245), TONE (tom H.245), RFC2833 (compatível com RFC2833).
AMAFLAGS DEFAULT OU **OMIT** OU **BILLING** OU **DOC**
Configura as opções de accounting automático (AMA). Valores possíveis: OMIT (não registra as chamadas), BILLING (prepara entradas para tarifação), DOC (prepara entradas para documentação), DEFAULT (padrão do sistema).
(NO-)ACCOUNTCODE <Account code> Configura o código da conta de chamadas H.323.
DEFAULTCONTEXT<Contexto> Configura o contexto padrão para tratamento de chamadas H.323.
ALIAS <Alias> Configura ou cria aliases para uso no contexto padrão.
PURGE Exclui o alias especificado do contexto padrão.
PREFIX <Prefixo> Configura ou cria prefixos para uso no contexto padrão.
PURGE Exclui o prefixo especificado do contexto padrão.

CONTEXT <Contexto>	Configura contextos para serem usados no tratamento de chamadas H.323.
ALIAS <Alias>	Configura ou cria aliases para uso no contexto especificado.
PURGE	Exclui o alias especificado do contexto especificado.
PREFIX <Prefix>	Configura ou cria prefixos para uso no contexto especificado.
PURGE	Exclui o prefixo especificado do contexto especificado.
PURGE	Exclui todas as entradas (aliases e prefixos) relativos a este contexto.
VOCODER	
ULAW	
ALLOW	Permite usar o codificador -Law em chamadas H.323.
DISALLOW	Inibe o uso do codificador -Law em chamadas H.323.

ATENÇÃO!
Um número muito grande de quadros por pacote causará um atraso excessivo na conversação. Verifique o tamanho do quadro (em milissegundos) antes de configurar este parâmetro.

FRAMES <Num Frames>	Configura o número de quadros de voz por pacote IP.
G723-1 ALLOW OU **DISALLOW** OU **FRAMES**	
G729A ALLOW OU **DISALLOW** OU **FRAMES**	
ORDER <Ordem dos codificadores>	Configura a ordem de preferência dos codificadores para chamadas H.323.
PURGE	Retorna as configurações relativas a H.323 aos valores padrões.

SHOW H323	
STATS	Mostra estatísticas das chamadas H.323.
CALLS	Mostra informações sobre as chamadas H.323 atuais.

Comandos avançados relacionados com PBX

SET PBX PURGE	Limpa todos os parâmetros do módulo pbx.
SET PBX CDR	Configura o parâmetro Call Detail Record para uso da base de dados MySQL.
HOST<nome de hospedeiro>	Nome do hospedeiro MySQL.
DATABASE<nome da base de dados>	Nome da base de dados MySQL.
USER<nome de usuário>	Configura o nome do usuário da base de dados.
PASS<senha>	Senha do usuário da base de dados.
PURGE	Não envia CDRs para a base de dados

Usando macros no plano de discagem

Macros são strings no formato ${<macro>} que podem ser atribuídos a parâmetros do plano de discagem para conferir a estes um caráter variável. Nesta versão, o NR2G dispõe da seguinte macro:

EXTEN Traduz-se na própria identificação da extensão onde a macro se encontra. É uma macro muito útil quando utilizada em extensões que são identificadas por máscaras (todas as extensões iniciadas com "_"). Além disso, esta macro permite que os caracteres (dígitos ou não) mais à esquerda sejam eliminados no momento da expansão, quando é utilizada da seguinte forma:

EXTEN: **n** (onde "n" é o número de caracteres que devem ser suprimidos).

Exemplo:

EXTEN=_[1-3]xx	Extensão discada; pode ser qualquer número contido entre 100 e 399.
TYPE=DIAL	
CHANNEL=SIP	
HOSTNAME=nr2g.proxy.sip.com.br	
DIALTO = ${EXTEN:1}	Realiza uma chamada SIP para o endereço do host nr2g.proxy.sip.com.br, para o usuário identificado pelos dois últimos dígitos da extensão discada. Neste caso, se a extensão discada tiver sido "122", o usuário contatado será o 22.

RECONFIGURAÇÃO DOS ENDEREÇOS IP (OPCIONAL)

O NetRouter 2G está originalmente configurado para habilitar somente as portas Console e LAN0. A porta LAN0 está inicialmente configurada com um endereço de IP específico (192.168.1.254, máscara de rede 255.255.255.0). Há, ainda, uma rota default para esta interface, com o endereço de gateway 192.168.1.1.

Se a configuração inicial de endereços IP do roteador não é adequada para a conexão à rede ou à estação de trabalho onde o WebConfig está instalado, ela pode ser facilmente alterada através da porta Console do equipamento. Para isso, execute os seguintes procedimentos:

1. Conecte a porta Console do NetRouter 2G a um terminal ou estação de trabalho com programa de emulação de terminal.
2. Certifique-se de que as dip-switches do painel traseiro do NetRouter 2G estejam posicionadas para cima.
3. Ligue o NetRouter 2G e aguarde que o indicador ST, no painel frontal, passe da cor alaranjada para a cor verde. O terminal deverá exibir informações sobre a inicialização do equipamento e do sistema operacional Linux. O processo de inicialização dura cerca de 20 segundos.
4. A aplicação de Console do NetRouter 2G solicita nome de usuário e senha para que o login seja efetuado. O equipamento está originalmente configurado com usuário **nr2g** e senha **digitel**.
5. Após o login, no prompt da Console, pressione enter ou digite **HELP** para obter ajuda, **SHOW LAN LAN0 ALL** para ver a configuração da porta LAN0 ou, ainda, **SHOW ROUTES ALL** para ver a tabela de rotas (incluindo a rota default).
6. Se necessário, altere a configuração da porta LAN0 através de um comando do tipo:

```
SET LAN LAN0 IP <NOVO_END_IP> MASK <NOVA_MÁSCARA> UP
```

7. Se necessário, altere a rota default através de uma seqüência de comandos do tipo:

```
SET ROUTES ROUTE0 DEVICE LAN0 GATEWAY <NOVO_GATEWAY> DEFAULT
```

Através da porta Console também é possível configurar e habilitar a porta eth1 (LAN1 nos modelos 3214 e 3218) e testar a conectividade com comandos ping, entre outras tarefas. Para saber mais detalhes, consulte o capítulo sobre Operação.

CONFIGURAÇÃO INICIAL VIA WEBCONFIG

Para proceder à configuração inicial via WebConfig, o usário deverá realizar os seguintes procedimentos:

1. Certifique-se de que o microcomputador usado para a configuração do NetRouter 2G está com o protocolo TCP/IP instalado e configurado apropriadamente.
2. Certifique-se de que o microcomputador tem um browser devidamente instalado.
3. Conecte a port LAN0 do NetRouter 2G à rede local que dá acesso à estação de trabalho onde está o microcomputador preparado para a configuração.
4. Ligue o NetRouter 2G e aguarde que o indicador ST, no painel frontal, passe da cor alaranjada para a cor verde.
5. Em seu browser, entre com a URL inicial: http://192.168.1.254.
6. Na tela de login, informe usuário e senha. O equipamento está originalmente configurado com usuário **nr2g** e senha **digitel**.
7. Depois clique em **OK**. Será efetuado o login no equipamento, e a tela principal do Webconfig será aberta.
8. Configure o equipamento de acordo com a sua aplicação. A configuração deve ser criada usando-se a sintaxe CLI, sendo escrita na caixa de comandos.
9. Clique no botão **Execute** para aplicar a configuração.

Feito isso, o NetRouter 2G tentará estabelecer conexão com os equipamentos remotos, de acordo com o que foi configurado no passo 8.

Para verificar a configuração criada, entre com o comando **DUMP ALL** na caixa de comandos e clique no botão **Execute**. Ou então, na árvore de módulos, localizada no lado esquerdo da tela, selecione DUMP e o módulo de configuração desejado.

ATENÇÃO!
O equipamento sai de fábrica pré-configurado para acesso via web através da URL http://192.168.1.254.

Para alterar a configuração, repita os passos 8 e 9.

CONFIGURAÇÃO INICIAL VIA CLI

Para proceder à configuração inicial do equipamento via CLI, o usuário deverá realizar os seguintes procedimentos:

1. Certifique-se de que o microcomputador usado para a configuração do NetRouter 2G esteja com o protocolo TCP/IP instalado e apropriadamente configurado.
2. Conecte a porta LAN0 do NetRouter 2G à rede local que dá acesso à estação de trabalho para acesso via Telnet, ou conecte a estação diretamente à porta Console.
3. Caso necessário, conecte as portas WAN a serem utilizadas aos seus respectivos modens, utilizando os cabos adaptadores adequados.
4. Caso necessário, reconfigure o endereçamento IP da porta LAN0 do NetRouter 2G, conforme descrito no item Reconfiguração dos endereços IP.
5. No caso do modelo NR-2G 4200, certifique-se de que as dip-switches no painel traseiro estejam posicionadas para cima.
6. Ligue o NetRouter 2G e aguarde que o indicador ST, no painel frontal, passe da cor alaranjada para a cor verde.
7. Com a estação de trabalho devidamente conectada ao NetRouter 2G, via um acesso Telnet, SSH ou diretamente conectada à porta Console, serão solicitados o usuário e a senha da unidade. O equipamento está originalmente configurado com usuário **nr2g** e senha **digitel.**
8. Logo em seguida será fornecido o prompt de operação avançada.
9. Configure o equipamento de acordo com a sua aplicação, utilizando os comandos CLI.

Consulte o capítulo Operação e Guia da CLI para obter uma explicação mais detalhada.

PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 3200

O painel apresentado a seguir correspondem ao modelo 3218, que é o mais completo de toda a série. Os outros modelos constituem variações do mesmo equipamento, porém cada modelo com suas particularidades e os indicadores luminosos (leds) e conectores correspondentes. Mais adiante, uma tabela informa quais leds e conectores estão presentes em cada modelo.

RD1: Dados recebidos na porta WAN0.
TD1: Dados transmitidos na porta WAN0.
RD0: Dados recebidos na porta WAN0.
TD0: Dados transmitidos na porta WAN0.
AUX: Dados recebidos ou transmitidos na porta WAN auxiliar.
LAN1: Atividade e colisões na porta LAN1.
LAN0: Atividade e colisões na porta LAN0.
ST: Estado de operação do equipamento.
POWER: Alimentação.

POWER: Entrada da fonte de alimentação.

ON: Chave liga/desliga da fonte de alimentação (exceto modelo 3201).

LAN0: Conector RJ45 para a porta LAN0.

LAN1: Conector RJ45 para a porta LAN1.

CON: Conector RJ45 da porta Console.

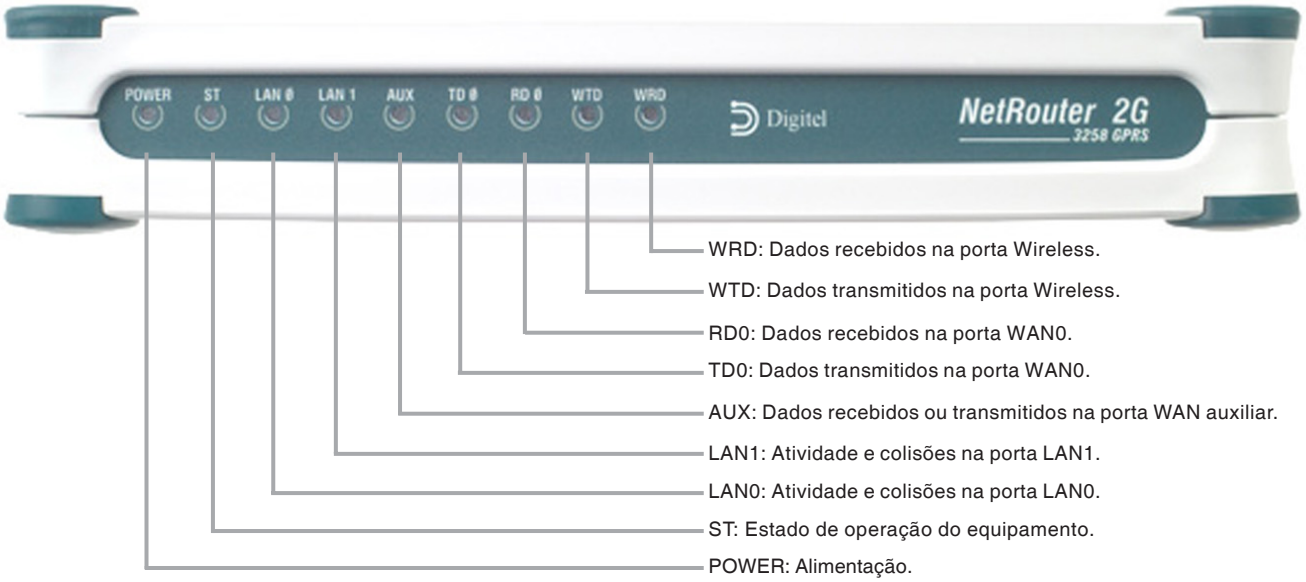
AUX: Conector RJ45 para a porta WAN auxiliar.

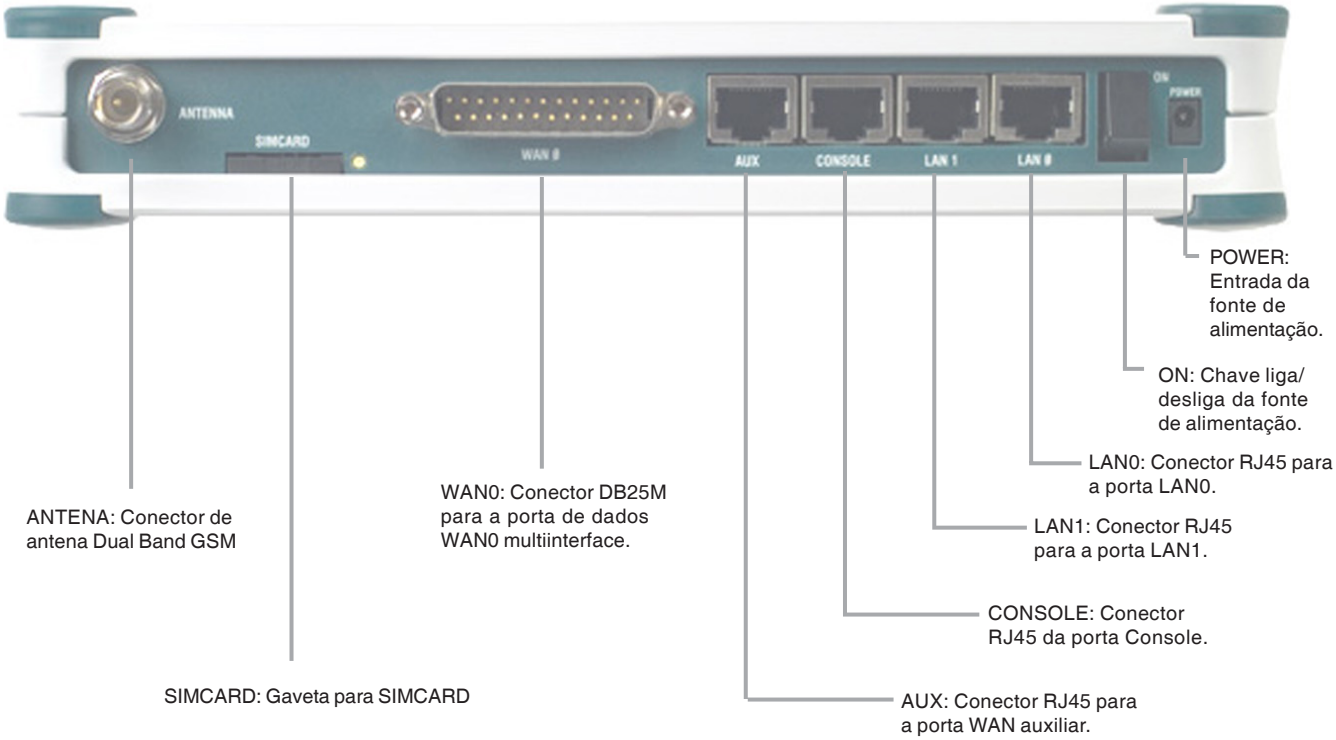
WAN0: Conector DB25M para a porta de dados WAN0 multiinterface.

WAN1: Conector DB25M para a porta de dados WAN1 multiinterface.

PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 3250

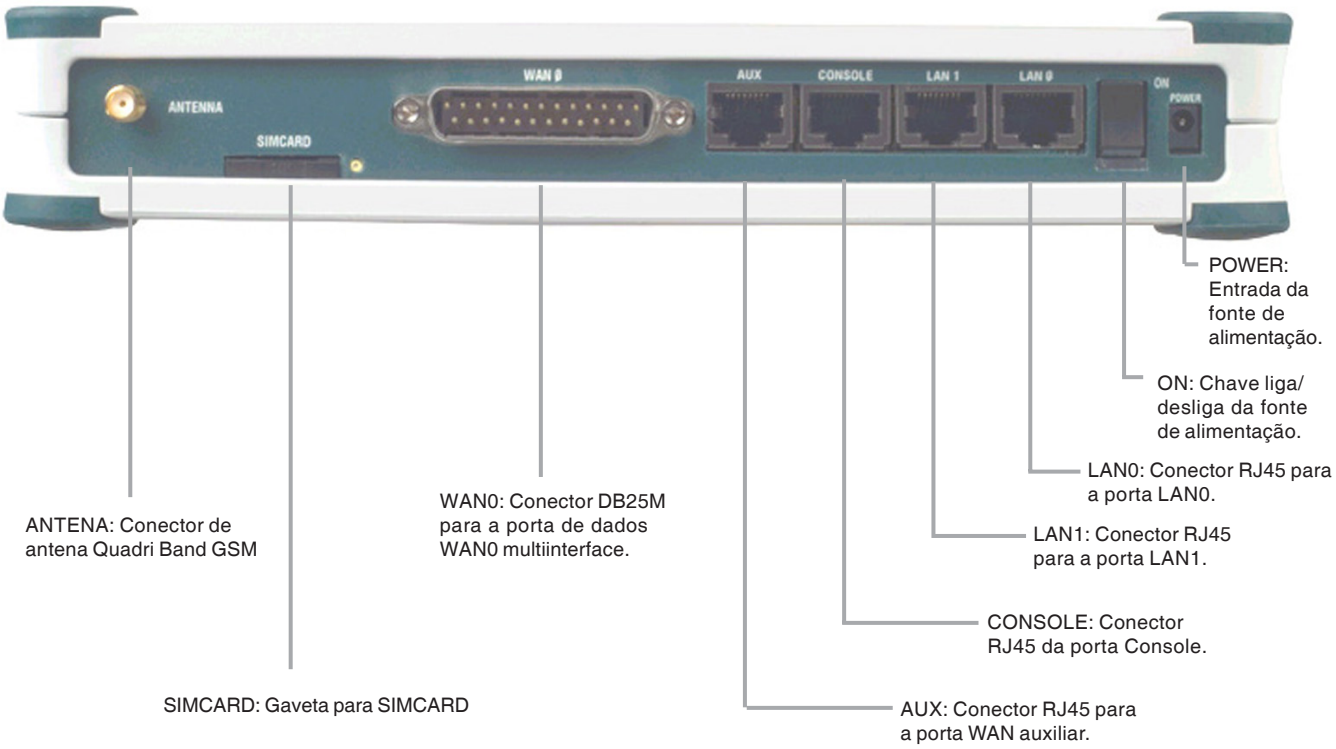
O painel apresentado a seguir correspondem ao modelo 3258, que é o mais completo de toda a série. Os outros modelos constituem variações do mesmo equipamento, porém cada modelo com suas particularidades e os indicadores luminosos (leds) e conectores correspondentes. Mais adiante, uma tabela informa quais leds e conectores estão presentes em cada modelo.





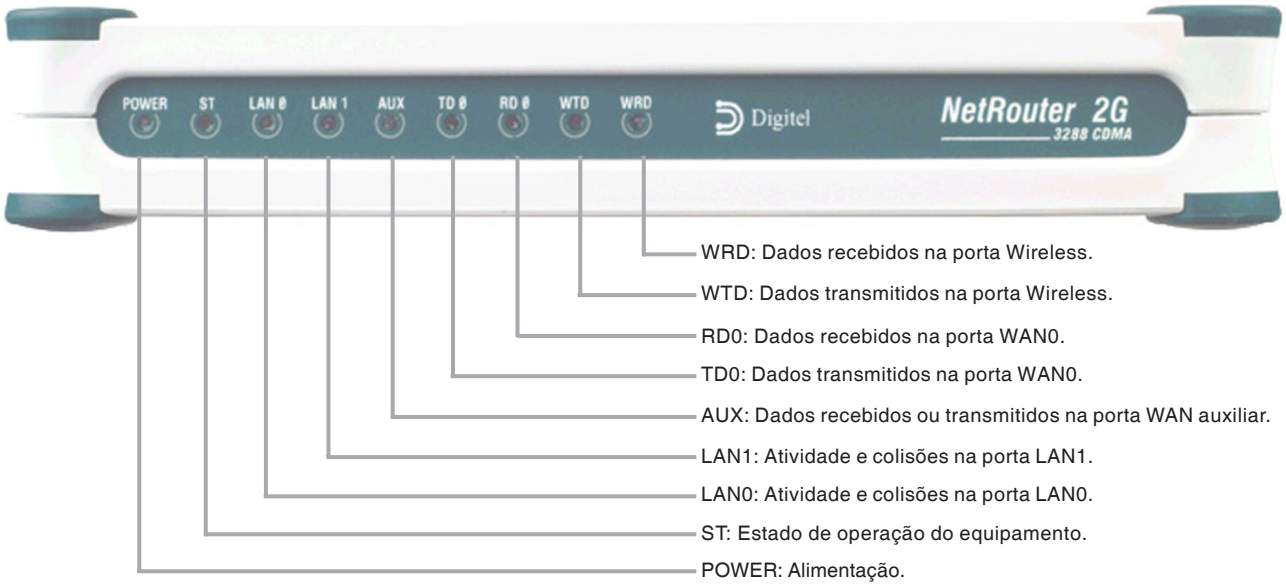
PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 3260

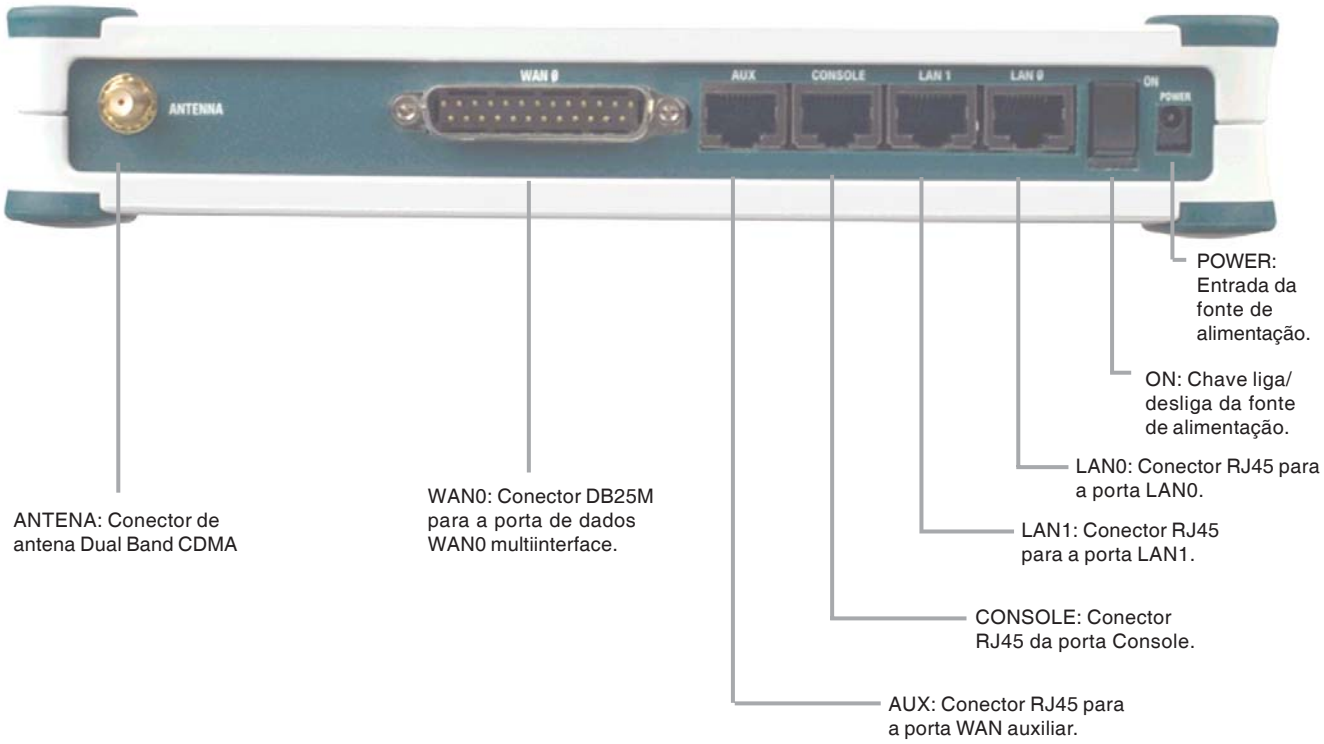
O painel apresentado a seguir correspondem ao modelo 3268, que é o mais completo de toda a série. Os outros modelos constituem variações do mesmo equipamento, porém cada modelo com suas particularidades e os indicadores luminosos (leds) e conectores correspondentes. Mais adiante, uma tabela informa quais leds e conectores estão presentes em cada modelo.



PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 3280

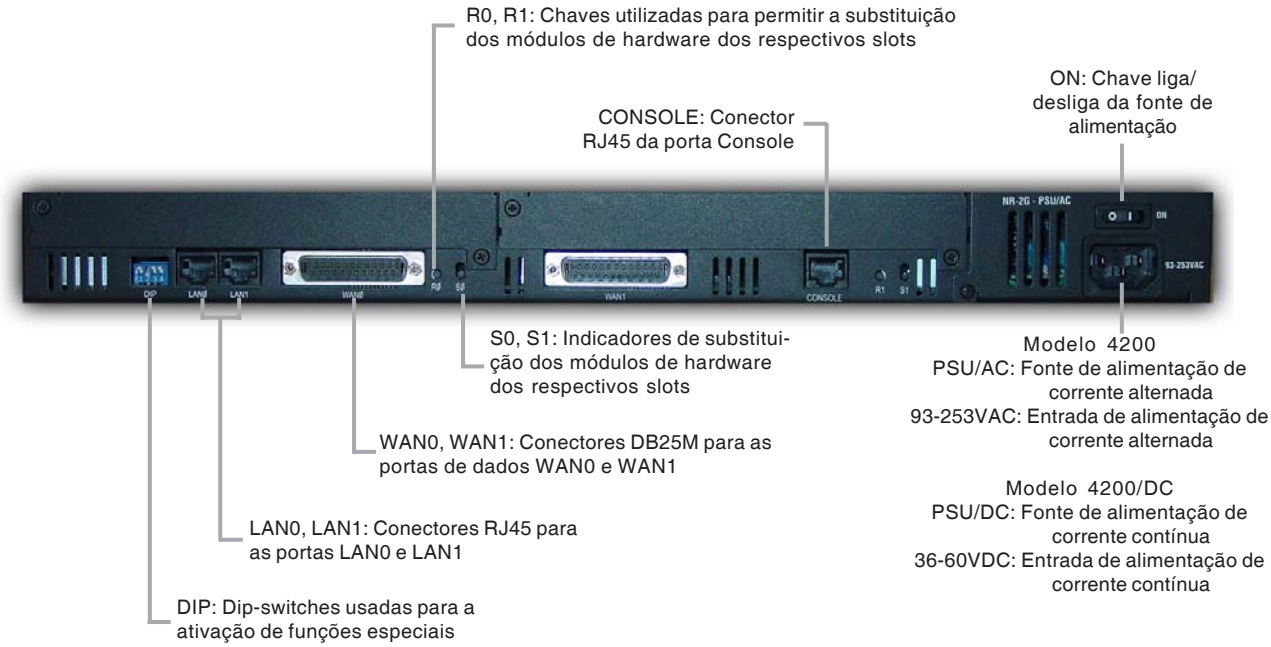
O painel apresentado a seguir correspondem ao modelo 3288, que é o mais completo de toda a série. Os outros modelos constituem variações do mesmo equipamento, porém cada modelo com suas particularidades e os indicadores luminosos (leds) e conectores correspondentes. Mais adiante, uma tabela informa quais leds e conectores estão presentes em cada modelo.





PAINÉIS FRONTAL E TRASEIRO DO NETROUTER 2G 4200

O painel frontal apresenta dez indicadores luminosos (leds), conforme mostra a figura a seguir:



Composição de leds e conectores dos modelos NetRouter 2G

Leds/Conectores	NR-2G																		
	3201	3211	3212	3214	3218	3238	3251	3252	3254	3258	3261	3262	3264	3268	3281	3282	3284	3288	4200
Led POWER	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
Led xx	x	x					x	x	x	x	x	x	x	x	x	x	x	x	x
Led LAN0	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Led LAN1				x	x	x			x	x			x	x			x	x	x
Led TD1					x	x													x
Led RD1					x	x												x	
Led TD0	x	x	x	x	x	x				x				x				x	
Led RD0	x	x	x	x	x	x				x				x				x	
Led AUX	x[1]		x	x	x	x	x	x	x		x	x	x		x	x	x		
Led WTD							x	x	x	x	x	x	x	x	x	x	x	x	
Led WRD							x	x	x	x	x	x	x	x	x	x	x	x	
Led S0																			x
Led S1																			x
Conector WAN1					x	x													x
Conector WAN0	x	x	x	x	x	x				x				x				x	x
Conector AUX	x[1]		x	x	x	x		x	x	x		x	x	x		x	x	x	
Conector CON	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Conector LAN1				x	x	x			x	x			x	x			x	x	x
Conector LAN0	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Conector POWER	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Chave ON		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
Chave R0																			x
Chave R1																			x
Conector Antena							x	x	x	x	x	x	x	x	x	x	x	x	
Gaveta SIMCARD							x	x	x	x	x	x	x	x					

[1] Apenas no modelo com WAN auxiliar (/Aux).

Indicador ST

O led ST indica o estado de operação do NetRouter 2G. Ao ligar o equipamento, o led ficará vermelho enquanto o autoteste estiver sendo efetuado. Se algum problema for detectado, o led permanecerá vermelho. Caso isso ocorra, consulte o item *Inicialização*, no capítulo *Operação* deste manual.

Após o autoteste, o equipamento passa a carregar o sistema operacional Linux. Durante esse período, que deve durar cerca de 20 segundos, o led ST permannecerá alaranjado.

Ao final da carga, inica-se a operação normal do equipamento. Isso é sinalizado pelo led ST na cor verde. Enquanto o equipamento estiver operando normalmente, o led deverá permanecer nessa cor; caso algum problema sério de operação seja detectado, o led passará à cor vermelha.

Indicador LAN

Os indicadores L0 e L1 (quando for o caso) são LEDs bicolores que apresentam, de forma compacta, todo o estado de operação da interface LAN correspondente.

Quando não há enlace fechado na interface LAN (por exemplo, o cabo não está conectado), o led L0 permance apagado. Quando o enlace é fechado, o led passa à cor verde, sinalizando que a interface está em modo half-duplex ou passa à cor laranja, sinalizando que a interface está em modo full-duplex.

A atividade é indicada pelo led piscando rápido (30ms apagado), quando a interface estiver operando a 100Mbits, e piscando lento (100ms apagado), quando estiver operando a 10Mbits.

No modelo NR-2G 4200, quando não houver enlace fechado na interface LAN (por exemplo, o cabo não está conectado), o led correspondente permanecerá apagado. Quando o enlace for fechado, haverá duas possibilidades:

• Enlace de 10 Mbps: neste caso, o led ficará ligado em verde enquanto não houver atividade na linha; quando houver atividade, passará à cor alaranjada por, pelo menos, 100 ms ou enquanto durar a atividade. Como o tráfego da LAN costuma ser em rajadas, o led fica apenas momentaneamente em laranja.

• Enlace de 100 Mbps: neste caso, o led ficará ligado em laranja enquanto não houver atividade na linha; quando houver atividade, passará à cor verde por, pelo menos, 100 ms ou enquanto durar a atividade. Como o tráfego da LAN costuma ser em rajadas, o led fica apenas momentaneamente em verde.

Indicador AUX

O indicador AUX é um led bicolor que indica a atividade na porta WAN auxiliar (a existência de dados sendo trasmitidos e/ou recebidos) através da cor verde.

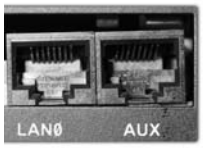
Indicadores TD e RD

Estes leds indicam, na cor verde, a existência de dados sendo trasmitidos (T) ou recebidos (R) na porta WAN multiinterface.

Indicadores WTD e WRD

Estes leds indicam, na cor verde, a existência de dados sendo trasmitidos (T) ou recebidos (R) na porta WAN/Wireless.

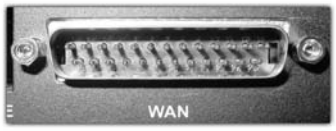
Conector AUX



Nos modelos 3201/Aux, 3212, 3214, 3218, 3252, 3254, 3258, 3262, 3264, 3268, 3282, 3284 e 3288, o conector AUX dá acesso à interface WAN auxiliar assíncrona do roteador, permitindo uma ligação de longa distância através de modens assíncronos, utilizando o cabo CONSOLE RJ e um adaptador MODEM

DB25.

Conector WAN multiinterface



A pinagem do conector WAN, localizado na parte traseira do gabinete , é apresentada na tabela a seguir:

DB25 macho	Sinal
1	FG
2	TD A
3	RD A
4	RTS
5	CTS
6	DSR
7	SG
8	DCD
9	RC B
11	XTC B
12	TC B
14	TD B
15	TC A
16	RD B
17	RC A
20	DTR
24	XTC A

Dip-switch (modelo NR-2G 4200)

A dip-switch somente precisa ser utilizada quando não se consegue acessar o NetRouter 2G através do EasyConfig ou do terminal Telnet no modo de operação normal.

Através da dip-switch é possível colocar o roteador no modo de segurança, permitindo que ele seja configurado através da porta Console e acessado através da rede com um endereço de IP conhecido.

A dip é composta de quatro chaves, numeradas de 1 a 4. Ao ser ligado, o roteador lê as chaves e assume o modo de operação especificado.

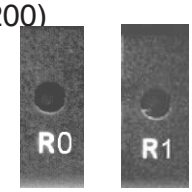
As chaves são ativadas na posição para baixo e desativadas na posição para cima. Na tabela a seguir, 1 significa chave ativada, e 0 significa chave desativada. A tabela apresenta a codificação utilizada na dip-

switch e seu significado.

Dip-switch 1 2 3 4	Modo	Função
0 0 0 0	Automático	O roteador inicia a operação do sistema Linux automaticamente e realiza todas as funções conforme a configuração existente no equipamento.
0 0 0 1	Segurança	O roteador exibe uma mensagem na porta Console e espera 5 segundos antes de iniciar a carga e a operação do Linux. Nesse tempo, o usuário pode evitar a carga pressionando a barra de espaço, o que lhe permite executar os comandos do modo de segurança. De qualquer forma, o roteador parte com um endereço de IP específico na interface LAN0.
0 0 1 1	Clear	O roteador opera no modo de segurança, mas inicialmente coloca os valores default de fábrica nos parâmetros de operação deste modo.
1 X X X	Teste	Este modo só deve ser utilizado pelos técnicos da Digitel ou sob sua orientação.
0 1 0 0	Manutenção	Este modo só deve ser utilizado pelos técnicos da Digitel ou sob sua orientação.

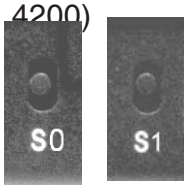
Nota:
As combinações não apresentadas na tabela são reservadas para uso futuro ou para os laboratórios de teste da Digitel. Não é recomendado utilizá-las sem a autorização expressa da Digitel.

Chaves R0 e R1 (modelo NR-2G 4200)



Estas chaves atuam em conjunto com os leds S0 e S1. Ao se pressionar uma dessas chaves, o módulo opcional do slot correspondente é desativado, permitindo a substituição do módulo sem desligar o equipamento (hot swap).

Indicadores S0 e S1 (modelo NR-2G 4200)



Estes leds indicam o estado de funcionamento dos módulos dos respectivos slots, conforme a tabela:

Apagado	Módulo ausente ou não conectado
Aceso	Módulo presente e operando
Piscando	Módulo desativado para remoção

Os leds passam de aceso para piscando quando se pressiona a chave R correspondente.

Alimentação (modelo NR-2G 4200)

A entrada de alimentação do NetRouter 2G 4200 pode ser feita através de corrente alternada ou contínua.

Modelo 4200: corrente alternada AC

Modelo 4200/DC: corrente contínua DC

ATENÇÃO!
Jamais remova um módulo do slot com o led S correspondente aceso, pois isso pode danificar os circuitos eletrônicos do módulo e do roteador.

Alimentação (modelo NR-2G 3200)

A entrada de alimentação do NR-2G 3200 é sempre através de uma fonte de alimentação externa, podendo ser feita por corrente alternada ou contínua, conforme o modelo.

NR-2G 3200: corrente alternada AC

NR-2G 3200/DC: corrente contínua DC

• Cabos

CABO LAN CROSS (CB-LAN/X-NR)

O cabo LAN crossover CB-LAN/X-NR (códigos Digitel: 810.0343/690.1938) é utilizado para conectar a interface LAN/Ethernet de uma estação de trabalho diretamente a uma das interfaces LAN do NetRouter 2G. Este cabo providencia o cruzamento dos sinais TD +/- com RD +/-.

Nota:
Este item é opcional. Para solicitar o cabo junto à Digitel, utilize o código 810.0343.

A pinagem do cabo CB-LAN/X-NR e os sinais utilizados são apresentados a seguir:

Função	Pinos RJ45	Pinos RJ45	Função
TD+	1	3	RD+
TD-	2	6	RD-
RD+	3	1	TD+
RD-	6	2	TD-

CABO CONSOLE RJ (CB-CONS/AUX-NR)

O cabo rollover RJ45-RJ45 CB-CONS/AUX-NR (códigos Digitel: 810.0344/690.4025) é utilizado para conectar um terminal ou modem à porta Console do NetRouter 2G. Deve ser utilizado em conjunto com um dos adaptadores descritos a seguir, ligando uma ponta do cabo ao conector RJ45 da porta Console do roteador e a outra ao conector RJ45 fêmea do adaptador.

Nota:
Este item acompanha o produto. Para solicitar o cabo separadamente junto à Digitel, utilize o código 810.0344.

A pinagem do cabo CB-CONS/AUX-NR e os sinais utilizados são apresentados a seguir:

Sinal	RJ45M	RJ45M	Sinal
RTS	1	8	CTS
DTR	2	7	DSR
TD	3	6	RD
GND	4	5	GND
GND	5	4	GND
RD	6	3	TD
DSR	7	2	DTR
CTS	8	1	RTS

ADAPTADOR TERMINAL DB9 (AD-RJ/TERM/DB9-NR)

O adaptador RJ45-fêmea/DB9-fêmea AD-RJ/TERM/DB9-NR (códigos Digitel: 810.0345/690.4022) é utilizado para conectar a porta Console do NetRouter 2G diretamente a uma porta serial assíncrona de um terminal ou microcomputador com conector DB9 macho. Deve ser utilizado em conjunto com o cabo Console RJ (CB-CONS/AUX-NR).

Nota:
Este item acompanha o produto. Para solicitar o adaptador separadamente junto à Digitel, utilize o código 810.0345.

A pinagem do adaptador AD-RJ/TERM/DB9-NR e os sinais utilizados são apresentados a seguir.

Sinal	RJ45F	DB9F
RTS	1	7
DTR	2	4
TD	3	3
GND	4	5
GND	5	5
RD	6	2
DSR	7	6
CTS	8	8

ADAPTADOR TERMINAL DB25 (AD-RJ/TERM/DB25-NR)

O adaptador RJ45-fêmea/DB25-fêmea AD-RJ/TERM/DB25-NR (códigos Digitel: 810.0346/690.4023) é utilizado para conectar a porta Console do NetRouter 2G diretamente a uma porta serial assíncrona de um terminal ou microcomputador com conector DB25 macho. Deve ser utilizado em conjunto com o cabo Console RJ (CB-CONS/AUX-NR).

Nota:
Este item é opcional. Para solicitar o adaptador junto à Digitel, utilize o código 810.0346.

A pinagem do adaptador AD-RJ/TERM/DB25-NR e os sinais utilizados são apresentados a seguir.

Sinal	RJ45F	DB25F
RTS	1	4
DTR	2	20
TD	3	2
GND	4	7
GND	5	7
RD	6	3
DSR	7	6
CTS	8	5

ADAPTADOR MODEM DB25 (AD-RJ/MODEM/DB25-NR)

O adaptador RJ45-fêmea/DB25-macho AD-RJ/MODEM/DB25-NR (códigos Digitel: 810.0347/690.4024) é utilizado para conectar a porta Console do NetRouter 2G diretamente a uma porta serial de um modem assíncrono com conector DB25 fêmea. Deve ser utilizado em conjunto com o cabo Console (CB-CONS/AUX-NR).

No caso dos modelos 3201/Aux, 3212, 3214, 3218, 3252, 3254, 3258, 3262, 3264, 3268, 3282, 3284 e 3288, em aplicação de dial backup, este adaptador é utilizado com o cabo Console (CB-CONS/AUX-NR) para a conexão da porta AUX ao modem.

Nota:
Este item é opcional. Para solicitar o adaptador junto à Digitel, utilize o código 810.0347.

A pinagem do adaptador AD-RJ/MODEM/DB25-NR e os sinais utilizados são apresentados a seguir.

Sinal	RJ45F	DB25F	SINAL
RTS	1	5	CTS
DTR	2	8	DCD
TD	3	2	RD
GND	4	7	GND
GND	5	7	GND
RD	6	3	TD
DSR	7	20	DTR
CTS	8	4	RTS

CABO PARA INTERFACE V.24/V.28 - RS232 (CB-V24-NR)

Opcionalmente, o cabo CB-V24-NR (códigos Digitel: 810.0293/690.1557) pode ser adquirido para se fazer a ligação ao conector DB25 macho do painel traseiro do NetRouter. Quando este cabo estiver instalado e o roteador for ligado, a porta WAN será automaticamente configurada para interface V.24/V.28 (RS-232), tipo DTE. Comprimento: 3 metros.

Nota:
Este cabo é opcional. Para solicitar o cabo junto à Digitel, utilize o código 810.0293.

Tanto a pinagem do cabo CB-V24-NR quanto os sinais atribuídos ao conector DB25 macho do cabo são apresentados na tabela a seguir.

Lado NetRouter Conector DB25 fêmea	Lado DCE Conector DB25 macho	Sinal V.24 (RS-232)
1	1	FG
2	2	TD
3	3	RD
4	4	RTS
5	5	CTS
6	6	DSR
7+21+23	7	SG

Lado NetRouter Conector DB25 fêmea	Lado DCE Conector DB25 macho (RS-232)	Sinal V.24
8	8	DCD
15	15	TC
17	17	RC
20	20	DTR
24	24	XTC

CABO PARA INTERFACE V.11/V.36 (CB-V36-NR)

Opcionalmente, o cabo CB-V36-NR (códigos Digitel: 810.0290/690.1556) pode ser adquirido para se fazer a ligação ao conector DB25 macho do painel traseiro do NetRouter. Quando este cabo estiver instalado e o roteador for ligado, a porta WAN será automaticamente configurada para interface V.11/V.36, tipo DTE. Comprimento: 3 metros.

Nota:
Este cabo é opcional. Para solicitar o cabo junto à Digitel, utilize o código 810.0290.

Tanto a pinagem do cabo CB-V36-NR quanto os sinais atribuídos ao conector DB37 macho do cabo são apresentados na tabela a seguir.

Lado NetRouter Conector DB25 fêmea	Lado DCE Conector DB37 macho	Sinal V.36
1	1	FG
2	4	TD A
3	6	RD A
4	7	RTS A
5	9	CTS A
7+21	19	SG
8	13	DCD A
9	26	RC B
10	31	DCD B
11	35	XTC B
12	23	TC B
13	27	CTS B
14	22	TD B

Lado NetRouter Conector DB25 fêmea	Lado DCE Conector DB37 macho	Sinal V.36
15	5	TC A
16	24	RD B
17	8	RC A
19	25	RTS B
24	17	XTC A

CABO PARA INTERFACE V.35/MRAC34 (CB-V35-NR)

Opcionalmente, o cabo CB-V35-NR (códigos Digitel: 810.0289/690.1555) pode ser adquirido para se fazer a ligação ao conector DB25 macho do painel traseiro do NetRouter. Quando este cabo estiver instalado e o roteador for ligado, a porta WAN será automaticamente configurada para interface V.35, tipo DTE. Comprimento: 2,6 metros.

Nota:
Este cabo é opcional. Para solicitar o cabo junto à Digitel, utilize o código 810.0289.

Tanto a pinagem do cabo CB-V35-NR quanto os sinais atribuídos ao conector V.35/MRAC34 macho do cabo são apresentados na tabela a seguir.

Lado NetRouter Conector DB25 fêmea	Lado DCE Conector V.35/M RAC34 macho	Sinal V.35
1	A	FG
2	P	TD A
3	R	RD A
4	C	RTS
5	D	CTS
6	E	DSR
7+23	B	SG
8	F	DCD
9	X	RCB
11	W	XTC B
12	AA (a)	TC B
14	S	TD B
15	Y	TC A

Lado NetRouter Conector DB25 fêmea	Lado DCE Conector V.35/M RAC34 macho	Sinal V.35
16	T	RD B
17	V	RC A
20	H	DTR
24	U	XTC A

CABO PARA INTERFACE V.35/PADRÃO TELEBRÁS (CB-V35/PT-NR)

O cabo DB25-fêmea/DB25-macho CB-V35/PT-NR (códigos Digitel: 810.0291/690.1611) é usado para fazer a conexão direta, sem cabos adaptadores, do roteador a modens V.35 padrão Telebrás (Prática Telebrás 225-540-750), como, por exemplo, DT64MI e DT256MI. Comprimento: 2,6 metros.

Nota:
Este cabo é opcional. Para solicitar o cabo junto à Digitel, utilize o código 810.0291.

Tanto a pinagem do cabo CB-V35/PT-NR quanto os sinais atribuídos ao conector V.35/DB25 macho do cabo são apresentados na tabela a seguir.

Lado NetRouter Conector DB25 fêmea	Lado DCE Conector DB25 macho	Sinal V.35
1	1	FG
2	2	TD A
3	4	RD A
4	5	RTS
5	7	CTS
6	9	DSR
7+23	13	SG
8	10	DCD
9	19	RC B
11	24	XTC B
12	16	TC B
14	15	TD B
15	3	TC A
16	17	RD B
17	6	RC A
24	11	XTC A

CABO PARA INTERFACE V.35/ISO2110 (CB-V35/ISO-NR)

O cabo CB-V35/ISO-NR (códigos Digitel: 810.0297/690.1724) é usado para fazer a conexão direta do roteador ao conector ISO 2110 (DB25) de modens (DCE), como, por exemplo, modens HDSL da Digitel (DT2048-HDSL). Quando este cabo estiver instalado e o roteador for ligado, a porta WAN será automaticamente configurada para interface V.35, tipo DTE. Comprimento: 3 metros.

Nota:
Este cabo é opcional. Para solicitar o cabo junto à Digitel, utilize o código 810.0297.

Tanto a pinagem do cabo V35/ISO2110 (CB-V35/ISO-NR) quanto os sinais correspondentes aos pinos são apresentados na tabela a seguir.

Lado NetRouter Conector DB25 fêmea	Lado DCE/Modem Conector DB25 macho	Sinal V.35
1	1	FG
2	2	TD A
3	3	RD A
4	4	RTS
5	5	CTS
6	6	DSR
7+23	7	SG
8	8	DCD
9	9	RC B
11	11	XTC B
12	12	TC B
14	14	TD B
15	15	TC A
16	16	RD B
17	17	RC A
24	24	XTC A

CABO PARA INTERFACE V.35/NEWBRIDGE (CB-V35/NB-NR)

O cabo CB-V35/NB-NR (códigos Digitel: 810.0323/690.1675) é usado para fazer a conexão direta do roteador a dispositivos de acesso Newbridge com configuração proprietária, modelos 270X. Quando este cabo estiver instalado e o roteador for ligado, a porta WAN será automaticamente configurada para interface V.35, tipo DTE. Comprimento: 3 metros.

Nota:
Este cabo é opcional. Para solicitar o cabo junto à Digitel, utilize o código 810.0323.

Tanto a pinagem do cabo V35/Newbridge (CB-V35/NB-NR) quanto os sinais correspondentes aos pinos são apresentados na tabela a seguir.

Lado NetRouter Conector DB25 fêmea	Lado Newbridge Conector DB25 macho	Sinal V.35
1	24	FG
2	20	TD A
3	2	RD A
4	11	RTS
5	5	CTS
6	4	DSR
7+23	12	GND
8	10	DCD
9	3	RC B
11	19	XTC B
12	1	TC B
14	7	TD B
15	14	TC A
16	15	RD B
17	16	RC A
20	9	DTR
24	6	XTC A

ADAPTADOR PARA INTERFACE G.703 (CB-G703-NR)

Opcionalmente, o cabo/adaptador para interface G.703 a 2 Mbps (CB-G703-NR, código Digitel 810.0349) pode ser adquirido para fazer a ligação de cabos coaxiais G.703 ao conector macho DB25 do painel traseiro do NetRouter. Quando este cabo estiver instalado e o roteador for ligado, a porta WAN será automaticamente configurada para interface G.703, tipo DTE.

Nota:
Este cabo é opcional. Para solicitar o cabo junto à Digitel, utilize o código 810.0349.

Observe que a conexão do cabo coaxial TX deve ser feita no conector TX do adaptador, e que a conexão do cabo coaxial RX deve ser feita no conector RX do adaptador.

O NetRouter 2G permite acesso a todos os aspectos configuráveis via Console, Telnet ou SSH, utilizando-se a interface de linha de comandos CLI.

Além das formas de acesso de configuração já disponíveis anteriormente, o NetRouter 2G também possibilita a configuração completa via WEB.

INICIALIZAÇÃO E REINICIALIZAÇÃO DO EQUIPAMENTO

Ao ser ligado, o NetRouter 2G realiza um autoteste das funções do hardware. Se repetidamente for detectada alguma falha (led ST em vermelho), conecte um terminal assíncrono ou estação de trabalho com programa equivalente na porta Console do equipamento (veja o capítulo sobre Instalação e configuração inicial). Ligue o roteador novamente, observe e anote as mensagens que aparecerão na tela do terminal e, tendo essas informações em mãos, entre em contato com o Centro de Assistência Técnica da Digitel.

Se nenhum erro ocorrer e o roteador estiver em modo automático, então o processo de inicialização (boot-up) do sistema operacional Linux é executado (led ST em laranja). Esse processo dura cerca de 20 segundos, sendo que, após esse período, o equipamento entra em operação normal (led ST em verde).

A partir deste momento, é possível operar o equipamento através das diversas interfaces de usuário disponíveis: WebConfig ou CLI (Telnet, SSH ou Console). Em cada uma dessas interfaces, um comando ou opção que permite reiniciar a operação do equipamento é disponibilizado. Por exemplo, através de um terminal assíncrono ligado à porta Console ou de um terminal Telnet, basta digitar o comando **`SET SYSTEM RESTART`** após o login.

NR2GBOOT E OS MODOS DE OPERAÇÃO

A operação normal do NetRouter 2G ocorre quando o equipamento é inicializado no modo automático, ou seja, quando ele é ligado ou reiniciado com todas as dip-switches do painel traseiro posicionadas para cima.

Em operação normal, o firmware de inicialização do equipamento (NR2GBoot) opera de forma completamente automática, procedendo imediatamente à carga do sistema operacional Linux e sua operação normal, utilizando a última configuração gravada na memória flash do equipamento.

O NR2GBoot possibilita colocar o roteador em outros modos de operação, que são úteis em casos de recuperação de erros de configuração, atualização de firmware do equipamento ou, ainda, manutenção.

Os erros de configuração e de atualização do firmware do NetRouter 2G são corrigidos iniciando ou reiniciando o equipamento no modo de segurança (veja o item a seguir).

Os modos de manutenção e teste somente devem ser utilizados por técnicos da Digitel ou sob sua orientação. A operação desses modos não está coberta neste manual.

MODO DE SEGURANÇA

Este modo de operação só deve ser utilizado quando não for mais possível acessar o equipamento em modo automático por nenhuma das interfaces de usuário disponíveis (WebConfig, Telnet, Console ou SSH). Isso pode ocorrer, basicamente, em três situações:

- o equipamento recebeu, gravou e tentou operar com uma configuração errada;
- ocorreu uma interrupção no processo de gravação de uma nova configuração (falta de energia elétrica);
- ocorreu uma interrupção no processo de transferência de uma nova versão de firmware para o equipamento (falta de energia elétrica).

Antes de colocar o NetRouter 2G para operar em modo de segurança, conecte um terminal assíncrono ou estação de trabalho com programa equivalente na porta Console do painel traseiro do equipamento.

Para colocar o equipamento no modo de segurança, ligue ou reinicie o roteador.

A tela do terminal deve mostrar uma série de mensagens do NR2GBoot, indicando o estado inicial do hardware do roteador e resultados do autoteste realizado. Nas últimas duas linhas, devem ser apresentadas as mensagens:

```
NetRouter 2G Security Mode
Press SPACE to stop autobooting in 5 seconds
```

Isso indica que o NetRouter 2G iniciou a operação em modo de manutenção e que a carga automática do sistema operacional Linux iniciará em 5 segundos, a não ser que, neste meio tempo, seja pressionada a barra de espaços no terminal ou estação de trabalho conectada à porta Console.

Para entrar em modo de segurança, entre com o comando **mode security**.

No modo de segurança, o sistema Linux é carregado com a seguinte configuração: apenas as portas Console e LAN0 são habilitadas, e esta última é configurada com o endereçamento IP específico deste modo (ipaddr=192.168.1.254, netmask=255.255.255.0 e gatewayip=192.168.1.1, quando o equipamento sai de fábrica).

Caso o erro que se deseja recuperar seja causado por um problema na configuração do roteador e as configurações atuais do modo de segurança sejam adequadas para comunicação do WebConfig com o equipamento através da LAN0, pode-se permitir que o NetRouter 2G prossiga no autoboot (carga automática do Linux); veja o item a seguir.

Em qualquer outro caso, deve-se interromper o processo de carga automática pressionando a barra de espaços no terminal conectado à porta Console do NetRouter 2G. Imediatamente, deve aparecer o prompt de comandos do programa NR2GBoot:

```
NR2GBoot>
```

Caso o processo de carga automática não seja interrompido a tempo, espere a carga completa do Linux, execute o login na Console (veja o item a seguir) e digite o comando **SET SYSTEM RESTART**. Preste atenção na próxima inicialização do equipamento, para não perder a janela de 5 segundos.

A tabela a seguir apresenta os comandos disponíveis no NR2GBoot e sua utilização:

Comando	Descrição
clear	Coloca valores de fábrica na configuração do modo de segurança e reinicia a operação do equipamento no modo determinado pelas dips.
help	Apresenta a descrição sucinta dos comandos do NR2GBoot.
linux	Inicia a carga do sistema operacional Linux.
restart	Reinicia imediatamente a operação do equipamento no modo determinado pelas dips.
setip	Mostra ou altera o endereçamento IP do modo de segurança.
setserv	Mostra ou altera o endereço do servidor de TFTP utilizado para atualizações de firmware.
update	Mostra ou atualiza a versão de firmware do equipamento.
version	Mostra a identificação da versão do NR2GBoot.
mode	Troca o modo de operação do NR2GBoot (Série 3200).

A sintaxe de cada um desses comandos é apresentada na própria tela do terminal, quando se digita o comando sem nenhum parâmetro, a não ser que o comando não necessite de parâmetros. Nesse caso, ele é imediatamente executado.

Os itens a seguir apresentam a utilização do modo de segurança para corrigir os erros ocorridos na atualização da configuração ou do firmware do equipamento.

IMPORTANTE!
Após corrigir o problema que originou a necessidade de operar no modo de segurança, reinicie o roteador.

Recuperando a configuração do roteador

Se, após uma alteração da configuração do roteador, não for mais possível operá-lo através do WebConfig, terminal Telnet ou porta Console, é provável que o equipamento tenha ficado mal configurado. Nesse caso, a utilização do modo de segurança permite novamente o acesso à operação do equipamento através de qualquer uma dessas interfaces, possibilitando a análise da configuração armazenada e sua correção ou completa substituição.

Para recuperar a configuração do roteador, execute os seguintes procedimentos:

1. Coloque o equipamento em modo de segurança e no prompt do NR2GBoot.
2. Verifique a configuração de endereçamento IP do modo de segurança:

```
setip show
```

3. Altere esta configuração de endereçamento caso isso seja necessário para acessar o equipamento através da LAN0 terminal Telnet, SSH ou WebConfig:

```
setip <novo_ip_lan0> <nova_mascara> <novo_gateway>
```

4. Verifique o estado do equipamento via Telnet e faça as alterações necessárias, ou, preferencialmente, verifique a configuração do equipamento via WebConfig e faça as alterações necessárias.
5. Agora reinicie o equipamento.

Recuperando a versão de firmware

Se, após uma tentativa de atualização do firmware do roteador, não for mais possível operá-lo através do WebConfig, SSH, terminal Telnet ou porta Console, é provável que o equipamento tenha ficado com o firmware incompleto ou incompatível com a versão de hardware do produto. Nesse caso, a utilização do modo de segurança permite atualizar novamente o firmware do roteador a partir do arquivo correto, colocado num servidor de TFTP acessível através da interface LAN0.

Para recuperar a versão de firmware do roteador, execute os seguintes procedimentos:

1. Coloque o equipamento em modo de segurança e no prompt do NR2GBoot.
2. Verifique a configuração de endereçamento IP do modo de segurança:

```
setip show
```

3. Altere esta configuração de endereçamento caso isso seja necessário para a comunicação com o servidor TFTP através da LAN0:

```
setip <novo_ip_lan0> <nova_mascara> <novo_gateway>
```

4. Verifique e altere, se necessário, o endereço IP do servidor TFTP:

```
setserv show
setserv <novo_ip_servidor>
```

5. Verifique a versão de firmware do equipamento:

```
update show
```

6. Caso necessário, coloque no servidor TFTP o arquivo com a versão mais estável ou mais recente do firmware do roteador.
7. Atualize a versão de firmware do equipamento:

```
update <nome_do_arquivo>
```

8. Acompanhe atentamente as mensagens exibidas no decorrer da atualização. Caso necessário, volte ao passo 2 ou a outro subseqüente.
9. Certifique-se de que a mensagem a seguir aparece ao final da atualização:

```
NetRouter 2G firmware correctly updated!
```

10. Reinicie a operação do equipamento, através do comando:

```
restart now
```

Limpando a configuração do roteador

Para limpar a configuração do NetRouter 2G, proceda de acordo com os seguintes passos:

1. Reinice o equipamento. Se o roteador já estiver ligado, execute o comando **SET SYSTEM RESTART** na interface de configuração.
2. A seguinte mensagem será apresentada:

```
NetRouter 2G Test Mode
Press SPACE to stop autobooting in 5 seconds
```

Pressione a barra de espaço antes que os 5 segundos se esgotem.

3. No prompt do Bootloader (**NR2GBoot>**), digite o comando **run clconf**.
4. Caso você deseje limpar a configuração do Bootloader, execute o comando **restart now**.

MODO DE OPERAÇÃO NORMAL

No modo de operação normal, após a inicialização do NetRouter 2G e a carga do sistema operacional Linux, que se dão de forma automática, o equipamento se encontrará pronto para ser configurado. Existem dois modos de configuração do NetRouter 2G:

1. Configuração via web: executada através do software configurador WebConfig;
2. Configuração via Console, Telnet ou SSH: executada através da interface de linha de comando (CLI).

A seguir, cada um desses modos de configuração será apresentado em detalhe.

CONFIGURAÇÃO VIA WEBCONFIG

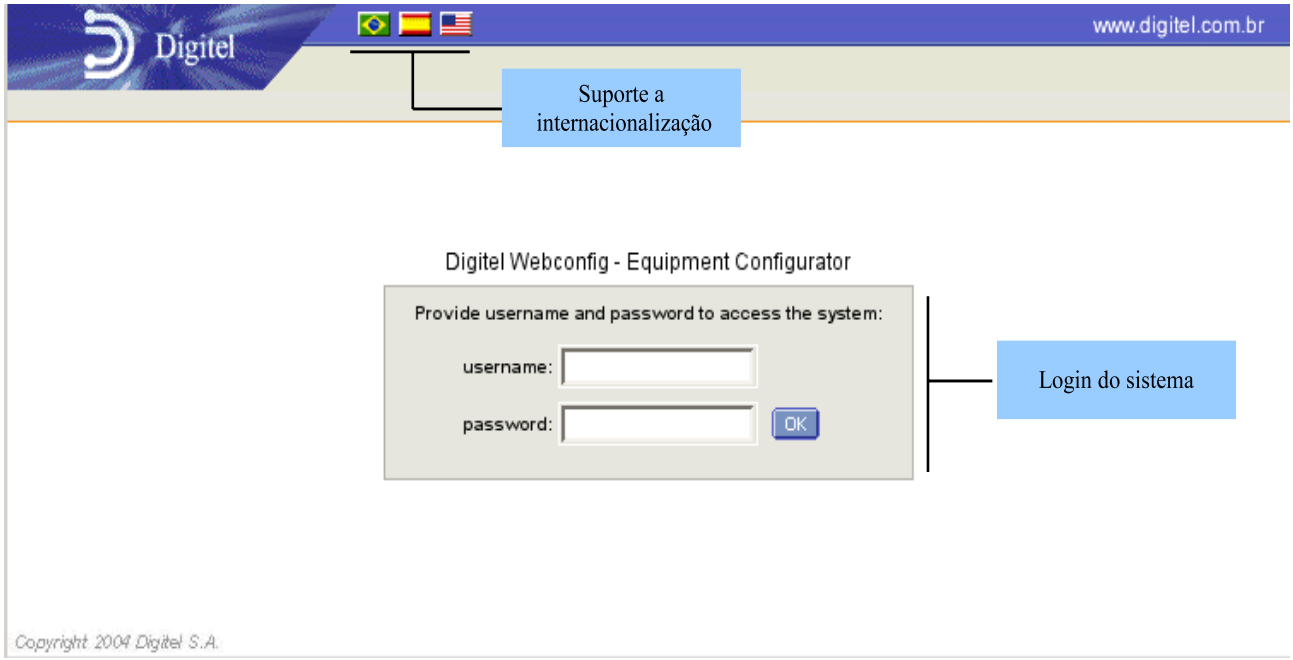
O WebConfig é o sistema de gerenciamento de configuração e diagnóstico da família NetRouter 2G, permitindo a configuração de todos os aspectos configuráveis do equipamento.

O WebConfig traz ao usuário o poder de configuração da CLI (*Command Line Interface*) através de seu browser, sem a necessidade de usar um cliente Telnet ou SSH.

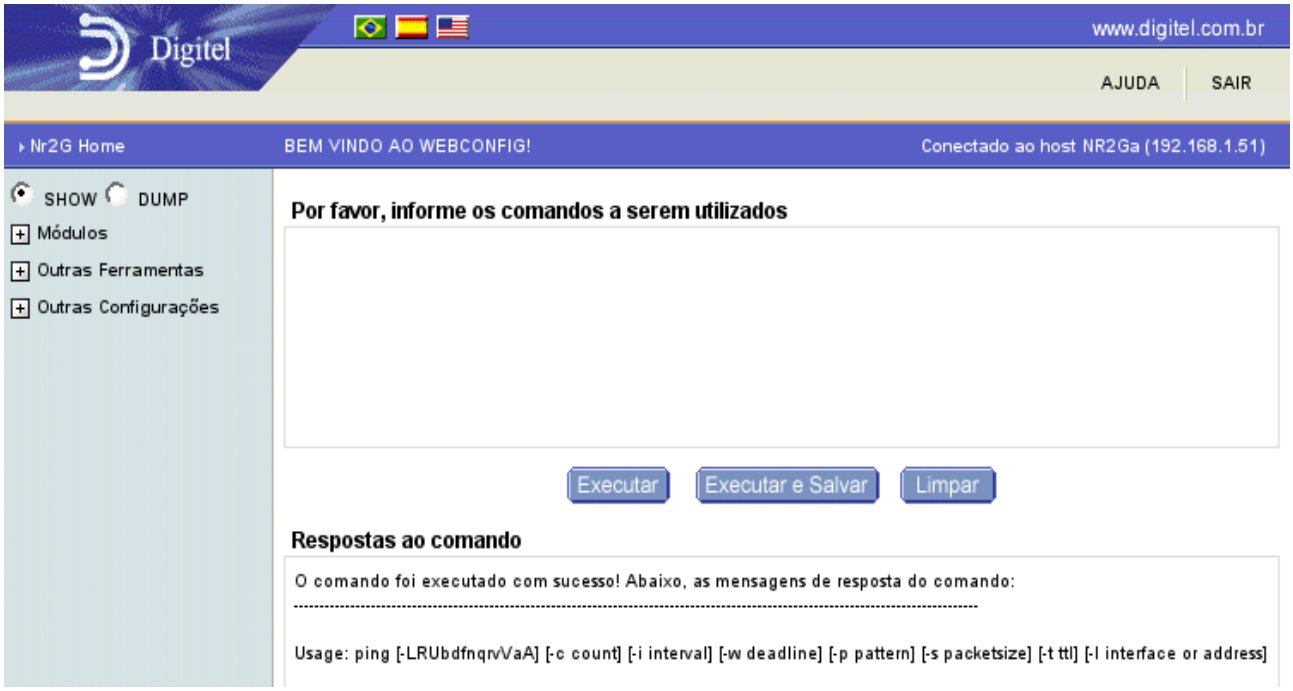
Dentre as suas principais vantagens, destacam-se:

- acesso via web (acessibilidade em qualquer lugar);
- utiliza a mesma sintaxe da CLI;
- ajuda on-line;
- controle total da configuração;
- internacionalização.

A partir da tela inicial do Webconfig, é possível escolher o idioma do sistema (suporte a internacionalização). Estão disponíveis os idiomas português, inglês e espanhol. Esse suporte permite a alteração do idioma a qualquer momento, desde a tela de login até a janela principal de configuração. A tela de login pode ser vista a seguir.



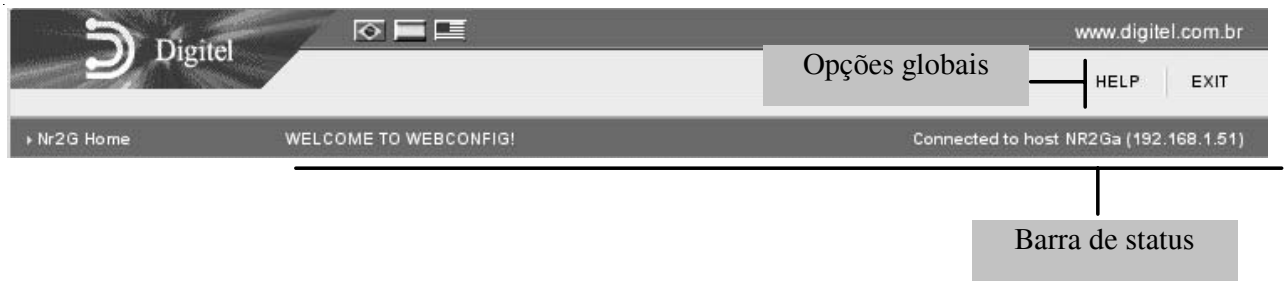
Através da tela principal do WebConfig, tem-se acesso a todas as funcionalidades presentes no configurador. Após o login, o usuário visualizará a seguinte tela:

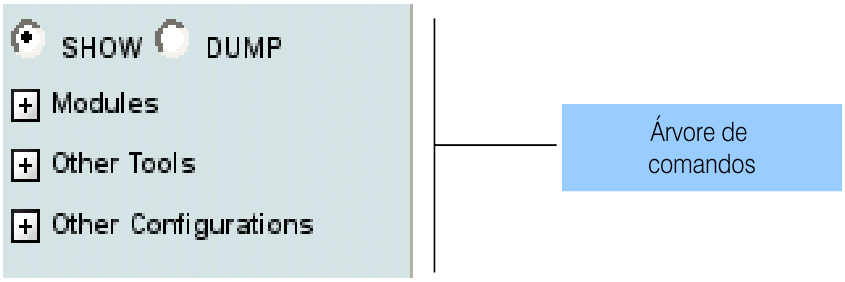


A tela principal está dividida em áreas funcionais, descritas a seguir:

- Internacionalização: Localizada na parte superior da tela.
- Opções globais: Localizada logo abaixo da internacionalização. Inclui a ajuda e o botão de logoff do sistema.
- Barra de status: Na barra de status encontram-se o nome e o endereço IP do equipamento conectado.
- Árvore de comandos: é dividida em três grupos funcionais, descritos a seguir:
    - *Módulos:* Refere-se à obtenção de informações de configuração de cada módulo de configuração do equipamento. É possivel obter tanto as estatísticas (por exemplo, estatísticas de LAN), quanto os comandos (comandos CLI) que representam uma dada configuração. Essa funcionalidade permite um acesso rápido à configuração, sem a necessidade de entrar com quaisquer comandos.
    - *Outras ferramentas:* Aqui encontram-se as ferramentas usadas para diagnóstico e depuração de problemas. Estão disponíveis atalhos para os comandos **`ping`**, **`traceroute`**, **`netstat`** e **`tcpdump`**. Ao clicar em **`ping`**, por exemplo, será exibido, na caixa de comandos (veja a seguir), o comando parcialmente preenchido, aguardando que o usuário complete com as opções desejadas. As opções disponíveis são exibidas na caixa de Resposta ao Comando.
    - *Outras configurações:* Aqui são apresentadas as opções de carga e salvamento de configuração. Para utilizar essas funcionalidades de forma automática, é necessária a configuração do mecanismo de importação/exportação de configuração (veja mais detalhes no *Guia do CLI*, seção *Exportando e importando arquivos de configuração*).
- Área de execução de comandos: É composta pela caixa de comandos (área de texto), onde são inseridos um ou mais comandos a serem executados. Os comandos seguem a sintaxe do CLI (consulte o *Guia do CLI*) e dispõem de botões de controle para a sua execução. Dentre os botões disponíveis estão: **`Executar`**, que simplesmente executa o conteúdo da caixa de comandos; **`Executar e Salvar`**, que atua da mesma forma que o botão anterior mas em seguida salva a configuração aplicada; e um botão **`Limpar`**, que limpa a caixa de comandos (ao executar um comando, a caixa de comandos fica limpa automaticamente).
- Resposta ao comando: É a área onde será exibida toda e qualquer resposta a um comando executado. Ao efetuar o login, essa área não estará presente, uma vez que, inicialmente, nenhum comando é executado. Para que a área de resposta ao comando se torne visível, basta executar algum comando, seja através da área de execução de comandos ou através da árvore de comandos.

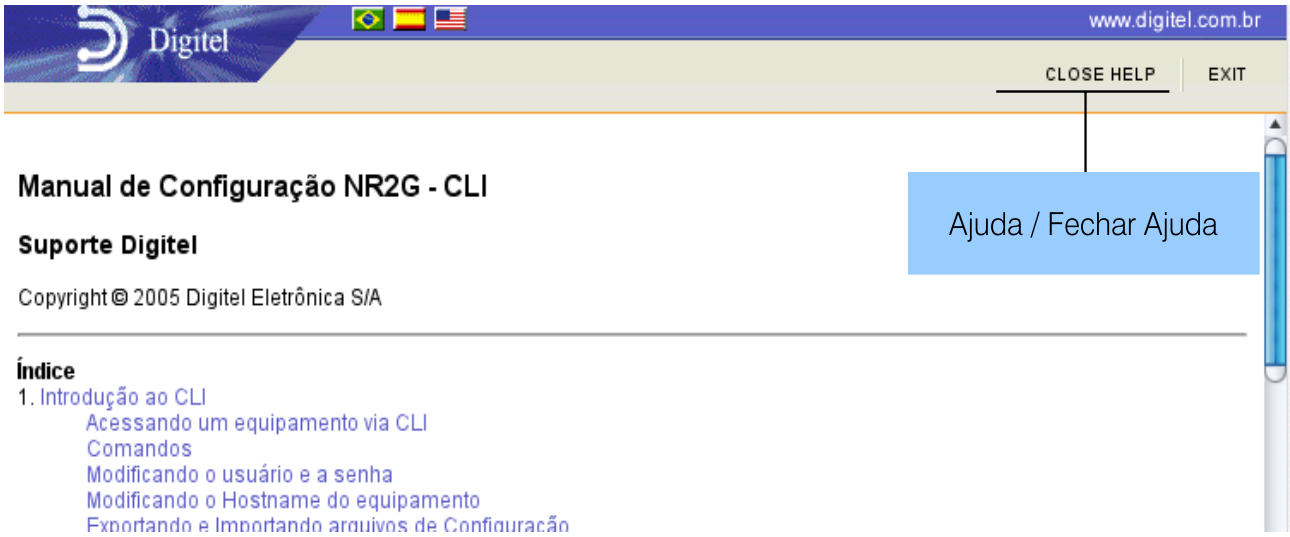
Para um melhor entendimento, as figuras a seguir ilustram os itens apresentados anteriormente.





Para ter acesso à ajuda on-line, clique no botão **Ajuda**, localizado na barra de opções globais. Além de uma apresentação do Webconfig, esse link também disponibiliza um guia de utilização dos comandos CLI, que demonstra como configurar diversos aspectos do equipamento através da linguagem CLI. Essa abordagem é muito vantajosa, visto que todas as formas de configuração (Console, Telnet, SSH e Web) utilizam a mesma linguagem.

Para sair da ajuda e voltar à tela principal, clique no botão **Ajuda**, que, após a abertura da ajuda on-line, estará sendo exibido como **Fechar Ajuda**. A ajuda pode ser visualizada na figura a seguir.



CONFIGURAÇÃO VIA CLI (TELNET/CONSOLE/SSH)

Após a carga do sistema operacional Linux, o NetRouter 2G disponibiliza uma interface de comandos CLI (Command Line Interface) que pode ser operada através da porta Console, SSH ou Telnet. O CLI permite suporte total a configuração, monitoração dos estados de operação do firewall, estatísticas e outros serviços suportados pelo equipamento.

Para realizar a operação do equipamento via porta Console (a porta Console está localizada no painel traseiro do equipamento), conecte um terminal assíncrono ou programa de emulação equivalente na referida porta. Consulte o item *Conexão da porta Console*, no capítulo *Instalação e configuração inicial* deste manual.

Para realizar a operação do equipamento via terminal Telnet ou SSH, execute um programa cliente (Telnet ou SSH) numa estação de rede com acesso ao NetRouter 2G. Por exemplo, num terminal Linux, digite:

```
telnet <endereço_ip_netrouter2g>
```

Uma vez realizada a conexão, uma mensagem semelhante à seguinte será apresentada na tela do terminal:

```
Linux 2.4.21 on Digitel NR2Ga

NR2G login:
```

Efetue o login, digitando um nome de usuário válido e, a seguir, a senha respectiva. O equipamento está originalmente configurado com usuário **nr2g** e senha **digitel**.

Após o login correto, é apresentada uma mensagem de boas vindas e o prompt de comandos da Console:

```
-----------------------------------
Welcome to NR2G from Digitel
-----------------------------------
Digitel Configuration Shell - CORE version: 1.42.0.97
Loading modules: SNMP LAN NAT ZEBRA IPSEC FIREWALL ROUTES DHCP SYSTEM
```

Pressione enter para obter uma lista dos comandos disponíveis.

Para obter mais informações, veja o capítulo Guia da CLI - Command Line Interface, que apresenta a relação de comandos e os respectivos parâmetros suportados por cada comando.

IMPORTANTE!
Aconselha-se a alteração da senha do usuário **nr2G** na primeira operação do equipamento. Para isso, utilize o comando **SET SYSTEM USER1**.

INTRODUÇÃO A CLI

Os equipamentos de rede Digitel estão equipados com um poderoso sistema de configuração conhecido como CLI (Command Line Interface). A CLI é um sistema de configuração modular, capaz de configurar todas as características de um determinado equipamento, bem como permitir a visualização de configuração e estatísticas, atualização de software e diversas outras funcionalidades.

A CLI pode ser acessado via terminal Console ou Telnet, sendo exigidos apenas usuário e senha previamente cadastrados. Cada linha de equipamentos sai de fábrica com um usuário e uma senha padrão, para permitir o acesso inicial ao equipamento.

A configuração é criada através de linhas de comandos baseadas em uma sintaxe simples e objetiva. A linguagem é estruturada de forma hierárquica, e a cada nível (subitem ou parâmetro) dentro de uma configuração, são exibidas as opções de configuração possíveis para aquele contexto.

Outros recursos importantes presentes na CLI são:

- Histórico de comandos;
- Exportação e importação de configuração;
- Níveis de acesso.

Acessando um equipamento via CLI

Para efetuar o login, é necessário ter uma conexão via Console ou de rede TCP/IP através da porta 23 (utilize um cliente Telnet). Ao estabelecer a comunicação com o equipamento, um rótulo com as informações de modelo e versão do equipamento será exibido, e o sistema ficará em espera aguardando o usuário e a senha do operador, como ilustrado a seguir:

```
NR2Ge Linux version 2.4.21-rc2-p2_13 (56116c) #47 Sat Jan 31 00:07:16 BRST 2004
NR2G login:
```

Após entrar com usuário e senha válidos, será exibida a apresentação da CLI, como ilustrado a seguir:

```
------------------------------------
Welcome to NetRouter 2G from Digitel
------------------------------------
Digitel Configuration Shell - CORE version: 1.40.5.17
Loading modules: GRE IPX SNMP LAN NAT QOS WAN L2TP ZEBRA OSPFZ IPSEC BACKUP
BRIDGE FIREWALL ROUTES PPTP DHCP SYSTEM PROXYARP RIPZ
NR2Gd >
```

Categorias de comandos

Os comandos da CLI estão divididos em categorias de ações. Uma ação indica à CLI que tipo de procedimento o usuário deseja fazer. Para exemplificar, vamos supor que o usuário deseje EXIBIR as configurações da interface LAN0. Para isso, ele deverá dizer à CLI que a ação a ser executada é um SHOW e, posteriormente, deverá indicar que deseja ver as configurações de LAN (LAN0, por exemplo). Assim, o comando ficaria SHOW LAN LAN0 ALL. Este princípio é obedecido em todas as categorias de ações. As ações disponíveis são:

- SET: indica que o usuário deseja inserir ou alterar a configuração de um determinado item da configuração.
- SHOW: indica que o usuário deseja visualizar a configuração ou estatísticas de um determinado aspecto da configuração.

- DUMP: solicita à CLI que informe quais são os comandos (comandos CLI) que representam a configuração atual de um determinado item.
- EXEC: informa que o usuário quer executar um dos utilitários disponíveis no equipamento.
- CONFIG: permite salvar ou exportar a configuração do equipamento. A configuração exportada é em formato de arquivo de texto, tendo como conteúdo uma listagem de comandos CLI que representa uma dada configuração.
- ?: informa quais são os módulos configuráveis suportados pelo CLI. Esses módulos são utilizados nas ações SET, SHOW e DUMP.
- QUIT: finaliza a execução do CLI. Caso o usuário altere a configuração e não a salve, o CLI solicitará a confirmação da modificação da configuração antes de finalizar a sessão.

A cada nível de um comando pode-se pressionar a tecla ENTER. Essa ação diz à CLI para exibir todas as opções de parâmetros para aquele determinado contexto de comando. Este recurso é bastante útil quando não se conhece previamente a sintaxe da configuração desejada. Esse recurso é ilustrado a seguir:

```
SET LAN <ENTER>
```

Saída após o ENTER:

```
SET LAN
       LAN0
```

Ou então:

```
SET LAN LAN0 <ENTER>
```

Saída após o ENTER:

```
IP              <IP address>
MASK            <Network mask>
BROADCAST       <Broadcast address>
RESETCOUNTERS   <Reset counters>
UP              <Enable interface>
DOWN            <Disable interface>
PURGE           <Clear configuration>
BROADCAST       <Broadcast address>
STATS
```

Sendo assim, para configurar a interface LAN0, o comando a ser aplicado poderá ser:

```
SET LAN LAN0 IP 192.168.1.99 MASK 255.255.255.0 UP <enter>
```

Além do recurso de informar as opções disponíveis, podemos também utilizar o recurso de histórico para não precisar reescrever o comando novamente (pressione a tecla “seta para cima”) e incluir/alterar a configuração.

Para verificar a configuração criada na LAN0, uma ação SHOW deverá ser utilizada:

```
SHOW LAN LAN0 ALL <enter>
```

Saída do comando:

```
Applying to interface: LAN0
IP                  192.168.1.99
MASK                255.255.255.0
BROADCAST           192.168.1.255
INTERFACE:          eth0
ADMINSTATUS:        UP
PACKETS SENT:       349
PACKETS RECEIVED:   81424
```

```
BYTES SENT:        26700
BYTES RECEIVED:    7666320
TX ERRORS:         0
RX ERRORS:         0
TX DROPPED:        0
RX DROPPED:        0
TX OVERRUN:        0
RX OVERRUN:        0
COLLISION:         0
CRC:               0
BROADCASTS RECEIVED: 80991
LAST RECEIVED PACKET TIME (s): 0.01
TRANSMIT QUEUE LENGHT: 0
TOTAL TRANSMIT QUEUE LENGHT: 100
LAST TRANSMITED PACKET TIME (s):0.01
LINK STATUS: UP
LAST LINK STATUS CHANGE TIME (s):65662.95
LAST ADMIN STATUS CHANGE TIME (s): 65662.95
```

Para descobrir quais os comandos que representam alguma configuração atual, utilize o comando DUMP. Assim, será possível conferir o comando que gerou a configuração das interfaces LAN:

```
DUMP LAN ALL <enter>
```

Saída do comando:

```
SET LAN LAN0 PURGE
SET LAN LAN0 IP 192.168.1.99 MASK 255.255.255.0 BROADCAST 192.168.1.255 UP
```

Existem utilitários que auxiliam no teste e na depuração dos equipamentos. Esses utilitários são acionados através da ação EXEC. Os utilitários disponíveis são:

- NETSTAT: provê estatísticas de interface, estado de conexões (TCP, UDP, etc.), informações sobre a tabela de rotas, etc.
- PING: executa comandos ping (ICMP ECHO_REQUEST).
- TCPDUMP: analisador de tráfego de rede.
- TRACEROUTE: informa o trajeto (hops) até alcançar um determinado host.
- TELNET: executa um cliente Telnet.

A título de exemplo, é possível verificar como está o estado das conexões TCP do equipamento. Para isso, use o comando NETSTAT e a opção “-t” (TCP connections), como demonstrado a seguir:

```
EXEC NETSTAT -t <enter>
```

Saída do comando:

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address       Foreign Address        State
tcp   0      0      192.168.1.99:telnet 192.168.1.107:42053    ESTABLISHED
```

Verificar a conectividade de um enlace:

EXEC PING 192.168.1.247 -c 4 <enter>

Saída do comando:

```
PING 192.168.1.247 (192.168.1.247) 56(84) bytes of data.
64 bytes from 192.168.1.247: icmp_seq=1 ttl=64 time=2.27 ms
64 bytes from 192.168.1.247: icmp_seq=2 ttl=64 time=0.820 ms
64 bytes from 192.168.1.247: icmp_seq=3 ttl=64 time=0.805 ms
64 bytes from 192.168.1.247: icmp_seq=4 ttl=64 time=0.789 ms
--- 192.168.1.247 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3034 ms
rtt min/avg/max/mdev = 0.789/1.171/2.272/0.636 ms
```

Efetuar a análise de pacotes em trânsitono equipamento:

EXEC TCPDUMP <enter>

Saída do comando:

```
Nov 6 06:45:05 NR2G-3200 kernel: eth0: Promiscuous mode enabled.
Nov 6 06:45:05 NR2G-3200 kernel: device eth0 entered Promiscuous mode tcpdump:
listening on eth0
06:45:05.828775 10.10.10.71.netbios-dgm > 10.10.10.255.netbios-dgm: NBT UDP
PACKET (138)
06:45:05.861125 10.10.10.71.netbios-dgm > 10.10.10.255.netbios-dgm: NBT UDP
PACKET (138)
06:45:06.294381 802.1d config 8000.00:01:00:f1:ea:48.8001 root
8000.00:01:00:f1:ea:48 pathcost 0 age 0 max 20
hello 2 fdelay 15
06:45:08.294571 802.1d config 8000.00:01:00:f1:ea:48.8001 root
8000.00:01:00:f1:ea:48 pathcost 0 age 0 max 20
hello 2 fdelay 15
06:45:10.294417 802.1d config 8000.00:01:00:f1:ea:48.8001 root
8000.00:01:00:f1:ea:48 pathcost 0 age 0 max 20
hello 2 fdelay 15
06:45:12.294531 802.1d config 8000.00:01:00:f1:ea:48.8001 root
8000.00:01:00:f1:ea:48 pathcost 0 age 0 max 20
hello 2 fdelay 15
06:45:14.294418 802.1d config 8000.00:01:00:f1:ea:48.8001 root
8000.00:01:00:f1:ea:48 pathcost 0 age 0 max 20
hello 2 fdelay 15

7 packets received by filter
0 packets dropped by kernel
Nov 6 06:45:14 NR2G-3200 kernel: device eth0 left promiscuos mode
```

Como já visto antes, a ação CONFIG é responsável por permitir o salvamento e a leitura da configuração, bem como a exportação e importação da mesma. Essas opções são representadas pelos seguintes comandos:

CONFIG <enter>
Saída do comando:

```
INPUT
EXTERN
LOAD
SAVE
PURGE
```

EXTERN: possibilita a importação ou exportação da configuração para/de um servidor ftp.

LOAD: efetua a leitura da última configuração gravada no equipamento.

SAVE: faz o salvamento da configuração atual.

PURGE: limpa a configuração.

IMPORTANTE!
Ao final de uma configuração, o comando **CONFIG SAVE** deve ser executado para que as configurações sejam salvas.

MODIFICANDO USUÁRIO E SENHA

Por padrão, o usuário previamente configurado para acessar o roteador é o nr2g. Existem ainda alguns usuários de sistema e a possibilidade de se adicionar diversos outros usuários. Os seguintes níveis de acesso estão disponíveis.

OPERATOR	Lê informações do equipamento (comando **SHOW**).
MODERATOR	Usuário utilizado para cadastro (cria e modifica permissão de usuários).
ADMINISTRATOR	Usuário administrador do sistema. Realiza qualquer operação.

Ao aplicar o comando **SHOW SYSTEM ALL**, podemos observar que existem quatro usuários criados, sendo dois deles reservados (user2 e user3):

USER0: Usuário ROOT. Não é acessado via Telnet e SSH; somente via Console. Utilizado somente para depuração por técnicos da Digitel.

```
Applying to:  USER0
TYPE          ADMINISTRATOR
LOGIN         root
```

USER1: Principal usuários para configuração do sistema.

```
Applying to:  USER1
TYPE          ADMINISTRATOR
LOGIN         nr2g
```

Para modificar o usuário nr2g, siga os procedimentos descritos abaixo:

```
NR2Gt > SET SYSTEM USER1 <enter>
Applying to: USER1
Valid SET options are:
     TYPE       Tipo de permissão
     LOGIN      Nome do usuário
     PASS       Senha para o usuário
     PURGE      Limpa as configurações do módulo USER1
NR2Gt > SET SYSTEM USER1 TYPE ADMINISTRATOR LOGIN usuário PASS senha
```

Para criar um outro usuário, aplique o comando **SET SYSTEM <enter>**. Note que o valor x (USERx) será incrementado. Utilize o último usuário para configurar uma nova conta:

SET SYSTEM USER4 TYPE OPERATOR LOGIN operador **PASS** operador 2003.

MODIFICANDO O HOSTNAME DO EQUIPAMENTO

Dentro de uma grande topologia de rede, muitas vezes podemos encontrar dificuldades ao tentar identificar determinado dispositivo. Para isso, é utilizado um hostname, sendo esta a forma mais simples de identificar o equipamento desejado dentro da rede. A configuração é feita da seguinte forma:

```
NR2Gt > SET SYSTEM HOSTNAME digitel
digitel >
```

Observe que o nome do roteador foi alterado para “digitel”.

EXPORTANDO E IMPORTANDO ARQUIVOS DE CONFIGURAÇÃO

Uma das características dos roteadores NetRouter 2G é a possibilidade de exportar ou importar as configurações existentes no equipamento. Isso é feito através do protocolo FTP (File Transfer Protocol). Segue a descrição dos parâmetros de configuração:

```
NR2Gt > CONFIG EXTERN <enter>
     SERVER        Configura o IP do servidor de FTP
     USER          Configura o usuário definido no servidor de FTP
     PASS          Configura a senha do usuário do FTP
     REMOTEFILE    Nome do arquivo a ser importado ou exportado
     IMPORT        Ação de importar
     EXPORT        Ação de exportar
     SHOW          Visualiza configurações do módulo EXTERN
     PURGE         Limpa configurações do módulo EXTERN
```

Para exportar a configuração, utilize:

```
NR2Gt > CONFIG EXTERN SERVER 10.10.10.63 USER digitel PASS digitel REMOTEFILE
config.dat EXPORT
```

Para importar a configuração, utilize:

```
NR2Gt > CONFIG EXTERN SERVER 10.10.10.63 USER digitel PASS digitel REMOTEFILE
config.dat IMPORT
```

ATUALIZAÇÃO DE SOFTWARE

Existem duas formas de atualização do NR-2G: via TFTP ou FTP. A seguir são apresentadas essas duas formas e, logo em seguida, também a atualização do BootLoader do roteador, caso seja indicado pela Digitel.

Para obter o arquivo da versão de software do sistema operacional ou boot, siga os passos descritos abaixo:

1. Acesse o servidor FTP da Digitel: ftp://ftp.digitel.com.br/Produtos/ROTEADORES/NR-2G/.

2. Em seguida, acesse a pasta correspondente ao modelo e versão de hardware do NR-2G a ser atualizado. O modelo e versão de hardware do equipamento (identificado pelo número 800.XXXX.XX-X, código Digitel) podem ser verificados na etiqueta adesiva afixada na parte inferior do roteador (tampa inferior). Veja as tabelas que identificam a versão do hardware de seu equipamento:

• Os modelos da Série NetRouter 2G 3200 possuem as seguintes opções de hardware:

Modelo com 8 MB de memória Flash e 16 MB de memória RAM:
800.1085.00-5 NR-2G 3201

Modelos com 16 MB de memória Flash e 32 MB de memória RAM:
800.1102.00-7 NR-2G 3211
800.1103.00-3 NR-2G 3212
800.1104.00-0 NR-2G 3214
800.1107.00-9 NR-2G 3218
800.1091.00-5 NR-2G 3251
800.1092.00-1 NR-2G 3252
800.1093.00-8 NR-2G 3254
800.1094.00-4 NR-2G 3258
800.1120.00-5 NR-2G 3261
800.1142.00-9 NR-2G 3262
800.1143.00-5 NR-2G 3264
800.1121.00-1 NR-2G 3268
800.1122.00-8 NR-2G 3281
800.1144.00-1 NR-2G 3282
800.1145.00-8 NR-2G 3284
800.1123.00-4 NR-2G 3288

• Os modelos da Série NetRouter 2G 4200 possuem basicamente duas opções de hardware:

Revisão 0 - Sem suporte a módulos de voz - códigos Digitel (Part Number)
800.0840.00-4 NR-2G 4200
800.0841.00-0 NR-2G 4200/DC

Revisão 1 - Com suporte a módulos de voz - códigos Digitel (Part Number)
800.0840.01-2 NR-2G 4200
800.0841.01-9 NR-2G 4200/DC

3. Faça o download do arquivo adequado, considerando o modelo e hardware utilizado, onde:

• a extensão DWN indica o arquivo do sistema operacional para atualização local via TFTP;

• a extensão IMx (x valendo de 0 a 5) indica os arquivos de uma única versão de software do sistema operacional para atualização remota via FTP;

• a extensão BOOT indica o arquivo de BootLoader para atualização local via TFTP (este arquivo só deve ser atualizado quando indicado pela Digitel).

Atualização do sistema operacional

Para atualizar o sistema operacional do NR-2G, será preciso um servidor TFTP ou FTP instalado em um host qualquer acessível pelo roteador, com o devido arquivo para ser carregado no mesmo diretório do servidor (DWN para TFTP e IMx para FTP).

Na Console que está acessando o NR-2G a ser atualizado, que pode ser um PC com hyperterminal do Windows (veja configuração para conexão à porta Console no capítulo Instalação e configuração inicial), aplicar o seguinte comando:

```
NR2Gt > SET SYSTEM UPDATE <enter>
Valid SET options for UPDATE are:
     TYPE       Tipo de atualização (FTP/TFTP)
     FILE       Nome do arquivo de atualização (FTP - *.imx | TFTP - *.dwn)
     SERVER     Endereço IP do servidor TFTP e/ou FTP
     USER*      No caso da atualização por FTP, identificar aqui o usuário
     PASS*      No caso da atualização por FTP, identificar aqui a senha do usuário
     EXECUTE    Inicia a atualização do roteador
*Only when TYPE=FTP
```

Atualização local via TFTP

O comando para executar a atualização via TFTP é:

SET SYSTEM UPDATE TYPE TFTP FILE 66101R0.dwn SERVER 10.10.10.63 EXECUTE

Neste exemplo, o arquivo de atualização é o 66101R0.dwn.

IMPORTANTE!
A atualização via TFTP deve ser utilizada somente para carga local, via LAN.

Atualização local ou remota via FTP

O FTP pode ser utilizado para os casos de atualização local do sistema operacional, via LAN, ou atualização remota, via porta WAN. O comando para executar a atualização via FTP é:

SET SYSTEM UPDATE TYPE FTP FILE 66101R0 SERVER 10.10.10.7 USER ftpuser PASS digitel EXECUTE

Neste exemplo, a versão a ser atualizada é a 66101R0. A atualização via FTP trabalha com um outro tipo de formato de arquivo, o IMx, onde x indica o número seqüencial do arquivo. No diretório do servidor FTP, os seguintes arquivos devem estar disponíveis:

66101R0.im0

66101R0.im1

66101R0.im2

66101R0.im3

Atualização do BOOTLOADER e SOFTWARE

Em casos especiais, a Digitel disponibiliza o arquivo de BOOT para ser atualizado no NR-2G. A atualização é feita no prompt "NR2Gboot" do roteador.

Os seguintes passos devem ser observados:

1. Reinicie o equipamento.

2. Com a Console ativa, que pode ser um PC com hyperterminal do Windows (veja o item Configuração para conexão à porta Console, no capítulo Instalação e configuração inicial), ligue o NR-2G, pressionando diversas vezes a tecla de espaço do teclado.

3. O roteador entrará no prompt de manutenção (**NR2Gboot**). Com o arquivo BOOT disponível em um host qualquer da rede local, no mesmo diretório do servidor TFTP, digite os seguintes comandos na Console do NR-2G:

```
setip "Endereço IP do Roteador" "Máscara de Rede" "Endereço IP do Gateway"
setserv "Endereço IP do Servidor de TFTP"
upboot "arquivo.boot"
```

Exemplo:

```
setip 10.10.10.1 255.255.255.0 10.10.10.2
setserv 10.10.10.2
upboot 66101R0.boot
```

4. Se a atualização do arquivo boot for bem-sucedida, a seguinte mensagem será exibida:

```
NetRouter 2G boot correctly update!
```

5. Ao final do processo, digite **clear now** e pressione <enter> para que os valores default do novo BootLoader sejam utilizados.

6. Digite **restart now** e pressione <enter> para validar a carga do novo BootLoader no NR-2G.

7. A seguinte mensagem será apresentada:

```
NetRouter 2G Maintenance Mode
Press SPACE to stop autobooting in 5 seconds
```

Pressione a barra de espaço antes que os 5 segundos se esgotem.

8. O roteador entrará novamente no prompt de manutenção (**NRG2boot>**). Digite **run clconf** e pressione <enter>.

IMPORTANTE!
Ao realizar a atualização do BootLoader, é necessário que a atualização de software do sistema operacional também seja realizada pelo prompt NR2Gboot, seguindo os próximos passos deste roteiro.

9. Para a carga do sistema operacional via prompt de manutenção **(NR2Gboot>)**, coloque o arquivo DWN em um host qualquer da rede local, no mesmo diretório do servidor TFTP, e digite os seguintes comandos:

```
setip "Endereço IP do Roteador" "Máscara de Rede" "Endereço IP do Gateway"
setserv "Endereço IP do Servidor de TFTP"
update "arquivo.dwn"
```

Exemplo:

```
setip 10.10.10.1 255.255.255.0 10.10.10.2
setserv 10.10.10.2
update 66101R0.dwn
```

10. Após esse procedimento, digite **run clconf** e pressione <enter>.

11. No painel traseiro do NR-2G, volte a dip número 2 para a posição para cima, colocando o roteador no Modo Normal de operação. Depois, digite **boot** e pressione <enter> para reiniciar o roteador.

CONFIGURANDO ENDEREÇO ETHERNET

```
NR2Gt > SET LAN <enter>
     LAN0
     LAN1
To create new virtual interfaces use:
        <Valid real interface name>:<New virtual interface number>
Examples:
     LAN0:1
     LAN1:1
     LAN1:2
```

Veja que, após adicionar o comando **SET LAN** e pressionar ENTER, pode-se verificar a sintaxe do comando e as informações de cada interface a ser configurada.

O comando a seguir será utilizado para configurar a interface LAN0. Note que o equipamento que está sendo configurado possui duas interfaces LAN (LAN0 e LAN1); portanto, trata-se dos modelos 3214, 3216 e 3218.

```
NR2Gt > SET LAN LAN0 IP 192.168.1.1 MASK 255.255.255.0 UP
```

Para verificar se as informações foram aplicadas corretamente, utilize o comando **SHOW**.

```
NR2Gt > SHOW LAN LAN0 <enter>
Valid options for this command are:
     IP
     MASK
     BROADCAST
     STATS
     ALL
```

As informações são apresentadas separadamente ou todas de uma única vez, utilizando o parâmetro **ALL**.

```
NR2Gt > SHOW LAN LAN0 ALL
Applying to interface: LAN0
IP              192.168.1.1
MASK            255.255.255.0
BROADCAST       192.168.1.255
INTERFACE:      eth0
ADMINSTATUS:    UP
PACKETS SENT:   0
PACKETS RECEIVED:   5530
BYTES SENT:     0
BYTES RECEIVED:     544494
TX ERRORS:      0
RX ERRORS:      0
TX DROPPED:     0
RX DROPPED:     0
TX OVERRUN:     0
RX OVERRUN:     0
COLLISION:      0
CRC:            0
BROADCASTS RECEIVED:              5340
LAST RECEIVED PACKET TIME (s):    0.08
TRANSMIT QUEUE LENGHT:            0
TOTAL TRANSMIT QUEUE LENGHT: 100
LAST TRANSMITED PACKET TIME (s): 3334.62
LINK STATUS:   UP
LAST LINK STATUS CHANGE TIME (s):414.63
LAST ADMIN STATUS CHANGE TIME (s):    416.5
```

CONFIGURANDO ENDEREÇO ETHERNET VIRTUAL

A possibilidade de criação de um endereço IP virtual, ou seja, uma interface virtual, é uma característica muito interessante dos roteadores NetRouter 2G. Note que, ao digitar o comando **SET LAN <enter>**, a resposta de saída do comando será:

```
NR2Gm > SET LAN <enter>
        LAN0
        LAN1
To create new virtual interfaces use:
        <Valid real interface name>:<New virtual interface number>
Examples:
     LAN0:1
     LAN1:1
     LAN1:2
```

Para a criação da interface virtual, deve-se utilizar a nomenclatura indicada acima. Um pequeno exemplo de interface virtual está descrito abaixo:

```
NR2Gm > SET LAN LAN0:1 <enter>
Valid options for this command are:
IP             <IP address>
MASK           <Network mask>
BROADCAST      <Broadcast address>
RESETCOUNTERS
UP
DOWN
PURGE
```

Os parâmetros de criação são os mesmos utilizados para a interface física. Para as demais interfaces criadas, basta seguir uma seqüência lógica de valores, como no exemplo acima.

CONFIGURANDO VLAN (802.1Q)

Os roteadores da Digitel permitem marcar pacotes com o padrão IEEE 802.1Q. Para fazer essa marcação, siga os passo abaixo.

```
SET  LAN
     To create VLAN interfaces use:
     <Valid real interface name>.<VLAN ID>
Examples:
        LAN0.1
        LAN1.1
        LAN1.2

SET LAN LAN0:1.100
```

No exemplo acima, está sendo marcado os pacotes passando pela LAN0 com o ID 100.

PROTOCOLO FRAME RELAY

O Frame Relay é hoje o protocolo de encapsulamento mais utilizado pelas operadoras de serviços de telecomunicações, pelo fato de ter um custo menor de instalação e manutenção. Na especificação do protocolo de LMI, a Digitel possui dois tipos, o ANSI e o CCITT, podendo-se, ainda, utilizar a opção NONE.

Para a configuração de um enlace Frame Relay existem os seguintes parâmetros:

```
NR2Gt > SET WAN WAN0 <enter>
Valid options for command SET are:
PROTO {NONE,HDLC,FRAMERELAY,PPPS,PPPA,DIALIN,X25}
Any other parameters depends on protocol defined to each interface
You must specify a protocol
```

Note que, neste ponto, deve ser definindo o protocolo a ser utilizado.

```
NR2Gt > SET WAN WAN0 PROTO FRAMERELAY
NR2Gt > SET WAN WAN0 <enter>
Valid options for command SET are:
PROTO {NONE,HDLC,FRAMERELAY,PPPS,PPPA,DIALIN,X25}
Any other parameters depends on protocol defined to each interface
Valid SET options for protocol FRAMERELAY:
     PROTOCOL           Configura o protocolo (ANSI, CCITT, NONE)
     DCE                Configura o modo de trabalho (DCE/DTE)
     CLOCK              Configura o clock (interno/externo)
     SPEED              Configura a velocidade do clock interno
     TXINV              Inverte a borda do clock
     TRAFFIC-SHAPE      Habilita o traffic shape
     BANDWIDTH*         Configura a largura de banda
     T391               Timer do Frame Relay
     T392               Timer do Frame Relay
     N391               Timer do Frame Relay
     N392               Timer do Frame Relay
     N393               Timer do Frame Relay
     RESETCOUNTERS      Resseta os contadores de estatística
     UP                 Levanta o protocolo
     DOWN               Derruba o protocolo
     PURGE              Limpa as configurações
     PVC0               Seta as configurações da interface PVC0
*Only when TRAFFIC-SHAPE=TRUE
NR2Gt > SET WAN WAN0 PROTOCOL ANSI
NR2Gt > SET WAN WAN0 PVC0 <enter>
Applying to interface: WAN0
Valid SET options for PVCs of FRAMERELAY protocol are:
     DLCI               Configura o DLCI
     MTU                Configura o MTU
     IP                 Configura o endereço IP da interface PVC0
     MASK               Configura a máscara de rede da interface PVC0
     PEER               Indica o endereço IP do PVC remoto
     CIR                Configura o CIR
     PEAK               Configura o pico de tráfego
     INVERSE-ARP        Configura o inverse arp
     RESETCOUNTERS      Resseta os contadores
     PURGE              Limpa a configuração do módulo PVC0
NR2Gt > SET WAN WAN0 PVC0 DLCI 16 MTU 1500 IP 10.10.10.1 MASK 255.255.255.252
PEER 10.10.10.2 <enter>
NR2Gt > SET WAN WAN0 UP
```

Para verificar se o protocolo está ativo, digite o comando a seguir:

```
NR2Gt > SHOW WAN WAN0 PVC0 STATS
Applying to interface:  WAN0
Applying to PVC:        PVC0
INTERFACE:              pvc0
ADMINSTATUS:            UP
PACKETS SENT:           0
PACKETS RECEIVED:       0
BYTES SENT:             0
```

```
BYTES RECEIVED:          0
TX ERRORS:               0
RX ERRORS:               0
TX DROPPED:              0
RX DROPPED:              0
TX OVERRUN:              0
RX OVERRUN:              0
COLLISION:               0
BROADCASTS RECEIVED:     0
LAST RECEIVED PACKET TIME (s):   5456.66
TRANSMIT QUEUE LENGHT:           0
TOTAL TRANSMIT QUEUE LENGHT: 100
LAST TRANSMITED PACKET TIME (s):5456.66
LINK STATUS:  DOWN
LAST LINK STATUS CHANGE TIME (s):338.19
LAST ADMIN STATUS CHANGE TIME (s):    338.19
```

O link status deve permanecer como UP enquanto estiver ativo.

PROTOCOLO PPP

Na configuração PPP síncrono, existem os seguintes parâmetros:

```
SET WAN
WAN0 PROTO
PPPS
SET WAN
WAN0 <enter>
     DEBUG              Habilita mensagens de depuração (TRUE / FALSE)
     VJ                 Compreensão Van Jacobson (TRUE / FALSE)
     *SPEED             Velocidade de Conexão
     PPPDEFROUTE        Habilita a rota default para a conexão (TRUE / FALSE)
     MRU                Configura o MRU
     MTU                Configura o MTU
     AUTH**             Define o tipo de autenticação
     USER**             Usuário para autenticação
     PASS**             Senha para autenticação
     CHAP**             Caso autenticação CHAP, configura CHAP
     PAP**              Caso autenticação PAP, configura PAP
     IPCP               Configuração IPCP (IP Local e Remoto)
     LCP                Configuração dos parâmetros de LCP
     TXINV              Inverte a borda do clock  (TRUE / FALSE)
     HOLDOFF            Intervalo entre tentativas de reconexão
     RESETCOUNTERS      Limpa os contadores de estatísticas da interface
     UP                 Levanta a interface
     DOWN               Derruba a interface
     PURGE              Limpa as configurações do módulo WANX
*Only when CLOCK=INTERNAL
*Only when AUTH is CHAP or RAP
```

Para exemplificar a configuração de PPP síncrono, segue o exemplo a seguir:

```
SET WAN WAN0 PROTO PPPS
SET WAN WAN0 IPCP LOCALIP ENABLED TRUE ADDRESS <IP WAN CLIENTE> MASK
<MARCARÁ WAN>
SET WAN WAN0 IPCP REMOTEIP ENABLED TRUE ADDRESS <IP WAN OPERADORA>
SET WAN WAN0 PPPDEFROUTE TRUE
SET WAN WAN0 UP
```

PROTOCOLO PPP ASSÍNCRONO

Na configuração de PPP assíncrono, existem os seguintes parâmetros:

```
NR2Gm > SET WAN WAN0 PROTO PPPA
NR2Gm > SET WAN WAN0
Valid options for command SET are:
        PROTO {NONE,HDLC,FRAMERELAY,PPPS,PPPA,DIALIN,X25}
Any other parameters depends on protocol defined to each interface
Valid SET options for PPPA are:
        CONNECTION          Conexão discada (NORMAL) ou linha privativa
        SPEED               Velocidade de conexão
        COMPRESSION         Define o tipo de compressão
        MAXCODESIZE*        Controle de fluxo
        FLOWCTRL**          Controle de fluxo
        MRU                 Configuração de MRU
        MTU                 Configuração de MTU
        AUTH**              Define o tipo de autenticação
        USER**              Usuário para autenticação
        PASS**              Senha para autenticação
        CHAP**              Caso autenticação CHAP, configura CHAP
        PAP**               Caso autenticação PAP, configura PAP
        DIALOUT**           Configurações de discagem (modem normal ou GPRS)
        IPCP                Configuração de IPCP
        LCP                 Configuração dos parâmetros de LCP
        RESETCOUNTERS       Limpa os contadores de estatísticas de interface
        UP                  Levanta a interface
        DOWN                Derruba a interface
        PURGE               Limpa as configurações do módulo WANx
*Only when COMPRESSION=BSD or DEFLATE
**Only when CONNECTION=NORMAL
Also, CHAP is only valid when AUTH=CHAP and PAP only when AUTH=PAP

SET WAN WAN0 DIALOUT

Applying to inteface: WAN0

Valid SET options for DIALOUT are:

        DEMAND              Indica discagem sobre demanda.

        IDLE*               Indica tempo de inatividade esperado para
                            desconexão.

        PERSIST             Conexão persistente, sempre tenta reestabelecer
                            a conexão.

        PPPDEFROUTE***      Quando PPP ativo cria rota default para o enlace.

        TYPE                Tipo de conexão (TONE, PULSE, GPRS ou CUSTOM)

        NUMBER              Número a ser discado.

        HOLDOFF             Intervalo entre uma tentativa e outra.

        MAXFAIL             Número de tentativas.

        VJ                  Ativa/desativa compressão Van Jacobsom

        USEPEERDNS          Solicitar endereço DNS do peer.

        NAME**              Access Provider Service

        KEEPALIVE**         Configuração de keepalive para a conexão.

        SCRIPT              Criação de script de conexão customizado.

*    Only available whem DEMAND = TRUE.
```

```
**   Only available whem TYPE = GPRS.
***  Only DIALOUT option available whem CONNECTION = LEASED.
```

Exemplo de configuração de PPP assíncrono:

Conexão a provedor de acesso através de modem cobre assíncrono, onde teremos autenticação CHAP, usuário "nr2g", senha "digitel", discando para o telefone 33371999 e utilizando um modem com velocidade de 57600kbs.

```
NR2Gm > SET WAN WAN0 PROTO PPPA
NR2Gm > SET WAN WAN0 CONNECTION NORMAL
NR2Gm > SET WAN WAN0 SPEED 57600 AUTH CHAP USER nr2g PASS digitel
NR2Gm > SET WAN WAN0  DIALOUT  PPPDEFROUTE TRUE PERSIST TRUE
NR2Gm > SET WAN WAN0 DIALOUT TYPE TONE NUMBER 33371999
NR2Gm > SET WAN WAN0 UP
```

CONFIGURAÇÃO GPRS/EDGE

Conexão a provedor de acesso via modem GPRS, onde teremos autenticação CHAP, usuário "nr2g", senha "digitel", discando para o APN "provedor.dominio.com".

```
NR2Gm > SET WAN WAN0 PROTO PPPA
NR2Gm > SET WAN WAN0 CONNECTION NORMAL
NR2Gm > SET WAN WAN0 SPEED 57600 AUTH CHAP USER nr2g PASS digitel
NR2Gm > SET WAN WAN0  DIALOUT  PPPDEFROUTE TRUE PERSIST TRUE
NR2Gm > SET WAN WAN0 DIALOUT TYPE GPRS/EDGE NAME  provedor.dominio.com
NR2Gm > SET WAN WAN0 UP
```

PROTOCOLO HDLC

Na configuração HDLC, existem os seguintes parâmetros:

```
NR2Gt > SET WAN WAN0 PROTO HDLC
NR2Gt > SET WAN WAN0 <enter>
Valid options for command SET are:
PROTO {NONE,HDLC,FRAMERELAY,PPPS,PPPA,DIALIN,X25}
Any other parameters depends on protocol defined to each interface
Valid options for protocol HDLC:
     IP                 Configura endereço IP da interface WAN0
     MASK               Configura máscara de rede da interface WAN0
     PEER               Indica endereço IP da interface WAN remota
     MTU                Configura o MTU
     INTERVAL           Keep alive intervalo
     TIMEOUT            Keep alive timeout
     CLOCK              Configura o clock (interno/externo)
     SPEED*             Configura a velocidade do clock interno
     TXINV              Inverte a borda do clock
     RESETCOUNTERS      Limpa os contadores de estatísticas da interface
     UP                 Levanta a interface
     DOWN               Derruba a interface
     PURGE              Limpa as configurações do módulo WAN0
*Only when CLOCK=INTERNAL
NR2Gt > SET WAN WAN0 IP 10.10.10.1 MASK 255.255.255.252 PEER 10.10.10.2
```

```
NR2Gt > SET WAN WAN0 UP
```

PROTOCOLO X25

Na configuração X25, existem os seguintes parâmetros:

```
NR2Gt > SET WAN WAN0 <enter>
Valid options for command SET are:
PROTO {NONE,HDLC,FRAMERELAY,PPPS,PPPA,DIALIN,X25}
Any other parameters depend on protocol defined to each interface
Valid SET options for X25 are:
     CLOCK              Configura CLOCK da interface
     SPEED              Configura velocidade do CLOCK
     TXINV              Inverte borda do CLOCK
     MODE               Define modo de operação (DTE/DCE)
     LAPB               Configura nível LAPB
     EXTENDED           Permite operação X25 estendida
     NEGOTIATE          Habilita negociação para tamanhos de pacote, tamanho
                        de janela e reverse
                        charging
     ROUTES             Adiciona/deleta rotas X25
     RESETCOUNTERS      Limpa contadores de interface
     UP                 Inicializa a interface SVCx
     DOWN               Derruba a interface SVCx
     PURGE              Limpa as configurações do módulo WANx
     SVC0               Configura a interface SVCx

NR2Gt > SET WAN WAN0 SVC0 <enter>
Applying to interface: WAN0
Valid SET options for IP SVC are:
     PROTOCOL           Habilita o protocolo (IP/IPX)
     WINSIZEIN          Tamanho de janela de entrada
     WINSIZEOUT         Tamanho de janela de saída
     PACSIZEIN          Tamanho de pacote de entrada
     PACSIZEOUT         Tamanho de pacote de saída
     REVCHARG           Habilita o reverse charging
     X121BIND           Configura endereço X121 local
     WAITCONNECTION     Habilita o roteador para somente receber chamadas X25
     X121TO             Configura endereço x25 remoto
     IP                 Configura endereço IP para interface SVCx
     MASK               Configura máscara de rede para interface SVCx
     PEER               Configura endereço de PEER remoto para interface SVCx
     MTU                Configura tamanho de MTU
```

Segue abaixo um exemplo de configuração conectando um roteador NR-2G a um roteador CISCO.

Exemplo de configuração X25 entre roteadores NR-2G e CISCO

Configuração NR-2G:

SET WAN WAN0 PROTO X25 CLOCK EXTERNAL TXINV FALSE MODE DTE LAPB EXTENDEDMODE FALSE WINDOWSIZE 7

SET WAN WAN0 EXTENDED FALSE NEGOTIATE WINDOWSIZE FALSE PACKETSIZE FALSE

```
REVERSECHARGING FALSE
     SET WAN WAN0 ROUTES ADD 724691111111
     SET WAN WAN0 SVC0 PROTOCOL IP WINSIZEIN 7 WINSIZEOUT 7 PACSIZEIN 512 PACSIZEOUT
512 REVCHARG FALSE X121BIND 724601099069 X121TO 724691111111 IP 172.16.1.1 PEER
172.16.1.2 MASK 255.255.255.252 MTU 128
     SET WAN WAN0 UP

     Configuração CISCO:
     interface Serial0
     description Exemplo de Configuracao CISCO X25
     ip address 172.16.1.2 255.255.255.252
     encapsulation x25
     no ip mroute-cache
     x25 address 724691111111
     x25 htc 64
     x25 win 7
     x25 wout 7
     x25 ips 512
     x25 ops 512
     x25 map ip 172.16.1.1 724601099069 broadcast
```

CONFIGURAÇÃO PARA INTERFACE UNNUMBERED

Uma interface é denominada UNNUMBERED quando não existe um endereço IP configurado diretamente a ela.

Para configurá-la, os endereços da interface serial e da máscara devem estar configurados como `0.0.0.0`.

Frame Relay

```
NR2Gt > SET WAN WAN0 PVC0 IP 0.0.0.0 MASK 0.0.0.0
IP Address for pvc0 is unnumbered dlci 16
```

PPP Síncrono

```
SET WAN WAN0 PROTO PPPS
SET WAN WAN0 IPCP LOCALIP ENABLED TRUE ADDRESS <IP WAN CLIENTE> MASK
<MARCARÁ WAN>
SET WAN WAN0 IPCP REMOTEIP ENABLED TRUE ADDRESS <IP WAN OPERADORA>
SET WAN WAN0 PPPDEFROUTE TRUE
SET WAN WAN0 UP
```

HDLC

```
NR2Gt > SET WAN WAN0 IP 0.0.0.0 MASK 0.0.0.0 UP
Applying to interface: WAN0
Ip Address for hdlc0 is unnumbered
```

ADICIONANDO ROTAS ESTÁTICAS

Uma rota deve ser configurada quando queremos atingir determinada rede. Para a configuração de uma rota estática, existem os seguintes parâmetros:

```
NR2Gt > SET ROUTES <enter>
     DEFAULT        Configura uma rota default
     ROUTE0         Configura uma rota numerada
     PURGE          Limpa as configurações do módulo routes
```

Para configurar uma rota default, ou seja, uma rota que pode alcançar qualquer rede (utilizada freqüentemente para rotear o tráfego da internet), utilize o seguinte comando:

```
NR2Gt > SET ROUTES DEFAULT <enter>
Valid options for SET are:
     GW1       Configura o endereço IP da interface serial remota
     COST1     Determina um custo para a rota
     GW2       Configura o endereço IP da interface serial remota (parâmetro
               utilizado para configurar duas rotas default)
     COST2     Determina um custo para a rota (parâmetro utilizado para
               configurar duas rotas default)
     POLL      Configura um timer para a verificação da primeira rota default
               (parâmetro utilizado para configurar duas rotas default)
     PURGE     Limpa as configurações do módulo DEFAULT
NR2Gt > SET ROUTES DEFAULT GW1 10.10.10.2
```

Para verificar se as configurações foram aplicadas corretamente, utilize o comando **SHOW**:

```
NR2Gt >  SHOW ROUTES <enter>
Valid SHOW options are:
     STATS          Verifica rotas estáticas
     DYNAMIC        Verifica rotas dinâmicas
     DEFAULT        Verifica rota default
     ALL            Mostra todas as configurações

NR2Gt > SHOW ROUTES ALL
Destination    Gateway       Mask               Cost     Device
10.10.10.0     *             255.255.255.252    0        hdlc0
10.10.10.0     *             255.255.255.0      0        eth0
default        10.10.10.2    0.0.0.0            0        hdlc0
DEFAULT GW1    10.10.10.2
DEFAULT COST1  0
DEFAULT GW2    PURGE
DEFAULT COST2  0
DEFAULT POLL   6
```

Fazendo a mesma configuração, mas somente indicando uma rede específica a ser alcançada, resulta no seguinte:

```
NR2Gt > SET ROUTES ROUTE0 <enter>
Valid options for SET are:
DEVICE          Interface de saída
     NET        Rede que se deseja alcançar
     MASK       Máscara da rede
     GATEWAY    IP da interface serial remota
     COST       Custo da rota
     PURGE      Limpa as configurações do módulo ROUTE0
NR2Gt > SET ROUTES ROUTE0 DEVICE WAN0 NET 172.16.1.0 MASK 255.255.255.0
GATEWAY 10.10.10.2
```

Note que, no caso de um enlace Frame Relay, a nomenclatura da interface seria WAN0-PVC0.

Para verificar se as configurações foram aplicadas corretamente, utilize o comando **SHOW**:

```
NR2Gt > SHOW ROUTES ALL
Destination    Gateway       Mask               Cost         Device
10.10.10.0     *             255.255.255.252    0            hdlc0
172.16.1.0     10.10.10.2    255.255.255.0      0            hdlc0
```

```
10.10.10.0     *              255.255.255.0      0            eth0
Applying to route: ROUTE0
DEVICE  WAN0
NET       172.16.1.0
MASK      255.255.255.0
GATEWAY   10.10.10.2
COST      0
DEFAULT GW1      PURGE
DEFAULT COST1    0
DEFAULT GW2      PURGE
DEFAULT COST2    0
DEFAULT POLL     6
```

PROTOCOLOS DE ROTEAMENTO DINÂMICO

Os protocolos de roteamento dinâmico são utilizados para minimizar a complexidade e o trabalho envolvidos na configuração das tabelas de roteamento nos grandes backbones.

Na maioria das grandes corporações, é necessário manter uma constante modificação na topologia de rede, sendo necessário fazer diversas alterações nas tabelas de roteamento. Os protocolos utilizados para o roteamento dinâmico permitem que todo esse trabalho seja feito sem esforço e com rapidez, atualizando dinamicamente as tabelas de rota dos equipamentos conectados a determinada topologia.

Nos roteadores NetRouter 2G, existem as seguintes opções de implementação:

- RIP V1 e V2
- OSPF

RIP (Routing Information Protocol)

O RIP (Routing Information Protocol) é um protocolo de roteamento de vetor de distância baseado no algoritmo de Bellman-Ford. Esse protocolo envia periodicamente as informações de rotas para seus vizinhos, permitindo que a topologia se mantenha conhecida pelos demais dispositivos dentro da rede.

Os parâmetros para a configuração do RIP são os seguintes:

```
NR2Gt > SET RIP <enter>
Valid SET options are:
     DEFAULTMETRIC       Modifica o valor da métrica default para redistribuir
                         as rotas
     VERSION             Configura a versão do RIP (1/2/default)
     REDIST-STATIC       Redistribui informações das rotas estáticas
     REDIST-CONNECTED    Redistribui as rotas conectadas para uma tabela RIP
     REDIST-OSPF         Redistribui as rotas de uma tabela OSPF para uma
                         tabela RIP
     UP                  Inicia o módulo RIP
     DOWN                Pára o módulo RIP
     PURGE               Limpa as configurações do módulo RIP
     LAN0                Configura a interface LAN0 para trabalhar com o RIP
     WAN0                Configura a interface WAN0 para trabalhar com o RIP
     LIST0               Cria uma lista de acesso para redes no módulo RIP
```

As interfaces somente serão habilitadas mediante sua ativação. Seguem os parâmetros de configuração:

```
NR2Gt > SET RIP LAN0 <enter>
Valid SET options are:
     ENABLED             Habilita o RIP na interface current (True/False)
     TYPE                Informa o tipo da interface (Active/Passive)
     RECEIVEVERSION      Habilita a interface a receber determinada versão do RIP
```

```
     SENDVERSION        Habilita a interface a enviar determinada versão do RIP
     AUTH               Habilita autenticação para o RIP (NONE/Simples/MD5)
     IN0                Habilita determinada lista de acesso de entrada
     OUT0               Habilita determinada lista de acesso de saída
```

Segue o exemplo de uma configuração habilitando as interfaces LAN0 e WAN0:

```
NR2Gt > SET RIP VERSION 2 REDIST-STATIC TRUE REDIST-CONNECTED TRUE
NR2Gt > SET RIP LAN0 ENABLED TRUE TYPE ACTIVE
NR2Gt > SET RIP WAN0 ENABLED TRUE TYPE ACTIVE
NR2Gt > SET RIP UP
NR2Gt > CONFIG SAVE
```

A configuração acima ativa as interfaces LAN0 e WAN0 para permitir a troca de informações RIP entre os diversos roteadores existentes na rede utilizando a versão dois (2). No final, é aplicado o comando **SET RIP UP**, para que o serviço de RIP seja habilitado.

OSPF (Open Shortest Path First)

O OSPF é um protocolo de estado de link que solicita o envio de anúncios de estado de link (LSAs) a todos os roteadores existentes na mesma área hierárquica.

Por ser um protocolo de roteamento de estado de link, o OSPF contrasta com o RIP, que é um protocolo de roteamento de vetor de distância.

O OSPF é um protocolo de roteamento amplamente utilizado para backbones internet e grandes redes corporativas.

Os parâmetros para a configuração do OSPF são os seguintes:

```
NR2Gt > SET OSPF <enter>
Valid SET options are:
     ROUTERID           Configura o ROUTERID
     NOROUTERID         Desabilita o ROUTERID
     RFC1583            Previne o acontecimento de loops no roteamento
     REDIST-CONNECTED   Redistribui as rotas conectadas para uma tabela OSPF
     REDIST-STATIC      Redistribui informações das rotas estáticas
     REDIST-RIP         Redistribui as rotas de uma tabela RIP para a tabela OSPF
     DEBUG              Debug de mensagens OSPF
     LOG                Log de mensagens OSPF
     UP                 Ativa o OSPF
     DOWN               Derruba o OSPF
     PURGE              Limpa as configurações do módulo OSPF
     LAN0               Ativa a interface LAN0 para propagar e receber OSPF
     LIST0              Cria uma lista de acesso para redes no módulo OSPF
     NETWORK0           Especifica a interface para habilitar OSPF
```

Segue exemplo de uma configuração habilitando as interfaces LAN0 e WAN0:

```
NR2Gt >   SET OSPF NETWORK0 ADDRESS 10.10.10.0 MASK 255.255.255.0 AREA 0.0.0.0
NR2Gt >   SET OSPF NETWORK1 ADDRESS 172.16.1.0 MASK 255.255.255.252 AREA 0.0.0.0
NR2Gt >   SET OSPF NETWORK2 ADDRESS 172.16.1.2 MASK 255.255.255.255 AREA 0.0.0.0
NR2Gt >   SET OSPF UP
NR2Gt >   CONFIG SAVE
```

Na configuração acima, estamos habilitando as redes configuradas para as interfaces LAN e WAN. Note que havia uma terceira rede, cujo endereço da interface WAN (listen) remota tinha máscara de 32 bits. Isso se deve ao fato de a interface ser ponto a ponto, sendo necessária a adição dessa rota para que os neighbors possam propagar suas rotas entre si. No final, é aplicado o comando **SET OSPF UP**, para que o serviço de OSPF seja habilitado.

Para definir melhorias nas interfaces, existem os seguintes parâmetros:

```
NR2Gt > SET OSPF WAN0 <enter>
Valid SET options are:
     PASS               Cria uma senha simples para autenticar pacotes OSPF
     NOPASS             Remove a senha para autenticação
     PRIORITY           Configura um valor inteiro para definir prioridade
     COST               Configura um custo para a interface current
     HELLOINTERVAL      Configura o número de segundos para o HELLOINTERVAL
     DEADINTERVAL       Configura o número de segundos para o DEADINTERVAL
     DELAY              Configura o número de segundos para o DELAY
     RETRANSMISSION     Configura o número de segundos para o RETRANSMISSION
     DIGEST0            Configura a chave de autenticação do OSPF para uma
                        senha criptografada (algoritmo utilizado: MD5)
     PURGE              Limpa as configurações do módulo INTERFACE (WAN0)
```

NAT (NETWORK ADDRESS TRANSLATOR)

Introdução

Os roteadores NR-2G contemplam cinco tipos diferentes de implementação de NAT/PAT.

- MASQUERADE
- REDIRECT
- NAT 1:1
- EXCLUSION
- NATPOOL

Configurando NAT MASQUERADE

Na configuração do NAT, o mais comum é utilizar o MASQUERADE, onde se faz com que uma rede utilize um endereço que está configurado em uma determinada interface. Um exemplo bem comum é um link de internet, quando é preciso que todos os microcomputadores de uma determinada rede possam navegar.

Segue a descrição de parâmetros:

```
NR2Gt > SET NAT MASQUERADE0 <enter>
Applying to: MASQUERADE0
Valid SET options are:
     INTERFACE      Interface para aplicar o NAT
     ADDRESS        Endereço de rede
     MASK           Máscara da rede
     PURGE          Limpa as configurações do módulo MASQUERADE0
NR2Gt > SET NAT MASQUERADE0 INTERFACE WAN0 ADDRESS 192.168.1.0 MASK 255.255.255.0
NR2Gt > SET NAT UP
```

Note que, no caso de um enlace Frame Relay, a nomenclatura da interface seria WAN0-PVC0.

Configurando NAT REDIRECT

Para redirecionar um determinado tráfego para um endereço IP, deve-se utilizar um recurso conhecido como REDIRECT. O REDIRECT é feito a partir de um endereço IP de origem, uma interface e uma porta TCP específica para um serviço.

Segue a descrição de parâmetros:

```
NR2Gt > SET NAT REDIRECT0 <enter>
Applying to: REDIRECT0
Valid SET options are:
     FROMINTERFACE      Interface de origem
     FROMADDRESS        Endereço IP da interface de origem
     FROMPORT           Porta TCP de origem
     TOADDRESS          Endereço de destino
     TOPORT             Porta TCP de destino
     PURGE              Limpa as configurações do módulo REDIRECT0
```

No exemplo abaixo, ao receber uma requisição de Telnet no endereço IP 200.238.60.1, o roteador está configurado para direcionar o tráfego para o endereço 192.168.1.1.

```
NR2Gt > SET NAT REDIRECT0 FROMINTERFACE WAN0 FROMADDRESS 200.238.60.1 FROMPORT
23 TOADDRESS 192.168.1.1 TOPORT 23
NR2Gt > SET NAT UP
```

Configurando NAT 1:1

Para transformar um endereço IP de origem em um endereço IP de destino, deve-se utilizar um recurso conhecido como NAT 1:1.

Segue a descrição dos parâmetros:

```
NR2Gt > SET NAT NAT0 <enter>
Applying to: NAT0
Valid SET options are:
     FROMADDRESS        Endereço de origem
     FROMMASK           Máscara de origem
     TOADDRESS          Endereço de destino
     TOMASK             Máscara de destino
     PURGE              Limpa as configurações do módulo NAT0
NR2Gt > SET NAT NAT0 FROMMASK 255.255.255.255 FROMADDRESS 192.168.1.1 TOMASK
255.255.255.255 TOADDRESS 200.238.60.1
NR2Gt > SET NAT UP
NR2Gt > SHOW LAN LAN0 IP
Applying to interface: LAN0
IP      192.168.1.1
NR2Gt > EXEC TCPDUMP -i eth0 &
NR2Gt > EXEC PING 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
22:38:53.598309 200.238.60.1 > 192.168.1.2: icmp: echo request (DF)
22:38:54.600432 200.238.60.1 > 192.168.1.2: icmp: echo request (DF)
22:38:55.600428 200.238.60.1 > 192.168.1.2: icmp: echo request (DF)
```

Note que, ao executar o comando **TCPDUMP** (debug de interface) na interface LAN0, o endereço que faz a requisição ICMP é o 200.238.60.1, sendo que o IP configurado na interface é 192.168.1.1. Nesse momento, pode-se observar que o endereço da interface LAN0 está sendo alterado.

Configurando NAT EXCLUSION

Uma característica interessante dentro das regras de NAT/PAT é a possibilidade de exclusão de um determinado host, ou até mesmo um pool de endereços IP, dentro do range de endereços que realiza, por exemplo, um masquerade. Para isso, utilizamos a característica EXCLUSION.

No exemplo abaixo, são criadas duas regras: a primeira indica qual o range de endereços IP que fará o MASQUERADE; a segunda faz a exclusão de um determinado endereço IP.

```
NR2Gt>SET NAT MASQUERADE0 INTERFACE WAN0-PVC0 MASK 255.255.255.0 ADDRESS 192.168.1.0
NR2Gt>SET NAT EXCLUSION0 MASK 255.255.255.255 ADDRESS 192.168.1.120
NR2Gt>SET NAT UP
```

A operação se dá quando a requisição chega ao roteador. Nas regras de NAT, verifica-se a origem do pacote. Quando o roteador verifica que o endereço de origem é 192.168.1.120/32, ele simplesmente roteia o pacote com o endereço de origem, sem levar em conta as regras do NAT MASQUERADE.

Configurando NATPOOL

O NATPOOL realiza uma translação do range IP para um pool de endereços IP predeterminado. Essa alocação ocorre dinamicamente. No exemplo abaixo, a rede 192.168.1.0/24 sofrerá a modificação no pool 200.239.60.1-200.239.60.5.

```
NR2Gt>SET NAT NATPOOL0 TOINTERFACE WAN0-PVC0 FROMMASK 255.255.255.0 FROMADDRESS
192.168.1.0 ADDRESS0 200.239.60.1 ADDRESS1 200.239.60.5

NR2Gt>SET NAT UP
```

HABILITANDO O SNMP (SIMPLE NETWORK MANAGMENT PROTOCOL)

O SNMP é o protocolo utilizado para gerenciar os diversos dispositivos de uma rede, enviando mensagens para uma NMS (Network Managment Station). A NMS será o dispositivo que concentrará todas as mensagens (TRAPS).

Abaixo são descritos os parâmetros utilizados na configuração:

```
NR2Gt > SET SNMP <enter>
Valid SET options for SNMP are:
     LOCATION           Configura a localização do dispositivo
     CONTACT            Configura o contato
     TRAPAUTHFAILURE    Habilita/Desabilita o envio das TRAPS
     ROCOMMUNITY0       String de comunidade de leitura
     RWCOMMUNITY0       String de comunidade de leitura/escrita
     TRAP0              Configura o endereço da NMS
     UP                 Inicia o serviço de SNMP
     DOWN               Pára o serviço de SNMP
     PURGE              Limpa as configurações do módulo SNMP

NR2Gt > SET SNMP LOCATION digitel CONTACT Suporte TRAPAUTHFAILURE TRUE
NR2Gt > SET SNMP ROCOMMUNITY0 <enter>
Valid SET options are:
        NAME       Nome do string da comunidade de leitura
        PURGE      Limpa o módulo de configuração ROCOMMUNITY0
        MANAGER0   Configura o IP da NMS
NR2Gt > SET SNMP ROCOMMUNITY0 NAME public MANAGER0 ADDRESS 192.168.1.2

NR2Gt > SET SNMP RWCOMMUNITY0 <enter>
Valid SET options are:
     NAME          Nome do string da comunidade de leitura/escrita
     PURGE         Limpa o módulo de configuração RWCOMMUNITY0
     MANAGER0      Configura o IP da NMS
NR2Gt > SET SNMP RWCOMMUNITY0 NAME private MANAGER0 ADDRESS 192.168.1.2
NR2Gt > SET SNMP TRAP0 <enter>
Valid SET options are:
         ADDRESS   Endereço da NMS
         PURGE     Limpa o módulo de configuração TRAP0
```

ATENÇÃO!
Nas configurações de TUNNELLOCAL e TUNNELREMOTE, os endereços IP devem ser definidos no momento da configuração. Esse endereço será utilizado para interligar as duas redes.

```
NR2Gt > SET SNMP TRAP0 ADDRESS 192.168.1.1
NR2Gt > SET SNMP UP
```

IP TUNNELING

Este item aborda as tecnologias de *IP Tunneling* para os modelos NetRouter 2G. Os protocolos suportados são:

GRE (*Generic Routing Encapsulation*)
PPTP (*Point to Point Tunneling Protocol*)
L2TP (*Layer 2 Tunneling Protocol*)

GRE (Generic Routing Encapsulation)

O protocolo GRE é utilizado normalmente para a criação de túneis entre subredes. Esta é a implementação de túnel mais simples entre roteadores, não possuindo nenhuma característica de segurança nem criptografia de dados.

Os seguintes parâmetros são utilizados na configuração do GRE:

```
NR2Gt > SET GRE <enter>
Valid SET options for GRE are:
        UP              Inicia o túnel GRE
        DOWN            Pára o túnel GRE
        PURGE           Limpa as configurações do módulo GRE
        GRE1            Configuração do túnel
NR2Gt > SET GRE GRE1 <enter>
Valid SET options are:
        INTERFACE       Interface de origem do túnel
        REMOTE          Endereço IP válido do túnel remoto
        TUNNELLOCAL     Endereço IP local para o túnel
        TUNNELREMOTE    Endereço IP remoto para o túnel
        UP              Iniciar o túnel
        DOWN            Parar o túnel
        PURGE           Limpa as configurações do módulo túnel
```

Para uma melhor compreensão dos dados acima, a seguir é apresentado um exemplo de configuração do GRE interligando duas subredes. Neste exemplo, a topologia compreende duas redes que serão interligadas através de um túnel GRE. O endereço de rede do lado A (LOCAL) é 192.168.10.0, tendo como endereço de interface serial 172.16.1.1/30. No lado B (REMOTO), o endereço de rede é 192.168.11.0/24 com endereço de interface serial 172.16.1.2/30. Seguem abaixo as configurações:

LOCAL:

```
SET LAN LAN0 IP 192.168.10.1 MASK 255.255.255.0 UP
SET WAN WAN0 PROTO FRAMERELAY PROTOCOL ANSI
SET WAN WAN0 PVC0 DLCI 16 IP 172.16.1.1 MASK 255.255.255.252 PEER 172.16.1.2
SET WAN WAN0 UP
SET GRE GRE1 INTERFACE WAN0-PVC0 REMOTE 172.16.1.2 TUNNELLOCAL 7.7.7.7
TUNNELREMOTE 7.7.7.6 UP
```

Configuração da interface GRE1. Note que são adicionados os endereços 7.7.7.7 e 7.7.7.6 para local e remoto, respectivamente, como endereços fictícios, apenas para identificar o túnel.

```
SET ROUTES ROUTE0 DEVICE GRE1 NET 192.168.11.0 MASK 255.255.255.0 GATEWAY
7.7.7.6
```

É necessária a criação de uma rota para a rede específica pela interface GRE1.

REMOTO:

```
SET LAN LAN0 IP 192.168.11.1 MASK 255.255.255.0 UP
SET WAN WAN0 PROTO FRAMERELAY PROTOCOL ANSI
```

```
SET WAN WAN0 PVC0 DLCI 16 MTU 1500 IP 172.16.1.2 MASK 255.255.255.252 PEER
172.16.1.1
SET WAN WAN0 UP
SET GRE GRE1 INTERFACE WAN0-PVC0 REMOTE 172.16.1.1 TUNNELLOCAL 7.7.7.6
TUNNELREMOTE 7.7.7.7 UP
SET ROUTES ROUTE0 DEVICE GRE1 NET 192.168.10.0 MASK 255.255.255.0 GATEWAY
7.7.7.7
```

Na configuração remota, temos apenas a inversão dos endereços IP.

Para a criação dos demais túneis, basta indicar quem é o próximo: GRE1, GRE2, GRE3 e assim sucessivamente.

PPTP (Point-to-Point Tunneling Protocol)

O PPTP é um protocolo originado do PPP, amplamente utilizado para prover interligações entre redes privadas virtuais (VPNs). A forma tradicional de atuação do PPTP é codificando pacotes PPP e encapsulando-os em pacotes GRE. Além do IP, ele também canaliza protocolos como o IPX.

Por questões de segurança, o PPTP garante um certo nível de criptografia nos dados, utilizando os algoritmos CHAP e PAP. Uma outra característica é o uso do protocolo MPPE (*Microsoft Point-To-Point Encryption Protocol*) para prover criptografia nos dados em túneis PPTP. Originalmente, o MPPE suporta chaves de sessão de 40 e 128 bits.

Os seguintes parâmetros são necessários para sua configuração:

```
NR2Gt > SET PPTP <enter>
Valid SET options are:
     SERVER        Define as configurações para um servidor PPTP
     PURGE         Limpa as configurações no módulo PPTP
     CHAP0         Configura autenticação CHAP
     CLIENT0       Define as configurações para um cliente PPTP
```

Para a configuração do PPTP, são utilizados dois modos: cliente e servidor.

```
NR2Gt > SET PPTP SERVER <enter>
Applying to: SERVER
Valid SET options for SERVER are:
     LISTEN        Interface de origem do túnel
     UP            Inicializa o servidor
     DOWN          Derruba o servidor
     PURGE         Limpa as configurações do módulo SERVER
     LOCALIP0      Configura endereços IP no túnel local
     REMOTEIP0     Configura endereços IP no túnel remoto
NR2Gt > SET PPTP CLIENT0 <enter>
Applying to: CLIENT0
Valid SET options are:
     DOMAIN        Configura autenticação em um domínio CHAP
     SERVER        Configura o endereço IP válido no túnel remoto
     UP            Inicia a conexão com o servidor PPTP
     DOWN          Pára a conexão com o servidor PPTP
     PURGE         Limpa as configurações no módulo CLIENT0
```

Para as configurações de CHAP:

```
NR2Gt > SET PPTP CHAP0 <enter>
Applying to domain: CHAP0
Valid SET options are:
     DOMAIN    Nome do domínio CHAP (também utilizado para a validação de usuários)
        USER   Usuário a ser utilizado na validação
        PASS   Senha para o usuário
        PURGE  Limpa as configurações no módulo CHAP0
```

Para uma melhor compreensão dos conceitos apresentados aqui, a seguir está um exemplo de configuração utilizando o PPTP em uma ligação ponto a ponto sobre um enlace Frame Relay.

```
SERVER:

SET LAN LAN0 IP 192.168.10.1 MASK 255.255.255.0 UP
SET WAN WAN0 PROTO FRAMERELAY PROTOCOL ANSI
SET WAN WAN0 PVC0 DLCI 16 MTU 1500 IP 172.16.1.1 MASK 255.255.255.252 PEER 172.16.1.2
SET WAN WAN0 UP
SET PPTP SERVER LISTEN WAN0-PVC0
SET PPTP SERVER LOCALIP0 BEGIN 10.10.50.1 END 10.10.50.50
SET PPTP SERVER REMOTEIP0 BEGIN 10.10.200.1 END 10.10.200.50
SET PPTP CHAP0 DOMAIN digitel
SET PPTP CHAP0 USER digitel
SET PPTP CHAP0 PASS digitel
SET PPTP SERVER UP

CLIENT:

SET LAN LAN0 IP 192.168.11.1 MASK 255.255.255.0 BROADCAST 192.168.11.255 UP
SET WAN WAN0 PROTO FRAMERELAY PROTOCOL ANSI
SET WAN WAN0 PVC0 DLCI 16 MTU 1500 IP 172.16.1.2 MASK 255.255.255.252 PEER 172.16.1.1
SET WAN WAN0 UP
SET PPTP CHAP0 DOMAIN digitel
SET PPTP CHAP0 USER digitel
SET PPTP CHAP0 PASS digitel
SET PPTP CLIENT0 DOMAIN CHAP0
SET PPTP CLIENT0 SERVER 172.16.1.1 UP
```

L2TP (Layer 2 Transport Protocol)

O L2TP é um protocolo também utilizado para permitir a canalização de redes IP. Da mesma forma que o PPTP, ele também é originado do PPP, mas tem como grande diferencial a capacidade de ser executado sobre um grande número de protocolos diferentes.

Pelo fato de não possuir criptografia, o L2TP é normalmente usado junto a outros protocolos que possam garantir a segurança das informações, sendo o mais comum deles o IPSec.

O L2TP é uma consolidação dos protocolos PPTP e L2F.

Na configuração do L2TP, existem os conceitos LNS e LAC, que correspondem ao início e fim do túnel, respectivamente. Os parâmetros são os seguintes:

```
NR2Gt > SET L2TP <enter>
Valid SET options for L2TP are:
        LNS        L2TP Network Server
        UP         Inicia um túnel L2TP
        DOWN       Derruba o túnel L2TP
        PURGE      Limpa as configurações no módulo túnel
        AUTH       Configuração do método de autenticação (CHAP/PAP/NONE)
        LAC0       L2TP Access Concentrator
        USER0      Configura um usuário para autenticar o túnel

CHALLENGE
        ENABLED { YES | NO } autenticação por L2TP
        SECRET*
                                HOSTNAME       nome do equipamento
                                REMOTEHOST     nome do eqpto remoto
                                PASSWORD       senha
                                PURGE          remove a entrada
```

```
NR2Gt > SET L2TP LNS <enter>
Valid SET options for LNS are:
        LOCALIP    Endereço IP da origem do túnel
        UP         Inicia o LNS
        PURGE      Limpa as configurações no módulo LNS
        IPPOOL0    Define pool de endereços IP para a utilização dos clientes
        LACRANGE0  Identifica os IDs permitidos para a conexão
NR2Gt > SET L2TP LAC0 <enter>
Valid SET options are:
        ID         ID da conexão
        LNS        Endereço IP do LNS remoto
        REDIAL     Habilita a rediscagem (TRUE/FALSE)
        PURGE      Limpa as configurações do módulo LAC0
```

Para uma melhor compreensão dos conceitos apresentados aqui, a seguir está um exemplo de configuração utilizando o L2TP em uma ligação ponto a ponto sobre um enlace Frame Relay.

```
LNS:

SET LAN LAN0 IP 192.168.10.1 MASK 255.255.255.0 UP
SET WAN WAN0 PROTO FRAMERELAY PROTOCOL ANSI
SET WAN WAN0 PVC0 DLCI 16 MTU 1500 IP 172.16.1.1 MASK 255.255.255.252 PEER 172.16.1.2
SET WAN WAN0 UP
SET L2TP AUTH PAP
SET L2TP USER0 USERNAME digitel
SET L2TP USER0 PASSWORD digitel
SET L2TP LNS LOCALIP 100.100.100.1
SET L2TP LNS IPPOOL0 BEGIN 100.100.100.2 END 100.100.100.254
SET L2TP LNS UP
SET L2TP UP
LAC:

SET LAN LAN0 IP 192.168.11.1 MASK 255.255.255.0 UP
SET WAN WAN0 PROTO FRAMERELAY PROTOCOL ANSI
SET WAN WAN0 PVC0 DLCI 16 MTU 1500 IP 172.16.1.2 MASK 255.255.255.252 PEER 172.16.1.1
SET WAN WAN0 UP
SET L2TP AUTH PAP
SET L2TP USER0 USERNAME digitel
SET L2TP USER0 PASSWORD digitel
SET L2TP LAC0 ID 1 LNS 172.16.1.1 REDIAL TRUE
SET L2TP UP
```

O IPSec também possui capacidade de *IP Tunneling*. Ele será visto detalhadamente no próximo item.

IPSEC - SECURE IP OVER THE INTERNET

Introdução

O IPSec é um protocolo de segurança que foi inicialmente desenvolvido para o Ipv6 e modificado para trabalhar no Ipv4. A sua principal característica é prover a segurança dos dados de um extremo a outro, utilizando criptografia.

Uma das implementações de IPSec mais conhecidas é o FreeS/WAN, que é nativo do sistema operacional Linux e que também é utilizado nos roteadores NerRouter 2G. Uma particularidade do IPSec em relação a outros protocolos de VPN é que ele trabalha no nível 3 do modelo OSI, podendo, assim, prover segurança para qualquer protocolo IP (TCP, UDP, ICMP, etc).

O IPSec também pode fornecer diversos serviços de segurança, como a relação de confiança entre a origem e o destino (o destinatário tem certeza de que está recebendo as informações do remetente correto),

integridade da informação, confidencialidade e diversas outras formas de proteção da informação.

Protocolos do IPSec

Existem protocolos que formam o IPSec e são utilizados para fazer as diversas tarefas de trocas de informação. São eles:

- AH (Authentication Header)
- ESP (Encapsulation Security Payload)
- ISAKMP (Internet Security Association Key Management Protocol)
- IKE (Internet Key Exchange)

O AH provê a autenticação de origem dos dados e também sua integridade. O ESP também inclui alguns serviços fornecidos pelo AH, mas, além disso, proporciona confidencialidade (codificação) e proteção limitada contra análise do fluxo de tráfego. O terceiro protocolo, ISAKMP, provê a estrutura para que o protocolo IKE configure chaves criptográficas para o AH e o ESP. O IKE é um protocolo de conexão para verificação da identidade, negociação e troca de chaves.

Uma questão importante quando falamos em IPSec é determinar o tipo de operação a ser utilizado para o AH e o ESP do tipo túnel. No modo túnel, todo o pacote é encapsulado, e um novo cabeçalho IP é gerado, mas preservando as características de qualidade de serviço do pacote original.

Os parâmetros para configurar o IPSec são:

```
NR2Gt > SET IPSEC <enter>
Valid SET options for IPSEC are:
     FRAGICMP       Informa a necessidade de fragmentação do pacote
     NOEROUTEPASS   Ação para pacotes que chegam ao KLIPS (Kernel Level
                    IP Security)
     HIDETOS        Copia o valor do campo TOS e o repassa para o pacote IPSec
     UNIQUEIDS      Substitui todos os IDs de conexões antigas por um novo ID
     UP             Inicia túnel IPSec
     DOWN           Derruba túnel IPSec
     PURGE          Limpa as configurações do módulo IPSEC
     CHANNEL0       Configura um canal IPSEC
     IPSEC0         Seleciona interface IPSec
NR2Gt > SET IPSEC CHANNEL0 <enter>
Valid SET options are:
     NAME           Define nome para o canal
     LEFT           Configura a rede do lado local
     RIGHT          Configura a rede do lado remoto
     KEY            Configura a parte de troca de chaves
     PURGE          Limpas as configurações do módulo CHANNEL0
NR2Gt > SET IPSEC IPSEC0 <enter>
Valid SET options are:
     INTERFACE      Habilita a interface de origem do túnel
     PURGE          Limpa as configurações do módulo IPSEC0

NR2Gt > SET IPSEC CHANNEL0 LEFT <enter>
Applying to: CHANNEL0
Valid SET options for LEFT are:
     ADDRESSTYPE [INTERFACE****]
     ADDRESS*
     SUBNET
     NET**
     MASK**
     USEGATEWAY
     GATEWAY***
     *Only when ADDRESSTYPE=USER
     **Only when SUBNET=TRUE
     ***Only when USEGATEWAY=TRUE
```

```
     ****Only when setting ADDRESSTYPE to BINDED
```

A seguir é apresentada a configuração dos mesmos parâmetros na configuração RIGHT.

```
NR2Gt > SET IPSEC CHANNEL0 RIGHT
Applying to: CHANNEL0
Valid SET options for RIGHT are:
     ADDRESSTYPE [INTERFACE****]
     ADDRESS*                    Endereço IP da interface de origem*
     SUBNET                      Habilita para configuração de subrede
     NET**                       Endereço de rede
     MASK**                      Endereço de máscara
     USEGATEWAY                  Habilita para utilização de gateway
     GATEWAY***                  Configura o gateway
     *Only when ADDRESSTYPE=USER
     **Only when SUBNET=TRUE
     ***Only when USEGATEWAY=TRUE
     ****Only when ADDRESSTYPE = BINDED

NR2Gt > SET IPSEC CHANNEL0 KEY
Applying to: CHANNEL0
Valid SET options for KEY are:
     AUTH                        Tipo de autenticação (ESP/AH)
     AUTHBY                      Método de autenticação (SECRET/RSA)
     PASS*                       Senha a ser utilizada (SECRET)
     BITS**                      Número de BITS para a chave (RSA)
     PEERPUBLICKEY**             Chave pública remota
     GENERATEKEY**               Geração da chave pública
     NEGRESTART                  Timers de reinício de tentativa de conexão
                                 (TIME/MARGIN)
     LOCALSIDE**                 Determina se o lado local do tunel é o left ou
                                 rigth
     KEYLIFE                     Tempo de vida da chave
     ISAKMP                      Tempo de validade do canal autenticado
     RETRIES                     Número de tentativas de autenticação
     PERFECTFORWARD              Habilitar ou desabilitar o protocolo PFS
     *Only when AUTHBY=SECRET
     **Only when AUTHBY=RSA
```

Exemplo de configuração entre roteadores NR-2G utilizando chave de autenticação RSA 512 bits

```
ROTEADOR A:
SET LAN LAN0 PURGE
SET LAN LAN0 IP 192.168.10.1 MASK 255.255.255.0 UP
SET WAN WAN0 PROTO FRAMERELAY PROTOCOL ANSI DCE TRUE
SET WAN WAN0 PVC0 DLCI 16 IP 172.16.1.1 MASK 255.255.255.252 PEER 172.16.1.2
SET WAN WAN0 UP
SET SYSTEM HOSTNAME routerA
SET IPSEC PURGE
SET IPSEC IPSEC0 INTERFACE WAN0-PVC0
SET IPSEC CHANNEL0 NAME canal LEFT ADDRESSTYPE BINDED IPSEC0 SUBNET TRUE NET
192.168.10.0 MASK 255.255.255.0
SET IPSEC CHANNEL0 RIGHT ADDRESSTYPE USER ADDRESS 172.16.1.2 SUBNET TRUE NET
192.168.11.0 MASK 255.255.255.0
SET IPSEC CHANNEL0 KEY AUTH ESP AUTHBY RSA
SET IPSEC CHANNEL0 KEY BITS 512
SET IPSEC CHANNEL0 KEY PERFECTFORWARD TRUE
SET IPSEC CHANNEL0 KEY GENERATEKEY
SET IPSEC CHANNEL0 KEY PEERPUBLICKEY
```

```
0:>0sAQN37vkUyKVgSx9foqZ95JcPlzZR6ua7+eVl50IqFDCIacNfwQIJFJzSqMhTb86RgWIyABcSp
4VXqpbD4wH0Kmcx
| Copiar e colar a senha gerada pelo equipamento remoto.|
1:> Pressione <CTRL-D> para abandonar a edição de senhas.


ROTEADOR B:
SET LAN LAN0 PURGE
SET LAN LAN0 IP 192.168.11.1 MASK 255.255.255.0 UP
SET WAN WAN0 PROTO FRAMERELAY PROTOCOL ANSI
SET WAN WAN0 PVC0 DLCI 16 IP 172.16.1.2 MASK 255.255.255.252 PEER 172.16.1.1
SET WAN WAN0 UP
SET SYSTEM HOSTNAME routerB
SET IPSEC PURGE
SET IPSEC IPSEC0 INTERFACE WAN0-PVC0
SET IPSEC CHANNEL0 NAME canal LEFT ADDRESSTYPE BINDED IPSEC0 SUBNET TRUE NET
192.168.11.0 MASK 255.255.255.0
SET IPSEC CHANNEL0 RIGHT ADDRESSTYPE USER ADDRESS 172.16.1.1 SUBNET TRUE NET
192.168.10.0 MASK 255.255.255.0
SET IPSEC CHANNEL0 KEY AUTH ESP AUTHBY RSA
SET IPSEC CHANNEL0 KEY BITS 512
SET IPSEC CHANNEL0 KEY PERFECTFORWARD TRUE
SET IPSEC CHANNEL0 KEY LOCALPUBLICKEY GENERATEKEY
SET IPSEC CHANNEL0 KEY PEERPUBLICKEY
0:>0sAQOH8fKU8M+eAniJmdlZhV8OihNXg9ItG7Tc8JoidlhXWMv8TmC9DZsCqX6BwS2ywevYh0xLoL
dsHFtcmKpvJWFP
| Copiar e colar a senha gerada pelo equipamento remoto.|
1:> Pressione <CTRL-D> para abandonar a edição de senhas.
```

Para visualizar o estado da conexão IPSec nos roteadores, digite **SHOW SYSTEM LOG MESSAGES** em ambos os equipamentos. Exemplo:

```
Apr 17 18:13:10 NR2Gt ipsec__plutorun: 004 "canal" #1: STATE_MAIN_I4: ISAKMP
SA established
Apr 17 18:13:10 NR2Gt ipsec__plutorun: 004 "canal" #2: STATE_QUICK_I2: sent
QI2, IPsec SA established
```

Note que os dois níveis (ISAKMP e Ipsec) estão indicados como established. Isso significa que a conexão foi estabelecida corretamente com o roteador remoto.

Exemplo de configuração entre roteadores NetRouter 2G e Cisco

```
CONFIGURAÇÃO CISCO:

crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key digitel address 200.198.105.45
!
!
crypto ipsec transform-set teste esp-3des esp-md5-hmac
!
!
crypto map test 1 ipsec-isakmp
```

```
 set peer 200.198.105.45
 set transform-set teste
 set pfs group2
 match address 101
!
!
!
!
interface Ethernet0
 ip address 10.0.3.200 255.255.0.0
 hold-queue 100 out
!
interface Ethernet1
 ip address 200.218.187.66 255.255.255.252
 crypto map test
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.218.187.65
!
!
access-list 101 permit ip 10.0.0.0 0.0.255.255 192.168.10.0 0.0.0.255

CONFIGURAÇÃO NetRouter 2G:

SET LAN LAN0 PURGE
SET LAN LAN0 IP 192.168.10.1 MASK 255.255.255.0 BROADCAST 192.168.10.255 UP
SET LAN LAN1 PURGE
SET LAN LAN1 IP 200.198.105.45 MASK 255.255.255.240 BROADCAST 200.198.105.47 UP
SET ROUTES DEFAULT GW1 200.198.105.33 COST1 0
SET IPSEC PURGE
SET IPSEC FRAGICMP FALSE NOEROUTEPASS FALSE HIDETOS FALSE UNIQUEIDS FALSE
SET IPSEC IPSEC0 INTERFACE LAN1
SET IPSEC CHANNEL0 NAME canal LEFT ADDRESSTYPE BINDED IPSEC0 SUBNET TRUE NET
192.168.10.0 MASK 255.255.255.0 USEGATEWAY TRUE GATEWAY 200.198.105.33
SET IPSEC CHANNEL0 RIGHT ADDRESSTYPE USER ADDRESS 200.218.187.66 SUBNET TRUE
NET 10.0.0.0 MASK 255.255.0.0 USEGATEWAY TRUE GATEWAY 200.218.187.65
SET IPSEC CHANNEL0 KEY AUTH ESP AUTHBY SECRET PASS digitel
SET IPSEC CHANNEL0 KEY NEGRESTART TIME 9 MARGIN 100
SET IPSEC CHANNEL0 KEY ISAKMP 1H RETRIES 0 PERFECTFORWARD TRUE KEYLIFE 8H
SET IPSEC UP
```

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

A Digitel provê três características de DHCP para seus roteadores: DHCP Server, DHCP Relay e Reserva de Endereços IP. O DHCP Server disponibiliza, de forma dinâmica, a configuração de TCP/IP nos hosts de uma subrede. Cada host (microcomputadores, servidores, impressoras, etc.) recebe diversas informações, incluindo endereço IP, máscara, gateway, etc., de forma totalmente dinâmica, bastando apenas que o host possua a feature de DHCP Client.

O DHCP Relay é a característica que permite a uma subrede buscar as informações de um servidor DHCP remoto. Para isso, você precisa habilitar as interfaces para que o servidor DHCP possa rotear as informações através das subredes. A terceira característica é chamada de RESERVATION, onde podemos alocar um endereço IP para um determinado host através do MAC ADDRESS de sua placa de rede.

Os parâmetros para configuração do DHCP são:

```
NR2Gm > SET DHCP <enter>
Valid SET options for DHCP are:
     TYPE               Tipo (NORMAL/RELAY)
```

```
     UNKNOWNCLIENTS      Atribuição de endereços a máquinas desconhecidas
     SHAREDNETWORK       Agrupa subredes que se encontrem fisicamente na
                         mesma rede
     SERVERNAME          Hostname do servidor DHCP
     SUBNET0             Define os parâmetros comuns para uma determinada subrede
     HOST0               Reserva configuração espefífica para um dado host
     UP                  Inicia o serviço de DHCP
     DOWN                Pára o serviço de DHCP
     PURGE               Limpa as configurações do módulo DHCP
NR2Gm > SET DHCP TYPE <enter>
You must provide one of these:
     NORMAL              Operação em modo servidor DHCP
     RELAY               Operação em modo DHCP Relay
```

Inicialmente, é preciso determinar o tipo de operação para o DHCP: NORMAL (servidor) ou RELAY.

DHCP Server

Para as configurações de um servidor DHCP, existem os seguintes parâmetros:

```
NR2Gm > SET DHCP SUBNET0 <enter>
Valid SET options are:
     ADDRESS        Define a subrede
     MASK           Define a máscara
     RANGEIP        Habilita o range de IPs
     RANGEBEGIN*    Define o início do range de IPs
     RANGEEND*      Define o final do range de IPs
     LEASE          Define o período máximo de aluguel de um endereço, mesmo
                    que um tempo tenha sido solicitado pelo cliente. Obs.:
                    tempo em segundos.
     AUTHORITATIVE  Habilita como servidor o DHCP oficial da rede
     DNSDOMAIN      Configura um Domain Name para o servidor DHCP
     *Only when RANGEIP=TRUE
     DNS0           Configura um endereço de DNS para os hosts
     ROUTER0        Configura um endereço de gateway para os hosts
     WINS0          Configura endereço de WINS para os hosts
     PURGE          Limpa as configurações do módulo SUBNET0
```

Para entender melhor como funcionam as configurações de um DHCP Server, a seguir é apresentado um script com comentários:

```
SET DHCP PURGE
Limpa módulo de configuração
SET DHCP TYPE NORMAL
Configura para operação de DHCP NORMAL
SET DHCP UNKNOWNCLIENTS TRUE SHAREDNETWORK TRUE SERVERNAME Digitel
SET DHCP SUBNET0 ADDRESS 192.168.1.0 MASK 255.255.255.0 RANGEIP TRUE
Especifica os endereços de uma subrede e habilita os ranges de endereçamento IP
SET DHCP SUBNET0 RANGEBEGIN 192.168.1.5 RANGEEND 192.168.1.254 LEASE 0
AUTHORITATIVE TRUE
Configura o início e o fim de um range de endereços IP
SET DHCP SUBNET0 DNSDOMAIN Digitel.com.br
Configura o Domain Name
SET DHCP SUBNET0 ROUTER0 ADDRESS 192.168.1.1
Configura o IP do gateway da rede
SET DHCP SUBNET0 DNS0 ADDRESS 192.168.1.2
Configura o endereço de DNS para os hosts
```

```
SET DHCP SUBNET0 WINS0 ADDRESS 192.168.1.3
Configura o endereço de Wins para os hosts
SET DHCP UP
Inicia serviço de DHCP Server
```

DHCP Reservation

Como apresentado anteriormente, o RESERVATION é uma característica que nos permite reservar endereços IP específicos para um determinado host (endereços que não estejam no range do DHCP Server). Tal característica é importante quando queremos diferenciar algum dispositivo de rede (servidor de impressão, por exemplo) dos demais componentes, tendo, assim, uma organização dentro de sua tabela de DHCP Server.

```
NR2Gm > SET DHCP HOST0 <enter>
Valid SET options are:
        NAME            Determina um hostname para um dispositivo de rede
        MAC             Determina o MAC ADDRESS do dispositivo ethernet da rede
        ADDRESS         Determina o endereço IP a ser reservado
        DNSDOMAIN       Configura um Domain Name para o host
        DNS0            Configura um endereço de DNS para o host
        ROUTER0         Configura um endereço de gateway para o host
        WINS0           Configura endereço de WINS para o host
        PURGE           Limpa as configurações do módulo HOST0
```

Para entender melhor como funcionam as configurações do RESERVATION, a seguir é apresentado um script utilizando as configurações acima:

```
SET DHCP HOST0 MAC 00:00:00:00:00:00 NAME impressora1 ADDRESS 192.168.1.250
DNSDOMAIN digitel.com.br
No local onde aparece "00:00:00:00:00", coloque o endereço MAC da placa de
rede do dispositivo.
SET DHCP HOST0 DNS0 ADDRESS 192.168.1.2
SET DHCP HOST0 ROUTER0 ADDRESS 192.168.1.1
SET DHCP HOST0 WINS0 ADDRESS 192.168.1.3
SET DHCP UP
```

DHCP Relay

Os parâmetros para sua configuração são:

```
NR2Gt > SET DHCP <enter>
Valid SET options for DHCP are:
     TYPE               Tipo (NORMAL/RELAY)
     SERVER             Define IP do servidor DHCP
     ALLINTERFACES      Habilita todas as interfaces
     LISTEN0            Seleciona a interface
     UP                 Inicia o serviço de DHCP
     DOWN               Pára o serviço de DHCP
     PURGE              Limpa as configurações do módulo DHCP tipo Relay
```

Note que, antes de serem aplicadas as configurações de RELAY, é preciso definir a operação como tal, definindo o parâmetro TYPE.

Para entender melhor como funcionam as configurações do RELAY, a seguir é apresentado um script:

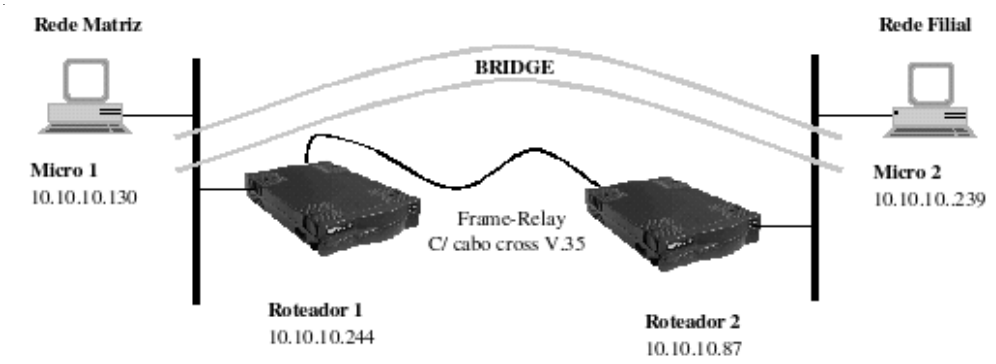
```
SET DHCP PURGE
SET DHCP TYPE RELAY
```

```
SET DHCP ALLINTERFACES TRUE
Aqui você habilita todas as interfaces para que sejam listadas
SET DHCP SERVER 10.50.30.1
Endereço IP do servidor de DHCP remoto
SET DHCP UP
```

CONFIGURAÇÃO DE PROTOCOLO BRIDGE

Bridge é o termo utilizado para designar um dispositivo que liga duas redes que usam protocolos distintos, ou dois segmentos da mesma rede que usam o mesmo protocolo.

Os parâmetros para configuração da bridge são:



Os roteadores da Digitel posibilitam a configuração de bridge somente sob um link Frame_Relay

```
SET BRIDGE
     BRIDGE              <Bridge identifier number>
     NAME                <Interface name>
     AGEING              <numeric value>
     ADDRESS             <IP address>
            GARBAGEINTERVAL <numeric value>
            SPANNINGTREE        {TRUE,FALSE}
            PURGE           <INTERFACE>
     ENABLED             {TRUE,FALSE}
SET BRIDGE BRIDGE0 WAN0-PVC0 INCLUDED
SET BRIDGE BRIDGE0 UP
```

Exemplo de configuração - Matriz

```
SET BRIDGE BRIDGE0 SPANNINGTREE TRUE
SET BRIDGE BRIDGE0 LAN0 INCLUDED
SET BRIDGE BRIDGE0 WAN0-PVC0 INCLUDED
SET BRIDGE BRIDGE0 UP
```

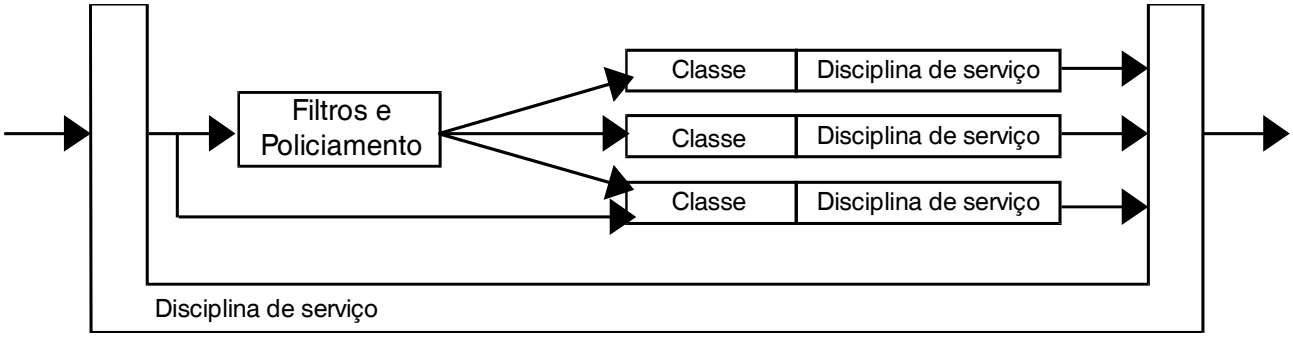
Exemplo de configuração - Filial

```
SET BRIDGE BRIDGE0 SPANNINGTREE TRUE S
SET BRIDGE BRIDGE0 LAN0 INCLUDED
SET BRIDGE BRIDGE0 WAN0-PVC0 INCLUDED
SET BRIDGE BRIDGE0 UP
```

QUALIDADE DE SERVIÇO (QOS)

Controle de tráfego

O controle de tráfego no NR-2G se baseia em três conceitos-chave: disciplina de serviço, classe e filtro. O controle é bastante flexível, permitindo uma série de combinações devido à sua arquitetura de caráter recursivo. Os conceitos-chave são descritos a seguir.



Disciplina de serviço é a forma de gerenciamento da(s) fila(s) de tráfego, podendo ser dotada de um algoritmo de escalonamento de filas, o que acontece na maioria dos casos (como HTB, TBF, SFQ). As disciplinas de serviço mais complexas contêm filtros e classes. Cada disciplina possui um identificador, denominado handle, e uma variável, que diz em que posição da hierarquia de classes foi instalada a disciplina de serviço. Tal variável é chamada classid.

Classe é um nó na hierarquia de controle de tráfego. Uma classe não é responsável pelo gerenciamento das filas. Para isso, ela recorre a uma disciplina de serviço, sendo possível um grande número de combinações a partir dessa recursividade. Assim, é possível criar uma hierarquia onde, em cada nó folha, esteja instalada uma disciplina de serviço diferente. Esses nós são os verdadeiros responsáveis pelo controle do tráfego.

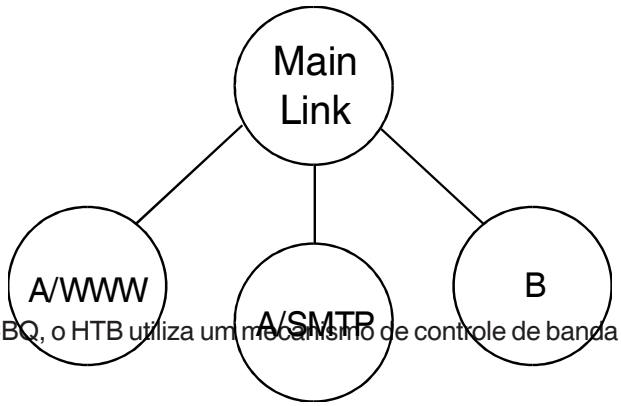
Essa flexibilidade é mais notável quando se usa a disciplina de serviço HTB, que permite a criação de várias classes, ao contrário de outras disciplinas, como TBF e SFQ.

Filtro é o mecanismo através do qual um pacote é atribuído a uma classe. Um filtro é chamado no momento em que um pacote passa pela unidade (forward) ou são geradas na unidade (output). Cada disciplina ou classe contém uma lista de filtros, distintos entre si pelo protocolo ao qual se aplicam (IP, ICMP, etc.) e por sua prioridade. O sistema de classificação dos equipamentos de rede Digitel utiliza todo o poder de seleção de pacotes do mecanismo de firewall. Assim como na disciplina de serviço, os filtros também possuem handle e classid, tendo também os mesmos significados.

Disciplinas de serviço

HTB (Hierarchy Token Bucket)

O HTB é uma disciplina intuitiva, rápida e flexível, sendo capaz de superar as características do CBQ. O HTB também é baseado na definição de classes, e estas podem ser subdivididas em subclasses, formando uma hierarquia de classes.



Diferentemente do CBQ, o HTB utiliza um mecanismo de controle de banda (shapes traffic based) baseado

no algoritmo Token Bucket Filter, que não depende das características físicas do link. Também não é preciso conhecer o comportamento da banda de saída.

É possível simular links mais lentos e determinar que classe de tráfego usará esse caminho lento, mudando, desta forma, a ordenação e priorização do fluxo corrente.

Parâmetro	Função
Priority	Define a prioridade da classe dentro do mecanismo de escalonamento. O mecanismo utilizado é um round-robin com prioridades.
Rate	Indica o máximo rate da classe. A soma dos rates dos filhos de uma dada classe são iguais ao rate do pai.
Ceil	Número máximo de dados que podem ser enviados.
Burst	A quantidade de bytes que podem ser enviados dentro de um determinando instante e que obedecem à velocidade fornecida pelo ceil.

TBF (Token Bucket Filter)

Disciplina de serviço que utiliza dois token buckets, um para o controle da vazão média e outro para o controle da vazão de pico. O token bucket de controle da vazão de pico permite que uma certa rajada de tráfego, controlada pelo parâmetro peak rate, seja enviada durante um período de ausência de tráfego. O token bucket de controle da vazão média especifica o fluxo corrente da classe. Caso não se utilize o parâmetro peak rate, o segundo token bucket não será ativado, e nenhum limite será especificado. Assim, a rajada é baseada na quantidade de tokens existentes. Esse algoritmo tem como objetivo o atraso dos pacotes que excedam a especificação, e não sua eliminação.

Parâmetro	Função
Limit	Especifica o tamanho da fila em bytes do token bucket principal.
Latency	Indica o atraso máximo sofrido por um pacote na fila.
Rate	Especifica a banda da classe.
Burst	Indica a profundidade do token bucket principal.
Mtu	Usado para calcular o tamanho dos pacotes, quer para a tabela de vazão média, quer para a tabela de pico.
Peakrate *(opcional)*	Ativa o token bucket de controle da vazão de pico e permite especificar seu valor médio.
Mpu	Indica o tamanho mínimo de pacote.

O valor de limit deve ser maior ou igual ao de mtu da interface, sob pena de pacotes com valores maiores serem eliminados. Caso o parâmetro latency seja utilizado, o tamanho da fila será calculado com base na fórmula limit = rate * latency + burst. Se o valor da mtu for maior que 2040, será necessário especificá-lo. Seu valor deve incluir o cabeçalho da camada de ligação lógica. Se o segundo token bucket for ativado através do parâmetro peakrate, o mtu indicará também a profundidade desse token bucket.

SFQ (Stochastic Fairness Queuing)

É uma variante do algoritmo FQ, no qual uma fila é mantida ordenada pelos instantes em que os pacotes teriam sua transmissão terminada se utilizado o algoritmo BR (bit-by-bit Round Robin). O BR trabalha efetuando Round Robin em filas de espera, tendo como unidade de transmissão apenas 1 bit. O pacote só é transmitido quando é feita a "leitura" de todo o pacote. Assim, pacotes menores são transmitidos primeiro.

Pelo fato de ser dispendioso manter uma fila ordenada, pouco escalável, o SFQ propõe a criação de uma quantidade elevada de filas, utilizando uma tabela de hash para fazer a atribuição de um fluxo a uma delas. Uma deficiência desse método é que, à medida que o número de fluxos ativos começa a se aproximar do número de

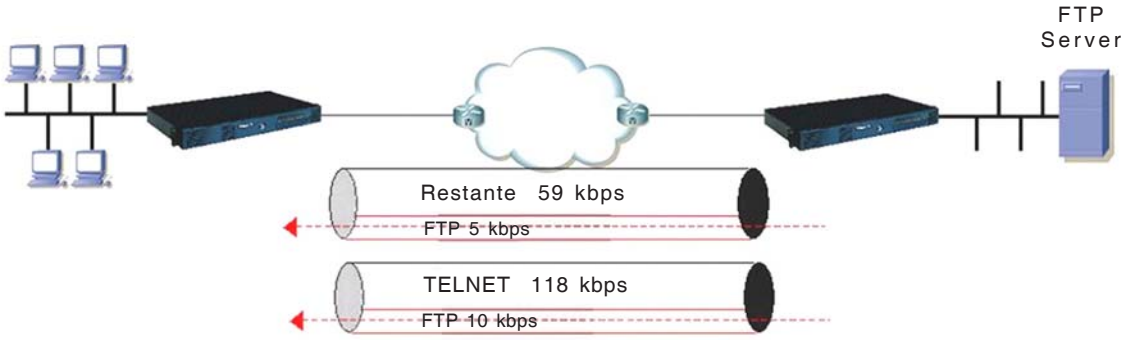
filas, a probabilidade de colisão na tabela hash deixa de ser desprezível.

As filas que possuem pacotes a serem transmitidos são servidas em modo Round Robin. Cada passagem transmite uma certa quantidade de dados, definida em quantum.

Parâmetro	Função
Perturb	Perturbação periódica que é feita no cálculo do hash para evitar colisões. SECS define o intervalo em que essa perturbação deve ser feita.
Quantum	Quantidade de dados, em bytes, que deve ser transmitida em cada passagem do Round Robin.

A seguir são apresentados dois exemplos de configuração. No primeiro exemplo, faremos a limitação fixa da banda em 5 kbps para o protocolo FTP. No segundo, faremos uma regra bem parecida, mas trabalharemos com uma característica denominada compartilhamento de link, onde prioridades são definidas para cada fila, e onde a prioridade mais baixa recebe banda da classe pai. A seguir está a topologia:

Podemos observar que criamos duas filas (1:1 e 1:2) sobre a classe raiz 1:, e limitamos a classe 1:1 em



5 kbps. Note que as regras de QoS devem ser aplicadas levando-se em conta o tráfego de saída da interface.

```
SET FIREWALL QOS RULE0 PROTOCOL tcp MARK 1
SET FIREWALL QOS RULE0 SOURCE ADDRESS 192.168.1.0 MASK 255.255.255.0
SET FIREWALL QOS RULE0 DESTINATION ADDRESS 192.168.2.0 MASK 255.255.255.0
SET FIREWALL QOS RULE0 TCP DPORT 20-21
SET FIREWALL UP
SET QOS WAN0-PVC0 ROOT-HTB HANDLE 1:
SET QOS WAN0-PVC0 HTB1: DEFAULT 2
SET QOS WAN0-PVC0 HTB1: NEW-HTB HANDLE 1:1
SET QOS WAN0-PVC0 HTB1:1 RATE 5KBIT BURST 5KBIT CEIL 5KBIT PRIORITY 1
SET QOS WAN0-PVC0 HTB1: NEW-HTB HANDLE 1:2
SET QOS WAN0-PVC0 HTB1:2 RATE 59KBIT BURST 5KBIT CEIL 59KBIT PRIORITY 0
SET QOS WAN0-PVC0 HTB1: NEW-FILTER HANDLE 1 PRIORITY 0 PROTOCOL IP CLASSID 1:1
SET QOS UP
```

No segundo exemplo, as filas 1:10 e 1:20 foram criadas sobre uma classe pai, que fará o empréstimo de banda de acordo com a prioridade definida (quanto menor o valor da prioridade, maior ela será). Note que, aqui, enquanto estivermos utilizando somente o FTP, os 128 kbps estarão alocados a ele, mas, quando o Telnet for iniciado, ocorrerá o compartilhamento de link:

```
SET FIREWALL PURGE
SET FIREWALL QOS RULE0 PROTOCOL TCP MARK 1
SET FIREWALL QOS RULE0 SOURCE ADDRESS 192.168.10.0 MASK 255.255.255.0
SET FIREWALL QOS RULE0 DESTINATION ADDRESS 192.168.11.0 MASK 255.255.255.0
SET FIREWALL QOS RULE0 TCP DPORT 20-21
```

```
SET FIREWALL QOS RULE1 PROTOCOL TCP MARK 2
SET FIREWALL QOS RULE1 SOURCE ADDRESS 192.168.10.0 MASK 255.255.255.0
SET FIREWALL QOS RULE1 DESTINATION ADDRESS 192.168.11.0 MASK 255.255.255.0
SET FIREWALL QOS RULE1 TCP DPORT 23-23
SET FIREWALL UP
SET QOS PURGE
SET QOS WAN0-PVC0 ROOT-HTB HANDLE 1:
SET QOS WAN0-PVC0 HTB1: NEW-HTB HANDLE 1:1
SET QOS WAN0-PVC0 HTB1:1 RATE 128KBIT BURST 15KBIT CEIL 128KBIT NO-PRIORITY
SET QOS WAN0-PVC0 HTB1:1 NEW-HTB HANDLE 1:10
SET QOS WAN0-PVC0 HTB1:10 RATE 10KBIT BURST 15KBIT CEIL 128KBIT PRIORITY 0
SET QOS WAN0-PVC0 HTB1:1 NEW-HTB HANDLE 1:20
SET QOS WAN0-PVC0 HTB1:20 RATE 118KBIT BURST 15KBIT CEIL 128KBIT PRIORITY 1
SET QOS WAN0-PVC0 HTB1:1 NEW-FILTER HANDLE 1 PRIORITY 1 PROTOCOL IP CLASSID 1:10
SET QOS WAN0-PVC0 HTB1:1 NEW-FILTER HANDLE 2 PRIORITY 0 PROTOCOL IP CLASSID 1:20
SET QOS UP
```

FIREWALL

Introdução

Os roteadores NR-2G possuem diversas características de Firewall. Aqui serão descritas algumas características dessa feature, e alguns exemplos de configuração também serão apresentados.

Existem dois níveis de aplicação de segurança em roteadores NR-2G: um é determinado por políticas (polices), e o outro, por regras (rules).

Política

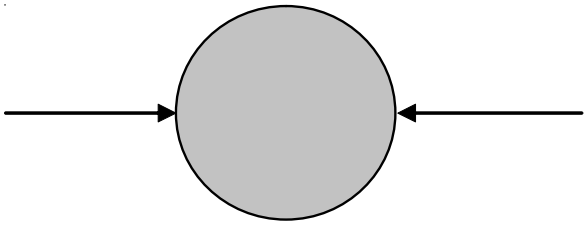
A política da chain determina o destino do pacote. Uma política atua quando um pacote chega ao fim de uma chain e não se enquadrou em nenhuma das regras. Neste caso, o kernel verifica qual a política da chain, para saber o que fazer com o pacote.

A política pode ser tanto ACCEPT (aceitar) quanto DROP (rejeitar). Por default, as chains INPUT/OUTPUT/FORWARD possuem suas políticas definidas como ACCEPT na inicialização.

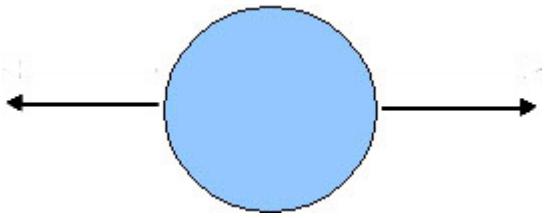
Cadeias (chains)

Uma chain é uma lista de regras (rules). Cada regra diz ao cabeçalho do pacote o que deve ser feito com o mesmo. Se a regra corrente não for associada ao pacote, então a próxima regra na chain será consultada. Quando não houver mais regras a consultar, o sistema operacional analisará a política da chain para decidir o que fazer.

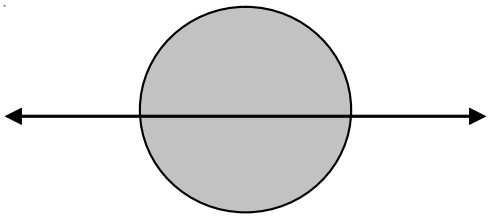
• INPUT: todo tráfego que decorre de um host (local ou remoto) em direção ao roteador.



• OUTPUT: todo tráfego que decorre do roteador e possui um destino qualquer.



• FORWARD: todo tráfego que decorre de um host qualquer (local ou remoto) e tem como destino algum host que seja alcançado através desse roteador.



Pacotes atravessando a chain INPUT não possuem interface de saída, e pacotes atravessando a chain OUTPUT não têm interface de entrada. No caso do FORWARD, ambas podem ou devem ser identificadas na criação das regras.

Nas regras, podemos criar diversas formas de manipular o tráfego. Os principais parâmetros a serem trabalhados aqui são listados a seguir.

• *Action* - Uma ação determina o que será feito quando um pacote se enquadrar em uma determinada regra.

As ações possíveis são ACCEPT, DROP e REJECT.

- ACCEPT: aceita o pacote que está sendo filtrado;

- DROP: descarta o pacote que está sendo filtrado;

- REJECT: tem o mesmo efeito de DROP, a não ser que o remetente tenha enviado uma mensagem de erro ICMP *port unreachable* (porta inalcançável). A mensagem de erro ICMP não será enviada se alguma das seguintes situações estiver ocorrendo (consulte também a RFC 1122):

  - O pacote que está sendo filtrado é uma mensagem de erro ICMP no início, ou um tipo desconhecido de ICMP;

  - O pacote que está sendo filtrado é um fragmento sem cabeçalho;

  - Muitas mensagens de erro ICMP já foram enviadas para o mesmo destinatário recentemente.

• *Protocolo* - As opções utilizadas aqui são TCP, UDP e ICMP.

• *Origem e Destino* - É onde determinamos os parâmetros de endereçamento e as portas.

• *Endereços IP* - Endereços IP de redes ou hosts a serem determinados.

• *Porta* - Range de portas UDP/TCP.

Além desses parâmetros, podemos criar diversas formas de manipulação através de flags de protocolo TCP, regras com inversão de lógica, tipos de pacote, etc.

Especificando inversão

Muitas opções de configuração podem ter seus argumentos precedidos de '!' (pronunciado "não"), que significa a inversão da lógica da regra para um determinado argumento. Por exemplo, se especificarmos uma regra que só permite a passagem de pacotes para uma dada interface e ligarmos a opção '!' para a interface de destino, a regra será invertida. Com isso, a passagem de pacotes será permitida para todas as interfaces, exceto a interface especificada. Veremos, mais adiante, alguns exemplos de como isso se aplica.

Especificando fragmentos

Às vezes um pacote é muito grande para ser enviado todo de uma vez. Quando isso ocorre, o pacote é dividido em fragmentos e enviado como múltiplos pacotes. Quem o recebe remonta os fragmentos, reconstruindo o pacote. O problema com os fragmentos é que o fragmento inicial tem os campos de cabeçalho completos (IP + TCP, UDP e ICMP) para examinar, mas os pacotes subseqüentes só têm o cabeçalho IP (sem os campos dos outros protocolos). Logo, examinar o interior dos fragmentos subseqüentes em busca de cabeçalhos de outros protocolos (como extensões de TCP, UDP e ICMP) é impossível.

Se você está fazendo o acompanhamento de conexões ou NAT, todos os fragmentos serão remontados antes de atingir o código do filtro de pacotes (assim, você não precisa se preocupar com os fragmentos). Caso contrário, é importante entender como os fragmentos são tratados pelas regras de filtragem. Qualquer regra que requisitar informações que não existem não será válida. Isso significa que o primeiro fragmento será tratado como um pacote qualquer; já o segundo e os seguintes não o serão. Então, uma regra com fragment (demais pacotes) habilitado analisará os pacotes de um fluxo de dados, exceto o pacote inicial. Também é interessante especificar uma regra que tenha a opção fragment (primeiro pacote) mas que não se aplique ao segundo e demais fragmentos.

Geralmente, considera-se seguro deixar o segundo fragmento e os seguintes passarem, uma vez que o primeiro fragmento será filtrado; isso vai evitar que o pacote todo seja remontado na máquina destinatária.

IMPORTANTE!
No caso da utilização da ferramenta Easyconfig, é importante lembrar que ele utiliza as portas TCP 14830 e 14832. Se essas portas forem bloqueadas, a comunicação com o roteador não será possível.

Parâmetros de configuração

Os seguintes parâmetros são necessários para a configuração do firewall:

```
NR2Gt > SET FIREWALL <enter>
Valid options are:
     INPUT     Determina POLICY ou RULE para INPUT
     OUTPUT    Determina POLICY ou RULE para OUTPUT
     FORWARD   Determina POLICY ou RULE para FORWARD
     QOS       Configuração para marcação de pacotes em QoS
     UP        Inicia o serviço de FIREWALL
     DOWN      Pára o serviço de FIREWALL
     PURGE     Limpa as configurações do módulo FIREWALL

NR2Gt > SET FIREWALL INPUT/OUTPUT/FORWARD <enter>
Valid options are:
     POLICY    Configura as políticas de acesso (DROP/ACCEPT)
     RULE0     Configura as regras de acesso

NR2Gt > SET FIREWALL INPUT/OUTPUT/FORWARD RULE0
Valid options are:
     PROTOCOL                          Protocolo (TCP/UDP/ICMP/ALL)
     PROTOCOLINVERTED                  Inversão da lógica de protocolo
     ACTION  (Only when not in QOS chain)  Ação (DROP/REJECT/ACCEPT)
     FRAGMENT                          Análise de fragmento do segundo pacote
                                       e dos que o sucedem
     SOURCE                            Regras para origem de pacote
     DESTINATION                       Regras para destino de pacote
     UDP  (Only when PROTOCOL = UDP)   Regras para protocolo UDP
     TCP  (Only when PROTOCOL = TCP)   Regras para protocolo TCP
```

```
     ICMP  (Only when PROTOCOL = ICMP)     Regras para protocolo ICMP
     PURGE                                 Limpa as configurações do módulo RULE0
NR2Gt > SET FIREWALL INPUT RULE0 SOURCE/DESTINATION <enter>
Valid options are:
     INTERFACE                Interface de origem/destino
     INTERFACEINVERTED*       Inverte a lógica para o campo INTERFACE
     ADDRESS                  Endereço de rede/host
     MASK                     Máscara de rede
     ADDRESSINVERTED          Inverte a lógica para o campo ADDRESS
*Only when INTERFACE != NONE
```

Para um melhor entendimento dessas regras, vamos criar um exemplo onde desabilitamos o tráfego decorrente de uma rede qualquer para o roteador (INPUT) e habilitamos o Telnet somente de um host específico.

Note que, no exemplo abaixo, estamos assumindo que o host (microcomputador) possui o endereço 10.10.10.63 e que o endereço do roteador é 10.10.10.66. Para testar se ele está funcionando corretamente, basta aplicar um ping contínuo para o endereço de destino; após o firewall estar iniciado, o ping deverá responder com TIME OUT, e somente deverá ser possível realizar um Telnet para o endereço 10.10.10.66 da máquina 10.10.10.63.

```
SET FIREWALL PURGE
SET FIREWALL INPUT POLICY DROP
SET FIREWALL INPUT RULE0 PROTOCOL TCP ACTION ACCEPT
SET FIREWALL INPUT RULE0 SOURCE INTERFACE LAN0 ADDRESS 10.10.10.63 MASK
255.255.255.255
SET FIREWALL INPUT RULE0 TCP DPORT 23-23
SET FIREWALL UP
CONFIG SAVE
```

Para o exemplo a seguir, utilizaremos uma inversão de lógica. Quando habilitamos a opção ADDRESSINVERTED nessa regra, dizemos que qualquer endereço pode realizar um Telnet no roteador 10.10.10.66, menos o endereço 10.10.10.63. A regra é a mesma; somente adicionamos o parâmetro ADDRESSINVERTED como TRUE.

```
SET FIREWALL PURGE
SET FIREWALL INPUT POLICY DROP
SET FIREWALL INPUT RULE0 PROTOCOL TCP ACTION ACCEPT
SET FIREWALL INPUT RULE0 SOURCE INTERFACE LAN0 ADDRESSINVERTED TRUE ADDRESS
10.10.10.63 MASK 255.255.255.255
SET FIREWALL INPUT RULE0 TCP DPORT 23-23
SET FIREWALL UP
CONFIG SAVE
```

Para fins de teste, realize o Telnet da máquina 10.10.10.63 para o roteador 10.10.10.66 e, depois, tente executar esse mesmo Telnet de qualquer outro microcomputador. Você verá que o acesso não será possível do host 10.10.10.63, pois há uma inversão de lógica que nos diz que qualquer máquina pode acessar esse equipamento, menos o endereço 10.10.10.63/32.

Para um terceiro exemplo, é necessário que uma rede consiga realizar uma requisição ICMP para uma rede remota, sem que a rede interna seja alcançada. Para o exemplo, é definido que a rede local é 10.10.10.0/24, e a rede remota, 192.168.11.0/24. Note que as mensagens de ECHO-REQUEST são enviadas, mas, para que o retorno seja efetivado (ECHO-REPLY), é necessária a criação de uma regra especial, que não abrange somente o protocolo, mas também o tipo de mensagem ICMP. As regras são apresentadas a seguir.

```
SET FIREWALL PURGE
SET FIREWALL INPUT POLICY ACCEPT
SET FIREWALL OUTPUT POLICY ACCEPT
SET FIREWALL FORWARD POLICY ACCEPT
SET FIREWALL FORWARD RULE0 PROTOCOL ICMP ACTION ACCEPT
SET FIREWALL FORWARD RULE0 SOURCE INTERFACE LAN0 ADDRESS 10.10.10.0 MASK
255.255.255.0
SET FIREWALL FORWARD RULE0 DESTINATION INTERFACE WAN0-PVC0 ADDRESS 192.168.11.0
```

```
MASK 255.255.255.0
SET FIREWALL FORWARD RULE1 PROTOCOL ICMP ACTION DROP
SET FIREWALL FORWARD RULE1 SOURCE INTERFACE WAN0-PVC0 ADDRESS 0.0.0.0 MASK
0.0.0.0
SET FIREWALL FORWARD RULE1 DESTINATION INTERFACE LAN0 ADDRESS 0.0.0.0 MASK
0.0.0.0
SET FIREWALL FORWARD RULE1 ICMP ENABLED TRUE INVERTED TRUE TYPE ECHO-REPLY
SET FIREWALL UP
```

O comando criado insere na regra uma inversão de lógica relacionada ao tipo de mensagem a ser filtrada. Isso é criado na regra número 1 (RULE1) da chain FORWARD.

```
SET FIREWALL FORWARD RULE1 ICMP ENABLED TRUE INVERTED TRUE TYPE ECHO-REPLY
```

Para visualizar as estatísticas da regra criada, aplique o comando SHOW FIREWALL STATS.

SISTEMAS DE AUTENTICAÇÃO

Introdução

O sistema de autenticação dos roteadores NR-2G é capaz de suportar diferentes tipos e protocolos de autenticação. A autenticação pode ser feita através dos comandos SHADOW, TACACS e RADIUS.

SHADOW é um sistema de autenticação que se baseia em uma criptografia contida no próprio equipamento, o MD5.

TACACS (Terminal Access Controller Access Control System) é um protocolo de autenticação para usuários remotos. Originalmente criado pela CISCO, hoje é usado por diversos fabricantes. Com o TACACS, é possível autenticar um usuário em uma base provida pelo servidor TACACS do cliente.

RADIUS (Remote Authentication Dial User Service) é um dos protocolos de autenticação remota mais difundidos. Também possibilita a autenticação de usuários em uma base remota provida pelo cliente. Está definido na RFC 2058.

Para configurar o sistema de autenticação, é preciso:

1. Definir o tipo de autenticação.
2. Em caso de mais de um tipo de autenticação, indicar uma ordem para os mesmos.
3. Configurar o método de autenticação.

A configuração da autenticação encontra-se disponível no módulo SYSTEM.

```
NR2Gt > SET SYSTEM <enter>
Valid SET options for SYSTEM are:
     TIMETYPE
     DATE*
     TIME*
     LOG
     UPDATE
     AAA
     HOSTNAME
     PURGEUSERS
     PURGEDNS
     RESTART
*Only when TIMETYPE=LOCAL
     OS
```

```
     USER0
     USER1
     USER2
     USER3
     USER4
     DNS0
```

Uma informação relevante é que, em caso de não haver nenhum método de autenticação configurado, o CLI assumirá o SHADOW como método padrão para autenticação.

A ordem de autenticação é definida com o seguinte comando:

```
NR2Gt > SET SYSTEM AAA AUTHENTICATION ORDER <enter>
You must provide order for UP auth types. Combination possibilities are:
     TACACS SHADOW
     SHADOW TACACS
     RADIUS SHADOW
     SHADOW RADIUS
```

RADIUS

Para definir como método de autenticação somente RADIUS, devemos habilitar a autenticação RADIUS e desabilitar a autenticação SHADOW.

```
SET SYSTEM AAA AUTHENTICATION RADIUS UP
SET SYSTEM AAA AUTHENTICATION SHADOW PURGE
```

As opções disponíveis para configuração são:

```
NR2Gt > SET SYSTEM AAA AUTHENTICATION RADIUS <enter>
Valid SET options for RADIUS are:
     DEBUG          Habilita a exibição de eventos via Syslog
     SERVER         Configura endereço IP do servidor RADIUS
     SECRET         Senha utilizada para negociação entre o RADIUS do equipamento
                    e o servidor
     TIMEOUT        Tempo de espera sem resposta para autenticação remota
     ONERROR**      Define o que será feito quando o RADIUS for o primeiro
                    método de autenticação(sendo a ordem RADIUS SHADOW)
     UP             Inicia o RADIUS
     PURGE          Limpa as configurações do módulo RADIUS
```

Como exemplo, temos a seguinte configuração:

```
SET SYSTEM AAA AUTHENTICATION RADIUS UP
SET SYSTEM AAA AUTHENTICATION RADIUS SERVER 20.20.20.20
SET SYSTEM AAA AUTHENTICATION RADIUS SECRET digitel
SET SYSTEM AAA AUTHENTICATION RADIUS ONERROR
```

ONERROR define o que será feito quando o **RADIUS** for o primeiro método de autenticação (sendo a ordem **RADIUS SHADOW**). Os valores válidos são **FAIL** ou **CONTINUE**. **FAIL** diz que, em caso de falha na autenticação utilizando o primeiro método, o processo de login deverá ser abortado; **CONTINUE** diz que se deve tentar realizar a autenticação utilizando o próximo método.

TACACS

Para definir como método de autenticação somente TACACS, devemos habilitar a autenticação TACACS e desabilitar a autenticação SHADOW.

```
SET SYSTEM AAA AUTHENTICATION TACACS UP
SET SYSTEM AAA AUTHENTICATION SHADOW PURGE
```

Para as configurações de **TACACS**, temos os seguintes parâmetros:

```
NR2Gt > SET SYSTEM AAA AUTHENTICATION TACACS <enter>
Valid SET options for TACACS are:
     ENCRYPT   Habilita a chave criptografada para SECRET
     DEBUG     Habilita a exibição de eventos via Syslog
     SERVER    Configura o endereço IP no servidor TACACS
     SECRET*   Senha utilizada para negociação entre o TACACS do equipamento e
               o servidor
     ONERROR** Define o que será feito quando o RADIUS for o primeiro método de
               autenticação (sendo a ordem RADIUS SHADOW)
     UP        Inicia o TACACS
     PURGE     Limpa as configurações do módulo TACACS
*Only when ENCRYPT=TRUE
**Only when SHADOW is UP and ORDER is TACACS SHADOW
```

Como exemplo, temos a seguinte configuração:

```
SET SYSTEM AAA AUTHENTICATION TACACS UP
SET SYSTEM AAA AUTHENTICATION ORDER TACACS SHADOW
SET SYSTEM AAA AUTHENTICATION TACACS ENCRYPT TRUE
SET SYSTEM AAA AUTHENTICATION TACACS SERVER 10.10.10.12 SECRET digitel
SET SYSTEM AAA AUTHENTICATION TACACS ONERROR
```

ONERROR define o que será feito quando o **TACACS** for o primeiro método de autenticação (sendo a ordem **TACACS SHADOW**). Os valores válidos são **FAIL** ou **CONTINUE. FAIL** diz que, em caso de falha na autenticação utilizando o primeiro método, o processo de login deverá ser abortado; **CONTINUE** diz que se deve tentar realizar a autenticação utilizando o próximo método.

ESTATÍSTICAS DE INTERFACE

Os roteadores NR-2G possuem diversas características de troubleshooting. Uma das mais utilizadas é a verificação de erros em interfaces. A seguir está a descrição dos contadores para os diversos protocolos de encapsulamento:

WAN (todos os protocolos - interface HDLC)

TX ERRORS:

- Frame descartado por timeout na interface (pode ocorrer, por exemplo, por problemas físicos, falta ou problemas no relógio de Tx)
- Erros físicos na transmissão (perda de CTS ou underrun - não devem ocorrer normalmente)

RX ERRORS:

- Frame descartado por limitação da capacidade de processamento na recepção (não deve ocorrer normalmente)
- Frame recebido com erro de CRC
- Frame recebido com erro de endereçamento (não deve ocorrer normalmente)
- Frame recebido com erro de sincronismo
- Frame recebido com violação de tamanho

• Frame recebido com número não inteiro de octetos
• Seqüência de abort recebida
• Frame recebido com perda de portadora

TX DROPPED:
• Frame descartado por reinicializacão da interface
• Frame descartado por falta de memória (não deve ocorrer normalmente)

RX DROPPED:
• Frame descartado por limitação da capacidade de processamento na recepção (não deve ocorrer normalmente)
• Frame descartado por erro de CRC
• Frame descartado por erro de endereçamento (não deve ocorrer normalmente)
• Frame descartado por falta de memória na recepção (não deve ocorrer normalmente)

TX OVERRUN:
• Não usado

RX OVERRUN:
• Frame recebido com erro de overrun

COLLISION:
• Não usado

CRC ERRORS:
• Frame recebido com erro de CRC

TX ABORTED:
• Frame descartado por timeout na interface (pode ocorrer, por exemplo, por problemas físicos, falta ou problemas no relógio de Tx)

TX FIFO ERROR:
• Underrun na transmissão (não deve ocorrer normalmente)

TX CARRIER ERROR:
• Perda de CTS na transmissão (não deve ocorrer normalmente)

RX LENGTH ERROR:
• Frame recebido com violação de tamanho

RX FRAME ERROR:
• Frame recebido com número não inteiro de octetos

RX MISSED ERROR:
• Frame recebido com perda de portadora

WAN (protocolo HDLC-Cisco)

RX ERRORS:
• Frame recebido com erro de protocolo (frame curto, erro de endereçamento, erro de tamanho)

WAN (protocolo FRAME RELAY - interface HDLC)

RX ERRORS:

- Frame recebido inválido (frame curto ou com formato errado)
- Frame LMI recebido quando LMI=NONE
- Erros no protocolo LMI
- Frame não LMI recebido no canal de controle
- Frame recebido com DLCI desconhecido
- Frame recebido para PVC desligado (interface DOWN)

WAN (protocolo FRAME RELAY - interface PVC)

TX DROPPED:
- Frame descartado por limitação da taxa de transmissão (buffers cheios)
- Frame descartado por canal não ativo

TX COMPRESSED:
- Frame transmitido com o canal congestionado

RX COMPRESSED:
- Frame recebido com canal congestionado

WAN (protocolo X25 - interface HDLC)

RX ERRORS:
- Frame recebido com erro no protocolo LAPB

LAN (todos os protocolos - interface ETH)

TX ERRORS:
- Frame descartado por timeout na interface (pode ocorrer, por exemplo, por problemas físicos, falta ou problemas no relógio de Tx)
- Frame retransmitido por colisão até o limite e descartado
- Frame transmitido com underrun
- Frame transmitido com perda de portadora
- Frame transmitido sem heartbeat
- Frame transmitido com late collision

RX ERRORS:
- Frame recebido com violação de tamanho
- Frame recebido com número não inteiro de octetos ou com late collision
- Frame recebido com erro de CRC ou FIFO overrun

TX DROPPED:
- Não usado

RX DROPPED:
- Frame descartado por limitação da capacidade de processamento ou de memória na recepção (não deve ocorrer normalmente)

TX OVERRUN:
- Não usado

RX OVERRUN:
- Não usado

COLLISION:
• Colisão durante a transmissão de um frame

CRC ERRORS:
• Frame recebido com erro de CRC ou FIFO overrun

TX ABORTED:
• Frame retransmitido por colisão até o limite e descartado

TX FIFO ERROR:
• Frame transmitido com underrun

TX CARRIER ERROR:
• Frame transmitido com perda de portadora

TX HEARTBEAT ERROR:
• Frame transmitido sem heartbeat

TX WINDOW ERROR:
• Frame transmitido com late collision

RX LENGTH ERROR:
• Frame recebido com violação de tamanho

RX FRAME ERROR:
• Frame recebido com número não inteiro de octetos ou com late collision

RX MISSED ERROR:
• Não usado

SYSLOG

Outra forma de realizar a verificação de erros é utilizando o Syslog, uma poderosa ferramenta para utilização em troubleshooting, que pode ser visualizada tanto na própria Console (buffer) como por um servidor remoto, onde as mensagens também podem ser armazenadas.

Para direcionar a saída das mensagens, podemos criar diversas entradas (ENTRYx) onde especificamos, por exemplo, um servidor de Syslog remoto ou o próprio terminal. A seguir são apresentados os parâmetros para configuração:

```
NR2Gt > SET SYSTEM LOG <enter>
Valid SET options for LOG:
     UP        Inicializa o daemon de Syslog
     DOWN      Pára o daemon de Syslog
     PURGE     Limpa o módulo Log
     ENTRY0    Gera uma configuração de entrada

NR2Gt > SET SYSTEM LOG ENTRY0 <enter>
Applying to: ENTRY0
Valid SET options are:
     FACILITY      Tipo de facilidade
     PRIORITY      Tipo de prioridade
     OUTPUTTYPE    Tipo de saída
     HOST*         No caso de um servidor de Syslog remoto, identifica o IP do
                   mesmo
     PURGE         Limpa o módulo ENTRY0
*Only when OUTPUTTYPE=REMOTE
```

Facility

O parâmetro **FACILITY** é usado para especificar qual tipo de programa vai gerar mensagens de log. Segue abaixo a descrição:

```
NR2Gt > SET SYSTEM LOG ENTRY0 FACILITY <enter>
Applying to: ENTRY0
You must provide one of these:
     ALL       Todas as mensagens
     AUTH      Mensagens de segurança/autenticação
     SECURITY  Mensagens de segurança
     AUTHPRIV  Mensagens de segurança/autenticação (private)
     CRON      Daemon de cron e at
     DAEMON    Outros daemons do sistema
     KERN      Mensagens de kernel
     LPR       Subsistemas de impressão
     MAIL      Subsistemas de mail
     MARK      Timer para mensagem MARK
     NEWS      Subsistema de notícias USENET
     SYSLOG    Mensagens internas do Syslog
     USER      Mensagens genéricas de nível de usuário
     UUCP      Subsistema UUCP
     LOCAL0    Reservado para uso local
     LOCAL1    Reservado para uso local
     LOCAL2    Reservado para uso local
     LOCAL3    Reservado para uso local
     LOCAL4    Reservado para uso local
     LOCAL5    Reservado para uso local
     LOCAL6    Reservado para uso local
     LOCAL7    Reservado para uso local
```

Priority (Level)

Determina a importância das mensagens. Os seguintes níveis são permitidos, por ordem de importância:

```
NR2Gt > SET SYSTEM LOG ENTRY0 PRIORITY <enter>
Applying to: ENTRY0
You must provide one of these:
     ALL       Todos os níveis
     DEBUG     Mensagens de depuração
     INFO      Mensagens de informação
     NOTICE    Condições normais do sistema
     WARNING   Condições de alerta
     WARN      Sinônimo para o nível warning
     ERR       Condições de erro
     ERROR     Sinônimo para o nível err
     CRIT      Condições críticas
     ALERT     Deverá ser providenciado algum tipo de ação imediatamente
     EMERG     O sistema está inutilizável
     PANIC     Sinônimo para o nível emerg
```

```
NR2Gt > SET SYSTEM LOG ENTRY0 OUTPUTTYPE <enter>
Applying to: ENTRY0
You must provide one of these:
     REMOTE    Define um servidor como remoto
     TERMINAL  Define um servidor como local
```

Por default, o Syslog já vem habilitado. Para habilitar o Syslog com todas as facilidades, execute o seguinte comando:

```
SET SYSTEM LOG ENTRY0 FACILITY ALL PRIORITY ALL OUTPUTTYPE TERMINAL
```

Para visualizar as mensagens na Console (TERMINAL), execute o seguinte comando:

```
SHOW SYSTEM LOG MESSAGES <enter>
```

Se você possui um servidor de Syslog na rede, somente altere o tipo de saída (REMOTE) e configure o endereço IP do host:

```
SET SYSTEM LOG ENTRY0 FACILITY ALL PRIORITY ALL OUTPUTTYPE REMOTE HOST
192.168.100.23
```

VRRP (VIRTUAL ROUTER REDUNDANCY PROTOCOL)

Quando um roteador é configurado com uma rota default (default gateway) e sem qualquer protocolo de roteamento dinâmico (como RIP), ele pode se tornar um ponto vulnerável da rede. Esse tipo de cenário se caracteriza por ter um ponto único de falha (o gateway). Para solucionar o problema, uma opção seria utilizar algum protocolo de roteamento dinâmico; no entanto, isso poderia tornar a rede lenta, devido à complexidade inerente a esses mecanismos. Uma solução mais apropriada para o cenário é ter um roteador operando como backup do gateway da rede, de forma que, quando o gateway falhar, o backup entrará em operação.

O Virtual Router Redundancy Protocol (VRRP) vai ao encontro dessa necessidade. Ele é definido na RFC 2338 e provê um backup automático, assumindo o IP do roteador principal (Master).

O VRRP possui a mesma funcionalidade que o Hot Standby Router Protocol (HSRP) da CISCO e o IP Standy Protocol (IPSTB) da Digital Equipment Corporation.

Definições

- VRRP Router: Roteador executando Virtual Router Redundancy Protocol.
- Virtual Router ID: Identificador associado ao IP da LAN. Tanto o Master quanto o Backup devem ter o mesmo identificador.
- IP Address Owner ou IP: IP que representa o endereço do VRRP Router.
- Virtual Router Master: Roteador VRRP que assume a responsabilidade de rotear pacotes através do IP associado com o Virtual Router (incluindo a ação de responder ao ARP request deste IP). Somente o Master envia pacotes VRRP na rede.
- Virtual Router Backup: Roteador VRRP disponível para assumir a responsabilidade do Virtual Router quando ocorrer uma falha.

Configuração

A configuração de VRRP nos roteadores NR-2G está disponível via interface de linha de comando (CLI). Para ver as opções de configuração, usamos o comando **SET VRRP**. As opções de configuração são apresentadas a seguir:

```
SET VRRP <enter>
Valid options for this command are:
     VRID          Identificador do Virtual Router (roteador executando VRRP).
     INTERFACE     Interface da rede LAN.
     IP            IP virtual utilizado pelo VRRP.
     PRIORITY      Define a prioridade entre o equipamento Master e o Backup.
                   Aquele que possui prioridade mais alta é tido como Master.
                   Quando a prioridade não é informada, assume-se o valor 255.
     ADVERT        Intervalo de envio de mensagens (pacotes VRRP).
```

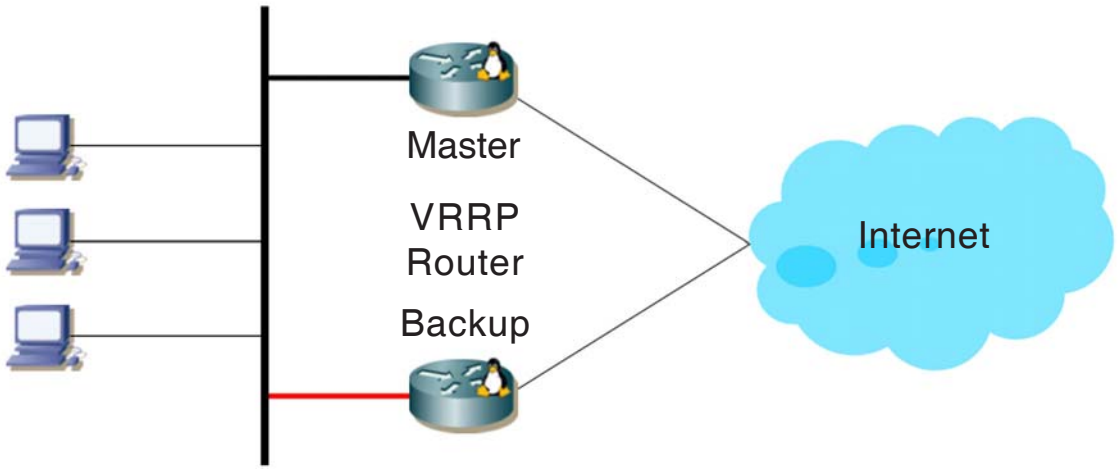
AUTH	Tipo de autenticação (NONE, PW ou AH).
PREEMPT	Previne que um roteador VRRP Backup de mais alta prioridade assuma o lugar do Master. O valor default é ser preenpitvo.
PASSWORD	Senha para autenticações do tipo pw ou ah.
NO-PASSWORD	Limpa a senha.
UP	Executa o VRRP.
DOWN	Finaliza a execução.
PURGE	Limpa a configuração.

Como exemplo, podemos configurar um roteador para ser um roteador VRRP Master. A configuração mínima para esse funcionamento seria configurar o VRID, a interface e o endereço IP, como visto a seguir:

```
SET VRRP STATE MASTER VRID 10 INTERFACE LAN0 PRIORITY 200 IP 20.20.20.20 UP
```

No nosso exemplo, a configuração do roteador VRRP Backup ficaria:

```
SET VRRP STATE BACKUP VRID 10 INTERFACE LAN0 PRIORITY 50 IP 20.20.20.20 UP
```



Protocolo CRTP

O protocolo CRTP é um método de compressão de datagrama IP/UDP/RTP, sendo utilizado para minimizar overhead em links de baixa velocidade.

Seu algoritmo consegue fazer uma compressão dos cabeçalhos de 40 bytes para 2 a 4 bytes, o que caracteriza uma ótima escolha quando o tamanho da banda é crítico - em especial, links de 14.400kbps ou 28.800kbps. Seu uso é desencorajado em links de maior capacidade, uma vez que pode aumentar o delay dos pacotes devido ao aumento do processamento.

Nota:

Atualmente, só é possível configurar o CRTP sob um link Frame_Relay.

```
SET WAN WAN<n>-PVC<n> CRTP
     ENABLED            {TRUE|FALSE}
     NON-TCP-SPACE      3 - 65535      (suggested 15 - default)
     F-MAX-PERIOD       1 - 65535      (suggested 256 - default)
     F-MAX-TIME         1 - 255        (suggested 5 - default)
     MAX-HEADER         60 - 1500      (suggested 168 - default)
     TIMEOUT            1 - 10         (suggested 3 - default)
     RETRIES            1 - 10         (suggested 3 - default)
```

```
SET WAN WAN<n>-PVC<n>

     CRTP                              Compressão de cabeçalhos (IP/UDP/RTP)
     ENABLED            {TRUE, FALSE}  (des)habilitar a compressão
     NEGOTIATION        {TRUE, FALSE}  (des)habilitar a negociação
     NON-TCP-SPACE                     Maximum value of a non-TCP context
                                       identifier (CID)
     F-MAX-PERIOD                      Largest number of compressed non-TCP
                                       headers
     F-MAX-TIME                        Maximum time interval between full
                                       header
     MAX-HEADER                        Largest header size that may be
                                       compressed
     TIMEOUT                           Handshake timeout (negociação)
     RETRIES                           Try again (negociação)
```

Habilitar o cRTP

```
SET WAN WAN0-PVC0 CRTP ENABLED TRUE
```

Protocolo NTP

O protocolo NTP oferece um mecanismo de sincronização de horário. RFC1305 - Network Time Protocol (Version 3)

Nota:
Nos roteadores da linha NR-2G, não é possível mapear o time zone.
Quando a diferença entre o horário do servidor NTP e o roteador for grande, será necessário dois servidores para atualizar o horário, senão, ele manterá o horário do roteador.

CONFIGURAÇÕES

Cenário 1

Apenas um servidor sem autenticação.

```
SET NTP SERVER0 TYPE SERVER IP 192.168.1.207
SET NTP UP
```

Cenário 2

Utilizando o roteador como servidor local.

```
SET NTP PURGE
SET NTP MASTER ENABLED TRUE STRATUM 7
SET NTP RESTRICT DEFAULT FLAG IGNORE
SET NTP RESTRICT RESTRICT0 IP 192.168.1.0 MASK 255.255.255.0 FLAG NOMODIFY
SET NTP UP
```

Nota:
Estações que não pertencem à rede 192.168.1.0/24 não conseguem acessar o servidor. A escolha do valor do stratum(7) é arbitrária, mas se recomenda um valor entre 5 e 10 devido a precisão limitada do relógio interno do roteador.

Cenário 3

Utilizando autenticação simétrica.

O lado servidor:

```
SET NTP PURGE
SET NTP AUTHENTICATION ENABLED TRUE
SET NTP AUTHENTICATION KEY0 SECRET B050B18564FD16A420176DD01744ABDF TRUSTED
TRUE
SET NTP MASTER ENABLED TRUE STRATUM 7
SET NTP RESTRICT DEFAULT FLAG IGNORE
SET NTP RESTRICT RESTRICT0 IP 192.168.1.0 MASK 255.255.255.0 FLAG NOTRUST
SET NTP UP
```

O lado cliente:

```
SET NTP PURGE
SET NTP AUTHENTICATION ENABLED TRUE
SET NTP AUTHENTICATION KEY0 SECRET B050B18564FD16A420176DD01744ABDF TRUSTED
TRUE
SET NTP SERVER0 TYPE SERVER IP 192.168.1.161 KEY 0
SET NTP UP
```

PARÂMETROS

Command	Options	Description
SET NTP		
PREFER	<server id>	Identify the preferred server
MASTER		
ENABLED	{TRUE, FALSE}	Enable/disable the NR2G as a NTP server
STRATUM	NR2G NTP	server number in the NTP hierarchy - usually stratum 3 or above
AUTHENTICATION		
ENABLED	{TRUE, FALSE}	Enable/disable NTP request authentication
REQUESTKEY	<key number>	Request key number
CONTROLKEY	<key number>	Control key number KEY<n>
SECRET		Password for this key
TRUSTED	{TRUE, FALSE}	Is this key trusted (has it been verified)?
RESTRICT		
DEFAULT		
FLAG	{IGNORE}	Define default restrictions for NTP access control. The
NOQUERY		options are non-exclusive: all of them can be set using
NOMODIFY		a white space between them.
NOTRUST		
PURGE		Clean the Default Restriction configuration
RESTRICT		<n>
IP	<IP address>	Along with the mask, set the IP range for this restriction
MASK	<IP address>	Define the mask
FLAG	{IGNORE}	Define default restrictions for NTP access control. The
NOQUERY		options are non-exclusive: all of them can be set using
NOMODIFY		a white space between them.
NOTRUST		
PURGE		Clean the configuration for this restriction only
UP		Start the NTP service
DOWN		Stop the NTP service
PURGE		Clean all NTP configuration
SERVER		<n>
TYPE	{SERVER, PEER}	Specify if it will be a server or a peer
IP	<IP address>	Server IP address
KEY	<number>	Identify the key to be used with this server
BURST	{TRUE, FALSE}	Set if this server should send bursts of eight NTP packets, instead of one by one - if the server is reachable
IBURST	{TRUE, FALSE}	Set if this server should send bursts of eight NTP packets, instead of one by one - if the server is unreachable
MAXPOLL	<number>*	Maximum NTP request interval
MINPOLL	<number>*	Minimum NTP request interval
PURGE		Clean this server configuration

* in seconds, as "power of two" values. Ex: value 4 = 16s; value 10 = 1024s.

VISUALIZANDO O ESTADO DO SERVIÇO

- SHOW NTP PEERS

```
Remote            refid            st t when poll reach   delay  offset  jitter
==================================================================================
santuario.pads.   .INIT. 16 u      - 1024    0    0.000    0.000   0.000
 ns1.pilikia.net  .INIT.16 u       - 1024    0    0.000    0.000   0.000
*LOCAL(0)         .LOCL.5  l       - 59   64   377     0.000    0.000   0.001
```

remote

URL do servidor NTP

refid

Reference Clock Identifier

st

stratum

t

tipo do peer (local, unicast, multicast ou broadcast)

when

quando o último pacote foi recebido

pool

período de pooling (s)

reach

Reachability Register

delay

RTT até o peer (ms)

offset

atraso entre o peer e o relógio de referência (ms)

jitter

dispersão (ms)

- SHOW NTP SYSINFO

STRATUM

Posição deste servidor na hierarquia NTP.

PRECISION

Precisão deste relógio conforme definido na RFC: "this is a signed integer indicating the precision of the various clocks, in seconds to the nearest power of two. The value must be rounded to the next larger power of two; for instance, a 50-Hz (20 ms) or 60-Hz (16.67 ms) power-frequency clock would be assigned the value -5 (31.25 ms), while a 1000-Hz (1 ms) crystal-controlled clock would be assigned the value -9 (1.95 ms)."

ROOTDISPERSION

Erro máximo conforme definido na RFC: "This is a signed fixed-point number indicating the maximum error relative to the primary reference source at the root of the synchronization subnet, in seconds. Only positive values greater than zero are possible."

LISTA COMPLETA DE COMANDOS

Sintaxe básica da linguagem

```
SET       <Module name>
          <Module specific options>
SHOW      <Module name>
          <Module specific options>
DUMP      <Module name>
     ALL  <Module specific options>
HELP      <Module name>
          <Module specific options>
EXEC
     PING           <Ping parameters>
     TRACEROUTE     <Traceroute parameters>
     NETSTAT        <Netstat parameters>
     TCPDUMP        <Tcpdump parameters>
CONFIG
     INPUT          {BATCH,KEYBOARD}
     SAVE
     LOAD
     EXTERN
          SERVER    <Server name>
          USER           <User name>
          PASS           <Password>
          REMOTEFILE     <Remote file name>
          IMPORT
          EXPORT
          SHOW
          PURGE
QUIT
```

Configuração de sistema - SYSTEM

```
SET SYSTEM
     TIMETYPE       {SERVER,LOCAL}
     TIMESERVER     <IP address>
     DATE           <Date>
     TIME           <Time>
     USER           <User identifier number>
          TYPE OPERATOR,MODERATOR,ADMINISTRATOR}
          LOGIN
          PASS
          PURGE
     AAA
          AUTHENTICATION
               TACACS
                    ENCRYPT   {TRUE,FALSE}
                    DEBUG     {TRUE,FALSE}
                    SERVER    <IP address>
                    SECRET    <String>
```

```
                    ONERROR   {FAIL,CONTINUE}
                    UP
                    PURGE
               RADIUS
                    DEBUG     {TRUE,FALSE}
                    SERVER    <IP address>
                    SECRET    <String>
                    TIMEOUT   <Numeric>
                    ONERROR   {FAIL,CONTINUE}
                    UP
                    PURGE
               SHADOW
                    UP
                    DOWN
               ORDER
          AUTHORIZATION
               TACACS
               SHADOW
          ACCOUNTING
               TACACS
               SHADOW
     LOG
          ENTRY          <Entry identifier number>
               FACILITY  {ALL,AUTH,SECURITY,AUTHPRIV,CRON,DAEMON,
                         KERN,LPR, MAIL,MARK,NEWS,SYSLOG,USER,UUCP,
                         LOCAL0,LOCAL1,LOCAL2,LOCAL3,LOCAL4,LOCAL5,
                         LOCAL6,LOCAL7}
               PRIORITY  {ALL,DEBUG,INFO,NOTICE,WARNING,WARN,ERR,ERROR,
                         CRIT,ALERT,EMERG,PANIC}
               OUTPUTTYPE     {TERMINAL,REMOTE}
               PURGE          (when OUTPUTYPE=REMOTE)
               HOST      <Host address>
          UP
          DOWN
          PURGE
     UPDATE
          TYPE      {TFTP,FTP}
          FILE      <File name>
          SERVER    <IP address>
          USER      <Username>
          PASS      <Password>
          EXECUTE
     RESTART
```

Configuração de Ethernet/LAN

```
SET LAN
     LAN  <interface identifier number>
          IP
          MASK
          BROADCAST
          RESETCOUNTERS
          UP
          DOWN
          PURGE
     LAN  <interface identifier number>:<virtual device number>
          IP
          MASK
          BROADCAST
          RESETCOUNTERS
          UP
          DOWN
          PURGE
```

Configuração de interfaces WAN

```
SET WAN   <interface>
          PROTO {HDLC, FRAMERELAY,PPPS,PPPA,DIALIN,X25}
          <protocol options>
```

Protocolo HDLC

```
IP              <IP address>
MASK            <Network address>
PEER            <Peer address>
CLOCK           {INTERNAL,EXTERNAL}
SPEED           {64,128,192,256,512,768,1024,1536,2048,3072,4096,4915.2}
TXINV           {TRUE,FALSE}
INTERVAL        <numeric value>
TIMEOUT         <numeric value>
RESETCOUNTERS
```

Protocolo Frame Relay

```
PROTOCOL        {ANSI,CCITT,NONE}
DCE             {TRUE,FALSE}
CLOCK           {INTERNAL,EXTERNAL}
SPEED           {64,128,192,256,512,768,1024,1536,2048,3072,4096,4915.2}
TXINV           {TRUE,FALSE}
WAITING         {TRUE,FALSE}
BANDWIDTH       <numeric value>
T391            <numeric value>
T392            <numeric value>
N391            <numeric value>
N392            <numeric value>
N393            <numeric value>
PVC             <number>
     DLCI            <numeric value>
     MTU             <numeric value>
     IP              <IP address>
     MASK            <Network address>
     PEER            <Peer address>
     CIR             <numeric value>
     PEAK            <numeric value>
     RESETCOUNTERS
     PURGE
RESETCOUNTERS
```

Protocolo PPP Síncrono - PPPS

```
IP              <IP address>
MASK            <Network address>
PEER            <Peer address>
CLOCK           {INTERNAL,EXTERNAL}
SPEED           {64,128,192,256,512,768,1024,1536,2048,3072,4096,4915.2}
TXINV           {TRUE,FALSE}
MTU             <numeric value>
MRU             <numeric value>
RESETCOUNTERS
```

Protocolo PPP Assíncrono - PPPA

```
CONNECTION      {LEASED,NORMAL}
```

```
SPEED          {9600,14400,19200,28800,33600,38400,57600,115200,230400}
COMPRESSION    {NONE,BSD,DEFLATE,PREDICTOR1}
MAXCODESIZE
     SENT      <numeric value>
     RECEIVED  <numeric value>
FLOWCTRL  {NONE,RTSCTS,XONXOFF}
MRU       <numeric value>
MTU       <numeric value>
AUTH      {CHAP,PAP}
USER      <username>
PASS      <password>
CHAP
     MAXCHALLENGE  <numeric value>
     RESTART       <numeric value>
PAP
     AUTHREQ       <numeric value>
     TIMEOUT       <numeric value>
     RESTART       <numeric value>
DIALOUT
     DEMAND        {TRUE,FALSE}
     IDLE          <numeric value>
     PERSIST       {TRUE,FALSE}
     PPPDEFROUTE   {TRUE,FALSE}
     TYPE          {TONE,PULSE,GPRS,CUSTOM}
     NUMBER        <phone number>
     NAME          <provider name>
     SCRIPT
     HOLDOFF       <numeric value>
     MAXFAIL       <numeric value>
     KEEPALIVE
          ENABLED   {TRUE,FALSE}
          IDLELIMIT <numeric value>
          PROBE     {TRUE,FALSE}
          MINRATE   {25,50,75,100}
IPCP
     ENABLED       {TRUE,FALSE}
     LOCALIP
          ENABLED   {TRUE,FALSE}
          ADDRESS   <IP address>
          MASK      <Network address>
     REMOTEIP
          ENABLED   {TRUE,FALSE}
          ADDRESS   <IP address>
     MAXCONFIGURE  <numeric value>
     MAXFAILURE    <numeric value>
     MAXTERMINATE  <numeric value>
     RESTART       <numeric value>
LCP
     ECHOFAILURE   <numeric value>
     ECHOINTERVAL  <numeric value>
     MAXCONFIGURE  <numeric value>
     MAXFAILURE    <numeric value>
     MAXTERMINATE  <numeric value>
     RESTART       <numeric value>
RESETCOUNTERS
```

Protocolo PPP Assíncrono para DIALIN

```
SPEED     {9600,14400,19200,28800,33600,38400,57600,115200,230400}
AUTH      {CHAP,PAP}
```

```
USER      <username>
PASS      <password>
CHAP
     MAXCHALLENGE  <numeric value>
     RESTART       <numeric value>
PAP
     AUTHREQ       <numeric value>
     TIMEOUT       <numeric value>
     RESTART       <numeric value>
IPCP
     LOCALIP
          ADDRESS  <IP address>
          MASK     <Network address>
     REMOTEIP
          ADDRESS  <IP address>
     MAXCONFIGURE  <numeric value>
     MAXFAILURE    <numeric value>
     MAXTERMINATE  <numeric value>
     RESTART       <numeric value>
DIALBACKUP
     ENABLED       {TRUE,FALSE}
     INTERFACE     <synchronous interface>
RESETCOUNTERS
```

Protocolo X25

```
CLOCK     {INTERNAL,EXTERNAL}
SPEED     {64,128,192,256,512,768,1024,1536,2048,3072,4096,4915.2}
TXINV     {TRUE,FALSE}
MODE      {DTE,DCE}
LAPB
     EXTENDEDMODE  {TRUE,FALSE}
     WINDOWSIZE         <numeric value>
EXTENDED  {TRUE,FALSE}
NEGOTIATE
     WINDOWSIZE         {TRUE,FALSE}
     PACKETSIZE         {TRUE,FALSE}
     REVERSECHARGING    {TRUE,FALSE}
ROUTES
     ADD       {X121 address}
     REMOVE    {X121 address}
PROTOCOL  {IP,IPX}
SVC  <number>
(when PROTOCOL=IP)
     X121BIND           {X121 address}
     WAITCONNECTION     {TRUE,FALSE}
     TOIPX              {X121 address}
     IP                 {IP address}
     PEER               {Peer address}
     MASK               {Network mask}
     MTU                <numeric value>
     PURGE              (when PROTOCOL=IPX)
     X121BIND           {X121 address}
     WAITCONNECTION     {TRUE,FALSE}
     TOIPX              {X121 address}
     NET                {IPX net number}
     NODE               {IPX node address}
     PURGE
RESETCOUNTERS
```

Configuração de Rotas Estáticas - ROUTES

```
SET ROUTES
     ROUTE          <route identifier number>
          DEVICE    {NONE,<Interface name>}
          NET       <Net address>
          MASK      <Mask address>
          GATEWAY   <Gateway address>
          COST      <Route cost>
          PURGE
     DEFAULT
          GW1       <IP address>
          COST1     <numeric value>
          GW2       {PURGE,<IP address>}
          COST2     <numeric value>
          POLL      <numeric value>
          DEVICE    {NONE,<Interface name>}
          PURGE
     PURGE
```

Configuração de Linha Backup - BACKUP

```
SET BACKUP
     TYPE      {ASYNCH,IP,NONE}
     BACKUP    <backup identifier number>
     (when TYPE=ASYNCH)
          FROM      <Interface>
          TO        <Interface>
          IDLELIMIT <1...65000>
          PROBE     {TRUE,FALSE}
          MINRATE   {25,50,75,100}
          PURGE
     (when TYPE=IP)
          FROM      <Interface>
          TO        <Interface>
          TARGET    <Target IP address>
          GATEWAY   <Gateway IP address>
          PURGE
     UP
     DOWN
     PURGE
```

Configuração de Roteamento Dinâmico RIP

```
SET RIPZ
     DEFAULTMETRIC <numeric value>
     VERSION       {1,2}
     <INTERFACE>
          ENABLED   {TRUE,FALSE}
          TYPE      {ACTIVE,PASSIVE}
          RECEIVEVERSION     {1,2,12,DEFAULT}
          SENDVERSION        {1,2,12,DEFAULT}
          AUTH
               TYPE      {NONE,SIMPLE,MD5}
               PASS      <password>
          IN   <In identifier number>
               LIST      <LIST>
               PURGE
```

```
                OUT  <Out identifier number>
                     LIST      <LIST>
                     PURGE
           LIST <List identifier number>
                ENTRY          <Entry identifier number>
                     ADDRESS   <Address>
                     MASK      <Network mask>
                     TYPE      {PERMIT,DENY}
                     PURGE
                PURGE
           UP
           DOWN
           PURGE
```

Configuração de Roteamento Dinâmico OSPF

```
      SET OSPFZ
           ROUTERID            <Router id number (x.y.z.w)>
           REDIST-CONNECTED    {TRUE,FALSE}
           REDIST-STATIC       {TRUE,FALSE}
           REDIST-RIP          {TRUE,FALSE}
           RFC1583             {TRUE,FALSE}
           DEBUG
                EVENT          {TRUE,FALSE}
                INTERFACE      {TRUE,FALSE}
                REDISTRIBUTE   {TRUE,FALSE}
                PACKET         {TRUE,FALSE}
           LOG
                STDOUT    {TRUE,FALSE}
                SYSLOG    {TRUE,FALSE}
                TRAP      {NONE,EMERGENCIES,ALERTS,CRITICAL,ERRORS, WARNINGS,
                          NOTIFICATIONS,INFORMATIONAL, DEBUGGING}
           AREA <area identifier number>
                ID        <Area ID number (x.y.z.w)>
                AUTH      {NONE,SIMPLE,MD5}
                STUB      {TRUE,FALSE}
                COST      <numeric value>
                VIRTUAL
                     ENABLED   {TRUE,FALSE}
                     TRANSIT   <IP address>
                RANGE          <range identifier number>
                     ADDRESS   <IP address>
                     MASK      <IP address>
                     PURGE
                EXPORT    <Export identifier number>
                     LIST <LIST>
                     PURGE
                IMPORT    <Import identifier number>
                     LIST <LIST>
                     PURGE
                PURGE
           LIST      <List identifier number>
                ENTRY          <Entry identifier number>
                     ADDRESS   <Address>
                     MASK      <Network mask>
                     TYPE      {PERMIT,DENY}
                     PURGE
                PURGE
           NETWORK   <Network identifier number>
```

```
            ADDRESS   <Address>
            MASK      <Network mask>
            AREA      <Area identifier>
            PURGE
        <INTERFACE>
            DIGEST    <Digest identifier number>
                KEYID     <numeric value>
                PASS      <Password>
                PURGE
            PASS      <Password>
            NOPASS
            PRIORITY  <numeric value>
            COST      <numeric value>
            HELLOINTERVAL <numeric value>
            DEADINTERVAL  <numeric value>
            DELAY         <numeric value>
            RETRANSMISION <numeric value>
        UP
        DOWN
        PURGE
```

Configuração de Roteamento Dinâmico Avançado - ZEBRA

```
SET ZEBRA
    ROUTES
    OSPF
    RIP
    UP
    DOWN
```

Configuração de NAT

```
SET NAT
    MASQUERADE          <Masquerad identifier number>
        INTERFACE       <Interface>
        ADDRESS         <IP address>
        MASK            <Network mask>
    REDIRECT        <Redirect identifier number>
        FROMINTERFACE       <Interface>
        FROMADDRESS         <IP address>
        FROMPORT            <numeric value>
        TOADDRESS           <IP address>
        TOPORT              <numeric value>
        PROTOCOL            <ICMP | UDP | TCP | protocol number>
        PURGE
    EXCLUSION <Exclusion identifier number>
        ADDRESS         <IP address>
        MASK            <Network address>
        TOADDRESS       <IP address>
        TOMASK          <Network address>
        TOINTERFACE     <Interface>
        PURGE
    NAT  <NAT 1:1 identifier number>
        SOURCEADDRESS       <IP address>
        SOURCEMASK          <Network address>
        DESTINATIONADDRESS <IP address>
        DESTINATIONMASK     <Network address>
        PURGE
```

Configuração de Túneis GRE

```
SET GRE
     GRE  <channel identifier number>
          INTERFACE      <Interface name>
          REMOTE         <IP address>
          TUNNELLOCAL    <IP address>
          TUNNELREMOTE   <IP address>
          KEEPALIVETIME  <1...300>
          KEEPALIVE      {TRUE,FALSE}
          UP
          DOWN
          PURGE
     UP
     DOWN
     PURGE
```

Configuração de VPN PPTP

```
SET PPTP
     CHAP <CHAP identifier number>
          DOMAIN    <Domain name>
          USER
          PASS
          PURGE
     CLIENT    <Client identifier number>
          DOMAIN    <CHAP identifier>
          SERVER    <IP of remote server>
          UP
          DOWN
          PURGE
     SERVER
          LISTEN         <Interface name>
          LOCALIP        <local ip identifier number>
               BEGIN     <IP address>
               END       <IP address>
               PURGE
          REMOTEIP  <remote ip identifier number>
               BEGIN     <IP address>
               END       <IP address>
               PURGE
          UP
          DOWN
          PURGE
     PURGE
```

Configuração de VPN L2TP

```
SET L2TP
     LAC  <LAC identifier number>
          ID        <numeric value>
          LNS       <IP address>
          REDIAL    {TRUE,FALSE}
          PURGE
     LNS
          IPPOOL    <Ippool identifier number>
               BEGIN     <IP address>
               END       <IP address>
               PURGE
```

```
            LACRANGE  <Range identifier number>
                 BEGIN     <numeric value>
                 END       <numeric value>
                 PURGE
            LOCALIP   <IP address>
            UP
            PURGE
       AUTH {NONE,PAP,CHAP}
       USER <User identifier number>
            USERNAME
            PASS
            PURGE
       UP
       DOWN
       PURGE
```

Configuração de VPN IPSEC

```
SET IPSEC
     IPSEC          <IPSEC identifier number>
          INTERFACE      <Interface name>
          PURGE
     CHANNEL   <Channel identifier number>
          NAME      <Channel name string>
          LEFT
               ADDRESSTYPE    {BINDED,ANY,DEFAULTROUTE,OPPORTUNISTIC}
               SUBNET         {TRUE,FALSE}
               NET            <IP net address>
               MASK           <Netmask address>
               USEGATEWAY     {TRUE,FALSE}
               GATEWAY        <Gateway address>
          RIGHT
               ADDRESSTYPE    {USER,ANY,DEFAULTROUTE,OPPORTUNISTIC}
               ADDRESS        <IP address>
               SUBNET         {TRUE,FALSE}
               NET            <IP net address>
               MASK           <Netmask address>
               USEGATEWAY     {TRUE,FALSE}
               GATEWAY        <Gateway address>
          KEY
               AUTH           {ESP,AH}
               AUTHBY         {SECRET,RSA}
               PASS           <Password>
               BITS           {128,256,512,1024,2048}
               PEERPUBLICKEY
               LOCALSIDE      {LEFT,RIGTH}
               GENERATEKEY
               NEGRESTART
                    TIME      <numeric value>
                    MARGIN    <numeric value>
               KEYLIFE        <numeric value>{H,M,S}
               ISAKMP         <numeric value>{H,M,S}
               RETRIES        <numeric value>
               PERFECTFORWARD{TRUE,FALSE}
          DPDACTION           {CLEAR,HOLD,NONE}
          DPDDELAY            <numeric value>
          DPDTIMEOUT          <numeric value>
          PURGE
          COMPRESS            {TRUE,FALSE}
          IKE                 <Identifier number>
```

```
          ESP                 <Identifier number>
     FRAGICMP       {TRUE,FALSE}
     HIDETOS        {TRUE,FALSE}
     UNIQUEIDS      {TRUE,FALSE}
     PACKETDEFAULT  {PASS,DROP,REJECT}
     NATT           {TRUE,FALSE}
     TYPE           {INTERFACE,DEFAULTROUTE}
     UP
     DOWN
     PURGE
```

Configuração de Protocolo DHCP

```
SET DHCP
     TYPE      {NORMAL,RELAY}
(when TYPE=NORMAL)
     UNKNOWNCLIENTS     {TRUE,FALSE}
     SHAREDNETWORK      {TRUE,FALSE}
     SERVERNAME         <Server name>
     SUBNET        <Subnet identifier number>
          ADDRESS       <IP network address>
          MASK          <Network mask address>
          RANGEIP       {TRUE,FALSE}
          RANGEBEGIN    <IP address>
          RANGEEND      <IP address>
          LEASE         <numeric value>
          AUTHORITATIVE {TRUE,FALSE}
          DNSDOMAIN     <DNS domain name>
          DNS           <DNS identifier number>
               ADDRESS   <IP address>
               PURGE
          ROUTER    <Router identifier number>
               ADDRESS   <IP address>
               PURGE
          WINS <Wins identifier number>
               ADDRESS   <IP address>
               PURGE
          PURGE
     HOST <Host identifier number>
          NAME      <Hostname string>
          MAC       <Hardware address>
          ADDRESS   <IP address>
          DNSDOMAIN <DNS domain name>
          DNS       <DNS identifier number>
               ADDRESS   <IP address>
               PURGE
          ROUTER    <Router identifier number>
               ADDRESS   <IP address>
               PURGE
          WINS <Wins identifier number>
               ADDRESS   <IP address>
               PURGE
          PURGE
     UP
     DOWN
     PURGE
(when TYPE=RELAY)
     SERVER        <IP address of the server>
     ALLINTERFACES {TRUE,FALSE}
     LISTEN        <Listen identifier number>
```

```
            INTERFACE <Interface name>
            PURGE
        UP
        DOWN
        PURGE
```

Configuração de Protocolo SNMP

```
SET SNMP
        LOCATION
        AGENTADDRESS
            ADDRESS        <IP address>
            PORT
            PURGE
        CONTACT
        ROCOMMUNITY
        RWCOMMUNITY
        TRAPAUTHFAILURE          {TRUE,FALSE}
        MANAGER             <Manager identifier number>
            ADDRESS   <IP address>
            TRAP      {TRUE,FALSE}
            PURGE
        UP
        DOWN
        PURGE
```

Configuração de Protocolo IPX

```
SET IPX
        <INTERFACE>    (when interface is a lan)
            FRAMETYPE {802.2,802.2TR,802.3,SNAP,ETHERII}
            NETWORK   <IPX Network address>
            UP
            PURGE
            (when interface is asynch ppp and TYPE=CLIENT)
            TYPE      {CLIENT,SERVER}
            UP
            PURGE
            (when interface is asynch ppp and TYPE=SERVER)
            TYPE      {CLIENT,SERVER}
            NETWORK   <IPX Network address>
            NODE      <IPX Node number>
            UP
            PURGE
            (when interface is not a lan)
            NETWORK   <IPX Network address>
            NODE      <IPX Node number>
            UP
            PURGE
```

Configuração de Protocolo BRIDGE

```
SET BRIDGE
        BRIDGE    <Bridge identifier number>
            NAME           <Interface name>
            AGEING         <numeric value>
            ADDRESS        <IP address>
            GARBAGEINTERVAL    <numeric value>
            SPANNINGTREE   {TRUE,FALSE}
```

```
PURGE                <INTERFACE>
    ENABLED   {TRUE,FALSE}
```

Configuração de Firewall

```
SET FIREWALL
INPUT
    POLICY {ACCEPT,DROP}
    RULE       <Rule identifier number>
        PROTOCOL                {TCP,UDP,ICMP,ALL}
        PROTOCOLINVERTED        {TRUE,FALSE}
        ACTION                  {ACCEPT,REJECT,DROP,RETURN,LOG}
        FRAGMENT
            ENABLED    {TRUE,FALSE}
            WHICH      {FIRST,REMAIN}
        SOURCE
            INTERFACE                <Interface name>
            INTERFACEINVERTED        {TRUE,FALSE}
            ADDRESS                  <IP address>
            MASK                     <IP address>
            ADDRESSINVERTED          {TRUE,FALSE}
        DESTINATION
            INTERFACE            <Interface name>
            INTERFACEINVERTED    {TRUE,FALSE}
            ADDRESS              <IP address>
            MASK                 <IP address>
            ADDRESSINVERTED      {TRUE,FALSE}
        PACKETTYPE
            ENABLED              {TRUE,FALSE}
            UNICAST
            BROADCAST
            MULTCAST
        MAC
            ENABLED         {TRUE,FALSE}
            SOURCE          <MAC address>
        LIMIT
            ENABLED         {TRUE,FALSE}
            RATE            <numeric value>{D,H,M,S}
            BURST           <numeric value>
        CONNECTIONSTATE
            ENABLED         {TRUE,FALSE}
            INVERTEDLOGIC   {TRUE,FALSE}
            INVALID         {TRUE,FALSE}
            ESTABLISHED          {TRUE,FALSE}
            NEW             {TRUE,FALSE}
            RELATED         {TRUE,FALSE}
        TOS
            ENABLED    {TRUE,FALSE}
            INVERTED   {TRUE,FALSE}
            VALUE      {MINIMIZEDELAY, MAXIMIZETHROUGHTPUT,
                       MAXIMIZERELIABILITY, MINIMIZECOST, NORMALSERVICE}
        TIME
            ENABLED    {TRUE,FALSE}
            START      <Time>
            END        <Time>
            SUNDAY     {TRUE,FALSE}
            MONDAY     {TRUE,FALSE}
            TUESDAY    {TRUE,FALSE}
            WEDNESDAY  {TRUE,FALSE}
            THURSDAY   {TRUE,FALSE}
            FRIDAY     {TRUE,FALSE}
```

```
            SATURDAY   {TRUE,FALSE}
        UDP
            SPORT                <numeric value>[-<numeric value>]
            DPORT                <numeric value>[-<numeric value>]
        TCP
            SPORT                <numeric value>[-<numeric value>]
            DPORT                <numeric value>[-<numeric value>]
            SYNENABLED           {TRUE,FALSE}
            SYNINVERTED          {TRUE,FALSE}
            TCPOPTION            <numeric value>=1 and <= 65536>
            TCPOPTIONINVERTED    {TRUE,FALSE}
            FLAGS
                INVERTED         {TRUE,FALSE}
                LIST
                   SYN       {TRUE,FALSE}
                   ACK       {TRUE,FALSE}
                   FIN       {TRUE,FALSE}
                   RST       {TRUE,FALSE}
                   URG       {TRUE,FALSE}
                   PSH       {TRUE,FALSE}
                   ALL       {TRUE,FALSE}
                   NONE      {TRUE,FALSE}
                ENABLED
                   SYN       {TRUE,FALSE}
                   ACK       {TRUE,FALSE}
                   FIN       {TRUE,FALSE}
                   RST       {TRUE,FALSE}
                   URG       {TRUE,FALSE}
                   PSH       {TRUE,FALSE}
                   ALL       {TRUE,FALSE}
                   NONE      {TRUE,FALSE}
        ICMP
            ENABLED    {TRUE,FALSE}
            INVERTED   {TRUE,FALSE}
            TYPE  {ECHO-REPLY, DESTINATION-UNREACHABLE,
                   NETWORK-UNREACHABLE, HOST-UNREACHABLE,
                   PROTOCOL-UNREACHABLE, PORT-UNREACHABLE,
                   FRAGMENTATION-NEDEED, SOURCE-ROUTE-FAILED,
                   NETWORK-UNKNOWN, HOST-UNKNOWN, NETWORK-PROHIBITED,
                   HOST-PROHIBITED, TOS-NETWORK-UNREACHABLE,
                   TOS-HOST-UNREACHABLE,COMMUNICATION-PROHIBITED,
                   HOST-PRECEDENCE-VIOLATION, PRECEDENCE-CUT-OFF,SOURCE-QUENCH,
                   REDIRECT, NETWORK-REDIRECT, HOST-REDIRECT,
                   TOS-NETWORK-REDIRECT, TOS-HOST-REDIRECT, ECHO-REQUEST,
                   ROUTER-ADVERTISEMENT, ROUTER-SOLICITATION,
                   TIME-EXCEEDED, TTL-ZERO-DURING-TRANSIT,
                   TTL-ZERO-DURING-REASSEMBLY, PARAMETER-PROBLEM,
                   IP-HEADER-BAD, REQUIRED-OPTION-MISSING, TIMESTAMP-REQUEST,
                   TIMESTAMP-REPLY,ADDRESS-MASK-REQUEST,  ADDRESS-MASK-REPLY}
OUTPUT
    <Same as the INPUT chain>
FORWARD
    <Same as the INPUT chain>
QOS
    <Same as the INPUT chain, without POLICY and including subtree below>
        RULE
                <Rule identifier number>
        MARK
                <numeric value>
REJET
      ENABLED       {TRUE,FALSE}
```

```
        WITH          {ICMP-NET-UNREACHABLE,NET-UNREACH,ICMP-HOST-UNREACHABLE,
                      HOST-UNREACH,ICMP-PROTO-UNREACHABLE,PROTO-UNREACH,
                      ICMP-PORT-UNREACHABLE,PORT-UNREACH,ICMP-NET-PROHIBITED,
                      NET-PROHIB,ICMP-HOST-PROHIBITED,HOST-PROHIB,TCP-RESET}
LOG
        ENABLED       {TRUE,FALSE}
        ENABLED
        LEVEL         {DEBUG,INFO,NOTICE,WARNING,ERROR,CRIT,ALERT,EMERG,PANIC}
        PREFIX         <string>
        NO-PREFIX
        TCPSEQUENCE   {TRUE,FALSE}
        TCPOPTIONS    {TRUE,FALSE}
        IPOPTIONS     {TRUE,FALSE}
CHAIN  <Chain identifier number>
    <Same as the INPUT chain, without POLICY and including subtree below>
NAME
    <User chain name>
PURGE
```

Configuração de Qualidade de Serviço IP - QOS

```
SET QOS   <INTERFACE>
          ROOT-HTB  <Commands for HTB node (Set this will release all tree
                    if root is not already a htb node)>
          ROOT-SFQ  <Commands for SFQ node (Set this will release all tree
                    if root is not already a sfq node)>
          ROOT-TBF  <Commands for TBF node (Set this will release all tree
                    if root is not already a tbf node)>
          HTB  <numeric value>:[< numeric value >]
               NEW-HTB   <Commands for HTB node (This will create a new
               child node)>
               NEW-SFQ   <Commands for SFQ node (This will create a new
               child node)>
               NEW-TBF   <Commands for TBF node (This will create a new
               child node)>
               HANDLE    <numeric value>:[< numeric value >]
               RATE      <numeric value>{BPS,KBPS,MBPS,KBIT,MBIT}
               BURST     <numeric value>{B,KB,MB,KBIT,MBIT}
               CEIL      <numeric value>{BPS,KBPS,MBPS,KBIT,MBIT}
               PRIORITY  <numeric value>
               PURGE
               HTB  <numeric value>:[< numeric value >] <Commands for HTB
                    node>
               SFQ  <numeric value>:[< numeric value >] <Commands for SFQ
                    node>
               TBF  <numeric value>:[< numeric value >] <Commands for TBF
                    node>
               FILTER    <Filter handle value>
                    HANDLE    <numeric value>
                    PRIORITY  <numeric value>
                    PROTOCOL  {IP,ICMP,UDP,TCP}
                    PURGE
               NEW-FILTER         <Commands for filter>
          SFQ  <numeric value>:[< numeric value >]
               HANDLE        <numeric value>:[< numeric value >]
               PERTURBATION  <numeric value>{S,MS,US}
               QUANTUM       <numeric value>{B,KB,MB,KBIT,MBIT}
```

```
                    PURGE
                    FILTER        <Filter handle value> <Commands for filter>
                    NEW-FILTER    <Commands for filter>
               TBF  <numeric value>:[< numeric value >]
                    HANDLE    <numeric value>:[< numeric value >]
                    RATE      <numeric value>{BPS,KBPS,MBPS,KBIT,MBIT}
                    BURST     <numeric value>{B,KB,MB,KBIT,MBIT}
                    MPU       <numeric value>{BPS,KBPS,MBPS,KBIT,MBIT}
                    PEAKRATE  <numeric value>{BPS,KBPS,MBPS,KBIT,MBIT}
                    MTU       <numeric value>{B,KB,MB,KBIT,MBIT}
                    TYPE      {LIMIT,LATENCY}
                    LATENCY   <numeric value>{S,MS,US}
                    LIMIT     <numeric value>{B,KB,MB,KBIT,MBIT}
                    PURGE
                    NEW-FILTER    <Commands for filter>
                    FILTER        <Filter handle value> <Commands for filter>
```

Configuração de Protocolo VRRP

```
SET VRRP
     STATE          <MASTER/BACKUP>
     VRID           <integer number> = 1 and <=255>
     INTERFACE      <interface name>
     IP             <Ip address>
     PRIORITY       <integer number> = 1 and <=255>
     ADVERT         <integer number> = 1 and <=1000>
     AUTH           <NONE, PASS, AH>
     PREEMPT        <TRUE, FALSE>
     PASSWORD       <password in hexadecimal format. (max. 8 chars)>
     NO-PASSWORD
     UP
     DOWN
     PURGE
```

Configuração de IP Accounting

```
SET IPACCT
     STATUS    <UP|DOWN>
     ADD
               AGGREGATE <SOCKET FROM socket TO socket INTO socket>
               AGGREGATE <IP ADDR ip/masklen STRIP maskbits>
               USER user MODE <ADMIN|IBACKUP|DEFAULT|VIEWONLY|DENY>
     MEM        <amount of memory in kylobytes, valid values are 0-1000>
     TTE        <time to live value>
     PURGE
     <Interface name>
          ENABLE <TRUE|FALSE>
          PROMISC
          INPUTONLY
          BPF <Berkeley Packet Filter according tcpdump man page>
```

Configuração da Tabela ARP

```
SET ARP
     DEL  <index arp table>
     FLUSH
```

Configuração de PPPoE (PPP over Ethernet)

```
SET PPPOE
     TYPE           {CLIENT,RELAY}
     INTERFACE      <interface name>
     DEBUG          {TRUE|FALSE}
     TIMEOUT        <numeric value>
     NAME           <service name>
     CONCENTRATOR   <concentrator name>
     USER           <username>
     PASS           <password>
     MAXCODESIZE
          SENT      <numeric value>
          RECEIVED  <numeric value>
     MRU       <numeric value>
     MTU       <numeric value>
     AUTH      {PAP,CHAP}
     PAP
          AUTHREQ   <numeric value>
          TIMEOUT   <numeric value>
          RESTART   <numeric value>
     CHAP
          MAXCHALLENGE  <numeric value>
          RESTART       <numeric value>
     DIALOUT
          DEMAND        {TRUE,FALSE}
          PERSIST       {TRUE,FALSE}
          PPDEFROUTE    {TRUE,FALSE}
     LCP
          ECHOFAILURE   <numeric value>
          ECHOINTERVAL  <numeric value>
          MAXCONFIGURE  <numeric value>
          MAXFAILURE    <numeric value>
          MAXTERMINATE  <numeric value>
          RESTART       <numeric value>
     DOWN
     UP
     PURGE
```

Configuração de Interface LoopBack

```
SET LOOPBACK
     LO: <interface number>
          IP   <IP address>
          MASK <network mask>
          RESETCOUNTERS
          UP
          DOWN
          PURGE
```

Configuração de XOT (X25 over TCP)

```
SET XOT
     REMOTE_IP      <IP address>
     DEBUG_LEVEL    {0,1,2,3}
     ROUTES
          ADD <route address>
          DELETE
     UP
     DOWN
     PURGE
```

ATUALIZAÇÃO DO SISTEMA OPERACIONAL

Para atualizar o firmware do sistema operacional do NetRouter 2G, execute os procedimentos a seguir:

1. Coloque o arquivo com a versão de firmware a ser instalada no NetRouter 2G no diretório de um servidor TFTP acessível pelo roteador (caso necessário, consulte o capítulo sobre Instalação e configuração inicial). O arquivo do sistema operacional deve ter uma extensão .dwn.

2. Execute o CLI.

3. Entre com o comando **SET SYSTEM UPDATE TYPE TFTP SERVER <ip_do_servidor_tftp> USER <usuário> PASS <senha> EXECUTE**. O equipamento iniciará o processo de atualização do firmware.

A atualização também pode ser feita via WebConfig, como descrito a seguir:

1. Coloque o arquivo com a versão de firmware a ser instalada no NetRouter 2G no diretório de um servidor TFTP acessível pelo roteador (caso necessário, consulte o capítulo sobre Instalação e configuração inicial). O arquivo do sistema operacional deve ter uma extensão .dwn.

2. Abra um browser e entre com o IP do equipamento.

3. Na janela de comandos, execute o passo 3 da atualização do sistema via CLI.

O arquivo com a última versão de firmware do produto encontra-se no site da Digitel S.A. (http://www.digitel.com.br), na página de suporte aos roteadores.

IMPORTANTE!
Caso ocorra uma interrupção na alimentação do NetRouter 2G durante o processo de atualização do firmware, é possível que o equipamento não funcione corretamente. Se isso ocorrer, proceda de acordo com o descrito no capítulo Operação.

ATUALIZAÇÃO DO BOOTLOADER (NR2GBoot)

Em casos especiais e somente com a indicação da Digitel, pode ser necessário atualizar o firmware do Bootloader do NetRouter 2G. Para isso, é preciso conectar um terminal à porta Console do NetRouter 2G e executar o seguinte procedimeto:

1. Ligue o NetRouter 2G e, no prompt do NR2GBoot, entre com o comando **mode test**. Se o roteador já estiver ligado, execute o comando **SET SYSTEM RESTART** na interface de configuração CLI.

2. A seguinte mensagem será apresentada:

```
NetRouter 2G Test Mode
Press SPACE to stop autobooting in 5 seconds
```

Pressione a barra de espaço antes que os 5 segundos se esgotem e execute o comando **mode test**. No caso do modelo 4200, posicione a dip 2 para baixo.

3. Verifique as configurações de endereçamento IP do servidor TFTP do Bootloader e coloque o arquivo contendo o novo firmware no servidor TFTP, que deve ser alcançável pelo NetRouter 2G através de sua interface LAN0. O arquivo de atualização do Bootloader deve ter uma extensão .boot.

4. No prompt do Bootloader (**NR2GBoot>**), digite o comando **upboot <nome do arquivo>** e pressione enter.

5. Após o processo de atualização (se bem-sucedido), a seguinte mensagem será exibida:

```
NetRouter 2G boot correctly updated!
```

6. Agora, execute o comando **clear now** para que os valores default do novo Bootloader sejam utilizados.

7. Execute o comando **`restart now`** para validar a carga do novo Bootloader no NetRouter 2G.

8. A seguinte mensagem será apresentada:

```
NetRouter 2G Test Mode
Press SPACE to stop autobooting in 5 seconds
```

Pressione a barra de espaço antes que os 5 segundos se esgotem.

9. Caso seja recomendado pela Digitel, deve-se proceder também à atualização do firmware do sistema operacional (ver os itens Recuperando a versão de firmware e Limpando a configuração do roteador, no capítulo Operação). Caso contrário, posicione as dip-switches no modo Automático e execute o comando **`restart now.`**

IMPORTANTE!
Uma eventual interrupção na alimentação do NetRouter 2G durante a execução do item 5 pode causar danos ao equipamento, de tal forma que ele não funcione mais. Se isso ocorrer, entre em contato com o suporte da Digitel.

Especificações gerais	
Capacidade	NR-2G 4200 • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 2 portas WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores) • 2 slots para a instalação de módulos opcionais NR-2G 3201 • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores) NR-2G 3211 • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores) NR-2G 3212 • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores) • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3214 • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores) • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3218 • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 2 portas WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores) • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3251 GPRS • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta Dual Band GSM/GPRS NR-2G 3252 GPRS • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta Dual Band GSM/GPRS • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3254 GPRS • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta Dual Band GSM/GPRS • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3258 GPRS • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta Dual Band GSM/GPRS • 1 porta WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores) • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232)

	NR-2G 3261 EDGE • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta Quadri Band GSM (GPRS/EDGE) NR-2G 3262 EDGE • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta Quadri Band GSM (GPRS/EDGE) • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3264 EDGE • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta Quadri Band GSM (GPRS/EDGE) • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3268 EDGE • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta Quadri Band GSM (GPRS/EDGE) • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) • 1 porta WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores) NR-2G 3281 CDMA • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta CDMA NR-2G 3282 CDMA • 1 porta LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta CDMA • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3284 CDMA • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta CDMA • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) NR-2G 3288 CDMA • 2 portas LAN 10/100 Mbps com autosense (detecção automática de velocidade) • 1 porta CDMA • 1 porta WAN auxiliar, assíncrona (interface V.24/RS-232) • 1 porta WAN multiinterface (V.24, V.36, V.35 e G.703 com adaptadores)

Portas LAN LAN edição)	• Conectores: RJ45 UTP sem função crossover • Monitoração de estado do enlace, atividade e colisão no painel frontal (leds multifuncionais) • Protocolo de acesso ao meio Ethernet de acordo com as normas ISO/IEC 8802-3 CSMA/CD (Ethernet; 4ª edição; julho/93) e ANSI/IEEE Std 802.3 CSMA/CD LAN (Ethernet; 4ª
Portas WAN (Multiinterface)	• Conector: dependente do cabo/adaptador de interface: conector DB25 macho (ISO 2110) para interface V.24/V.28 e V.35/DB25; conector MRAC34 macho (ISO 2593) para interface V.35/ MRAC34; conector macho DB37 (ISO 4902) para interface V.36; adaptador para interface G.703 • Pinagem: tipo DTE • Transmissão/recepção: modo síncrono HDLC ou modo assíncrono • Velocidades: o modo síncrono HDLC opera somente com relógio externo (qualquer velocidade menor ou igual a 5 Mbps); o modo assíncrono opera com as velocidades de 9600, 14400, 19200, 28800, 38400, 57600, 115200 e 230400 bps • Monitoração dos sinais de interface TD e RD no painel frontal • Protocolos PPP, HDLC-Cisco e Frame Relay
Porta WAN auxiliar assíncrona	• Conector: dependente do cabo/adaptador de interface: conector DB25 macho (ISO 2110) para interface V.24/V.28, utilizando cabo CONSOLE RJ e adaptador MODEM DB25 • Pinagem: tipo DTE • Transmissão/recepção: modo assíncrono • Velocidades: 9600, 14400, 19200, 28800, 38400, 57600, 115200 e 230400 bps • Monitoração dos sinais de interface TD e RD no painel frontal (AUX) • Protocolo PPP assíncrono

Porta
Dual Band
GSM
	• Freqüência: GSM 900 MHz e 1800 MHz
	• Acompanha antena com:
	  • Ganho: 3 dB
	  • Tamanho do cabo: 3 metros
	  • Conector: FME fêmea
	  • Base magnética

Porta
Quadri Band
GSM
	• Freqüência: GSM 800 MHz, 900 MHz, 1800 MHz e 1900 MHz
	• Acompanha antena com:
	  • Ganho: 36 dB
	  • Tamanho do cabo: 3 metros
	  • Conector: SMA macho
	  • Base magnética

Porta
CDMA
	• Freqüência: CDMA 800 MHz e 1900 MHz
	• Acompanha antena com:
	  • Conector: SMA macho
	  • Sem cabo

Protocolos		
IETF (Internet Engineering Task Force)		
Protocolo	RFC	Título
CRTP	2508/3345	CRTP
UDP	0768	User Datagram Protocol
TFTP	0783	TFTP Protocol (revision 2)
IP	0791	Internet Protocol
ICMP	0792	Internet Control Message Protocol
TCP	0793	Transmission Control Protocol
IP	0815	IP datagram reassembly algorithms
ARP	0826	Address Resolution Protocol
TELNET	0854	Telnet Protocol Specification
TELNET	0861	Telnet Extended Options - List Options
IP	0894	Standart for the transmission of IP datagrams over Ethernet networks
IP-E	0894	Internet Protocol on Ethernet Networks
	0919	IP Broadcast Datagrams
	0922	IP Broadcast Datagrams with Subnets
	0950	IP Subnets Extension
FTP	0959	File Transfer Protocol
DNS	1034	Domain Names - Concepts and Facilities
DNS	1035	Domain Names - Implementation and Specification
RIP V1 e V2	1058/1723	RIP - Routing Information Protocol
	1122	Requeriments for Internet host - communication layers
	1123	Requeriments for Internet host - Application and Support
IP-CMPRS	1144	Compressing TCP/IP Headers
SMI	1155	Structure of Management Information
MIB-I	1156	Management Infomation Base-I
SNMP	1157	Simple Network Management Protocol
	1166	Internet numbers
MIB-II	1213	Management Information Base-II
SNMP-TRAPS	1215	Defining traps for use with SNMP
SFQ	1254	Gateway Congestion Control Survey/Stochastic Fairness Queuening
MD5	1321	The MD5 Message - Digest Algorithm
PPP-IPCP	1332	PPP IP Control Protocol
PAP	1334	PPP Autentication Protocol
TFTP	1350	Trivial File Transfer Protocol rev.2
X.25	1356	Multiprotocol Interconnect over X.25 and ISDN in the Packet Mode
FRAME RELAY	1490	Multiprotocol Interconnect over Frame Relay, IETF
TACACS	1492	Access Control Protocol
XOT	1613	X.25 over TCP
NAT	1631	The IP Network Address Translator
IPX	1634	Novel IPX over Various WAN Media (IPX WAN)
Bridge	1638	PPP Bridging Control Protocol

SNMP	1643	Definitions of Managed Object for the Ethernet - Like Interfaces Type
PPP	1661	Point-to-Point (PPP)
PPP-HDLC	1662	PPP in HDLC Framing
	1700	Assigned Numbers
SNMP	1902	SNMPv2
IP	1918	Address Allocation for Private Internets
CHAP	1994	PPP Challenge Handshake
RIP-2 MD5	2082	RIP-2 MD5 Authentication
DPD	2119	Key words for use in RFCs to Indicate Requirement Levels
DHCP SERVER	2131/1542	Dynamic Host Configuration Protocol
DHCP RELAY	2132/1542	DHCP Relay
RADIUS	2865/2866	Radius Accounting
OSPF	2328	Open Shortest Path First
VRRP	2338	Virtual Routing Redundancy Protocol
PF_KEY	2367	PF_KEY Key Management API, Version 2
OSPF-LSA	2370	The OSPF Opaque LSA Option
INVERSE ARP	2390	Inverse Address Resolution Protocol
IPComp	2393	IP Payload Compression Protocol (IPComp)
IPSEC	2401	Security Architecture for the Internet Protocol
AH	2402	IP Authentication Header
HMAC-MD5	2403	The Use of HMAC-MD5-96 within ESP and AH
HMAC-SHA1	2404	The Use of HMAC-SHA1-96 within ESP and AH
ESP DES-CBC	2405	The ESP DES-CBC Cipher Algorithm With Explicit IV
ESP	2406	IP Encapsulation Security Payload (ESP)
ISAKMP	2407	The Internet IP Security Domain of Interpretation for ISAKMP
ISAKMP	2408	Interner Security Association and Key Management Protocol (ISAKMP)
IKE	2409	The Internet Key Exchange (IKE)
OAKLEY	2412	The OAKLEY Key Determination Protocol
3DES	2420	The PPP Triple-DES Encryption Protocol
RSA	2437	PKCS#1: RSA Cryptography Specifications Version 2.0
ESP-CBC	2451	The ESP CBC - Mode Cipher Algorithms
RIP II	2453	Routing Information Protocol version 2
TBF	2475	Architectore for Differentiated Services/Token Bucket Filter, Condicionador de Tráfego - Shaper
HTB	2475	Architectore for Differentiated Services/Hierarquical Token Bucket, Condicionador de Tráfego - Shaper
GRED	2475	Architectore for Differentiated Services/Generalized Random Early Detection/Discard, Condicionador de Tráfego - Dropper
RSA/MD5 KEY	2537	RSA/MD5 KEYs and SIGs in the Domain Name System (DNS)
OSPF-NSSA	3101	The OSPF Not-So-Stubby Area (NSSA) Option
RSA/SHA-1 KEY	3110	RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)
MODP (IKE)	3526	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange
DPD	3706	A ttrafic-Based Method of Detection Dead Internet Key Exchange (IKE) Peer

NAT TRAVERSAL	3947	Negotiation of Nat - Traversal in the IKE

ITU-T		
Protocolo	Referência	Título
FRAME RELAY	Q.922, Anexo A	Core Aspects of Q.922 for Use with Frame Relaying Bearer Service, ITU, 1992
FRAME RELAY	Q.933 revisada, Anexo A	Additional Procedures for PVCs Using Unnumbered Information Frames, ITU, 1995
FRAME RELAY	T1.617, Anexo D	Additional Procedures for PVCs Using Unnumbered Information Frames, ANSI, 1991
FRAME RELAY	T1.617a, Anexo F	Multiprotocol Encapsulation over Frame Relay, ANSI, 1994
FRAME RELAY	T1.618 - ISDN	Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service, ANSI, 1991
	V.35 (Red Book)	V.35 (1998) Data transmission at 48 kbps using 60-108 kHz group band circuits

ANSI/IEEE	
Referência	Título
802.3	CSMA/CD LAN (Ethernet) Quarta edição
802.1 D	Transparent Bridge
802.1 Q	VLAN

Especificações físicas	
Condições ambientais	• Temperatura de operação: 0 a 45 ºC • Temperatura de armazenamento: -40 a 70 ºC • Umidade relativa: <95% (não condensado)
Dimensões	Série NR-2G 4200: • Largura: 445 mm • Altura: 55 mm • Profundidade: 270 mm • Peso: 3,1 kg Série NR-2G 3200: • Largura: 230 mm • Altura: 40 mm • Profundidade: 157 mm • Peso: 700 g Série NR-2G 3250: • Largura: 230 mm • Altura: 40 mm • Profundidade: 157 mm • Peso: 750 g Série NR-2G 3260: • Largura: 230 mm • Altura: 40 mm • Profundidade: 157 mm • Peso: 750 g

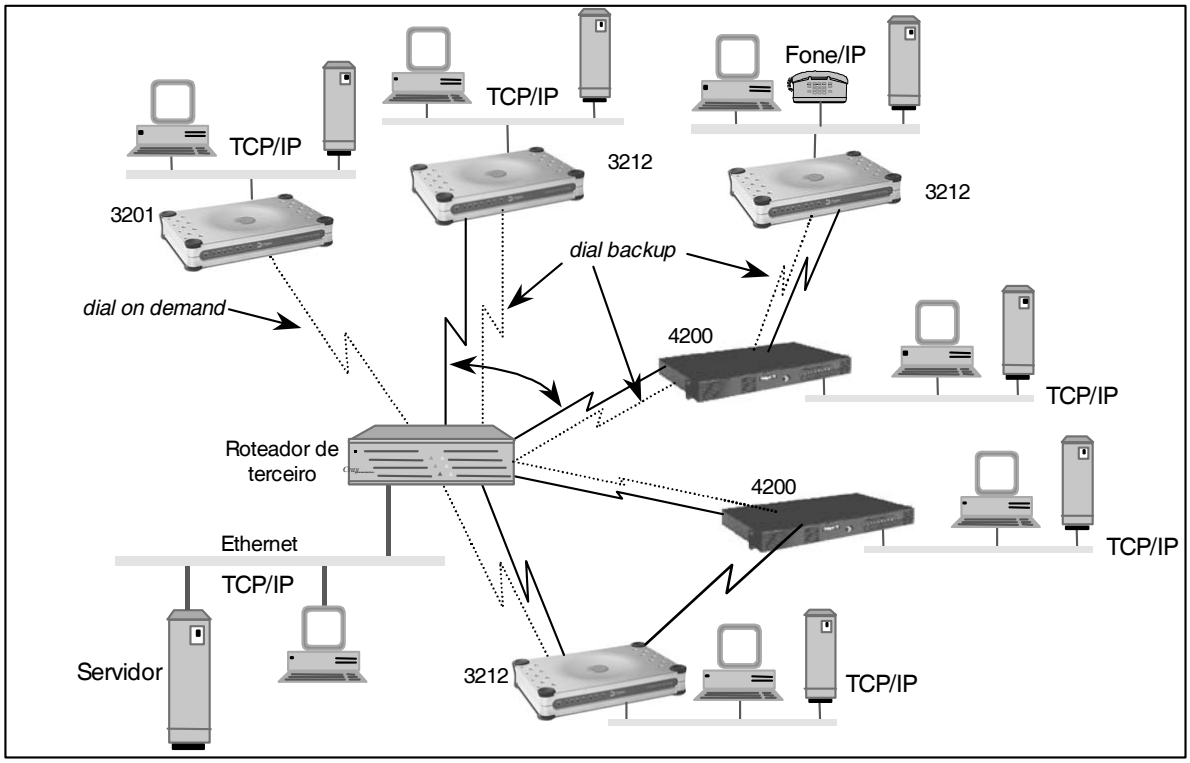
	Série NR-2G 3280: • Largura: 230 mm • Altura: 40 mm • Profundidade: 157 mm • Peso: 750 g
Alimentação	• AC: FULL-RANGE 93,5 a 253 VAC (47 a 63 Hz) para alimentação em corrente alternada • DC: FULL-RANGE 36 a 60 VDC para alimentação em corrente contínua
Consumo	Série NR-2G 3200 = 3 W Série NR-2G 3250 GPRS = 3 W Série NR-2G 3260 = 4W Série NR-2G 3280 = 4W Série NR-2G 4200 = 19 W

MTBF		
NR-2G 3200	- NR-2G 3201 - NR-2G 3211 - NR-2G 3212 - NR-2G 3214 - NR-2G 3218 - NR-2G 3238	472.850 hs 453.680 hs 423.840 hs 415.860 hs 385.550 hs 366.710 hs
NR-2G 4200	- NR-2G 4200 - NR-2G MW1 - NR-2G FXS - NR-2G FXO	275.130 hs 502.098 hs 810.570 hs 602.450 hs
NR-2G 3250 GRPS	- NR-2G 3251 - NR-2G 3252 - NR-2G 3254 - NR-2G 3258	382.990 hs 373.170 hs 366.970 hs 346.970 hs
NR-2G 3260 EDGE	- NR-2G 3261 - NR-2G 3262 - NR-2G 3264 - NR-2G 3268	372.991 hs 363.175 hs 356.979 hs 336.970 hs
NR-2G 3280 CDMA	- NR-2G 3281 - NR-2G 3282 - NR-2G 3284 - NR-2G 3288	396.981 hs 382.971 hs 372.091 hs 368.981 hs

A Série NetRouter 2G é uma família de roteadores destinada principalmente às aplicações sobre enlaces de alta velocidade dedicados ou comutados ou sobre redes Frame Relay públicas ou privadas, na conexão de escritórios remotos (remote office) ou conexões corporativas a provedores de acesso (ISPs) ou diretamente à Internet. Devido à característica de VPN/IP, é possível realizar a interconexão segura de redes através de túneis criptografados sobre um backbone público IP. Por outro lado, devido à compatibilidade do NetRouter 2G com roteadores de terceiros e redes públicas Frame Relay e IP, também é possível formar qualquer topologia de interligação. A seguir serão apresentadas algumas das aplicações mais freqüentes para a série NetRouter 2G.

ESCRITÓRIOS REMOTOS

Empresas com várias unidades remotas distribuídas geograficamente, com necessidade de automatização/informatização de processos em todas as localidades e com alta disponibilidade de conexão a uma unidade central (dial backup) são potenciais usuários desta aplicação (tipicamente, empresas de varejo com uma cadeia de lojas de atendimento e/ou postos de serviços espalhados geograficamente, como, por exemplo, bancos e agências financeiras, redes de supermercados, drogarias, lojas de materiais de construção, lojas de departamentos, etc.). A figura abaixo ilustra o NetRouter 2G nessa aplicação.



NetRouter 2G em escritórios remotos

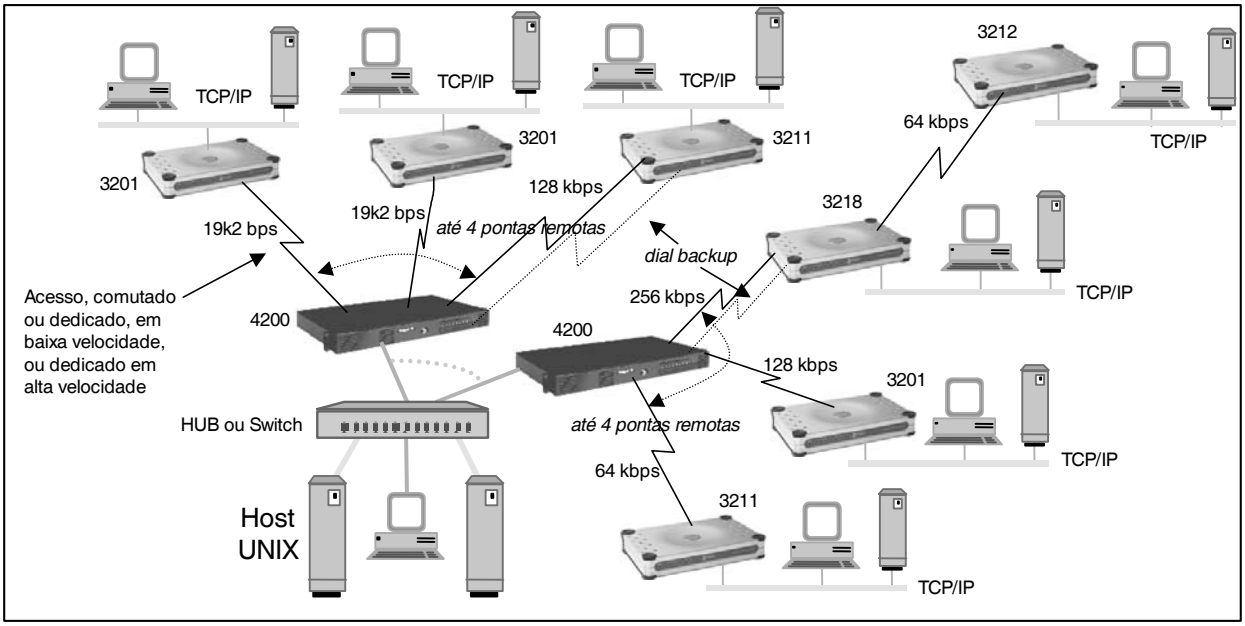
O modelo NR-2G 4200 possui a opção de instalação de módulos de voz.

Devido à compatibilidade do NetRouter 2G com roteadores de terceiros, é possível colocá-lo em um escritório remoto conectado a outro roteador de terceiro no ponto central. Aplicações deste porte quase sempre exigem soluções heterogêneas, multi-vendor, pois os fabricantes de roteadores de maior porte, localizados quase sempre apenas no ponto central, não possuem alternativas de baixo custo para os vários pontos remotos.

A utilização dos modelos 3200 em localidades remotas possibilita uma alta disponibilidade de conexão com o ponto central, devido a características de uma porta auxiliar para dial backup.

Os enlaces digitais podem ser de alta ou baixa velocidade devido à característica de múltiplas interfaces. Pode-se, inclusive, começar com um enlace de baixa velocidade e depois migrar para um circuito de alta velocidade, trocando-se apenas o tipo de cabo do NetRouter 2G.

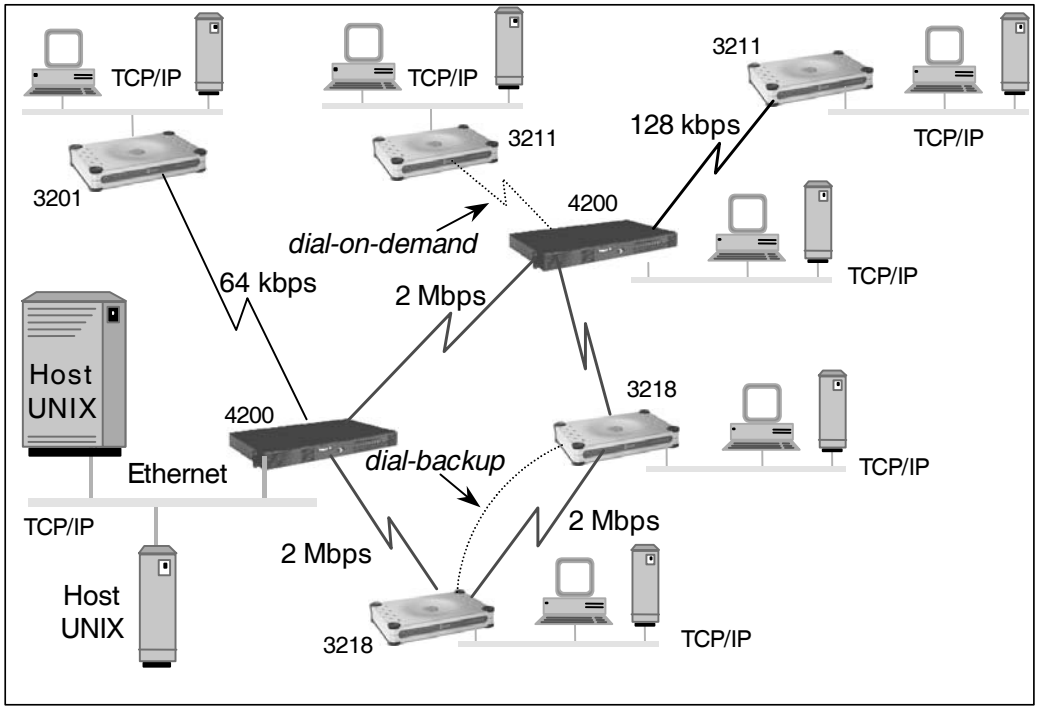
No caso de enlaces dedicados para cada localidade remota, é necessário utilizar um roteador com várias portas WAN, onde se poderá fazer a composição com vários NetRouter 2G, cada um atendendo até quatro acessos remotos (já considerando a utilização de módulos WAN para adicionar mais portas seriais). A figura a seguir ilustra essa situação.



NetRouter 2G em centro de rede

BACKBONE REGIONAL

Devido à característica de mais de uma porta síncrona de alta velocidade, é possível de constituir pequenos backbones de redes WAN, tipicamente regionais, com os modelos de NetRouter 2G. A figura a seguir ilustra essa aplicação.



NetRouter 2G em backbone WAN regional

ACESSO À INTERNET

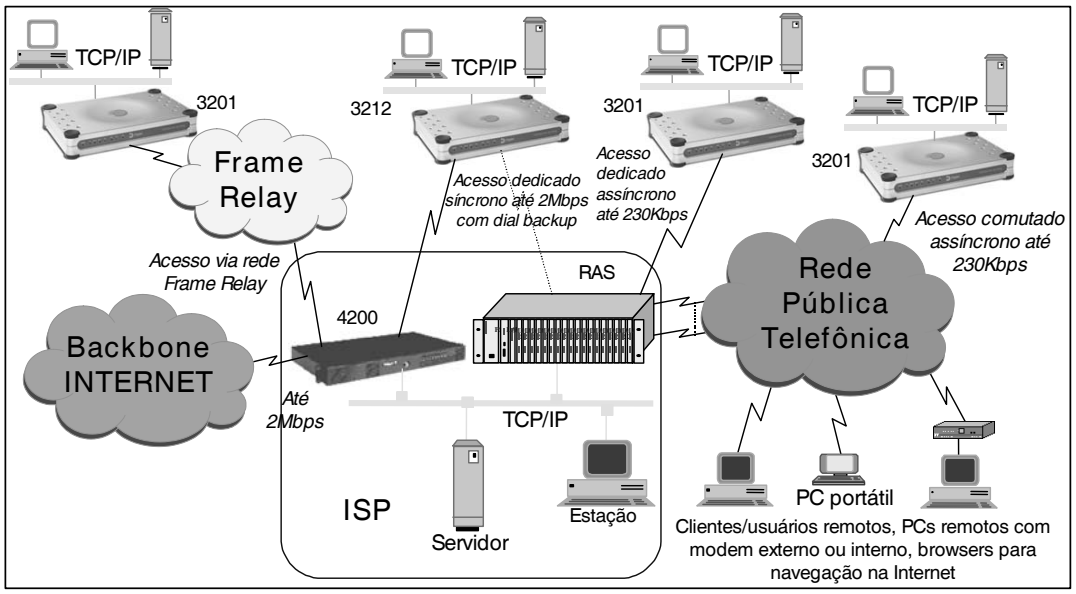
Um ISP (Internet Service Provider) pode utilizar o NetRouter 2G para realizar o uplink com um backbone Internet de alguma operadora/prestadora ou para atender acessos corporativos à Internet sobre enlaces dedicados síncronos ou Frame Relay.

Empresas ou escritórios podem utilizar o NetRouter 2G para fazer uma conexão comutada ou dedicada a um ISP. O acesso corporativo à Internet via ISP substitui os vários acessos comutados dos usuários corporativos, conectando a rede local de toda a organização diretamente ao provedor e, por conseguinte, à Internet. Esta aplicação traz ganhos de disponibilidade e velocidade na conexão. No caso de conexão de uma empresa/organização à Internet utilizando um acesso dedicado, funcionários em campo ou trabalhando em casa podem acessar a Intranet da empresa pela Internet através do mesmo ISP ou outro provedor de acesso.

Normalmente, o ISP utiliza portas assíncronas de um RAS (Remote Access Server) para acessos com velocidades menores do que 64 kbps, onde o modelo 3200 pode ser aplicado no lado da empresa sobre circuitos dedicados ou comutados. Normalmente, para velocidades a partir de 64 kbps, são utilizadas portas síncronas de um roteador do ISP, podendo-se utilizar o modelo 3212, com a alternativa de configurar uma segunda porta WAN para dial backup. É possível também utilizar acesso comutado síncrono de alta velocidade (Data Fone ou ISDN/RDSI) com o NetRouter 2G, embora esta aplicação não seja comum em provedores de acesso à Internet. No caso do ISDN, deve-se utilizar um terminal adaptador externo, também chamado de NT (Network Terminator).

Outra possibilidade de uso cada vez mais freqüente é o acesso corporativo à Internet via um serviço Frame Relay. Neste caso, o ISP mantém um acesso único com um provedor de serviço Frame Relay, por onde atende a todos os seus clientes corporativos, economizando em portas síncronas, roteadores e acessos dedicados.

A figura a seguir ilustra essas aplicações.

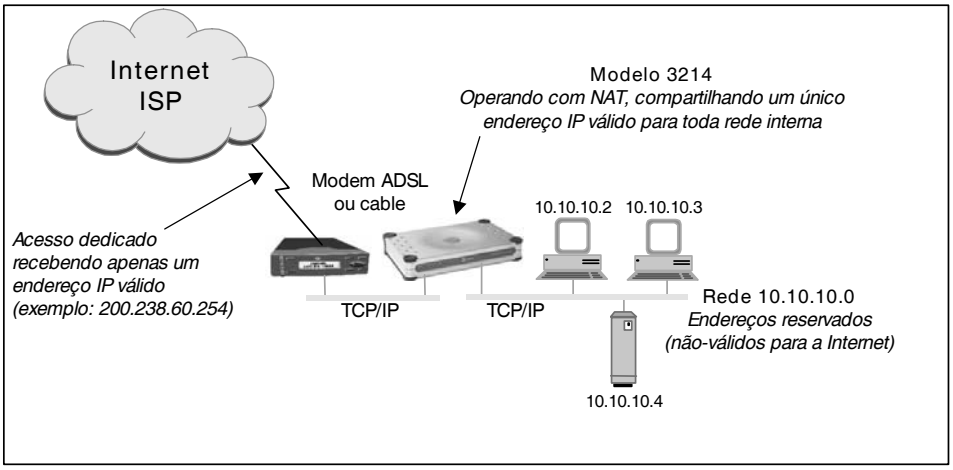


NetRouter 2G em acesso à Internet

Outro grande benefício do uso do NetRouter 2G para acesso à Internet é a característica de compartilhamento de endereços IP (NAT/PAT). Assim, vários endereços da rede corporativa podem compartilhar um único endereço IP válido fornecido pelo provedor. Essa característica confere um alto grau de segurança à rede corporativa, pois, além de esconder o esquema de endereçamento interno da rede (através de uma tabela de compartilhamento configurada no NetRouter 2G), utiliza endereços que não são válidos (não são roteados) para a Internet. Apenas alguns serviços podem ser acessados externamente, desde que devidamente configurados. Esta facilidade possibilita uma grande economia no fornecimento de endereços válidos por parte do provedor e simplifica os esquemas de roteamento.

A utilização de uma segunda porta LAN no NetRouter 2G, associada às características de Firewall, oferece uma conexão segura à Internet em acessos de banda larga (cable modem, ADSL ou wireless). A figura a seguir ilustra essa aplicação.

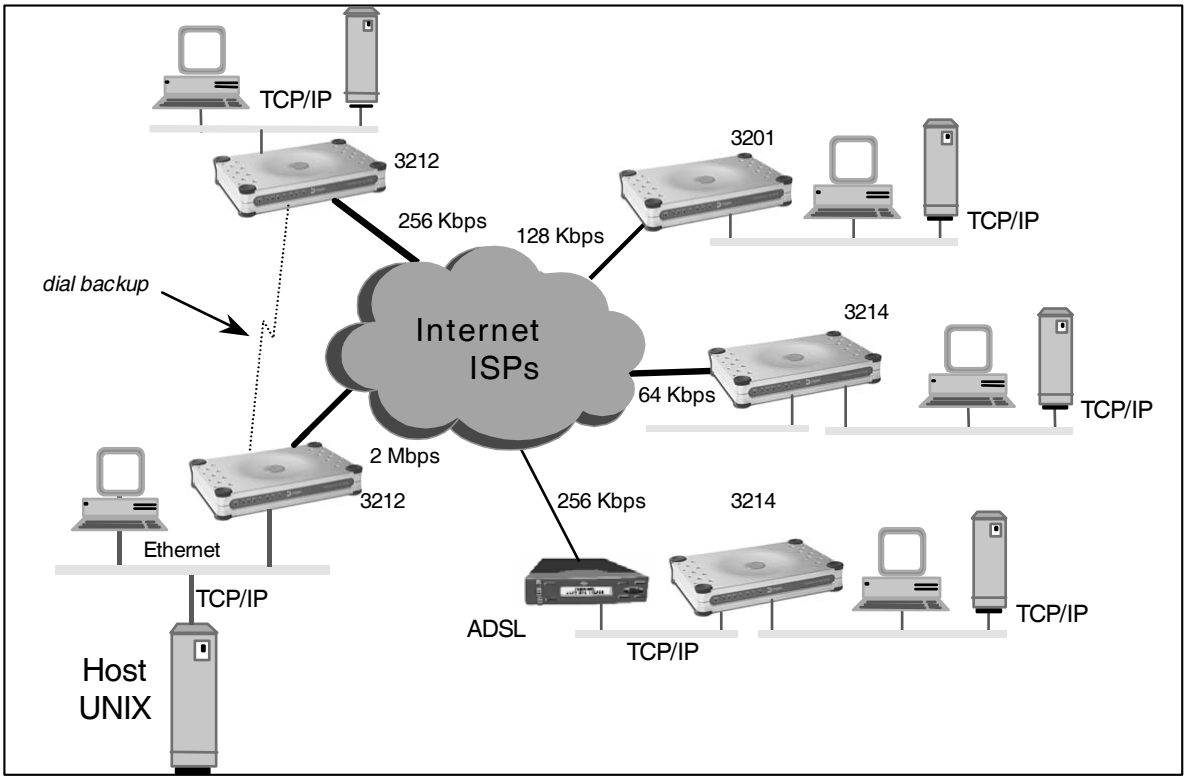
INTERCONEXÃO VIA INTERNET - EXTRANET



NetRouter 2G compartilhando endereços IP (NAT/PAT)

As empresas podem interligar suas unidades através da Internet, via provedores de acesso (ISPs) ou conectando-as diretamente ao backbone de uma operadora/prestadora de serviços. Nesse caso, pode-se ter uma conexão em alta velocidade diretamente ao backbone Internet no ponto central, utilizando o NR-2G, e uma segunda porta WAN para a contingência (dial backup) de um ou mais pontos remotos. Também é possível utilizar as portas WAN adicionais para conexão direta de alguns pontos remotos estratégicos ao ponto central. Para o acesso dos escritórios remotos com ISPs locais através de enlaces de baixa velocidade dedicados ou comutados, ou através de enlaces dedicados de alta velocidade, pode-se utilizar o modelo 3212, que possui uma porta auxiliar para a opção de dial backup. Já para os acessos através de serviços de banda larga, como ADSL ou cable modem, pode-se utilizar o modelo 3214, que possui uma segunda porta LAN para isolar fisicamente a rede interna. Os modelos de NetRouter 2G permitem a formação de VPN/IP, com túneis criptografados (IPSec/3DES ou AES), para realizar uma interconexão extremamente segura sobre a Internet. A figura a seguir ilustra essa aplicação.

INTERNETWORKING SOBRE REDE FRAME RELAY

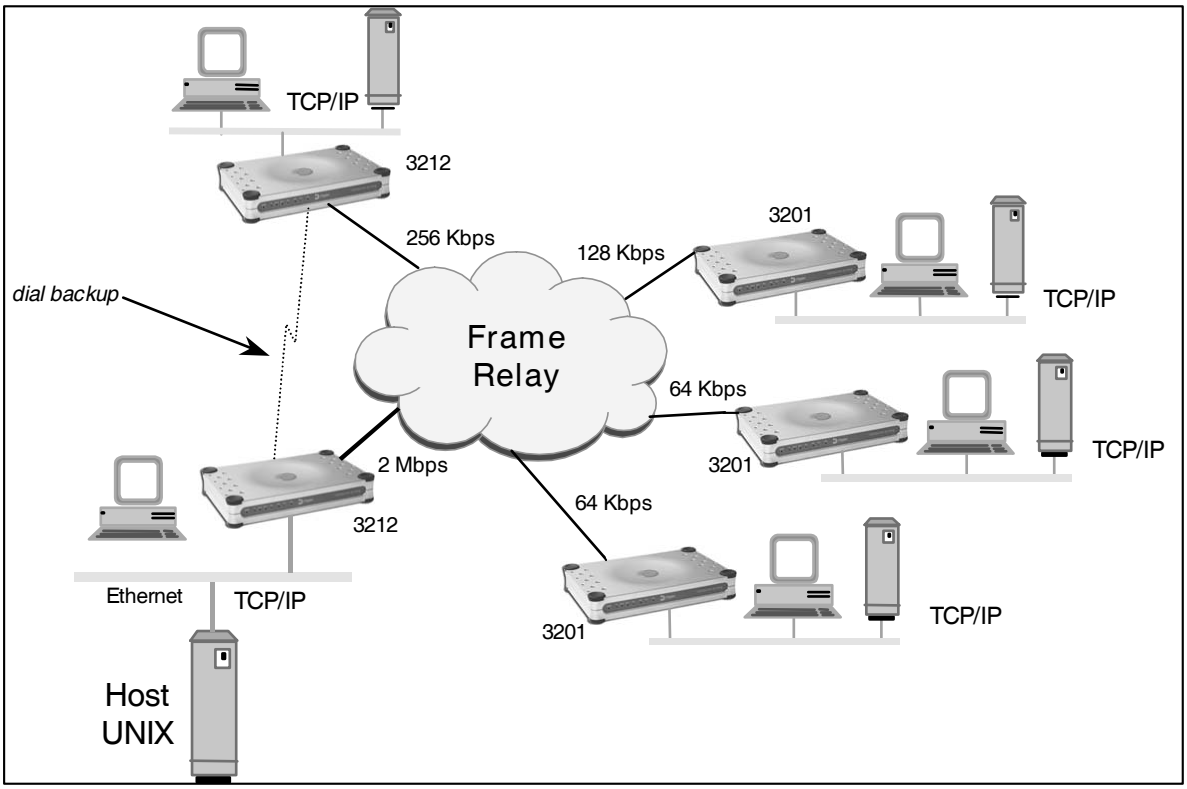


Interconexão de NetRouter 2G via Internet

Ao utilizar uma rede Frame Relay pública ou privada como um backbone de interligação dos escritórios remotos com o ponto central, ou até mesmo entre os próprios escritórios, pode-se utilizar um único acesso físico em cada localidade, economizando em portas WAN de roteadores e na quantidade de enlaces dedicados. Caso contrário, ou seja, sem o uso de uma rede Frame Relay e havendo muitos pontos remotos, seria necessário um roteador de grande capacidade no ponto central, o que elevaria muito o custo do projeto.

Com o NetRouter 2G, um roteador de baixo custo porém de alta performance, é possível estabelecer uma conexão de até 2 Mbps com a rede Frame Relay e atender a até 256 escritórios remotos (256 DLCIs) através de um único acesso físico. A grande vantagem no uso de uma rede Frame Relay é a garantia de banda disponível através da contratação de um CIR (Committed Information Rate), além de um custo de serviço mais baixo se comparado ao enlace dedicado.

O NetRouter 2G suporta os modos ANSI ou ITU de formação de frame. É possível, ainda, utilizar portas WAN adicionais para conexão direta ao ponto central ou para a contingência (dial backup) de escritórios remotos. A próxima figura ilustra essa aplicação.



NetRouter 2G sobre rede Frame Relay

APLICAÇÕES COM ROTEADORES GPRS, EDGE E CDMA

A seguir serão apresentadas algumas aplicações com os modelos de Roteadores GPRS da Digitel, Série NR-2G 3250 GPRS. As mesmas aplicações podem ser seguidas com os modelos das Séries NR-2G 3260 EDGE e NR-2G 3280 CDMA, variando apenas a operadora celular, em função da tecnologia wireless utilizada.

Aplicação Típica

Para uma aplicação típica com Roteador GPRS com uma interface LAN 10/100 Mbps é indicado o NR-2G 3251 GPRS, podendo ser conectado diretamente a uma única máquina com interface ethernet ou a uma rede LAN com vária máquinas.

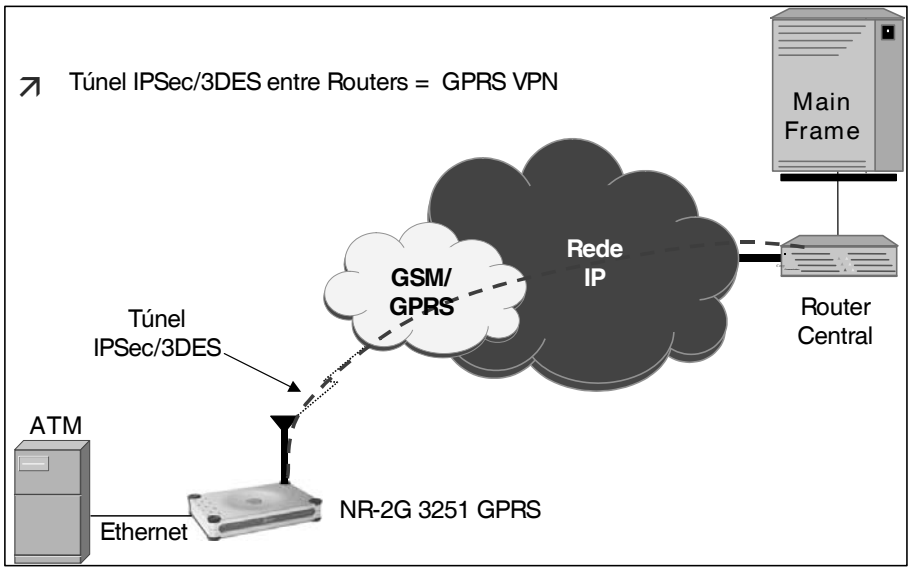


Figura Aplicação típica de Roteador GPRS com uma interface LAN

A interface LAN suporta o protocolo XOT (X.25 sobre TCP/IP), atendendo aplicações legadas que ainda utilizem o protocolo X.25, mas sobre uma interface Ethernet.

Roteador GPRS como Backup de outro Roteador

Uma outra possibilidade de aplicação para o NR-2G 3251 GPRS é de ser o gateway backup de outro roteador que não possui interfaces físicas para contingência, utilizando como alternativa uma rede GSM/GPRS e o protocolo VRRP para controle de qual o dispositivo é o ativo e qual é o *standby*.

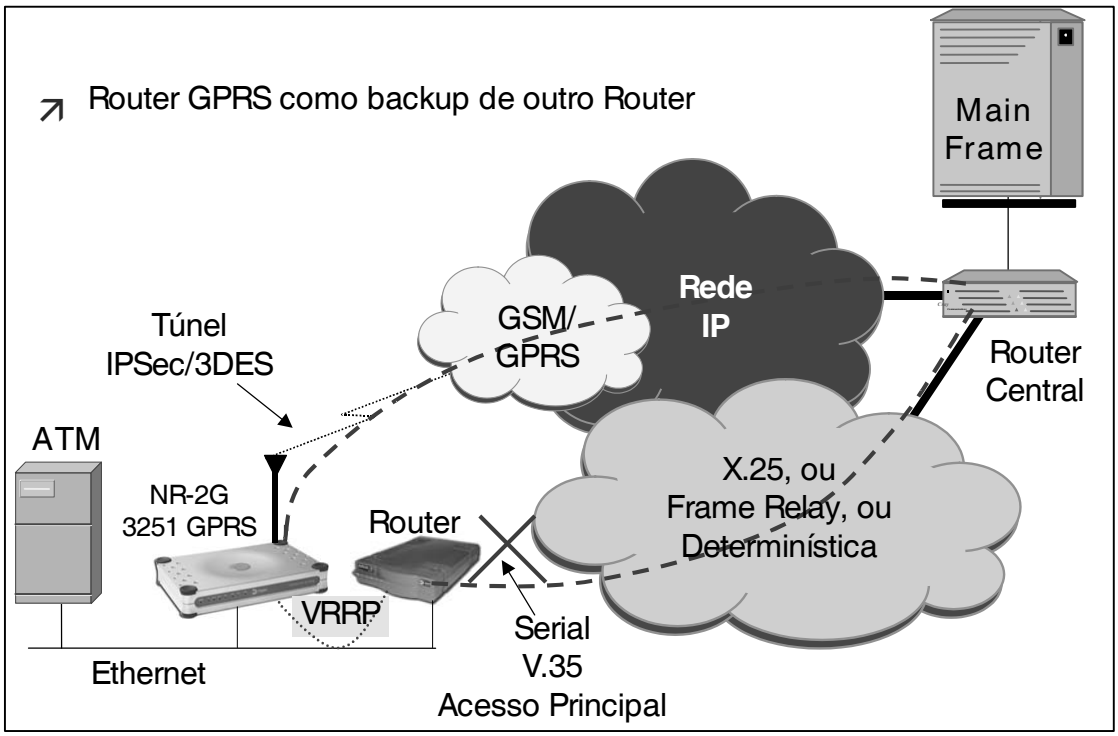


Figura Roteador GPRS como backup de outro gateway

Máquinas X.25 sobre GSM/GPRS

Para a conexão de máquinas X.25 (DTE) sobre redes GSM/GPRS é indicado o modelo NR-2G 3258 GPRS, onde a porta serial é conectada ao DTE utilizando o protocolo X.25 do roteador, que para transportar sobre a rede GPRS utiliza o protocolo XOT (X.25 sobre TCP/IP).

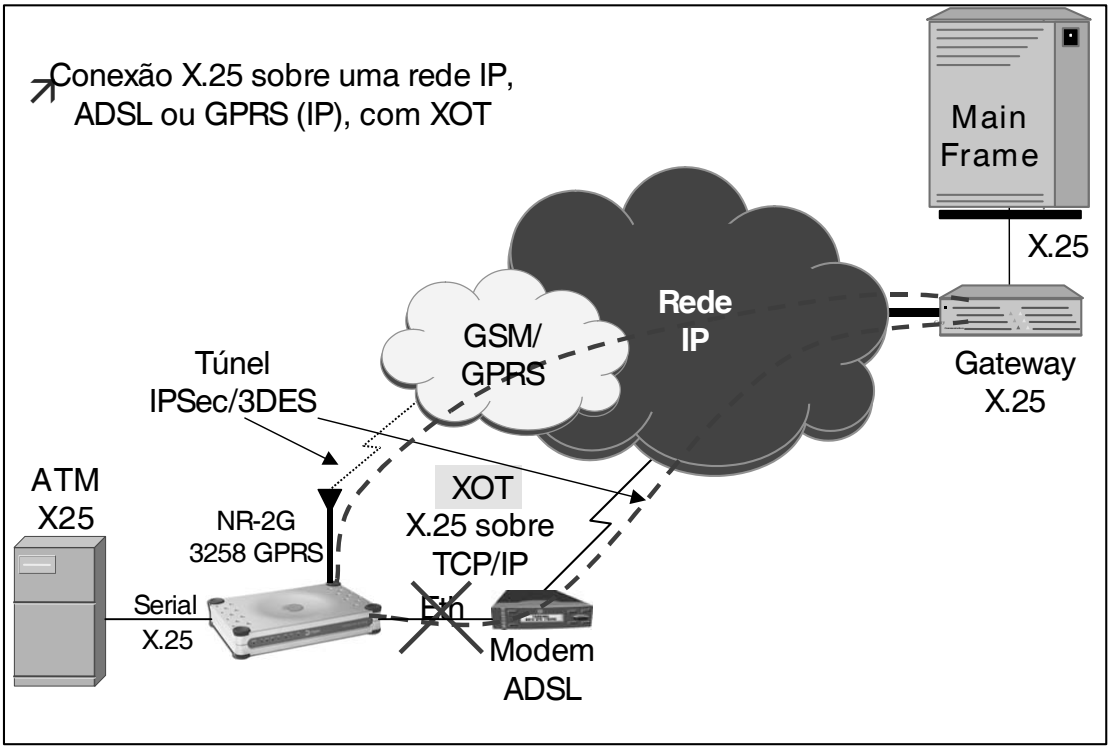


Figura Roteador GPRS para o transporte de X.25 sobre rede GSM/GPRS

Com o NR-2G 3258 GPRS sendo utilizado para esta aplicação, ainda resta a porta LAN, que pode ser conectada a um acesso com interface Ethernet (ADSL ou Cable Modem, por exemplo) para servir de contingência ou para balanceamento de carga. Neste caso, também será utilizado o protocolo XOT para transporte do X.25 sobre a rede IP.

Roteador GPRS com Dial Backup

Em casos de acessos críticos, que necessitam operar com SLA, é indicado o modelo NR-2G 3252 GPRS, onde a interface serial pode ser conectada a um modem analógico/discado para operar como contingência do acesso GSM/GPRS. Neste caso, num evento de falha do acesso GSM/GPRS, link principal, o roteador Digitel comanda a discagem no modem, faz a autenticação em um servidor de acesso remoto (RAS) e estabelece uma rota alternativa para o tráfego IP. Quando o acesso GSM/GPRS retornar, desconecta o modem analógico e volta a rota para o caminho original.

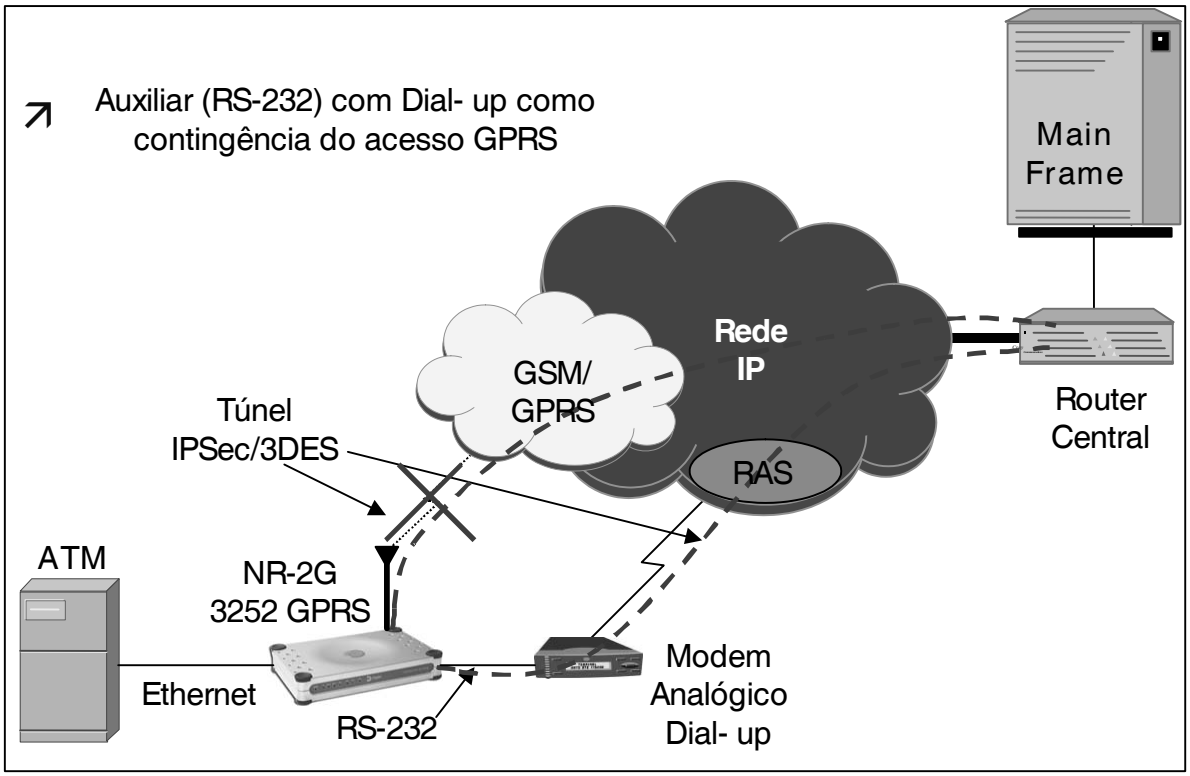


Figura Roteador GPRS com dial backup

GSM/GPRS como Backup de Porta WAN Serial

O GPRS é uma excelente opção de contingência para acessos dedicado, Frame Relay ou X.25. Neste caso, o modelo indicado é o NR-2G 3258 GPRS, onde a porta WAN/Serial será o link principal, sobre uma rede multiserviço (IP), Frame Relay ou X.25, e a interface GSM/GPRS será o acesso backup. No evento de falha do link principal, o Roteador GPRS automaticamente desviará o tráfego IP para a interface GSM/GPRS, retornando a porta WAN/Serial quando o link principal voltar a operar sem problemas.

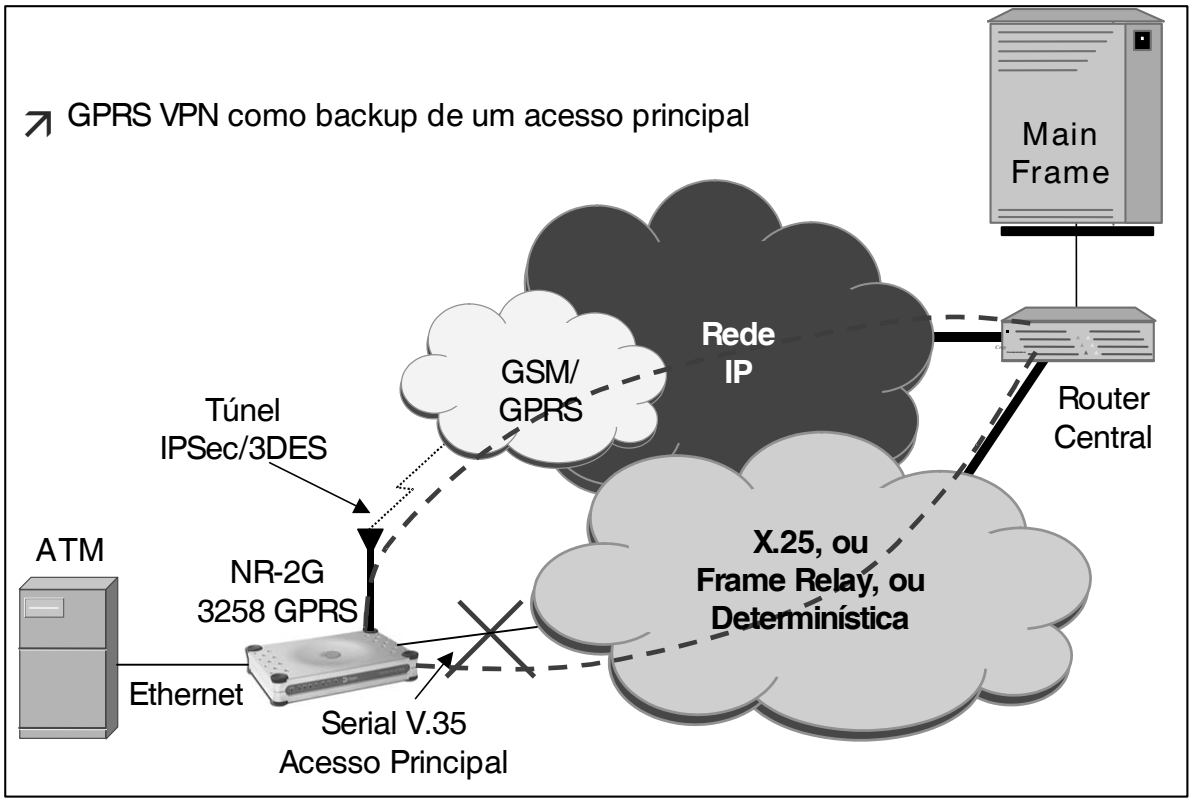


Figura Roteador GPRS como backup de porta WAN/Serial

GSM/GPRS como Backup de Acesso Ethernet

Ocasionalmente o link principal pode ser um acesso ADSL, Cable ou WiFi, onde a interface de *uplink* (WAN) é do tipo Ethernet. O GPRS também pode ser uma excelente opção de contingência para esses tipos de acessos. Neste caso, o modelo indicado é o NR-2G 3254 GPRS, onde uma porta Ethernet estará conectada ao link principal (WAN Ethernet ou LAN uplink), a outra porta Ethernet estará conectada a rede local (LAN) e a interface GSM/GPRS será o acesso *backup*. No evento de falha do link principal, o Roteador GPRS automaticamente desviará o tráfego IP da porta WAN Ethernet para a interface GSM/GPRS, retornando a porta WAN Ethernet quando o link principal voltar a operar sem problemas.

Como o acesso GPRS possui a característica de estar sempre ativo (*allaways on*) é possível estar realizando também um balanceamento de carga entre as duas interfaces de *uplink*.

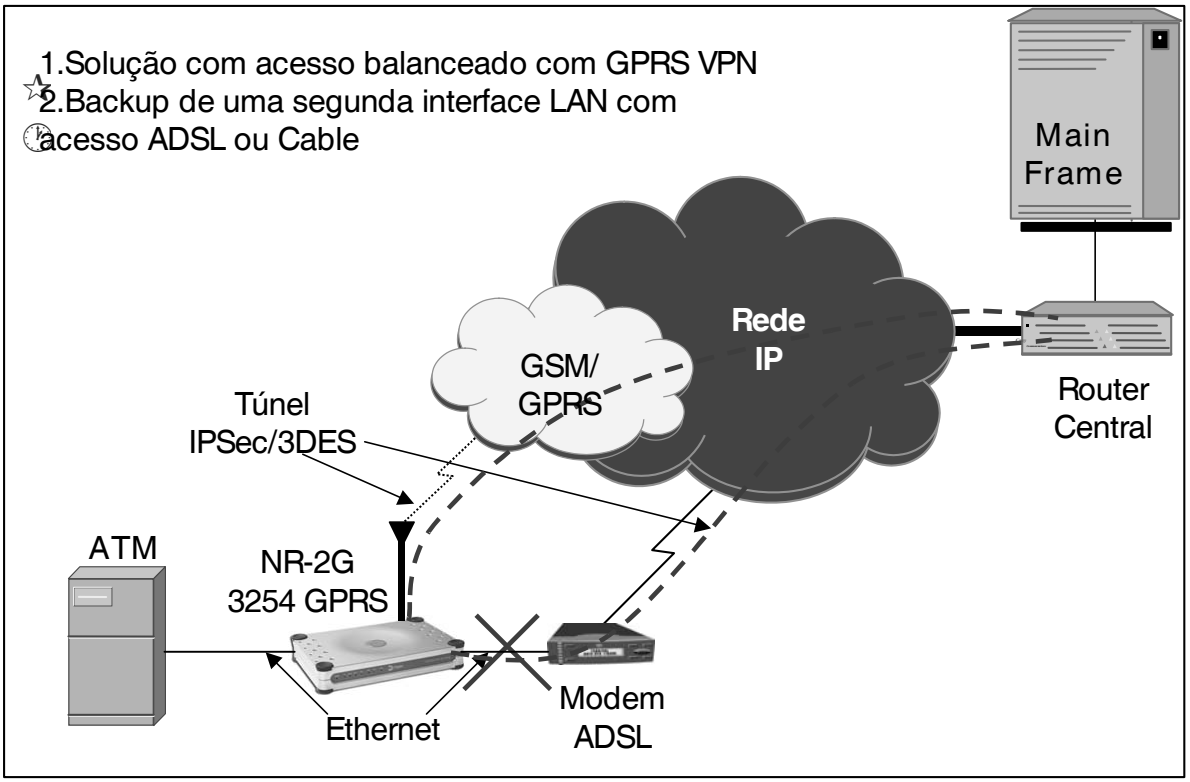


Figura Roteador GPRS como backup de um acesso Ethernet

Esta página foi deixada intencionalmente em branco.

• Assistência técnica e garantia

Durante o período de garantia do produto (especificado na nota fiscal), a Digitel assegura seu perfeito funcionamento, de acordo com as características e especificações existentes no seu manual de instalação e operação. Caso seja constatado algum problema no produto, entre em contato com o Centro de Assistência Técnica Digitel, em Porto Alegre, relatando o tipo de defeito.

Esta garantia inclui conserto e substituição dos componentes ou partes defeituosas sem ônus para o cliente, sendo executada no Centro de Assistência Técnica Digitel. Não estão cobertos defeitos ocasionados por má utilização de equipamento conectado a este produto ou utilização em desacordo com as instruções contidas no manual. Também não estão cobertos consertos efetuados por estabelecimentos não credenciados pela Digitel.

A garantia dos produtos é de "balcão" (Porto Alegre), ou seja, não cobre atendimento em campo. O frete de remessa e devolução para conserto é por conta do cliente.

Porto Alegre

DIGITEL S.A. INDÚSTRIA ELETRÔNICA
Rua Dr. João Inácio, 1165
Navegantes
CEP 90230-181 Porto Alegre, RS
Fone: 51 3337-1999
Fax: 51 3337-1923
CNPJ: 89.547.269/0001-04
Inscrição Estadual: 0960602577
http://www.digitel.com.br
E-mail: info@digitel.com.br

Esta página foi deixada intencionalmente em branco.