Manual de Operações

AG 30 Plus

Novembro 2012, 200.0515.00-0 Rev. 022

Sumário

Prezado Cliente:

Leia atentamente este Manual de Operações para entender o funcionamento de seu AG 30 Plus Digistar, além de providenciar o local adequado para sua instalação.

Caso persista alguma dúvida, entre em contato com o seu instalador.

Considere-se bem-vindo à Digistar Telecomunicações.

É motivo de grande satisfação para nossa empresa tê-lo como cliente.

Termo de Garantia:

Para utilizar os serviços de garantia de seu AG 30 Plus, você precisará apresentar cópia da Nota Fiscal de Compra do produto, com data de emissão legível e enviar para o Centro de Reparos da Digistar (CRD). As despesas com frete serão por conta do cliente.

Suporte Técnico:

Ao contatar o Suporte Técnico da Digistar, tenha as seguintes informações disponíveis:
- Modelo do produto;
- Informações sobre a garantia - dados da Nota Fiscal de Compra;
- Uma breve descrição do problema e os passos executados para resolvê-lo;
- Nome da empresa que instalou o produto.

Método	Descrição
E-mail Suporte	suporte@digistar.com.br
Telefone	(51) 3579-2200
Fax	(51) 3579-2209
WEB Site	www.digistar.com.br

1. Conhecendo o seu AG 30 Plus Digistar

O AG 30 Plus, converte a tecnologia digital de um PABX TDM (E1) em IP, permitindo o uso da tecnologia VoIP, sem alterar o PABX existente. Além disso, o AG 30 Plus opera como router de dados para a sua rede de computadores, provendo com um único link IP a solução para dados e voz.

Observação: Ao longo deste manual o AG 30 Plus será denominado de "Gateway Digistar."

1.1. Conteúdo da Embalagem

- ✓ 1 AG 30 Plus
- ✓ 1 Manual de instalação
- ✓ 1 CD de Documentação do Produto
- ✓ Fonte de alimentação

1.2. Características Técnicas

Rede: • Roteamento Estático: host ou rede • DNS Dinâmico • Certificados digitais: Garantia de autenticidade e segurança, cada Gateway Digistar terá um FQDN ou IP diferente. • VLAN (802.1q)	**Interface WAN:** • Modo Bridge • Cliente DHCP • IP Fixo • Cliente PPPoE
Interface LAN: • DHCP Avançado fixando IP ao MAC • Servidor DHCP • IP Fixo	**Segurança:** • NAPT • Server VPN: PPTP, L2TP e IPSEC • Client VPN: PPTP, L2TP e IPSEC • Firewall: Firewall Stateful, Configurações gerais, Filtros: DoS, Conteúdo e Usuários, Habilitar máquina DMZ
Configurações Gerais: • Gerenciamento WEB • Configuração das Portas: HTTPS, SSH e Telnet	**Filtros**: • Gerais: Bloqueio Messengers, Chat, ICQ, Peer-to-Peer, Trojan Horses, Traceroute: pacotes por UDP e ICMP. • DoS: SYN Flood, UDP Flood, ICMP Flood, Port Scan, Conexões por host, IP Options, Ping of Death, Smurf Attack e IP Spoofing. • Conteúdo: até 12 URLs bloqueadas • Usuário: até 12 regras de bloqueio por usuário
QoS: • Traffic Shaping • Marcação DSCP dos pacotes de áudio (RTP)	**Vídeo:** • Multicast - Triple Play e Túneis DVMRP
Gerência: • SNMP • Configurador Multiusuários	**NATT:** • STUN • UPNP-Cliente • FQDN Externo
Data/Hora: • NTP • RDATE	**Protocolos VoIP:** • SIP (Registrar/Proxy) • Cancelamento de eco automático G 168-2002 • Jitter Buffer de 20 ms a 80 ms (automático)
Codecs de Áudio: G.729AB (8kbps), G.711A (64kbps) e G.711U (64kbps)	**Codecs para Fax:** G.711 e T.38
DTMF: dentro ou fora da banda	**Contas SIP:** até 1.000 contas
Linhas Digitais: capacidade máxima de 30	**Impedância (Porta Digital):** 100 ohms
Sinalização Digital R2/MFC: • De linha: R2 digital ou R2 analógico (E M contínuo) • De registradores: entrada e saída MFC	**E1 (R2):** Master
Proteção de Programação: Memória não volátil FLASH	**Alimentação AC:** Entrada full-range: 95 Vac à 240 Vac
Processador: Power Quicc de 32 Bits com 64MB RAM e 32MB de Flash	**Consumo Máximo:** 25 VA
Temperatura de Operação: 10ºC a 40ºC	**Umidade Relativa do Ar:** 20% a 90%
Falta de Energia: Deve ser adicionado No-break	**Instalação:** Mesa, Parede e [1]Rack 19" *[1]Opcional*
Dimensões (mm): A: 40 / L: 220 /P: 130	**Peso Máximo:** 0,9 Kg

1.3. Descrição do Hardware

1.3.1. Painel traseiro do Gateway Digistar

Descrição dos conectores do Gateway Digistar

Item	Descrição
PWR	Conector para entrada de alimentação (5 VDC)
WAN	Conector Superior RJ-45
LAN	Conector Inferior RJ-45
E1/T1	Conector E1/T1 RJ-45
CONSOLE	Entrada para console USB

1.3.2. Painel frontal do Gateway Digistar

Descrição dos LED's do Gateway Digistar

LED	Descrição
PWR	Ligado: quando a fonte do Gateway Digistar está funcionando.
VOIP	Piscando indica ligação VoIP ativa
LAN	Desligado indica "*link up" em* 10Mbps. Ligado indica "*link up" em* 100Mbps
	Piscando indica fluxo de dados pela porta. Ligado indica "*link up"*
WAN	Desligado indica "*link up" em* 10Mbps. Ligado indica "*link up" em* 100Mbps
	Piscando indica fluxo de dados pela porta. Ligado indica "*link up"*
E1	Link E1

2. Acessando o Configurador Web Digistar

As configurações do seu Gateway Digistar são realizadas através de páginas WEB que se encontram dentro do equipamento.

Inicialmente para acessar o Configurador Web Digistar, devemos conectar a interface de rede de um PC na interface LAN do Gateway Digistar. As interfaces de rede do Gateway Digistar são auto cross-over, ou seja, podem ser conectadas a qualquer cabo de rede.

Com a conexão correta, devemos configurar o PC para acessar a página.

O Gateway Digistar fornecerá o IP no caso do PC requisitar DHCP. Caso o PC não solicitar DHCP, o PC deve ser configurado com o gateway 192.168.10.1 e um IP nesta rede.

Após isto, acessaremos o Configurador Web Digistar. Para tanto, através de um WEB Browser, digitamos:

https://192.168.10.1

2.1. Multiusuários

Ao acessar a página, aparece a tela de logon, conforme abaixo:

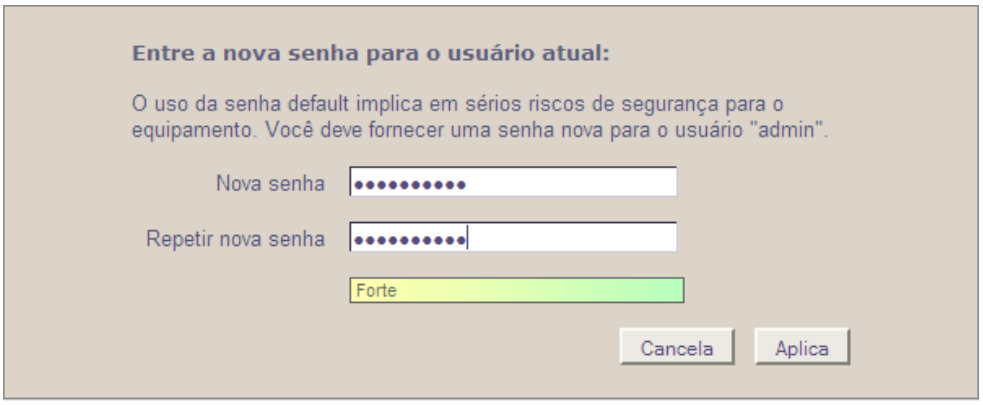
Nesta página o usuário “admin” e usuários autorizados podem optar pela configuração rápida ou configuração normal. Ao escolher a configuração rápida o usuário tem acesso somente às opções mais críticas para o funcionamento do Gateway Digistar. Esse modo foi criado para a primeira customização de uma máquina nova. **Atenção**: Ao se encerrar o configurador rápido, todas as configurações atuais serão perdidas!

Para acessar, o usuário deve fornecer usuário e senha.

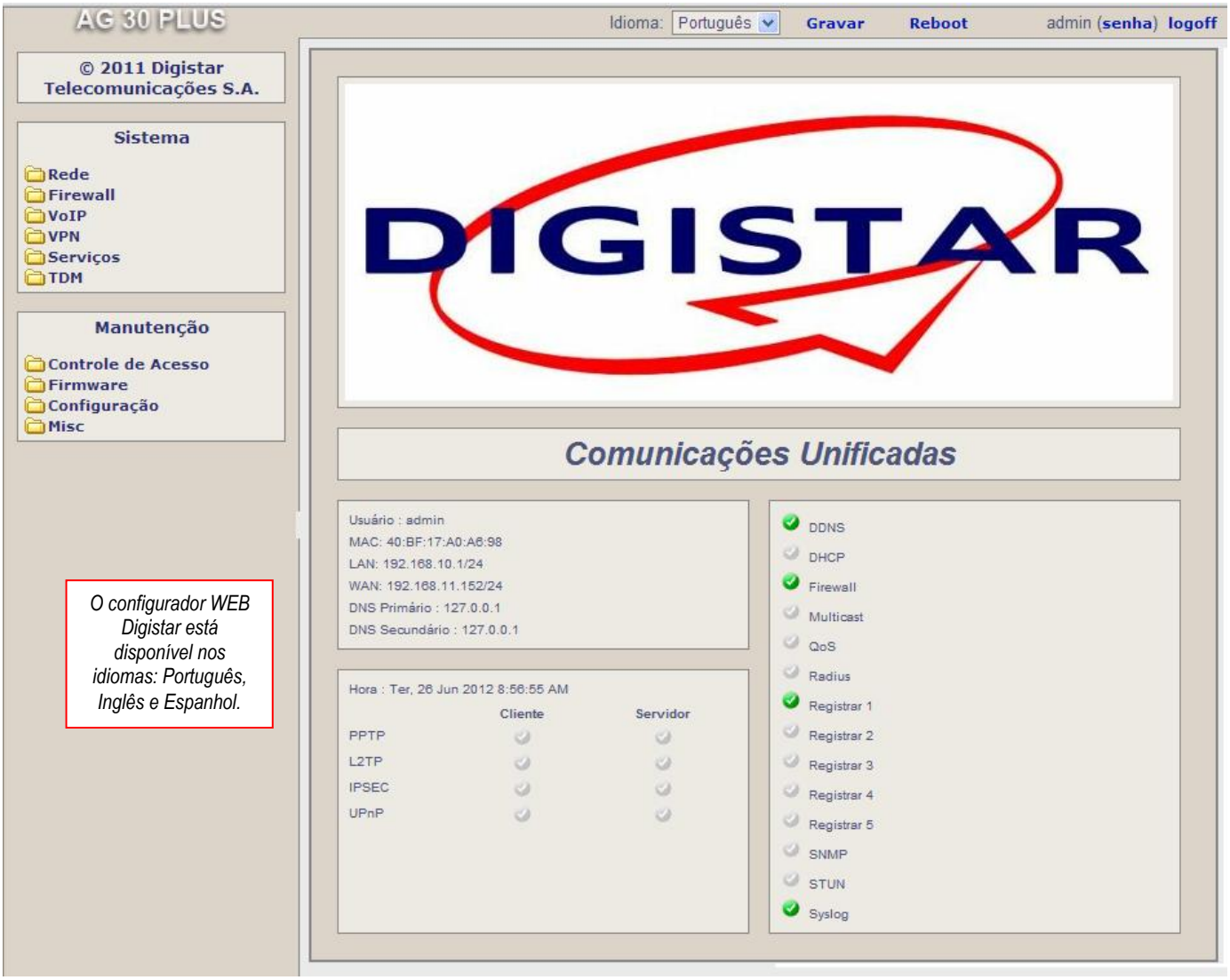
Usuário default: admin e senha default: admin

Usuário: até 20 caracteres
Senha: até 16 caracteres

OBS.: *No primeiro acesso do usuário admin com senha default, será requisitada a troca da senha deste usuário. O programa irá validar a senha entrada e indicará sua força com uma barra de progresso. O Botão Aplica só estará habilitado com uma senha forte.*



Após acessar o configurador com o usuário admin, aparece a tela abaixo:

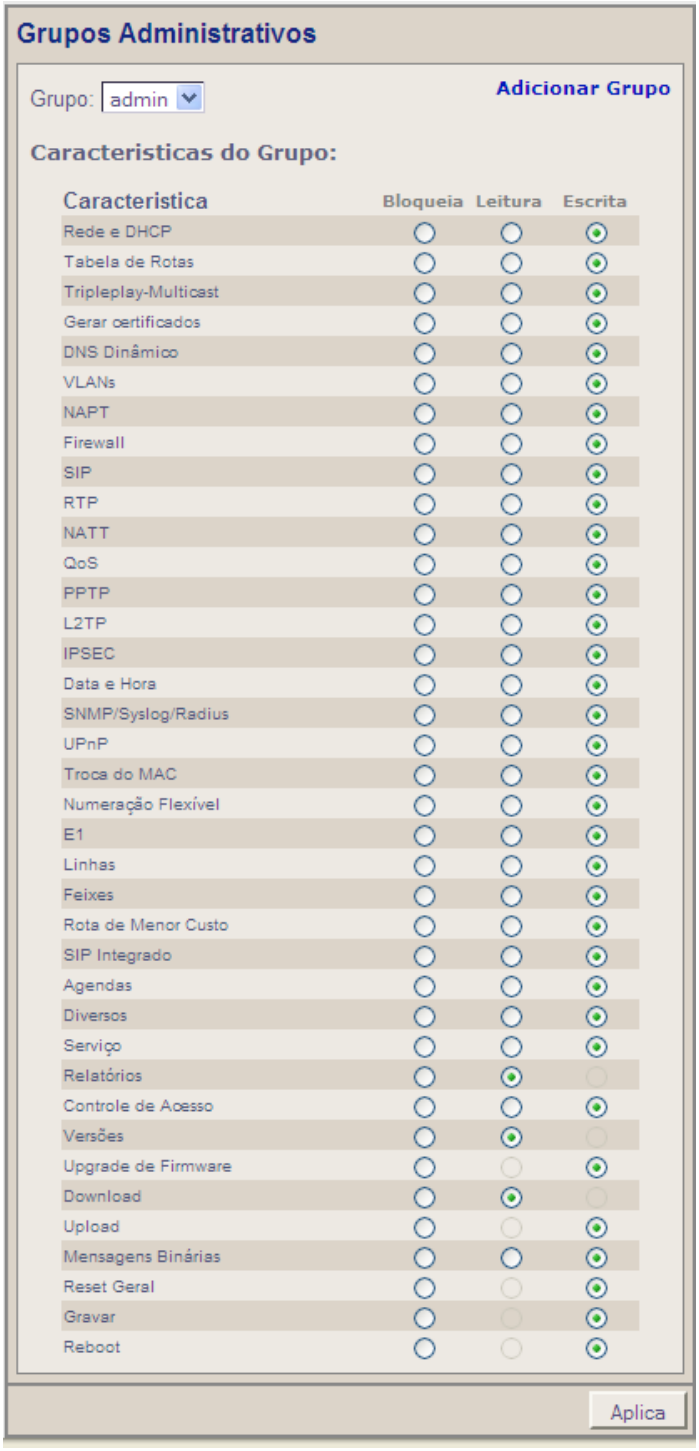


O configurador WEB Digistar está disponível nos idiomas: Português, Inglês e Espanhol.

Nela estão localizados um menu a esquerda e uma janela, que exibe algumas configurações de serviços configurados no Gateway Digistar. Estas configurações podem ser acessadas clicando-se sobre os “títulos” ou acessadas através do menu que se encontra no lado esquerdo da tela.

Cadastro Grupos de Usuários (Editar Grupos)

Com o usuário admin é possível cadastrar novos grupos de usuários (em Editar Grupos) e configurar os acessos de cada grupo.



Ao clicar em cima das palavras “Bloqueia”, “Leitura” ou “Escrita” habilita todos os itens.

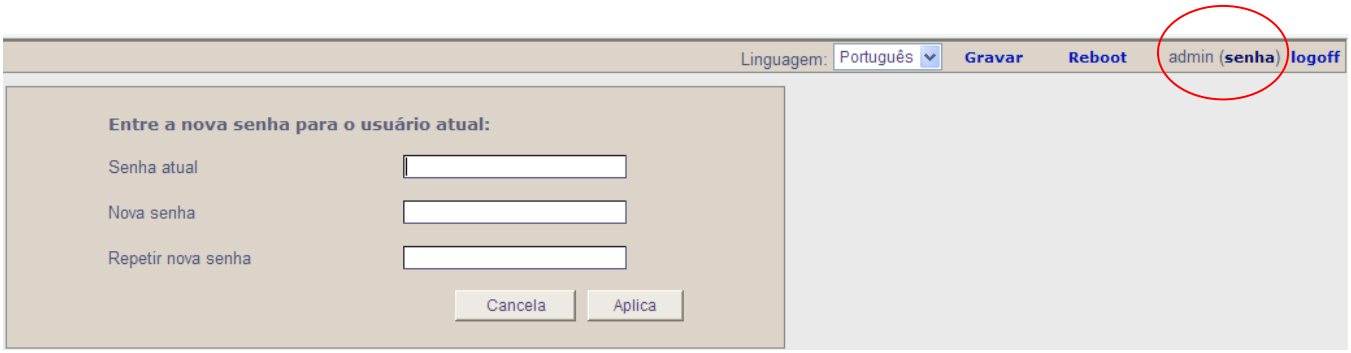
Cadastro de Usuários (Editar Usuários)

Em “Editar Usuários” podem ser cadastrados os usuários com suas senhas. Cada usuário deve ser associado a um grupo de usuários, pois é lá que são definidas suas permissões.

.

Alteração da senha

Cada usuário, após logado, poderá alterar sua senha, clicando em “senha” que aparece no canto superior direito, conforme tela abaixo.



OBS.:

O tempo de inatividade do usuário admin é de 5min.

O tempo de inatividade dos demais usuários pode ser configurado. Os tempos disponíveis são: 1 min, 5 min, 10 min ou 15 min.

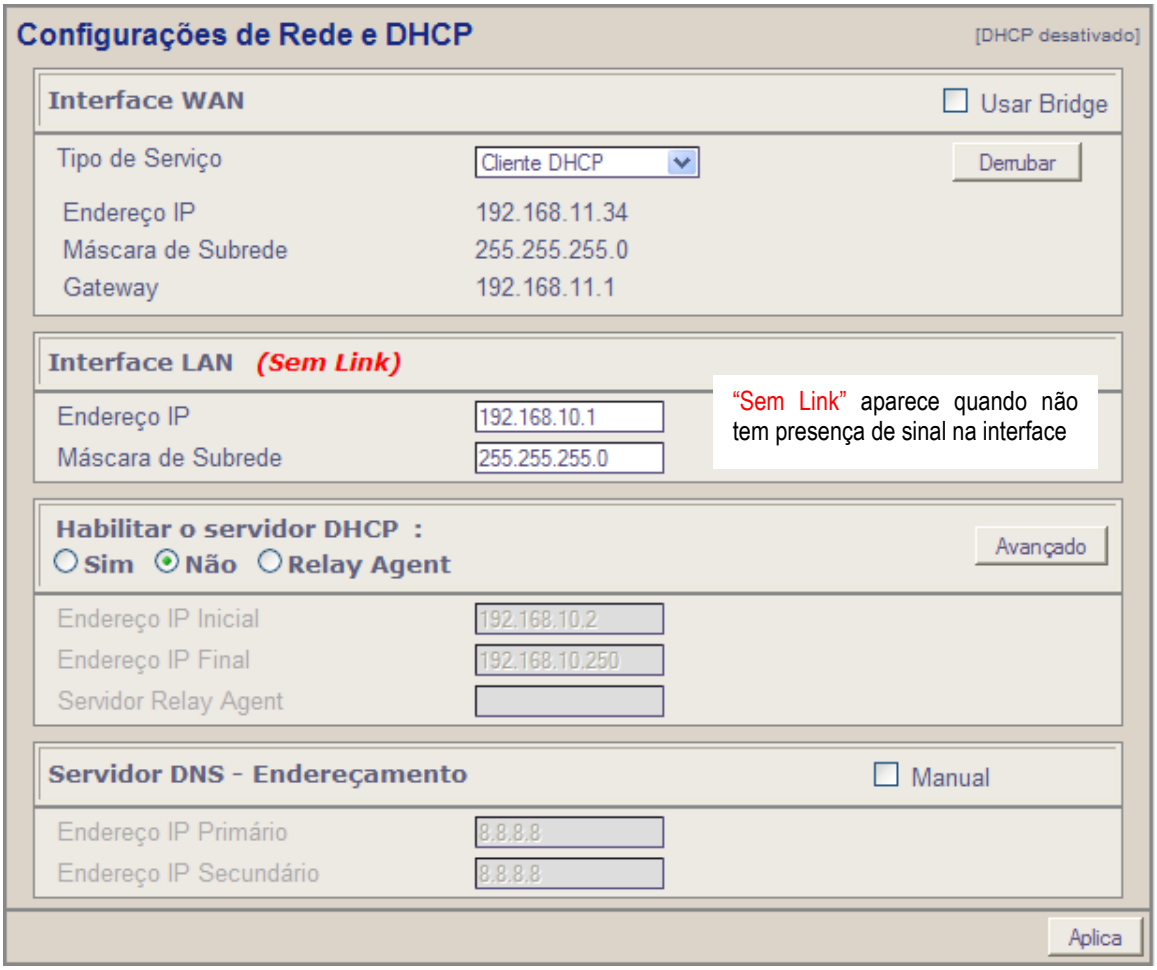
É permitido o cadastro de 8 grupos de usuários e 16 usuários.

Não é permitido alterar os acessos do Grupo Admin.

3. Configurações de Sistema
3.1. Rede

Para usufruir o máximo de recursos de seu Gateway Digistar é necessário que ele tenha um IP público da interface WAN, ou seja, que o Gateway Digistar esteja na "ponta da rede". Somente desta forma haverá o correto funcionamento de recursos como QOS, VPN e firewall, além de facilitar em muito a comunicação VoIP.

3.1.1. Configurações de Rede e DHCP



Usar Bridge

Para configurar o Gateway Digistar em modo bridge, basta selecionar o checkbox "modo Bridge". Neste modo as duas interfaces ficam ligadas como se fossem um switch de dados e o Gateway Digistar passa a responder por um único endereço IP.

No modo bridge vários campos do configurador ficam desabilitados.

Para evitar problemas de "looping de rede", onde equipamentos são acessáveis através das duas interfaces de rede do Gateway Digistar, o mesmo possui Spannig Tree Protocol que serve para definir qual será a interface de comunicação com os equipamentos.

Interface WAN

A interface WAN tem 3 possibilidades de configuração:

- **Cliente DHCP:** DHCP significa *Dynamic Host Configuration Protocol*, ou seja, Protocolo de Configuração de Host Dinâmico. Em redes TCP/IP, todo computador precisa ter um número de IP diferente. Para que não haja conflito de duas máquinas terem o mesmo número IP, seleciona-se uma máquina que forneça os IPs para todas as máquinas da rede. Clicando na opção SIM para a interface WAN o endereço IP será obtido automaticamente. Esta é a opção padrão. Dependendo do servidor DHCP utilizado o endereço IP obtido pode mudar cada vez que o Gateway Digistar for religado.

> ***OBS.:***
>
> *Se ligar o Gateway Digistar sem o cabo de rede, é necessário "Aplicar" as "Configurações de Rede e DHCP" após conectar o cabo para obter o endereço IP.*

- **IP Fixo:** Usa uma configuração de IP fixo. É normalmente usada quando não há servidores DHCP ou há a necessidade de fixar um IP dentro da rede. Para usar IP fixo devem ser configurados o endereço IP, a máscara de rede e o gateway (roteador).

- **Cliente PPoE :** Quando usado um modem bridge na interface WAN, existe a possibilidade do Gateway Digistar efetuar a autenticação. Para isso você deve entrar com o login, ou o nome do usuário e a senha. O protocolo de autenticação utilizado é PAP ou CHAP, selecionado automaticamente.
  Muitas vezes podem existir problemas na camada física em uma conexão do tipo PPPoE, que é de responsabilidade do modem externo. Assim, o link fica sem receber dados e o gateway não tem como saber se os dados pararam de chegar por inatividade ou por algum problema. Para resolver este problema foi implementado um comando de eco (echo em inglês) para que um pacote seja enviado pelo Gateway Digistar e o outro lado responda. Caso não seja recebida a resposta do eco, a interface do Gateway Digistar é reiniciada. Vale lembrar que nem todas as operadoras respondem ao echo. Também é possível configurar o intervalo de envio dos echos para ajustar o sistema.

Interface LAN

Endereço IP: Este endereço será o IP no qual se tem acesso ao configurador WEB a partir da interface LAN. No Gateway Digistar sempre será feito NAPT (Ver "Configurações NAPT") de endereços, portanto o endereço interno deve obedecer ao range de IP privados definidos pela RFC-1918, que são:

10.0.0.0	-----	10.255.255.255
172.16.0.0	-----	172.31.255.255
192.168.0.0	-----	192.168.255.255

O valor padrão da interface LAN é 192.168.10.1

Máscara de Subrede: Máscara de Sub-rede que deverá ser igual em todas as máquinas conectadas a porta LAN do Gateway Digistar. Este parâmetro define o número máximo de máquinas que podem ser conectadas na rede interna.

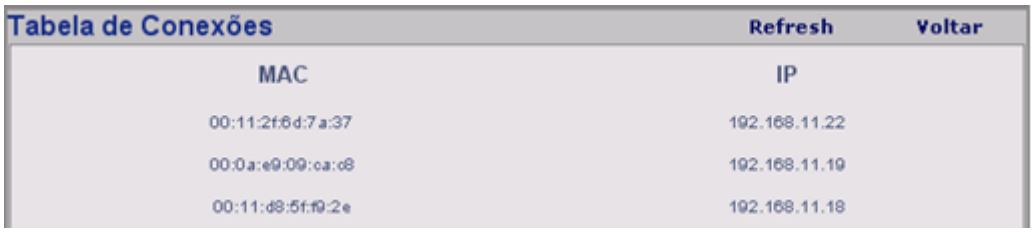
O valor padrão para a máscara de rede é 255.255.255.0 permitindo até 253 máquinas na rede interna do Gateway Digistar.

Servidor DHCP

Para que a máquina que irá acessar o configurador WEB ou as máquinas ligadas na LAN do Gateway Digistar possam usar IP dinâmico, o Gateway Digistar possui um servidor DHCP. Para configurar o servidor é necessário entrar com o endereço IP inicial e o endereço IP final que devem estar contidos no endereçamento da LAN.

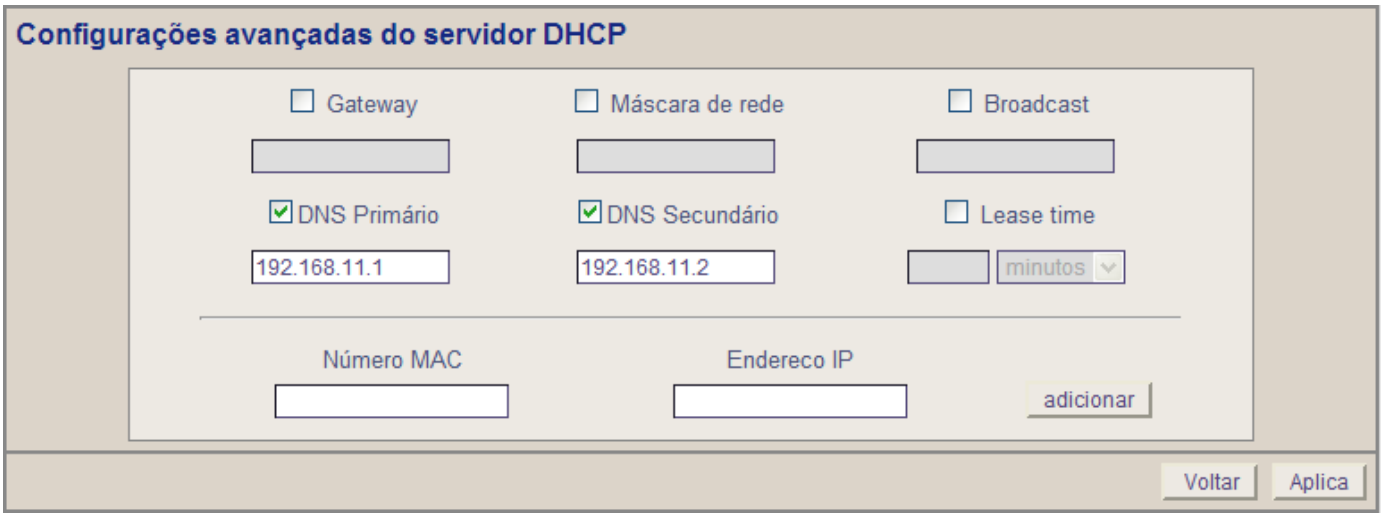
Caso alguma outra máquina dentro da mesma rede esteja fazendo o servidor DHCP é possível usar a opção DHCP *relay* onde é especificado o número IP desta máquina.

Existe a possibilidade de visualizar quais os IP que foram fornecidos pelo servidor DHCP. Clicando na opção *"Ver Tabela fornecida pelo DHCP"* mostra os números MAC de cada máquina com seus respectivos números IP.



DHCP Avançado

Além das configurações básicas como IP inicial e IP final do servidor DHCP, também é possível configurar no Gateway Digistar, em "DHCP Avançado", o gateway, máscara de rede, broadcast, DNS primário e secundário, Lease Time (tempo de validade) e fixar o IP para cada número MAC.



Servidor DNS

Para transformar os nomes em endereços IP (p.ex www.digistar.com.br no IP 200.234.200.30), existem espalhados pela rede diversos servidores de nome. Existe a possibilidade de usar até dois servidores de nomes. O Gateway Digistar também pode ser utilizado como um DNS relay, desde que se configure nas máquinas da rede interna o DNS com o IP da LAN.

3.1.2. Configurações de Roteamento Estático

O processo de roteamento de pacotes da rede funciona de forma semelhante a uma ligação telefônica. Quando uma ligação é efetuada de uma origem até um destino a ligação passa por diversas centrais telefônicas. Se o número de destino não faz parte da central, a ligação é direcionada para outra central. Para que auxilie no processo existe uma série de códigos de operadoras, países, estados e cidades.

Bastante parecido com o processo das ligações telefônicas, ocorre o roteamento em uma rede de dados. Quando um dado é transmitido de uma origem até um destino, existem diversas máquinas na rede que estabelecem quais os caminhos que os mesmos devem percorrer. Estas máquinas são chamadas de *roteadores* ou *gateways* e o processo de decisão do caminho dos pacotes é chamado de roteamento.

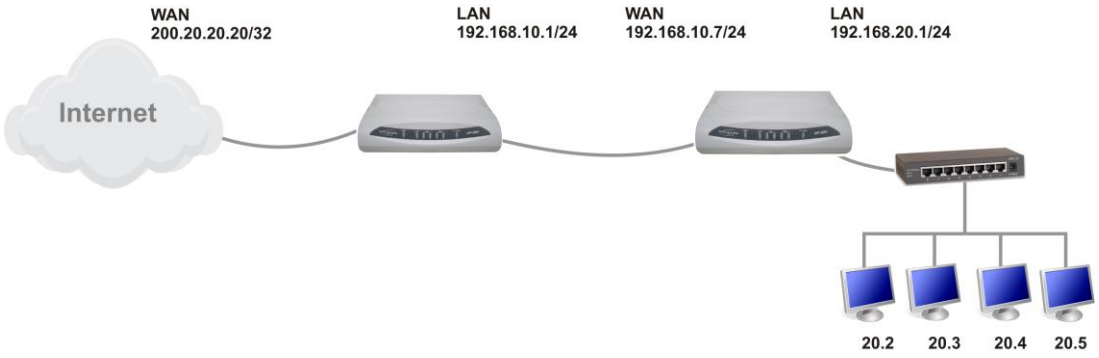
Os roteadores possuem tabelas que contêm informações de quais redes e máscaras de redes que estão conectados a eles. Se a rede de destino especificada não estiver nas tabelas de rotas, os dados são encaminhados para uma rota padrão (*default* ou 0.0.0.0).

Existem dois tipos de roteamento: rotas estáticas e rotas dinâmicas. As rotas estáticas são explicitamente configuradas pelo usuário, e as rotas dinâmicas podem ser "aprendidas" e divulgadas através da utilização de protocolos especiais.

No Gateway Digistar o usuário pode configurar as rotas estáticas de duas formas: como host ou como rede. Deve-se usar uma rota do tipo *host* quando houver a conexão de uma máquina isolada na rede LAN do Gateway Digistar. Quando houver outra rede na LAN do Gateway Digistar, deve-se adicionar uma rota do tipo rede para que os dados sejam roteados corretamente.

A rota padrão do Gateway Digistar é sempre a conexão da WAN, quer ela esteja configurada como dinâmica, estática ou PPPoE.

Se, por exemplo, estivermos cascateando dois Gateway Digistar, conforme diagrama abaixo:

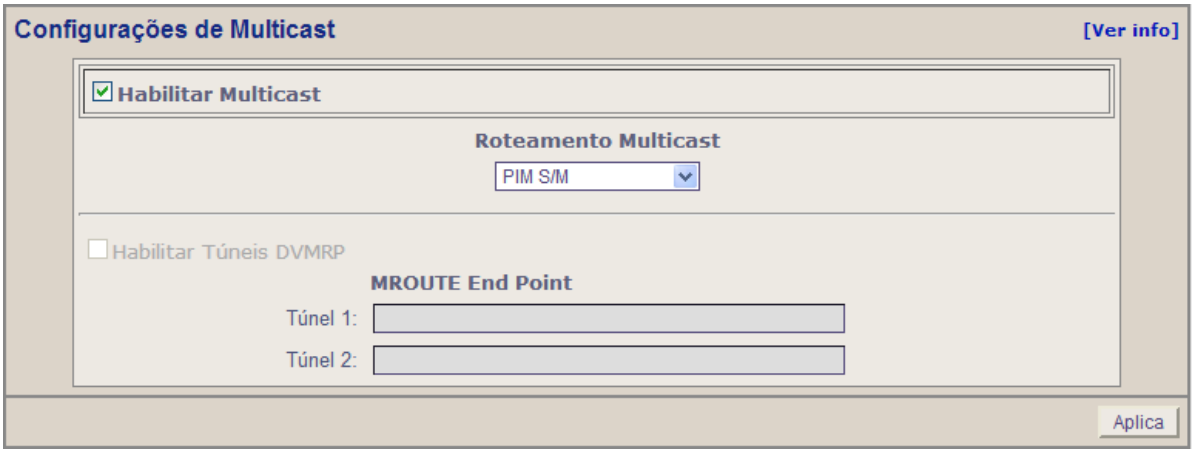


Se quisermos que o primeiro gateway (o conectado a INTERNET) acesse as máquinas que estão atrás do segundo gateway (na sub-rede 192.168.20.0/24), temos que criar uma rota estática informando que existe uma rede 192.168.20.0 através do endereço 192.168.10.7.

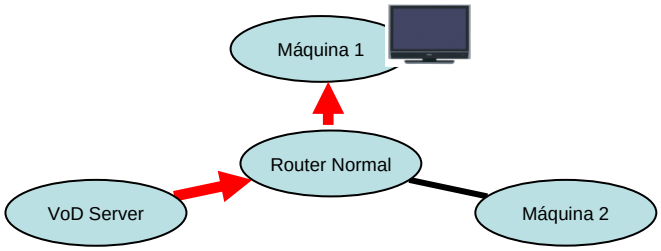
Para visualizar as tabelas de roteamento que estão ativas, basta clicar na opção "*Ver Tabela de Roteamento*"

OBS.: *As métricas são automáticas.*

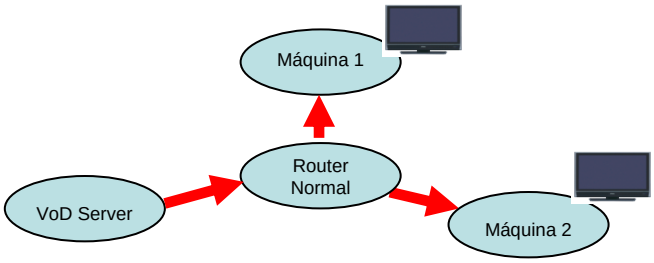
3.1.3. Configurações de Multicast



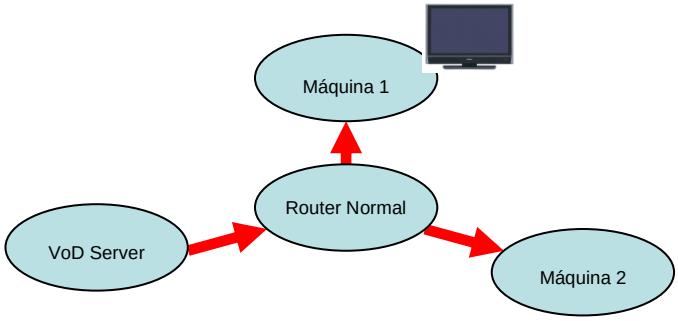
Multicast - Triple Play: O triple play é a união de dados, voz e vídeo na Internet. O Gateway Digistar faz somente redirecionamento dos pacotes de vídeo, não fazendo transcodificação (mudança de padrão) ou redimensionamento. Atualmente os vídeos utilizam pacotes do tipo Unicast. Abaixo podemos ver uma máquina de Vídeo sobre Demanda (VoD) transmitindo para a Máquina 1:



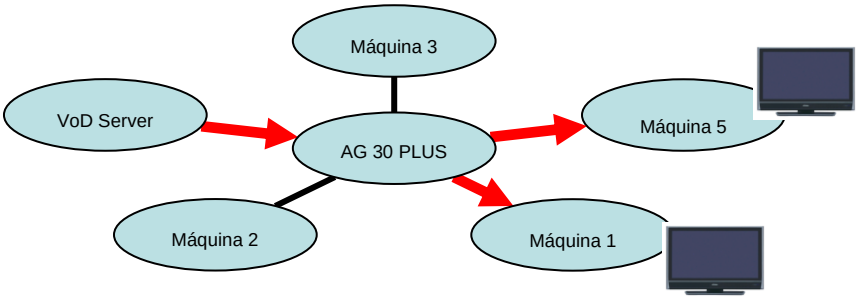
Para a Máquina 2 ver o vídeo, o VoD tem que transmitir o dobro de banda para as duas máquinas poderem assistir o vídeo.



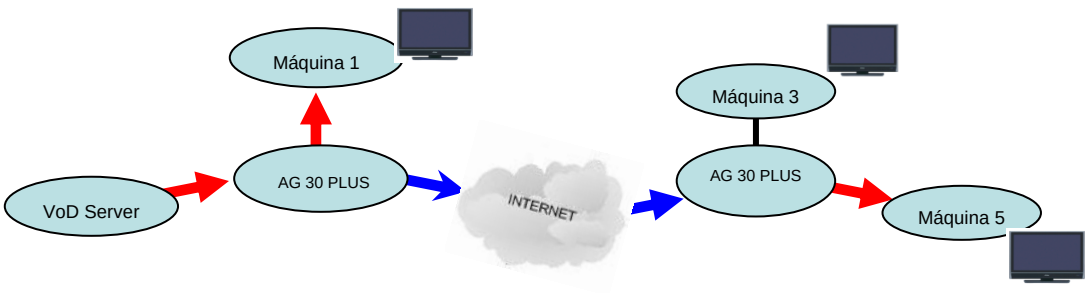
Outra alternativa para economizar banda do VoD seria utilizar pacotes do tipo broadcast. Todas as máquinas do roteador estariam recebendo vídeo, querendo ou não vê-los.



Com o Multicast podemos economizar banda do servidor de vídeo e mandar apenas para quem precisa:



Isso viabiliza sistemas de vídeo-conferência, vídeo-aula, treinamentos on-line e IPtv. Atualmente poucos roteadores no mercado suportam multicast assim como a própria WEB. A Digistar, já preparando o Gateway Digistar para a necessidade de transmissão de vídeo pela WEB, tem como recurso os túneis DVMRP, que capturam os pacotes multicast para serem enviados unicast para outro roteador.



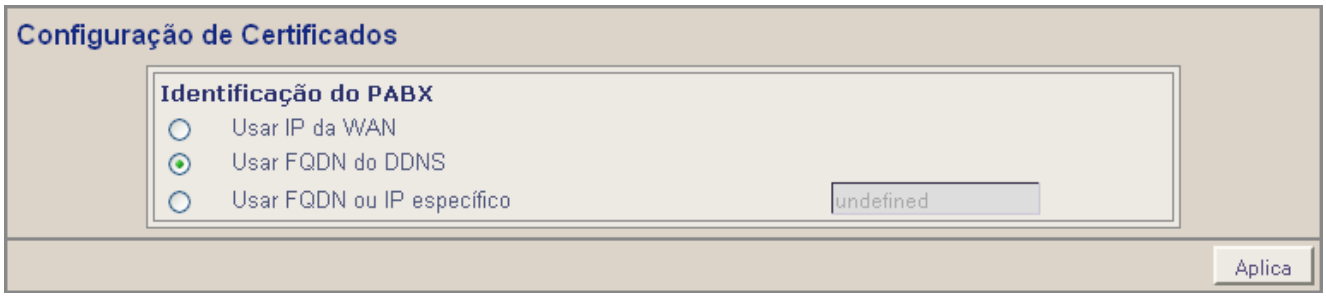
3.1.4. Configuração de Certificados

Certificados digitais são arquivos que tem o propósito de identificar realmente cada máquina. Em um certificado digital há informações pessoais da empresa, mas a principal informação presente em um certificado é a sua chave pública. A criptografia usada na Internet se baseia no sistema de chaves. O algoritmo usado na criptografia faz com que sejam geradas duas chaves, uma pública e outra privada. A chave pública, que está presente no certificado digital, é usada para criptografar dados a serem enviados ao dono do certificado. Já a chave privada, que só o dono do certificado conhece, serve para descriptografar a informação que foi criptografada com a sua chave pública. É importante notar que não é possível descriptografar a informação sem ter a chave privada e não há meios de, através da chave pública, deduzir a chave privada.

Outro ponto importante para a geração do certificado é a identidade de cada Gateway Digistar, chamado de nome comum. O nome comum é o endereço do Gateway Digistar. É importante lembrar que para a geração de certificados não existe a tradução de nomes para endereços, ou seja, se o nome comum do certificado for "www.digistar.com.br" o certificado só será válido se o usuário digitar especificamente o nome "www.digistar.com.br". Se for digitado o IP correspondente ao site www.digistar.com.br, que é 200.234.200.30, irá aparecer uma mensagem indicando um erro no certificado.

Cada nome na internet também é chamado de FQDN, ou Nome de Domínio Totalmente Qualificado e pode ser configurado com seu IP fixo através de um provedor de nome (DNS providers) ou até mesmo com IP dinâmico através de provedores de DNS dinâmicos (ver *"seção abaixo"*).

Como cada Gateway Digistar terá um FQDN ou IP diferente, é necessário criar um certificado próprio para garantir mais autenticidade e segurança.



3.1.5. Configurações do DNS Dinâmico

A internet com IPv4 utiliza endereçamento de 4 octetos em que cada um pode ir de 0 a 255. Assim para cada máquina conectada temos que ter um número do tipo 200.200.200.200. Uma solução para que não precisássemos saber o número IP de cada site na internet foi usar um servidor de nomes que faz a troca de endereços do tipo *www.digistar.com.br* para 200.234.200.30.

Em alguns casos, os números IP fornecidos pelos servidores DHCP da WAN ou pelo provedor no PPPoE podem mudar em intervalos de tempo. Se houver uma troca de número IP, a associação com o nome irá falhar.

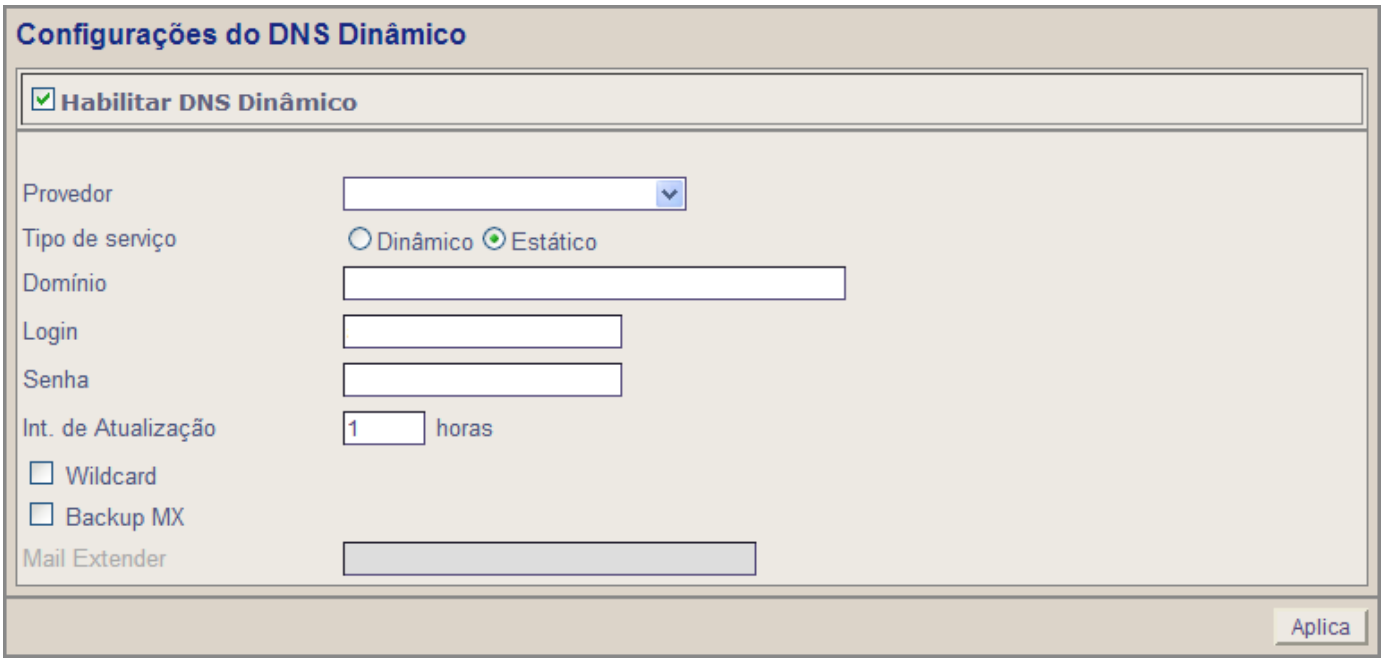
Para resolver estes problemas alguns provedores oferecem serviços conhecidos como DNS dinâmicos. Estes serviços registram um nome associando ao IP fornecido pela operadora. Em intervalos de tempo ou toda vez que houver uma troca de IP, todos os servidores de nome da internet serão atualizados. Se você possuir um IP fixo, também é possível configurar o Tipo do Serviço como estático, assim só haverá atualização de registro quando o Gateway Digistar for ligado.

Normalmente os servidores de nomes fornecem um nome do tipo *nome.servidor.com*. É possível usar um wildcard (coringa) na frente do nome, assim qualquer coisa na frente do nome.servidor.com é vista como um sinônimo. Por exemplo, se for marcado o wildcard, o domínio *www.servidor.no-ip.com*, *www2.nome.servidor.no-ip.com* ou *nome.servidor.no-ip.com* são sinônimos, ou seja, fornecem o mesmo número IP.

Também existe a opção de redirecionar os e-mails recebidos no *mail.nome.servidor.no-ip.com*, de acordo com nosso exemplo, para um outro servidor de e-mails, caso o Gateway Digistar estiver desligado. Para isso, basta ligar a opção backup MX, especificando onde os e-mails serão guardados. Todas as opções devem ser suportadas pelos provedores de DNS dinâmico.

Se o Gateway Digistar estiver atrás de um NAPT, ou seja, possuir um IP privado na interface WAN, o DNS dinâmico será automaticamente desabilitado. Alternativamente é possível usar o DNS dinâmico com a opção STUN do NATT (*Ver Configuração do NATT*). Usando o STUN, o Gateway Digistar irá descobrir qual o IP externo para mandar para o servidor DDNS.

Dependendo do intervalo de tempo em que o endereço da WAN sofre atualizações, é possível atualizar o endereço com o FQDN (nome do domínio completo) no Intervalo de Atualização de 0.1 horas (6 minutos) à 99 horas.



3.1.6. Configuração de VLAN

O nome VLAN é uma abreviatura de Rede de Acesso Local Virtual. A principal vantagem é de computadores ligados em locais físicos diferentes se comportarem como se estivessem conectados no mesmo fio. A configuração de VLANs é feita por software, tornando as redes extremamente flexíveis, assim um computador pode se mover para outro local físico (dentro da mesma LAN) sem a necessidade de nenhuma mudança de configuração de hardware ou software.

As VLANs são definidas pela IEEE 802.1Q operando em camada 2 pelo modelo OSI. Porém como cada definição de VLAN mapeia uma rede e sub-rede, existe a impressão de estar trabalhando em camada 3, a nível de rede. Reduzindo o tamanho das redes, reduzimos também o tamanho de domínio de broadcast.

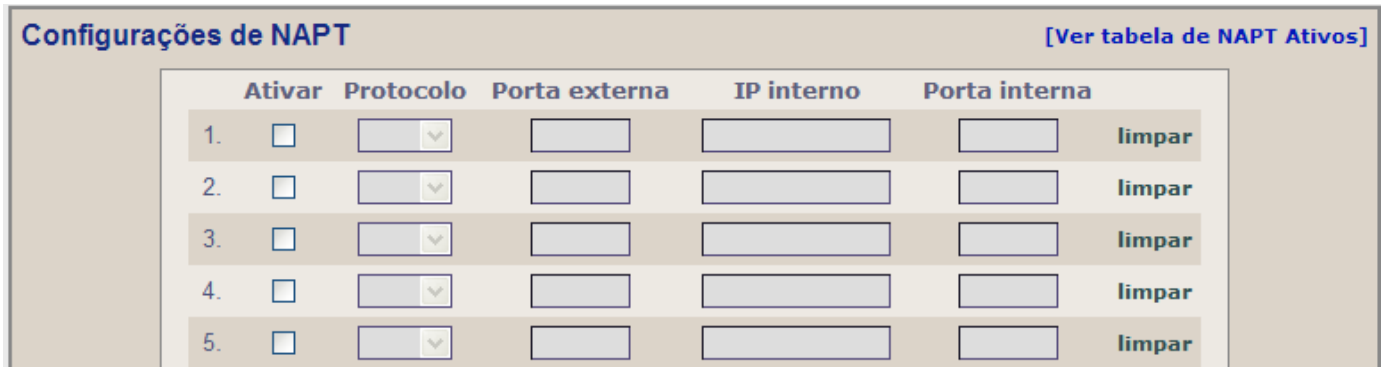
É possível criar dentro de cada LAN até 4096 VLANs (ID). Cada VLAN também tem oito possibilidades de priorização de pacotes no campo QOS. As VLAN podem ser do tipo host (para ligar apenas uma máquina) ou do tipo rede (para criar realmente uma rede virtual). As VLAN podem ser criadas dentro da rede interna (LAN) ou para a interface externa (WAN).

3.1.7. Configurações de NAPT

NAPT (Network Address and Port Translation) é a tradução de endereços e portas de rede, sendo ambos utilizados para mapear endereços e/ou portas de uma rede interna para um IP público real. NAT/PAT também é uma ferramenta de proteção contra ataques, uma vez que as máquinas conectadas na rede interna não são visíveis à rede externa.

De maneira geral o uso do NAT/PAT se dá de forma automática e transparente. Um computador ligado à rede interna (LAN) do Gateway Digistar pode fazer um acesso externo sem qualquer problema.

Em alguns casos, existe a necessidade de instalar um servidor em uma máquina na rede interna. Isso é muito utilizado em servidores de página WEB ou servidores de e-mail. Para isso é possível especificar qual a translação do IP e/ou a porta do serviço externo para uma máquina interna.



Por exemplo, se existe um servidor http (WEB) na porta 80 da máquina 192.168.10.12 conectada na rede LAN do Gateway Digistar é possível criar uma regra:
Protocolo – TCP (para servidor http), porta externa - 80, IP interno 192.168.10.12 (IP da máquina na rede interna que possui o serviço) e porta interna 80 (a porta utilizada pelo serviço).

Com o exemplo acima, toda vez que for acessado o IP externo a WAN na porta 80, o Gateway Digistar fará uma conexão com a máquina interna 192.168.10.12.

3.2. Firewall

Um firewall tem a tarefa de restringir o tráfego entre uma **rede protegida** e uma **rede não-confiável.** Este procedimento visa aumentar a segurança da rede protegida, minimizando a possibilidade de atividade maliciosa. Porém, deve-se notar que qualquer serviço cujo acesso seja permitido através do firewall ainda é um risco potencial. As abordagens utilizadas para segurança de uma rede em ordem crescente de grau de limitação de tráfego são descritas abaixo:

Tudo é permitido: Permite todo tráfego de rede, ou seja, não existe proteção.

Tudo que não é proibido é permitido: Proíbe explicitamente determinados tráfegos. Todo o resto do tráfego é permitido. É difícil determinar todos os tipos de tráfego potencialmente maliciosos.

Tudo que não é permitido é proibido: Permite explicitamente determinados tráfegos. Todo o resto do tráfego é proibido. O tráfego que deve ser permitido é mais fácil de determinar que o tráfego que não deve ser permitido. Se o tráfego não for explicitamente permitido será bloqueado.

Tudo é proibido: Sem tráfego entre a rede protegida e a rede não-confiável. Utilizada por exemplo em casos de suspeita de invasão.

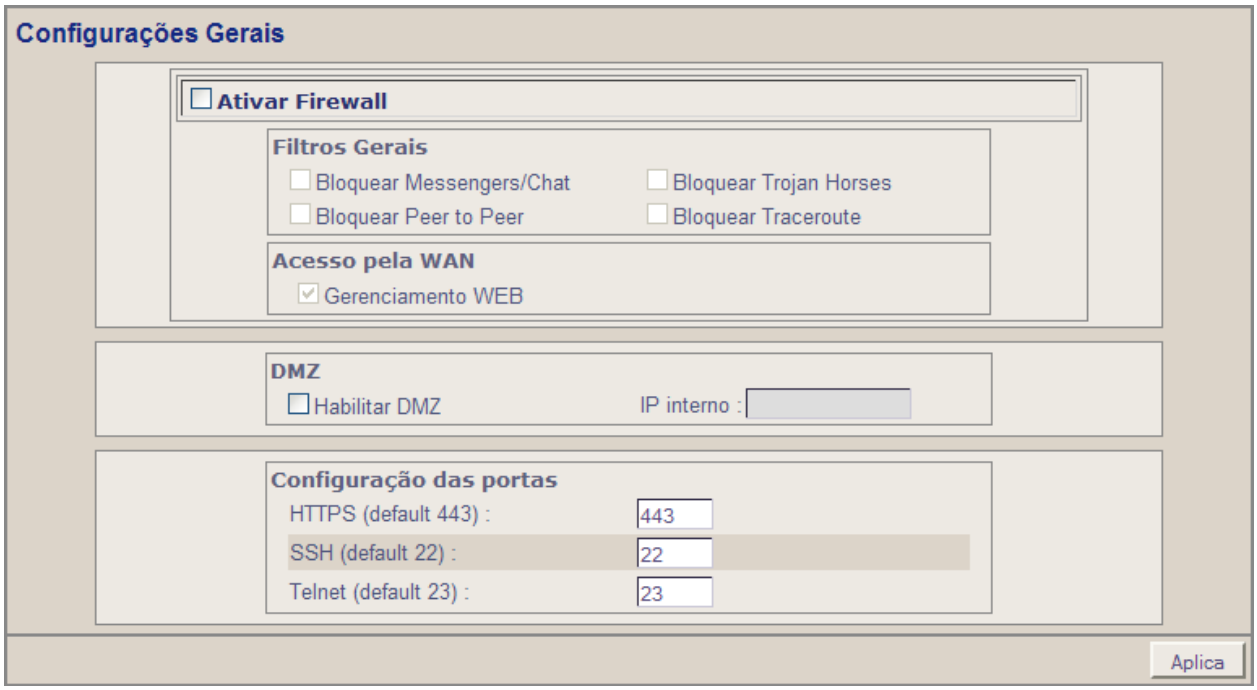
A abordagem utilizada pelo firewall implementado no Gateway Digistar é a **tudo que não é permitido é proibido.** Este é o tipo de firewall mais recomendado e utilizado por ser o mais seguro. A rede protegida engloba as máquinas acessíveis pela interface da LAN e por túneis VPN. A rede não-confiável é formada pelas máquinas acessíveis pela interface da WAN. O firewall do Gateway Digistar é um firewall stateful, ou seja, guarda o estado do tráfego recente de pacotes. Por padrão o firewall ativado permite os seguintes tipos de tráfego:

- Pacotes originados da rede protegida para qualquer destino.
- Pacotes TCP de conexões já estabelecidas ou sendo iniciadas pela rede protegida.
- Pacotes UDP onde já houve tráfego em alguma das direções.
- Pacotes ICMP relacionados a outros pacotes.
- Pacotes ICMP echo-request.
- Pacotes TCP e UDP para portas explicitamente abertas.
- Outros tráfegos explicitamente permitidos, determinados pelas configurações dos serviços Gateway Digistar.

As configurações do firewall pela interface Web estão divididas em quatro páginas. A primeira página contém configurações gerais e as páginas seguintes as configurações para proteção contra ataques de DoS, regras de firewall do usuário e filtros de conteúdo. Para que o firewall possa estar ativo é necessário que a interface da WAN esteja configurada.

3.2.1. Configurações Gerais

Nesta página pode ser ativado/desativado o firewall, configurar o acesso a serviços pela interface da WAN e ativar os filtros gerais e configurar uma máquina de DMZ



- **Ativar Firewall:** Ativa/Desativa o Firewall. A ativação ou desativação afeta as configurações das demais páginas do firewall, ou seja, para que as configurações das outras páginas do firewall tenham efeito, o firewall deve estar ativado aqui.

- **Filtros Gerais:** permitem bloquear determinados tráfegos de dados.
  - Bloquear Messengers/Chat: protocolos de troca de mensagens instantâneas como ICQ e MSN Messenger.
  - Bloquear Peer-to-Peer: protocolos peer-to-peer de compartilhamento de arquivos como pelas redes eDonkey, Kazaa e BitTorrent.
  - Bloquear Trojan Horses: portas comuns de cavalos de tróia. As portas TCP bloqueadas são: ”135 à 139, 444, 666, 1234, 1524, 3127 à 3149, 4000, 6000, 6006, 12345, 12346, 16660, 27665, 31337, 33270". As portas UDP são: ”135 à 139, 444, 995 à 999, 6667, 6711, 8998, 12345, 12346, 27444, 31335, 31337, 60001”.
  - Bloquear Traceroute: pacotes de traceroute por UDP e ICMP.
- **Habilitar DMZ** Especifica uma máquina da rede protegida para ser utilizada como DMZ (De-Militarized Zone). Se o DMZ estiver habilitado os pacotes serão tratados respeitando a seguinte ordem de precedência:
  - Pacotes para portas abertas pelo Gateway Digistar não são redirecionados.
  - Pacotes para portas com redirecionamento por NAT são enviados para as máquinas da rede protegida correspondentes ao redirecionamento.
  - Pacotes para as demais portas são redirecionados para a máquina configurada como DMZ.

- **Acesso pela WAN:**
  - Gerenciamento WEB: Habilita/Desabilita o acesso ao Configurador Web Digistar pela interface da WAN. Se estiver desabilitado então o gerenciamento só pode ser realizado a partir da rede protegida.

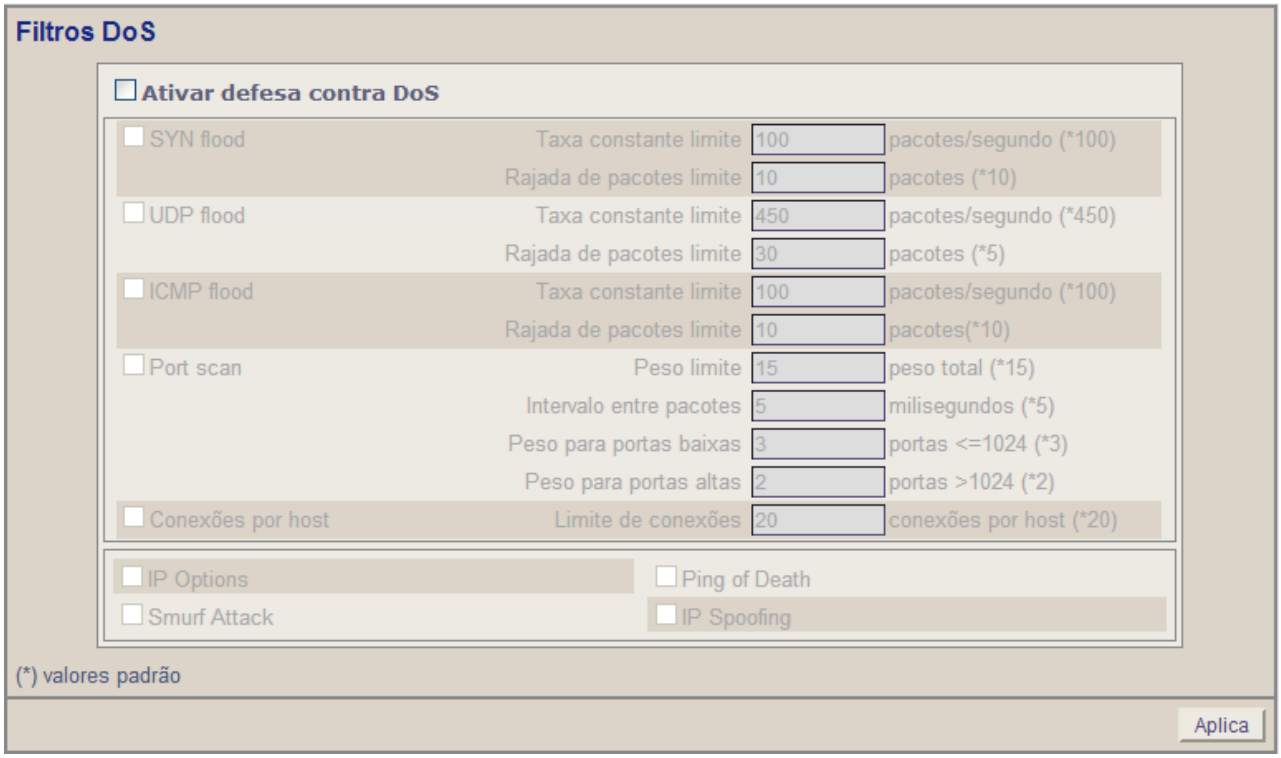
- **Configuração das Portas:**
  - HTTPS: especifica a porta que será utilizada pelo servidor https do Configurador. Por padrão é utilizada a porta 443. No caso de alteração desta porta, a página do configurador deve ser recarregada no browser especificando a nova porta.

- SSH: É utilizada para fins de depuração do equipamento. Se em sua rede há algum servidor SSH, para que esta porta (padrão 22) seja redirecionada pelo NAPT ou DMZ, há a necessidade de trocar a porta SSH do Gateway Digistar para outra diferente da porta 22.

- Telnet: É utilizada para fins de depuração do equipamento. É semelhante ao protocolo SSH, mas este não possui criptografia. Se em sua rede há algum servidor telnet, para que esta porta (padrão 23) seja redirecionada pelo NAPT ou DMZ, há a necessidade de trocar a porta SSH do Gateway Digistar para outra diferente da porta 23.

3.2.2. Filtros DoS

Nesta página são feitas as configurações de proteção contra ataques comuns de DoS (*Denial of Service ou Negação de Serviço*). Ataques deste tipo comprometem a disponibilidade das máquinas atingidas, seja por alguma vulnerabilidade de segurança ou por sobrecarga de processamento, fazendo com que estas não consigam atender a demanda de requisições dos clientes. As configurações a seguir devem ser utilizadas com cautela sob o risco de comprometer a eficiência da rede ou mesmo torná-la inutilizável através do Gateway Digistar. Deve-se tomar cuidado, sobretudo, com as configurações de proteção contra flood e limite de conexões. Caso deseje alterar os parâmetros pré-configurados para as configurações dos filtros DoS é recomendado que se verifique se o desempenho da rede não foi prejudicado antes de salvar as configurações. Cada configuração de filtro DoS possui parâmetros, com valores padrão que podem ser utilizados com segurança.



- **Ativar defesa contra DoS:** Ativa/Desativa as configurações de defesa contra DoS.

Os filtros de proteção contra flood se baseiam em algoritmos de baldes de fichas (token bucket algorithms), bastante utilizados para controle de tráfego em dispositivos roteadores. A implementação do algoritmo permite configurar a taxa limite para rajadas de pacotes (limit burst) e o valor para taxas constantes de pacotes (limit rate). No caso de suspeita de flood é gerado log com informações. Para pacotes TCP SYN, os pacotes originados da máquina suspeita são descartados durante 10 segundos.

SYN Flood: Limita a entrada dos pacotes TCP com flag SYN setada. Este tipo de pacote é utilizado para iniciar uma conexão TCP. Como cada recebimento de pacotes SYN acompanha a alocação de estruturas de dados para posterior estabelecimento da conexão TCP, um flood destes pacotes acabaria consumindo muitos recursos do sistema. Para minimizar este problema uma solução é descartar pacotes SYN excessivos originados de uma mesma máquina.

UDP Flood: Descarta pacotes UDP originados de uma mesma máquina em caso de suspeita de flood para evitar sobrecarga do sistema.

ICMP Flood: Descarta pacotes ICMP originados de uma mesma máquina em caso de suspeita de flood para evitar sobrecarga do sistema.

Port Scan: Proteção contra as técnicas de port scan mais conhecidas como TCP SYN, TCP connect, UDP, Stealth FIN, Xmas e Null Scans. Estes tipos de técnicas servem para encontrar portas abertas em máquinas e são os passos iniciais para a maioria dos ataques. Em caso de suspeita de port scan, o tráfego com a máquina remota é interrompido por 10 segundos e é gerado log com as informações. Quando um pacote de port scan é recebido na interface da WAN é criado um contador associado ao IP da máquina originadora deste pacote. Os pacotes de port scan seguintes originados desta mesma máquina incrementam o contador. Considera-se que o IP de origem está tentando realizar um port scan caso o contador atinja um valor limite pré-determinado. O mecanismo para detecção de port scan é configurado com os parâmetros a seguir:

- **Peso limite**: Valor limite do contador.
- **Intervalo entre pacotes**: Intervalo máximo de tempo, em centésimos de segundo, entre dois pacotes com portas diferentes e mesmo IP de origem para que o último pacote possa ser considerado um pacote de port scan.
- **Peso para portas baixas e para portas altas:** Os port scans são mais comuns em portas baixas (menores ou iguais a 1024), onde estão as portas padrão dos serviços mais visados por atacantes. Por causa desta tendência em ataques a portas mais baixas, o mecanismo de detecção permite especificar pesos distintos para pacotes destinados a portas baixas e para portas altas. Este peso é o valor que é acrescido ao contador do IP da máquina origem para cada potencial pacote de port scan recebido nas portas baixas, menores ou iguais a 1024, ou nas portas altas, maiores que 1024.

Por exemplo, considere que a proteção para port scan está habilitada e configurada com os seguintes parâmetros: peso limite igual a 15, intervalo entre pacotes igual a 5, peso das portas baixas igual a 4 e peso das portas altas igual a 3. Suponha a tentativa de port scan pela técnica TCP Stealth FIN a seguir: A máquina 10.20.30.40 envia uma seqüência de 5 pacotes para o IP da WAN do Gateway Digistar em cada uma das portas no intervalo de 21 a 25. O intervalo de tempo entre os envios é de 4 centésimos de segundo. Este intervalo está dentro do intervalo máximo configurado, então o contador será incrementado para cada um destes pacotes recebidos pela WAN do Gateway Digistar. O valor de cada incremento será de 4 unidades, pois todos os pacotes são para portas baixas. Com isso o contador para o IP 10.20.30.40 irá atingir o peso limite no quarto pacote de port scan recebido. A tentativa de port scan será registrada em log e os pacotes originados de 10.20.30.40 serão descartados durante 10 segundos.

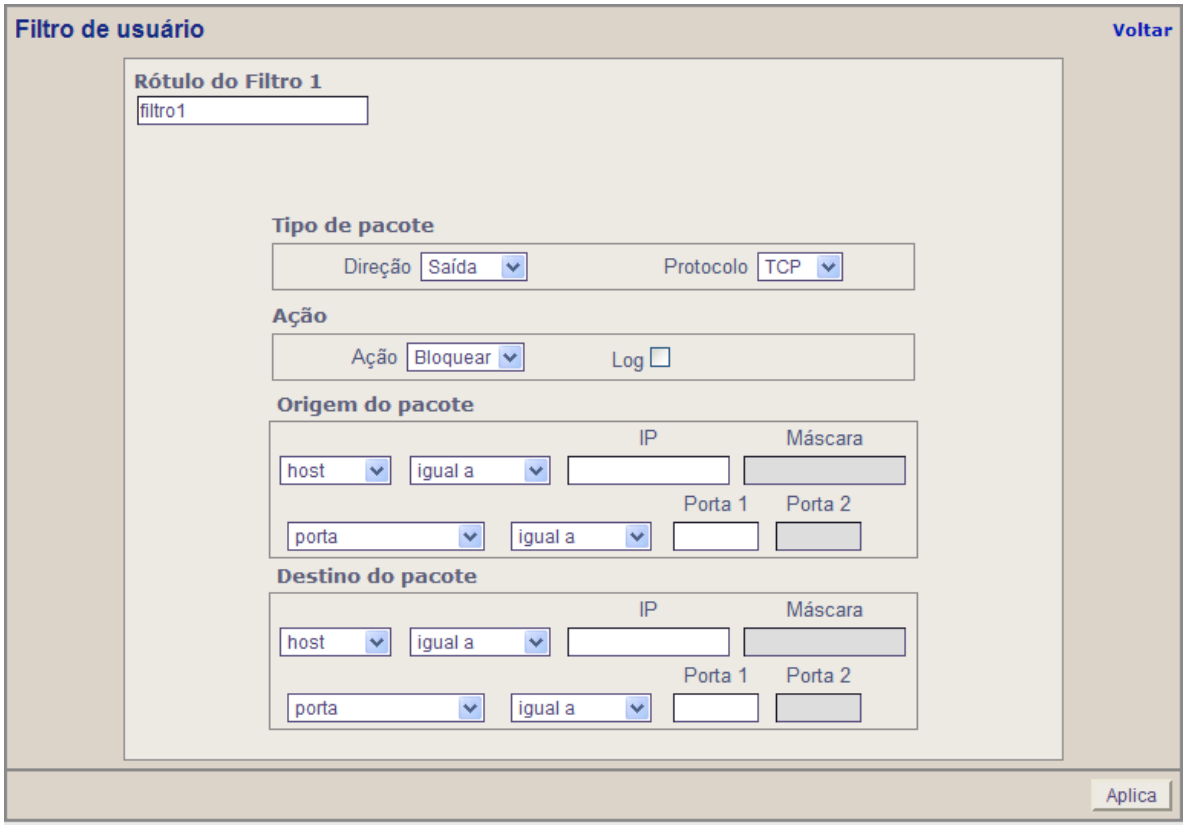
- **Conexões por host:** Limita o número de conexões TCP entre o Gateway Digistar e cada IP de máquina remota. Tentativas de novas conexões além do limite são ignoradas.
- **IP Options:** Descarta pacotes IP com IP Options setadas. Estes tipos de pacotes podem ser utilizados para comprometer sistemas com vulnerabilidades no protocolo IP.
- **Ping of Death:** Proteção contra pacotes ping of death. Pacotes icmp com tamanho muito grande. Alguns sistemas como o Windows 95 possuem vulnerabilidades a esse tipo de ataque. Para proteger as máquinas da LAN do Gateway Digistar os pacotes ICMP com tamanho muito grande são descartados.
- **Smurf Attack:** Protege contra ataques Smurf. Pings em broadcast com spoofing no IP de origem. Neste tipo de ataque o atacante envia pacotes ICMP echo-request em broadcast para uma subrede com IP de origem falsificado com o IP da vítima. Assim a vítima receberá tantos ICMP echo-replies quantas forem as máquinas da subrede que responderem ao ICMP echo-request. Esta subrede é chamada de smurf amplifier. Dependendo do número de máquinas na subrede e do número de ICMP echo-requests enviados pelos atacantes o acesso à máquina vítima poderá ficar comprometido. Para evitar que este tipo de ataque utilize a subrede do Gateway Digistar como smurf amplifier os pacotes ICMP em broadcast são descartados.
- **IP Spoofing:** Protege contra IP spoofing. Esta técnica consiste na alteração do IP de origem de pacotes fazendo que uma máquina atacante se passe por outra máquina. Diversos tipos de ataque são realizados em conjunto com IP spoofing, dentre elas o Smurf Attack. Para minimizar esses tipos de ataque o Gateway Digistar pode utilizar a técnica de reverse path filtering. O reverse path filtering verifica se a rede do IP de origem de cada pacote é alcançável pela interface que o pacote foi recebido, caso não seja o pacote é descartado.

3.2.3. Filtros de Usuário

Os filtros de usuário permitem que o usuário especifique suas próprias regras de firewall. Na versão atual do firewall é possível adicionar até 12 regras que serão cascateadas, uma após a outra.

O casamento de pacotes IP é feito pelo **tipo, origem** e **destino** do pacote. Pelo tipo indica-se a **direção** do pacote, ou seja, se ele está entrando na interface da WAN ou saindo por ela, e o **protocolo**, que pode ser TCP, UDP, ICMP ou IGMP.

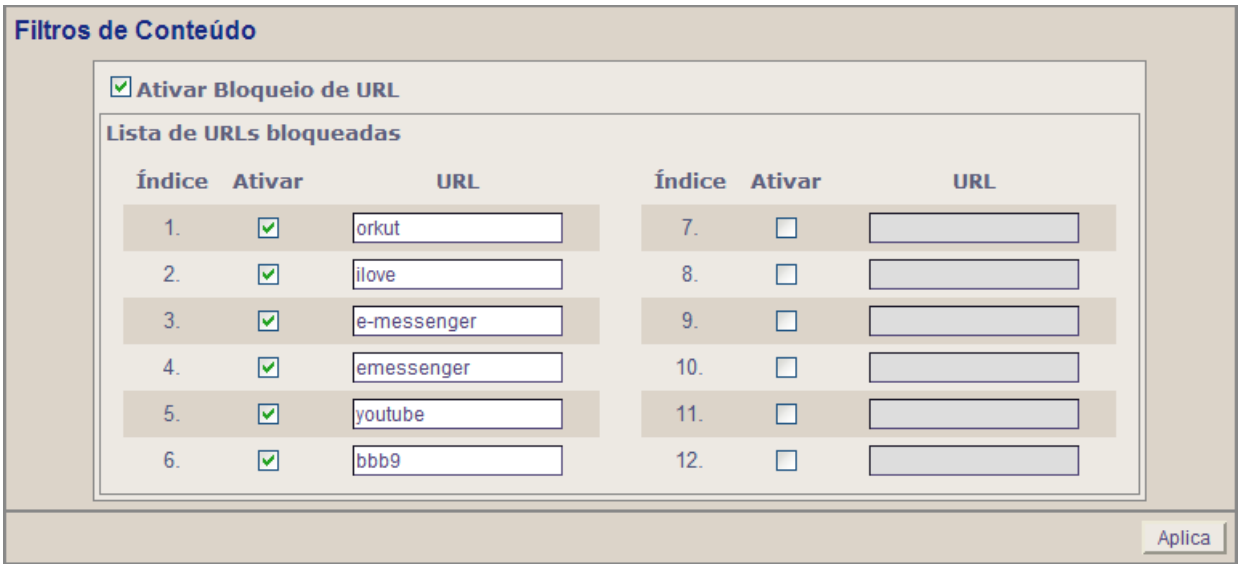
Pela origem e pelo destino pode-se indicar a máquina ou subrede e, no caso dos protocolos UDP e TCP, também podem ser informadas as portas utilizadas pelos pacotes. Quanto mais informações forem fornecidas, mais restrita será a regra. Quanto mais informações forem omitidas, mais ampla será a regra. Por exemplo, a regra que aceita pacotes TCP entrando na WAN da subrede 10.20.30.0 com máscara 255.255.255.0 é mais ampla que a regra que aceita pacotes TCP entrando na WAN da subrede 10.20.30.0 com máscara 255.255.255.0 com portas de destino entre 10000 e 20000. A primeira regra além de casar com os pacotes que casariam com a segunda regra também casa com pacotes com porta origem fora do intervalo de 10000 a 20000.



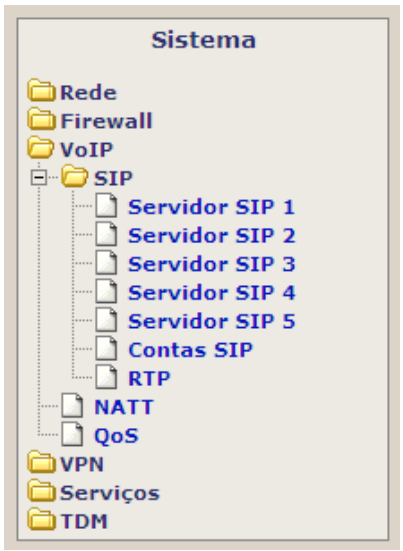
No caso de um pacote casar com alguma regra, a **ação** correspondente é executada e as demais regras são ignoradas. As ações possíveis são aceitar ou bloquear o pacote. Opcionalmente pode-se gerar **log** para cada pacote trafegado que casa com a regra criada.

3.2.4. Filtros de Conteúdo

Os filtros de conteúdo oferecem bloqueio de URLs para serviços de http. Até um total de 12 URLs podem ser bloqueadas. Para utilizar este recurso, basta adicionar a URL desejada e ativar a regra. Todas as requisições para URLs bloqueadas serão descartadas.



3.3. VoIP



As ligações IP são feitas no VoIP usando o protocolo SIP (Session Initiation Protocol, RFC3261). Este serve para negociar os parâmetros da comunicação via rede, escolhendo endereço e compactação para o envio e recepção de áudio. Depois de estabelecida a chamada, os pacotes de áudio trafegam usando o protocolo RTP (Real-time Transport Protocol, RFC3550 e RFC3551).

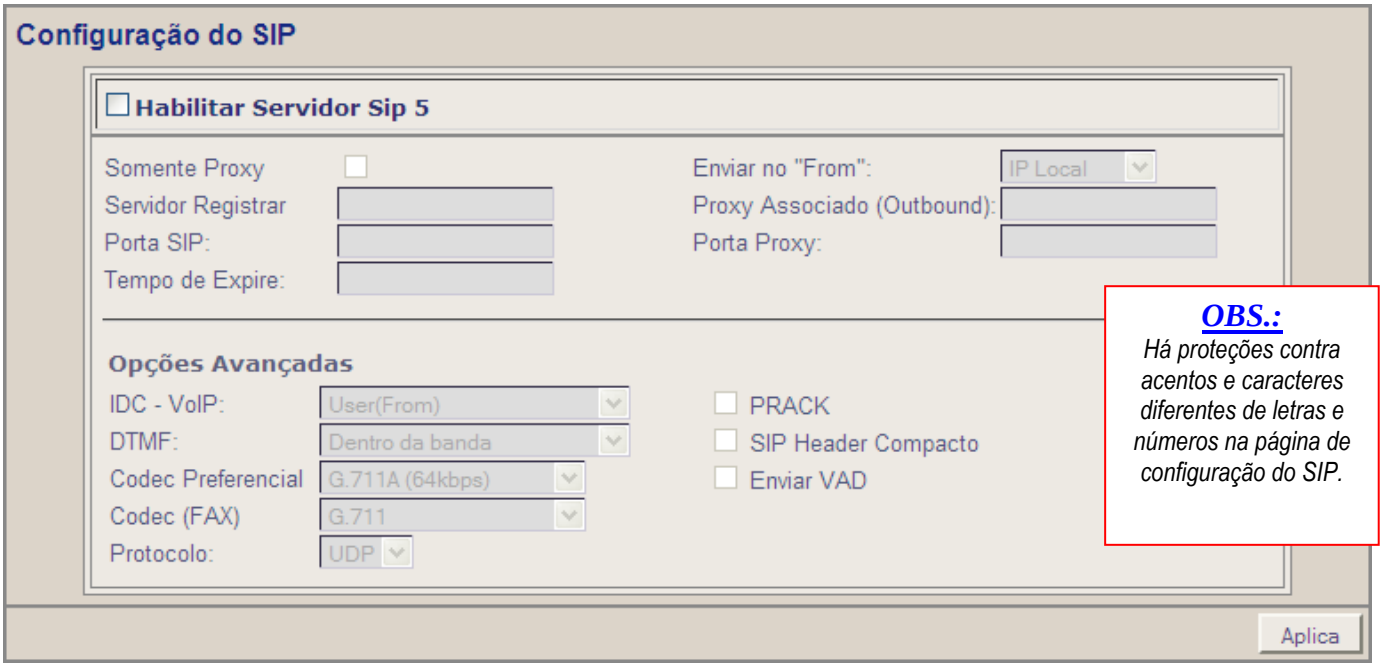
O protocolo SIP oferece a opção de usar um servidor SIP (Registrar/Proxy), que funciona como uma central de endereços SIP, onde cada ponto tem um nome de usuário associado ao seu endereço real. Nesse caso todas as mensagens SIP para outros pontos registrados no servidor Registrar/Proxy serão encaminhadas para o servidor, que através de seu banco de dados de usuários registrados irá encaminhá-las para o endereço correto. Isso é usado pelas operadoras VoIP.

Quando uma chamada é negociada, o protocolo de sinalização usado (SIP) precisa passar para o outro ponto de comunicação o endereço para onde deve ser enviado o áudio. Esse endereço precisa ser acessível a partir do outro ponto de comunicação, caso contrário a conexão não terá áudio. Se a WAN do Gateway Digistar estiver conectada à Internet através de um NAPT, ou seja, tiver um endereço IP de uma rede interna não-roteável, o STUN deverá ser habilitado para que as ligações VoIP tenham áudio.

3.3.1. Configuração do SIP

3.3.1.1. Habilitar Servidores SIP

Configuração dos servidores SIP (Registrar/Proxy) que serão utilizados para realizar e receber as ligações VoIP. É possível configurar até cinco (5) servidores SIP.



- **Habilitar Servidor SIP:** Habilita/Desabilita a utilização do servidor VoIP configurado.

    - ***Somente Proxy:*** Esta opção desabilita o envio do pedido de registro para o servidor SIP. As chamadas são encaminhadas para o endereço do servidor SIP Registar/Proxy sem que a mensagem REGISTER seja enviada.
        - ***Enviar no From*:** indica qual IP será usado na identificação do Access Gateway quando este originar uma chamada ao Servidor Proxy, sendo as opções disponíveis: o IP Local do Access Gateway ou o IP do Proxy. Para efetuar essa configuração a operadora deve ser consultada quanto à identificação da origem das chamadas.

    - ***Servidor Registrar/Proxy:*** endereço IP do servidor Registrar/Proxy.
    - ***Porta SIP:*** porta do servidor para a qual serão direcionadas as mensagens do protocolo SIP enviadas pelo Gateway Digistar. A porta padrão é 5060.
    - ***Tempo de Expire*:** duração dos registros em segundos. Após esse tempo, caso não tenha sido renovados, os registros são apagados do servidor.
    - ***Proxy Associado (Outbound):*** endereço do servidor que irá redirecionar os pacotes para o servidor Registrar/Proxy.
    - ***Porta Proxy:*** porta do Proxy Associado (*Outbound*) para a qual serão direcionadas as mensagens SIP. A porta padrão é a 5060.

- **Opções Avançadas:**
  - **IDC – VoIP:** permite configurar qual campo da mensagem INVITE do SIP será utilizado como o identificador da chamada (IDC) nas ligações de entrada efetuadas por esse Servidor ao Access Gateway.
    São disponíveis os campos User(From), que é o caso mais comum, DISPLAYNAME(From), que permite uma identificação mais amigável, porém é um campo não obrigatório, e URI(Contact), que comumente identifica o dispositivo de origem da ligação. O valor que vier no campo selecionado será utilizado nas regras de redirecionamento do VoIP para o TDM nas ligações provindas do domínio desse Servidor SIP. (ver seção: Redirecionamento).
    Obs.: caso for selecionada a opção DISPLAYNAME (From) e o INVITE chegar com esse campo vazio, será utilizado o valor do campo User (From).

  - **DTMF:** Método de transmissão de dígitos DTMF, pode ser dentro ou fora da banda. Quando estiver selecionado dentro da banda o DTMF é enviado com o áudio, podendo apresentar distorções que impossibilitam sua detecção pelo equipamento que irá recebê-lo.
    No DTMF fora da banda é usada a norma RFC2833, onde o dígito é enviado em um pacote RTP.

  - **Codec Preferencial:** compressão de áudio que terá preferência na negociação da chamada. Caso a outra ponta da chamada não suporte a codificação escolhida, outro codec será usado automaticamente.
    - Codecs disponíveis: G.729AB (8kbps), G.711A (64kbps) e G.711U (64kbps).

  - **Codec (FAX):** Escolha do codec que será usado para a recepção de FAX via VoIP. Para que o T.38 funcione, o aparelho de FAX que irá receber deve estar configurado para recepção automática. Ao enviar um FAX via VoIP é o ponto que recebe o FAX que determina o protocolo a ser usado. Codecs disponíveis: G.711 e T.38.

  - **Protocolo:** Define o protocolo de transporte da sinalização SIP desse servidor. Atualmente tem-se disponível o protocolo UDP.

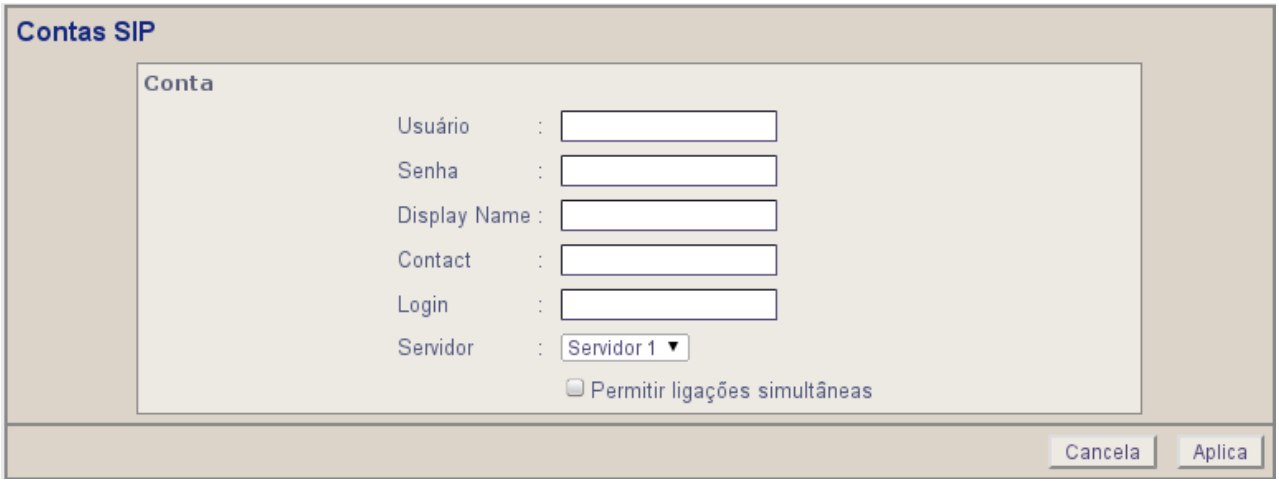
  - **PRACK:** Habilita a RFC 3262 (Reliable Provisional Responses).

  - **SIP Header Compacto**: Envia as mensagens SIP com headers compactos (RFC 3261 e RFC 6262)

  - **Enviar VAD:** Não envia pacotes ou envia pacotes menores quando detecta silêncio.

3.3.1.2. Configurar Contas SIP

Para que seja possível realizar as ligações VoIP é necessário cadastrar as contas SIP e associá-las a um dos servidores SIP cadastrados. É possível cadastrar até 1.000 contas.



- ***Usuário**:* identificação usada para o registro no servidor e nas chamadas VoIP que utilizam o servidor SIP Registrar/Proxy. Este é o campo a ser analisado pela operadora VoIP para identificar o usuário de destino.

- ***Senha**:* usada para a autenticação no servidor SIP Registrar/Proxy.

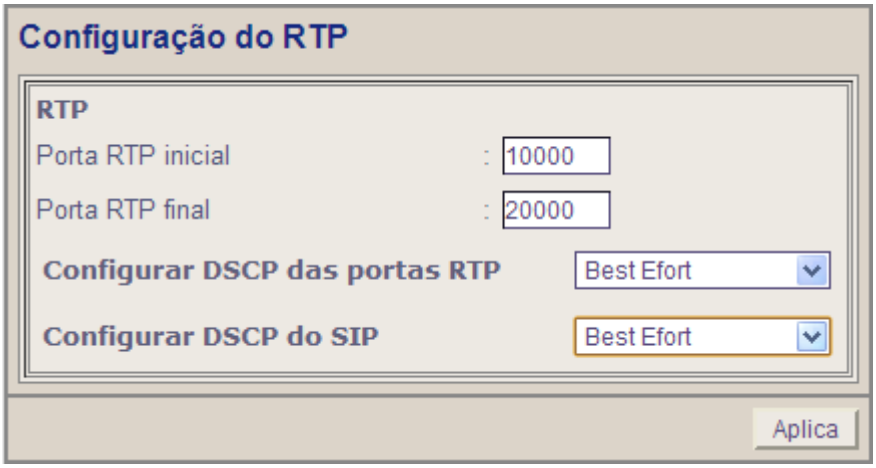
- ***Display Name**:* campo de texto opcional para identificação do usuário que utiliza a conta.

- ***Contact***: ***Login***: usuário usado para autenticar a conta no Servidor SIP. Só é preenchido se o usuário de autenticação for diferente da identificação de registro da conta. Se não for preenchido o Gateway Digistar usa o campo *Usuário* para autenticar a conta.

- ***Servidor***: número do servidor SIP Registrar/Proxy onde a conta SIP irá se registrar e encaminhar as ligações.

- ***Permitir ligações simultâneas***: permite ou bloqueia que uma conta SIP, mesmo ocupada, possa fazer outras ligações. Isso evita que o Gateway Digistar fique enviando ligações não permitidas pela operadora, diminuindo o tempo de resposta ao usuário e as mensagens na rede. (Obs.: essa opção não vale para as ligações de entrada, VoIP para TDM, a quais sempre são aceitas, mesmo que a conta SIP esteja ocupada).

3.3.1.3. Configurações de RTP



• **RTP:** Permite especificar o intervalo de portas que será usado para a recepção do áudio. Somente são usadas as portas pares do intervalo.

- Porta RTP inicial: primeira porta do intervalo de portas disponíveis para RTP.
- Porta RTP final: última porta do intervalo de portas disponíveis para RTP.

• **Configurar DSCP das portas RTP**: Permite configurar a prioridade dos pacotes de áudio (RTP) do VoIP (Serviços diferenciados, DiffServ). (*Ver Configurações de QoS*)

A taxa de amostragem padrão é de 20 ms para o G711 e G729. O cancelamento de eco é de até 128ms.

• **Configurar DSCP SIP:** Permite configurar a prioridade dos pacotes do protocolo SIP.

3.3.1.4. Status

Tem como finalidade exibir o status das ligações. O status pode ser: "Discando", "Conversando" e "Encerrada".

Como nos exemplos das telas abaixo:

Tabela de Conexões do SIP

Canal	Estado	Origem	Destino	Codec	Tempo de conexão
1	Conversando	digistarpoa@vono.net.br	05135792278@vono.net.br	G.729	35 segundos
3	Discando	digistarpoa@vono.net.br	05135792266@vono.net.br	G.729	

Tabela de Conexões do SIP

Canal	Estado	Origem	Destino	Codec	Tempo de conexão
1	Encerrada	digistarpoa@vono.net.br	05135792278@vono.net.br	G.729	52 segundos
3	Conversando	digistarpoa@vono.net.br	05135792266@vono.net.br	G.729	33 segundos

O status da ligação será exibido até o canal ser ocupado por uma nova ligação.

Quando a ligação está no status "Conversando" aparecerá uma "Lupa", que poderá ser selecionada para verificar outros parâmetros da ligação em curso, conforme a tela abaixo:

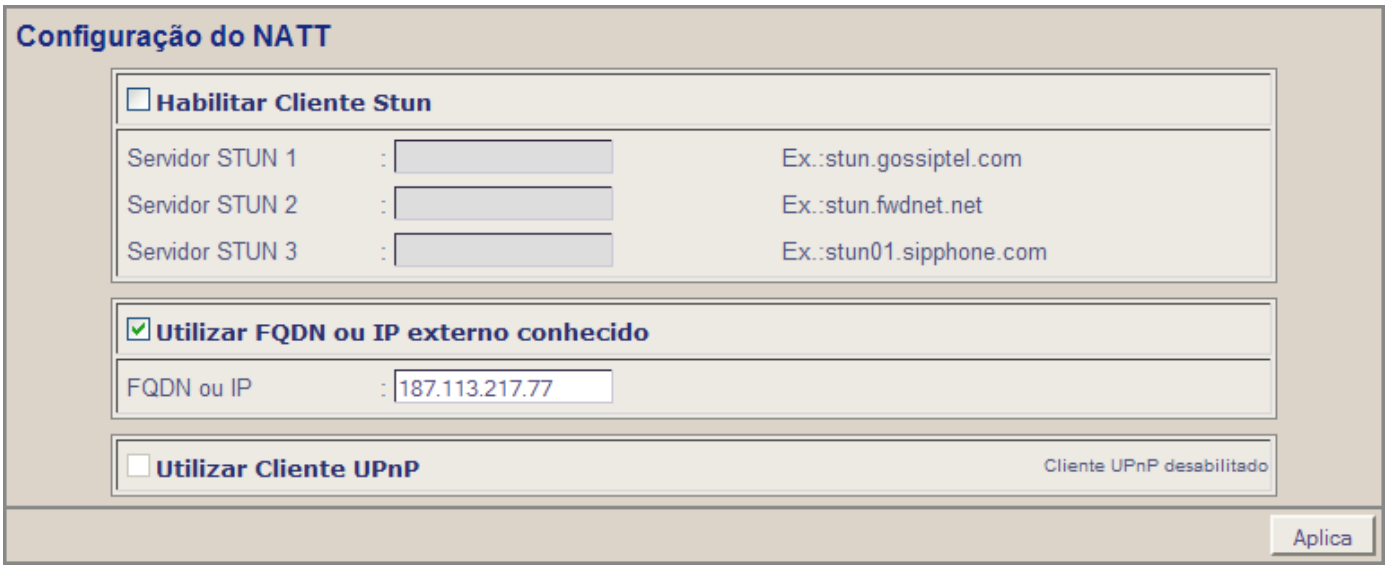
RTP Info Voltar

Channel:	1
Local RTP SSRC:	ea9bc771
Remote RTP SSRC:	eb9a9a3d
RTCP Period:	5000 ms
RTP Packets Sent:	16349
non-Header RTP Octets Sent:	326980
Last Sender Report:	4.94 ms
Count of RTCP BYE received:	0
Count of RTCP Sender Reports:	76
Round-trip Time Measurement:	9.99 ms
Count of Lost Packets Observed:	0
Received Jitter Estimation:	31 ms
Last Receiver Report Received:	-
RTP Packets Received:	16250
non-Header RTP Octets Received:	325000
Count of RTCP Receiver Reports:	0
Local Port:	10002
Remote Address:	192.168.11.122
Remote Port:	10002
Sender Payload Type:	18

Descrição dos campos:

Channel: Número do canal
Local RTP SSRC: Valor do SSRC do RTP local
Remote RTP SSRC: Valor do SSRC do RTP remoto
RTCP Period: Tempo do período do RTCP
RTP Packets Sent: Número de pacotes RTP enviados
non-Header RTP Octets Sent: Número de octetos RTP enviados (descontando o cabeçalho)
Last Sender Report: Tempo em que o último Send Report foi enviado pelo RTCP
Count of RTCP BYE received: Número de mensagens RTCP BYE recebidos pelo RTCP
Count of RTCP Sender Reports: Número de mensagens Send Reports enviado pelo RTCP
Round-trip Time Measurement: Medida de Tempo de Round-trip
Count of Lost Packets Observed: Número de pacotes perdidos observados pelo receptor RTP
Received Jitter Estimation: Estimativa do valor do Jitter da Ligação, quanto menor o Jitter melhor a qualidade de áudio.
Last Receiver Report Received: Tempo em que o último Receiver Report foi recebido pelo RTCP
RTP Packets Received: Número de pacotes RTP recebidos
non-Header RTP Octets Received: Número de octetos RTP recebidos (descontando o cabeçalho)
Count of RTCP Receiver Reports: Número de mensagens Receiver Reports recebidos pelo RTCP
Local Port: Porta de rede local
Remote Address: Endereço remoto da ligação
Remote Port: Porta de rede remota
Sender Payload Type: Valor do payload (codec).

3.3.2. Configuração do NATT



- **Habilitar Cliente Stun:** Simple Traversal of UDP through NAT (RFC3489). O STUN deve ser ativado somente se o Gateway Digistar estiver conectado à Internet através de um NAPT.

  - Servidor STUN: endereço do servidor STUN na Internet. Podem ser preenchidos até três endereços para o caso de algum deles não estar funcionando.

- **Utilizar FQDN ou IP externo conhecido:** Caso seja conhecido o IP externo ou o FQDN (nome do domínio, por exemplo, www.digistar.com.br) e o Gateway Digistar estiver conectado à Internet através de um NAPT.

- **Utilizar cliente UPNP:** Para os casos em que o Gateway Digistar estiver atrás de um NAPT que tenha um Servidor UPNP rodando. Para utilizar é necessário habilitar o campo cliente UPnP no campo serviços/ UPNP. (*Ver Configurações do UPnPTM*)

OBS.: *Esta opção só pode ser habilitada quando o firewall estiver desabilitado*

3.3.3. Configurações de QoS

Introdução:

Originalmente a Internet não foi desenvolvida para suportar tráfegos de tempo real, tal como VoIP. Com o avanço desses tipos de aplicações necessitou-se elaborar mecanismos para a garantia de qualidade. Assim, surgiu o conceito de QoS, que é a sigla em inglês para Qualidade de Serviço. Basicamente, nessa técnica são aplicadas políticas para assegurar um tratamento diferenciado dependendo das necessidades de cada tipo de aplicação.

QoS em VoIP

A qualidade das ligações VoIP está relacionada com fatores como: o atraso total desde a captura da voz até a sua reprodução no usuário final; a variação do atraso (ou *jitter*), o qual provoca uma sensação de desconforto nas conversações; o descarte de pacotes, que ocasiona a interrupção da voz; e também o *codec* utilizado, que pode codificar e comprimir a voz com maior ou menor impacto no áudio original.

Assim, para garantir premissas de qualidade nas ligações devem-se aplicar mecanismos que diminuam o tempo em que os pacotes ficam retidos nos roteadores, que possibilitem a cadência dos fluxos e que diminuam a probabilidade de perdas dos pacotes.

Para isso, são utilizadas técnicas de QoS, onde os fluxos são classificados e tratados com maior ou menor prioridade dependendo do tipo de aplicação. Nesses métodos se abrage também a reserva de faixas da banda conforme as necessidades para o encaminhamento dos pacotes.

A seguir é apresentada uma visão de métodos de QoS e como é possível configurá-lo no Gateway Digistar.

Classificação dos Pacotes

Historicamente se utilizava como política de QoS o conceito de Intserv (Serviços Integrados) que é um modelo baseado em reserva de recursos, onde a máquina final envia para toda a rede sua necessidade de banda. Atualmente um número muito pequeno de roteadores no mercado utiliza o Intserv, pois esse protocolo só funciona se todos os roteadores estiverem configurados corretamente.

A técnica evolutiva consiste no conceito de "Serviços Diferenciados" ou DiffServ, em que os pacotes são marcados de acordo com classes de serviços pré-determinadas e desse modo são tratados, diferencialmente, nos roteadores que suportam esse protocolo. Nessa abordagem cada roteador tratará as diferentes classes conforme as configurações nele previamente determinadas, não necessitando a interação com outros componentes. Assim, caso algum roteador não suporte esse protocolo, o tratamento privilegiado ainda poderá ser realizado nos demais roteadores.

Com esse mecanismo pode-se, como exemplo, marcar os pacotes de voz com maior prioridade e assim privilegiá-los nas filas dos roteadores com suporte ao DiffSev, diminuindo a latência, o *jitter* e o descarte dos pacotes no caso de congestionamento.

A marcação dos pacotes no "Serviço Diferenciado" é realizada por meio do campo DSCP (*Differenciated Services Code Point)* do cabeçalho IP *(Internet Protocol),* o qual substitui a utilização do campo TOS *(Type of Service).* Podem-se marcar os pacotes com as seguintes classes pré-definidas:

• **Best Efort - BE: (Melhor Esforço):** Sem alteração no campo de Serviços Diferenciados (RFC – 2474);

• **Class Selector (Seleção de Classe):** Semelhante às categorias de precedência utilizadas no campo do ToS. Podem ser definidas como IP-Precedence 1 a IP-Precedence 7 (RFC – 2474);

• **Assured Forwarding-AF (Encaminhamento Garantido):** A marca AF é a forma intermediária de marcação entre o Class Selector e o Expedicted Forwarding. Ela pode ser dividida em 4 classes de precedência e 3 níveis de probabilidade de pacotes (alto, médio, baixo). (RFC – 2597);

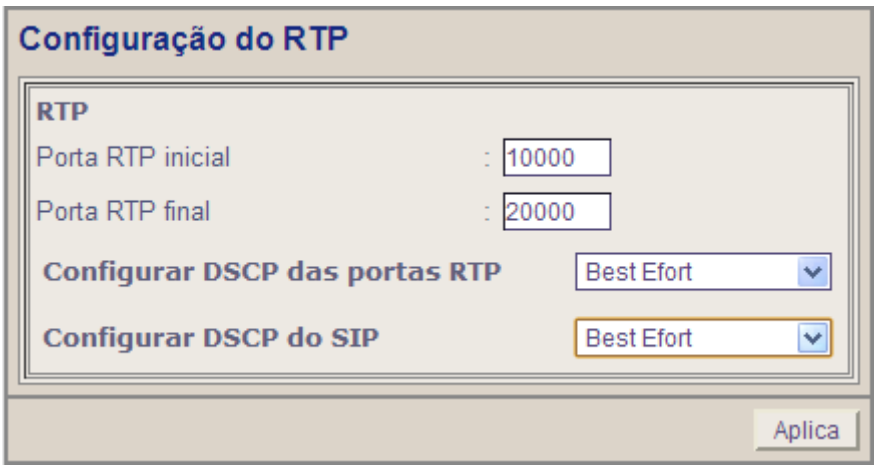
• **Expedicted Forwarding-EF (Encaminhamento de expedição):** A marca EF é a forma de garantir o menor atraso, menor perda, menor variação de atraso e maior qualidade, utilizado principalmente para aplicações VoIP(RFC -2598).

Observa-se que a marcação dos pacotes não garante que eles serão tratados com os privilégios definidos, uma vez que é necessário que o roteador envolvido tenha suporte ao DiffServ.O Gateway Digistar apresenta um suporte completo ao DiffServ, onde além de realizar a marcação também implementam políticas para tratar os pacotes recebidos conforme a sua classe. Os pacotes com maior prioridade são tratados mais rapidamente, sendo encaminhados à rede antes dos pacotes com menor prioridade, diminuindo assim o tempo de espera nas filas do Gateway Digistar.

A seguir são apresentados os modos de classificação dos pacotes no Gateway Digistar. Pode-se realizar a marcação classificando todos os pacotes RTP para uma determinada classe DiffServ.Também é possível definir uma classe para uma máquina ou um intervalo específico de máquinas e serviços.

Classificando todos os pacotes RTP (VoIP):

Na página de configuração do RTP é possível mudar o parâmetro DSCP dos fluxos RTP e SIP.



Com isso, pode-se privilegiar o tráfego de voz na saída do Gateway Digistar e nos roteadores, no caminho até o destino final, que apresentem suporte ao DiffServ.

Classificando tráfegos específicos

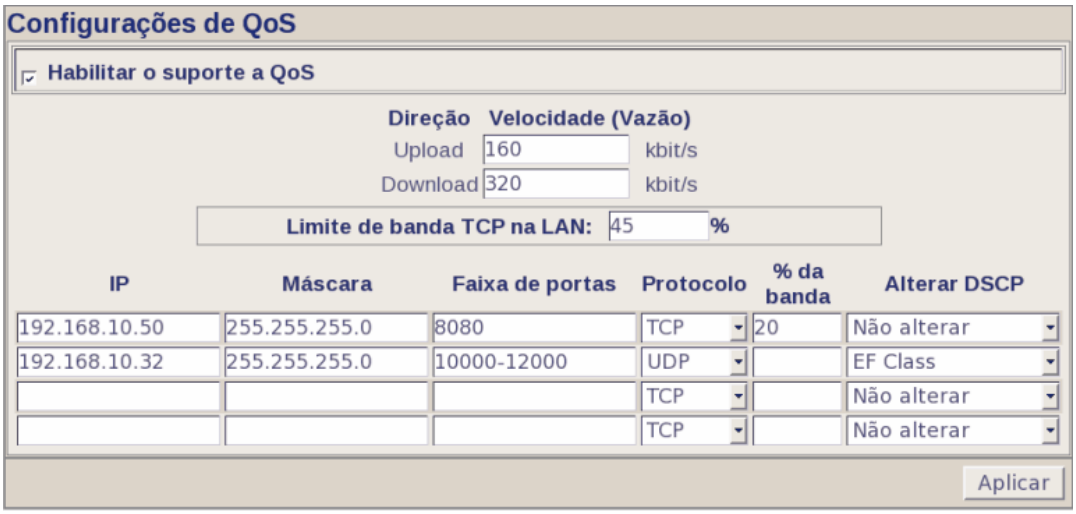
Na página de configuração do QoS pode-se determinar a marcação DSCP para outros tipos de tráfegos (TCP, UDP, GRE ou TODOS), onde pode-se ainda definir computadores específicos, ou um intervalo de computadores, uma rede e até portas específicas.

Como exemplo dessa classificação poderia-se alterar o campo DSCP do fluxo de voz dentro do intervalo de portas entre 10000 a 12000 de um telefone IP com endereço 192.168.10.32 para a classe de maior prioridade (EF Class). Assim, esse telefone específico teria um maior privilégio em relação aos demais, caso eles não fossem marcados ou apresentassem uma classe com menor prioridade.

Reserva de Banda:

Uma outra maneira de garantir premissas de QoS para as ligações consiste em reservar a banda. Aplicações VoIP utilizam, consideravelmente, tanto os canais de download quanto os de upload para a transmissão dos pacotes de voz. Desse modo, em cenários onde a voz é transmitida no mesmo link que fluxos de dados, existirá uma concorrência pela ocupação da banda, em que, nos casos de congestionamento, poderá ocasionar o atraso ou até o descarte dos pacotes de voz. Desse modo, uma maneira de minimizar esse problema consiste em definir regras de QoS para reservar uma percentagem da banda para uso dos tráfegos de voz.

No Gateway Digistar pode-se reservar a banda de duas maneiras: limitando o tráfego total de TCP na banda ou determinando a reserva especificamente para uma máquina ou um intervalo determinado de máquinas e serviços. A seguir serão explicados os modos de reservar a banda no Gateway Digistar.



Reservando a banda para todos as ligações VoIP

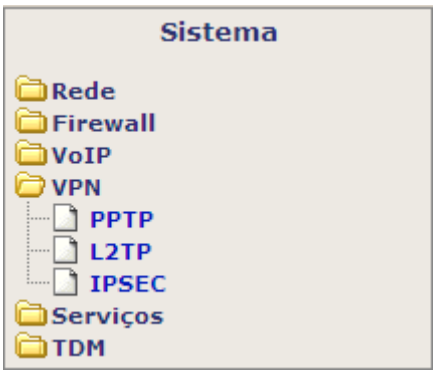
Utilizando-se do campo "Limite de banda TCP na LAN" é possível restringir a um valor percentual a ocupação da banda pelo tráfego TCP (percentual do valor preenchido em "Upload" e "Download"), reservando o restante para as ligações VoIP. Essa reserva é realizada de modo dinâmico, ou seja, caso a percentagem de banda reservada para as ligações VoIP não esteja totalmente ocupada, o tráfego TCP poderá extrapolar o limite definido, não prejudicando as ligações ativas e ocupando a faixa de banda ociosa. Observa-se que esses controles também valem para o tráfego VoIP, ou seja, os tráfegos das ligações só poderão ocupar a banda do tráfego TCP quando esse não estiver utilizando o percentual para ele destinado. Essa política permite garantir a qualidade das ligações, utilizando a banda de um modo eficiente e justo aos tráfegos envolvidos.
Para determinação da reserva deve-se definir na página de configuração o limite de ocupação máximo do tráfego TCP quando existem ligações ativas (Limite de banda TCP na LAN) e os parâmetros de velocidade do uplink (Upload) e velocidade do downlink (Download).

Reservando a banda para tráfegos específicos

Tal como a marcação DSCP pode-se reservar a banda para máquinas e serviços específicos. Para isso, utiliza-se a mesma maneira de configuração específica de QoS, ou seja, pode-se determinar um computador ou intervalo de computadores, definir as portas associadas e o tipo de tráfego (TCP, UDP, GRE ou TODOS). Com isso, pode-se, por exemplo, reservar 20% do total da banda para um servidor WEB no endereço 192.168.10.50.

Nota-se que na configuração específica de QOS é possível reservar a banda e marcar (classificar) os pacotes ao mesmo tempo.

3.4. VPN



VPN (Redes Virtuais Privadas) é uma extensão das redes privadas, pois fazem a união de redes privadas que estão separadas fisicamente como uma ligação ponto a ponto. Usualmente a união destas redes é feita através de um meio público, como a Internet, onde o uso de criptografia faz-se necessário.

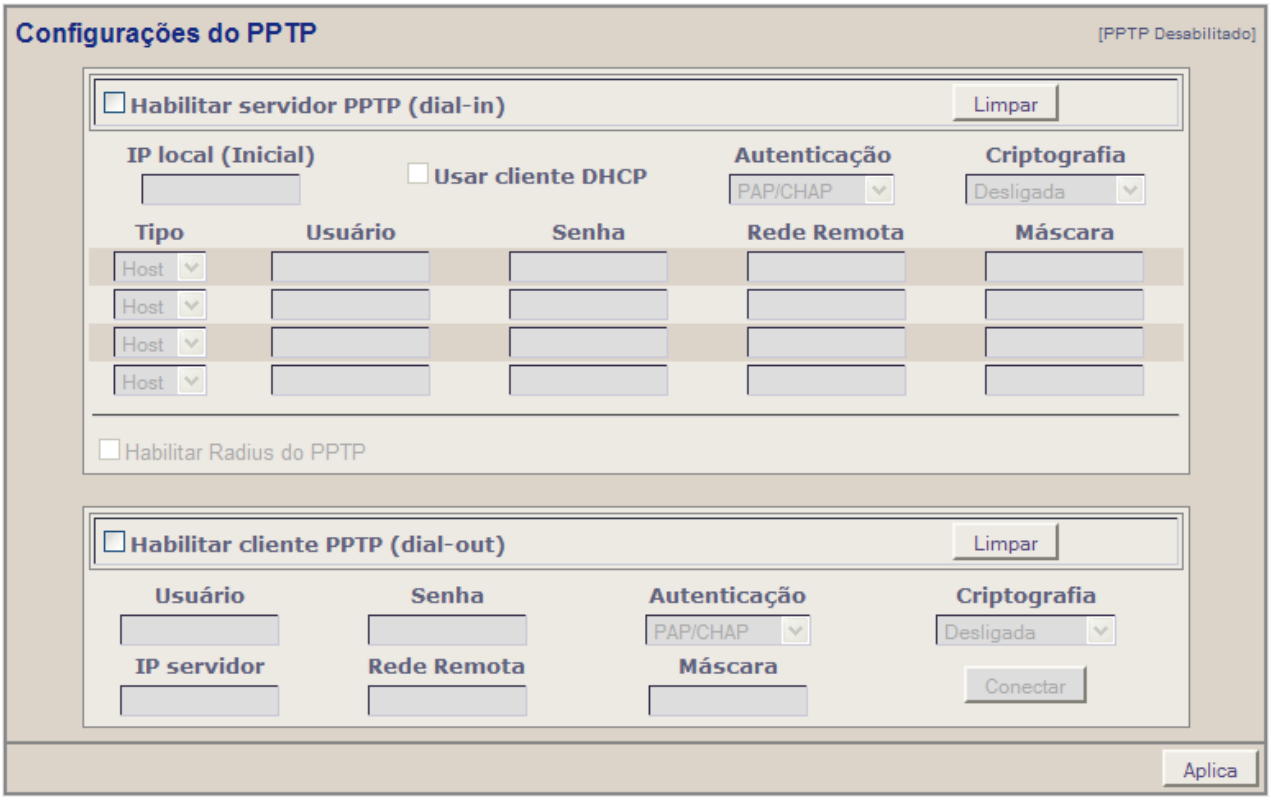
Podem ser divididas em dois grandes grupos:

- Conexão de discagem remota, também chamada de Cliente-LAN. Usada para que um usuário remoto, por exemplo, um usuário em um hotel, possa acessar a rede privada de maneira segura.

- Conexão entre redes, também chamada de LAN-to-LAN ou GW-to-GW. Usada para que se estabeleça uma conexão segura entre redes privadas. É usada muito entre clientes - fornecedores e matriz - filiais.

O Gateway Digistar tem os três protocolos mais comuns para estabelecer até 4 VPNs. Os protocolos são PPTP, L2TP e o IPSEC. Todos os protocolos podem ser utilizados para fazer conexões do tipo LAN-to-LAN, Para as conexões do tipo Cliente-LAN são mais utilizados os protocolos PPTP e L2TP.

3.4.1. Configurações do PPTP



A sigla PPTP significa protocolo de túnel ponto a ponto. É um mecanismo de encapsulamento para transferir quadros PPP, onde é possível utilizá-lo para fazer criptografia e autenticação de usuários.
O PPTP utiliza a porta TCP 1723 para controle e utiliza encapsulamento com o protocolo GRE (Generic Routing Encapsulation) para a transmissão de dados. (RFC 2637)

Como servidor permite:

- **Sem RADIUS e sem DHCP:** Permite até 4 conexões VPN. Configura-se um IP inicial fora do range do servidor DHCP e cada usuário que se conectar irá ganhar um IP entre o IP inicial e o IP inicial + 3. Assim se eu tiver 4 usuários User1, User2, User3 e User4, com o IP inicial 192.168.10.100, quando o usuário User1 se conectar irá ganhar o IP 192.168.10.100, quandoL o usuário User2 se conectar ganhará o IP 192.168.10.101, e assim até o User4 com o IP 192.168.10.103. Para que não haja conflito de IPs, é necessário usar o servidor DHCP (tela Rede e DHCP) com os limites de IPs que não colidam com os endereços do PPTP. Assim, no nosso exemplo, deveria ser configurado o servidor DHCP com IP final até 192.168.10.99 ou com o IP inicial a partir de 192.168.10.104.

- **Com RADIUS e sem DHCP:** Permite até 4 conexões. Semelhante a forma acima, com a diferença que os usuários e senhas devem ser colocados no servidor RADIUS, para o mesmo fazer a autenticação. Para habilitar o RADIUS 3.5.2.

- **Sem RADIUS e com DHCP:** Permite múltiplas conexões com até 4 usuários distintos. Não há mais configuração do IP inicial e os IP são fornecidos para os usuários através do servidor DHCP da rede. É a maneira mais fácil de estabelecer uma conexão PPTP. Desta forma, a cada conexão é fornecido um IP diferente, mesmo sendo o mesmo usuário. Assim, por exemplo, podemos criar um usuário "*vendedores"* e um usuário "*fornecedores"*. Todos os vendedores podem acessar a rede privada usando o mesmo login "*vendedores",* assim como todos os fornecedores o login "*fornecedores"*.

- **Com RADIUS e com DHCP:** Permite múltiplas conexões com até 4 usuários distintos. Irá usar o servidor DHCP para fornecer IPs e irá fazer autenticação usando o servidor RADIUS.

Existem três formas de autenticação:

- PAP – (Protocolo de Autenticação por Senha) – É a forma de autenticação que envia o usuário e a senha em aberto na rede, sem nenhuma criptografia. É a maneira menos segura de autenticação.

- CHAP – (Protocolo de Autenticação de Desafio de Resposta) – Utiliza protocolo de codificação Message Digest 5 (MD5) de um só sentido. A senha é enviada de forma codificada.

- MS-CHAPv2 (Protocolo de Autenticação de Desafio de Resposta da Microsoft versão 2) – Utiliza protocolo de codificação Message Digest 4 (MD4) em ambos os sentidos ou autenticação mútua.
- Para a criptografia dos dados é possível usar o protocolo MPPE (Encriptação Ponto a Ponto da Microsoft) que cria chaves criptográficas diferentes para cada sentido de transmissão, além de trocar a chave periodicamente. As chaves podem ser de 40 ou 128bits RSA RC-4. Para usar a criptografia é preciso selecionar a forma de autenticação para MS-CHAPv2. Existe também um campo para usar criptografia opcional, ou seja, cria a conexão mesmo sem criptografia. A maneira mais segura é usar autenticação por MS-CHAPv2 e criptografia de 128 bits.

Com o PPTP é possível criar conexões do tipo Cliente-LAN ou LAN-to-LAN. A forma de uso é definida pelo campo TIPO. Se o campo estiver como *rede* irá se estabelecer uma conexão do tipo LAN-to-LAN, assim como se estiver como *host* irá se estabelecer uma conexão do tipo Cliente-LAN. Para conexão do tipo LAN-to-LAN é necessário informar o número de rede remota e a máscara da rede remota. Vale lembrar que é necessário que as redes privadas das máquinas sejam diferentes para que o túnel LAN-to-LAN se estabeleça.

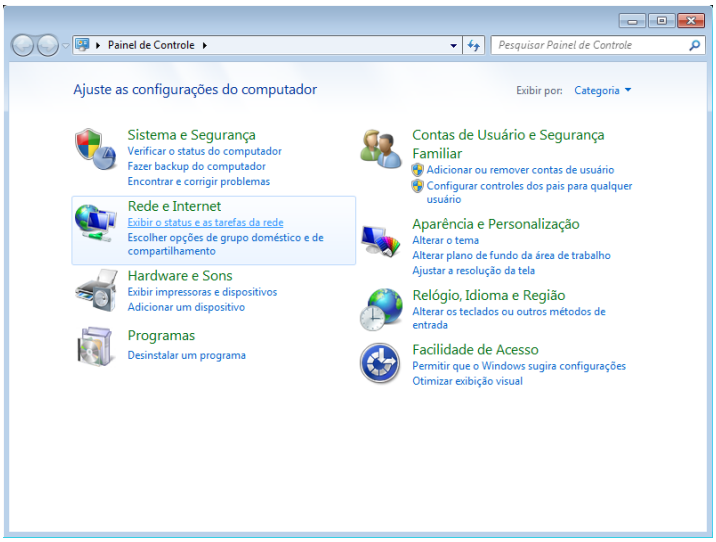
O Gateway Digistar pode funcionar como cliente PPTP, neste caso ele irá fazer a discagem para outra máquina (dial-out). Basta entrar com as configurações, aplicá-las e clicar no botão CONECTAR. O Gateway Digistar também pode atuar como servidor PPTP.

Para ver quais os túneis que estão ativos no momento, verifique na opção "Ver tabela de túneis PPTP".

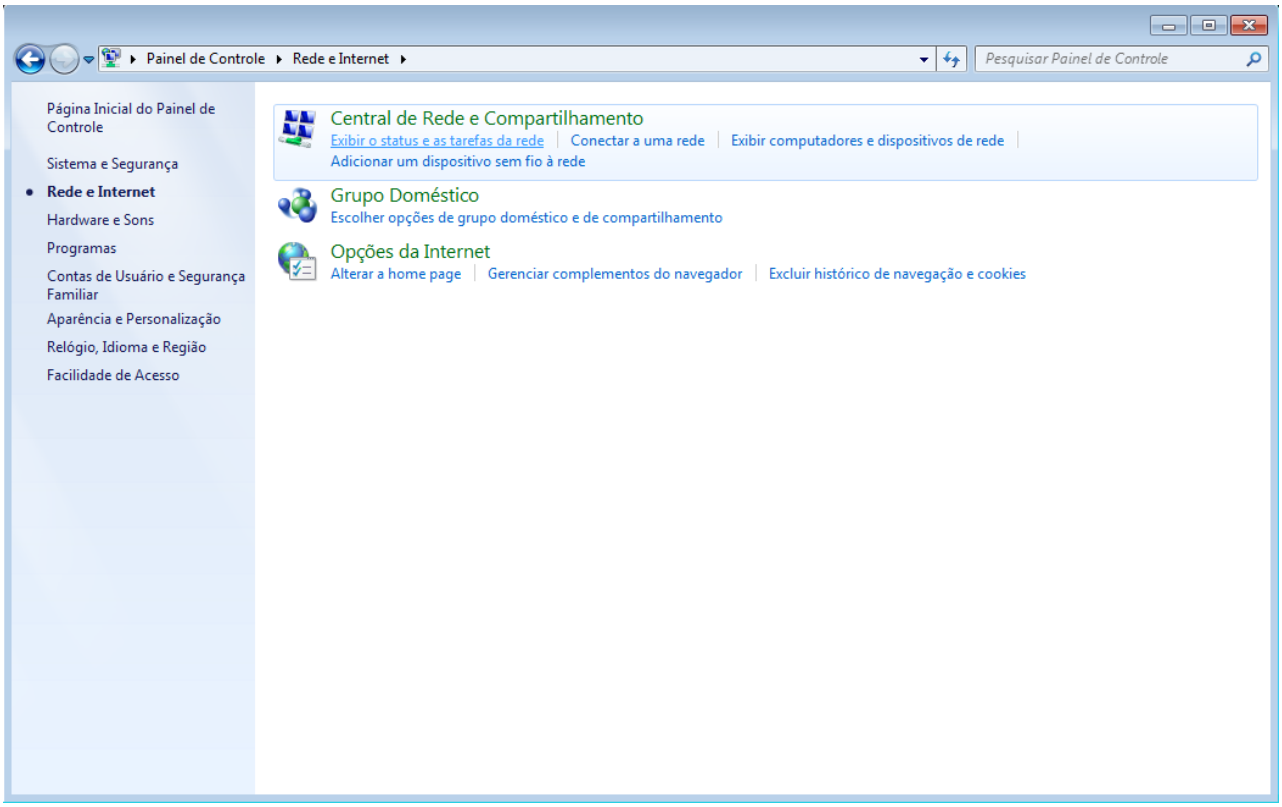
Quanto à compactação, o servidor PPTP do Gateway Digistar aceita o protocolo MPPC, ou Protocolo de Compactação Ponto a Ponto da Microsoft. O MPPC é definido pela RFC 2118 e utiliza compressão dos pacotes PPP, utilizando algoritmo baseado em LZ (também chamado de Lempel-Ziv) com buffer histórico de janela deslizante.

Os passos para fazer o túnel em ambiente Windows 7 são:

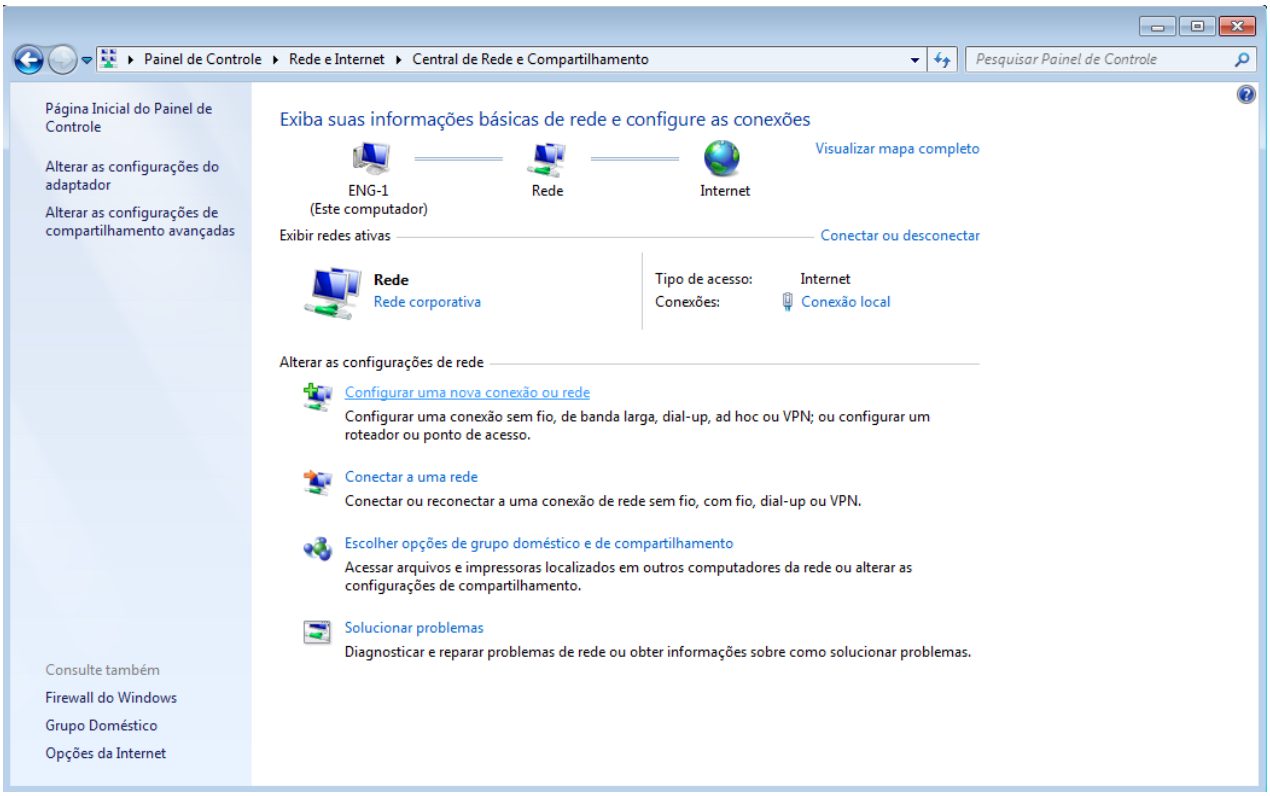
1 - Vá em "Painel de controle" e clique em "Rede e Internet"



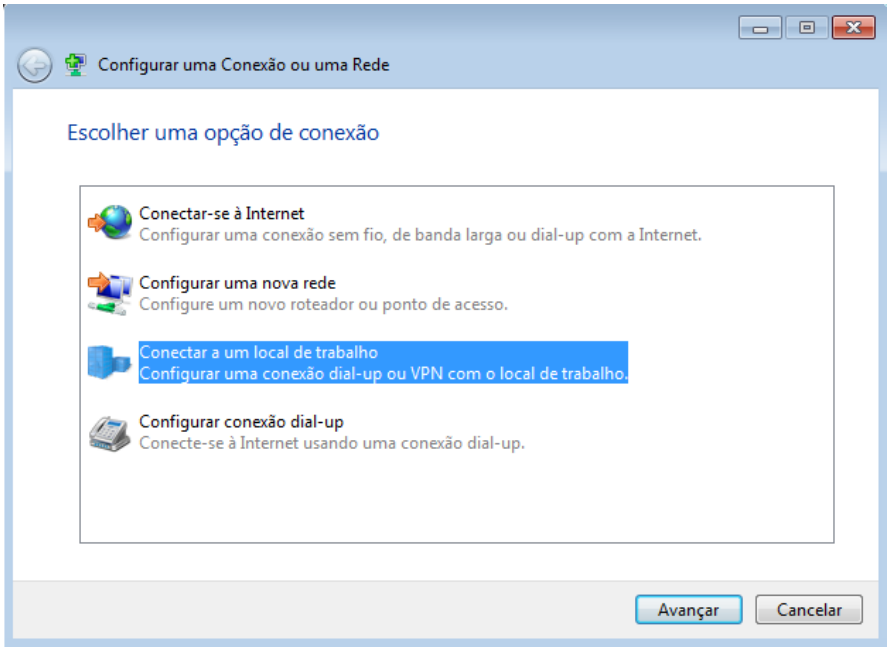
2 - Clique em "Exibir o status e as tarefas da Rede"



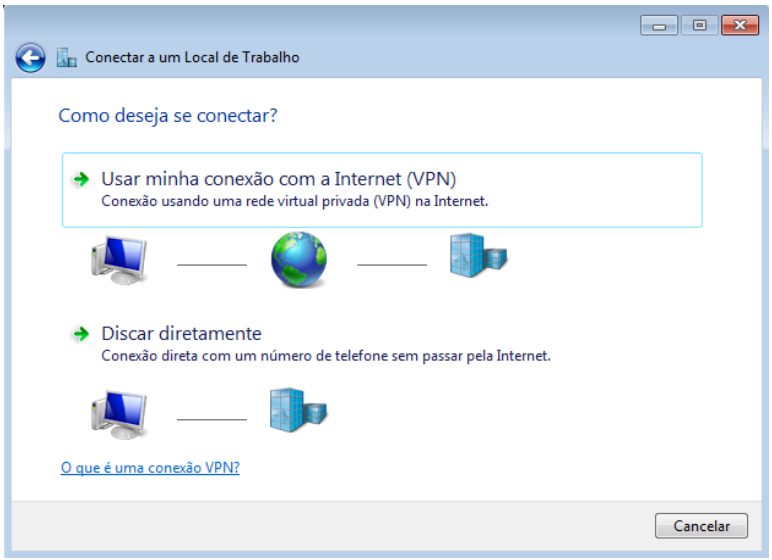
3 - Clique em "Configurar uma nova conexão ou rede"



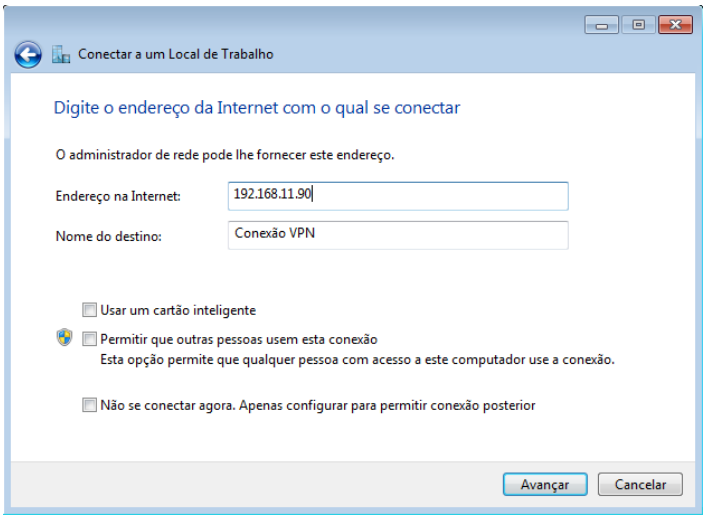
4 - Clique em "Conectar a um local de trabalho" e depois em "avançar"



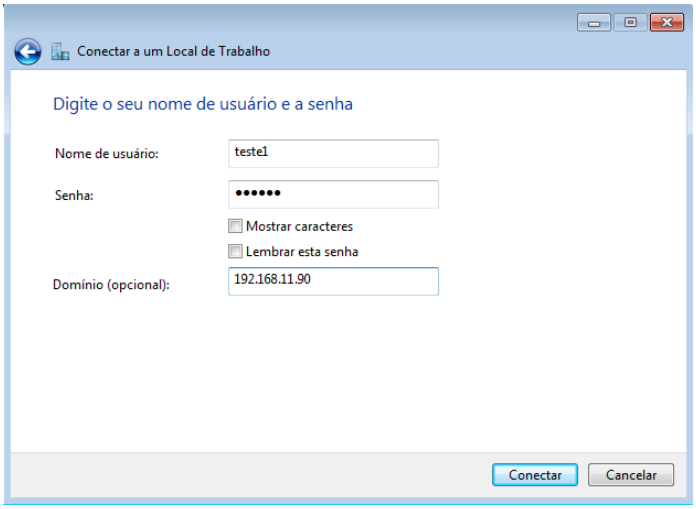
5 - Clique em "Usar minha conexão com a internet (VPN)"



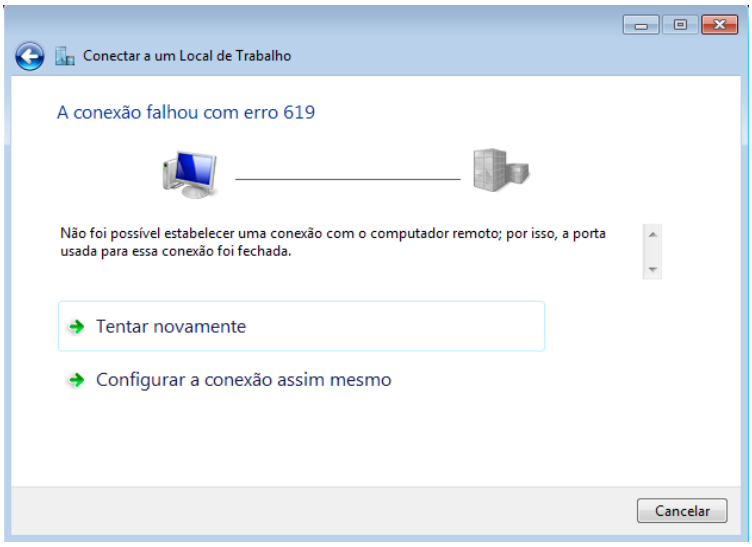
6 - Configure o IP onde será conectada a VPN e o nome da conexão e após clique em “Avançar”



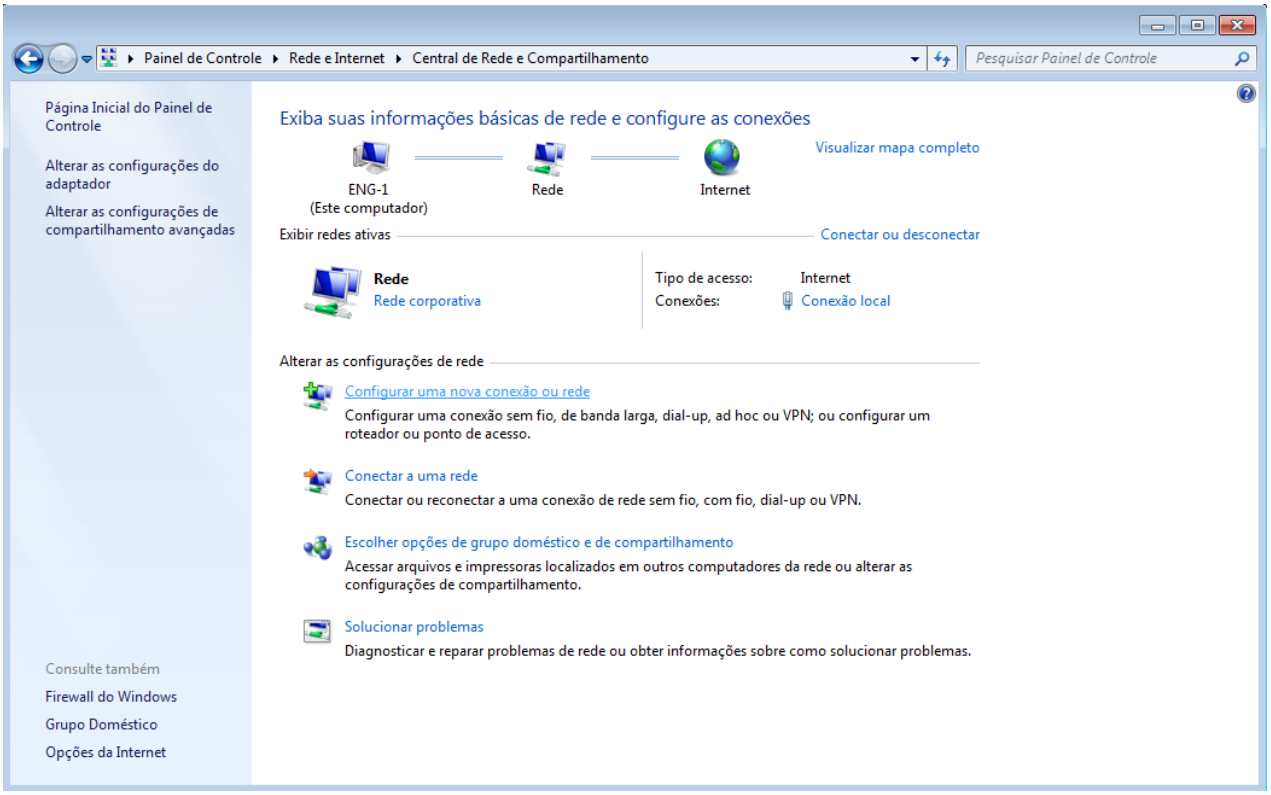
7 - Programe o usuário, a senha e o IP do destino e clique em “Conectar”.

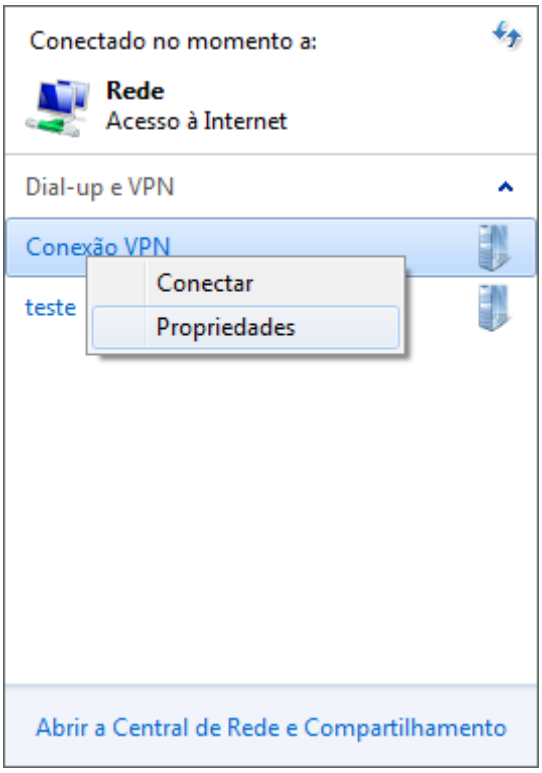


8 - Após aparecerá a conexão, mas essa conexão não irá funcionar pois será necessário configurar mais alguns itens. Clique em "Configurar a conexão assim mesmo"

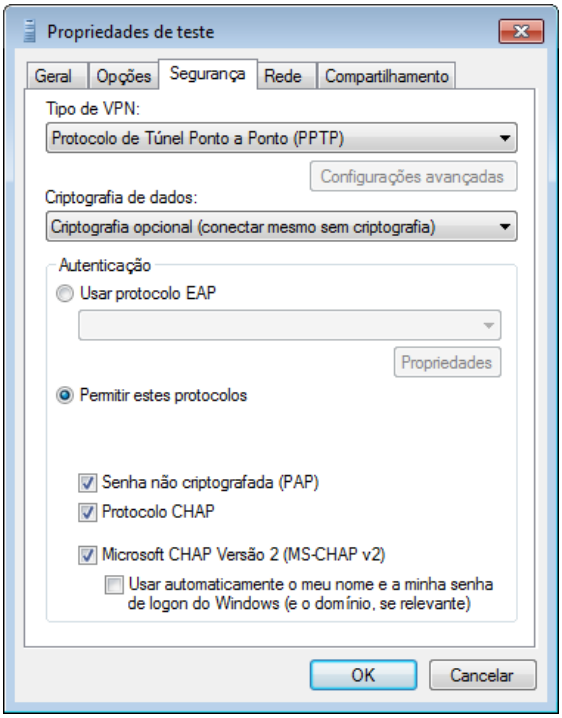


9 - Entre no item "Conectar a uma rede" e com botão direito do mouse clique sobre a conexão configurada e selecione o item “propriedades”.

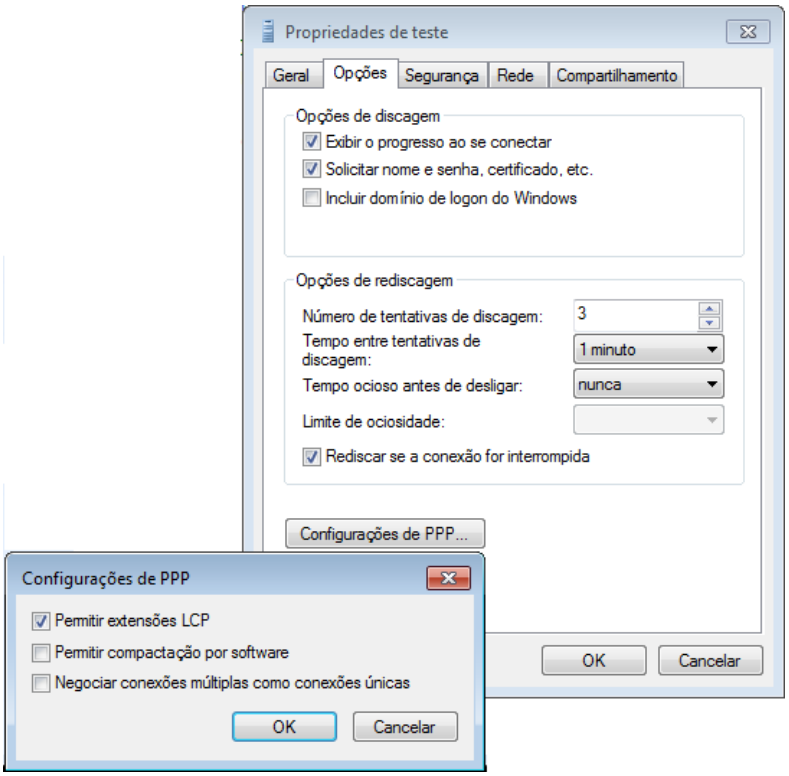




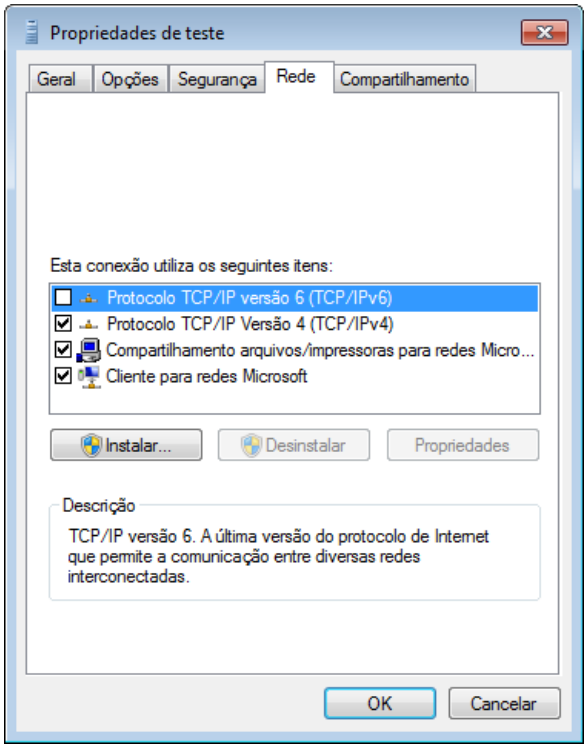
10 - Clique na aba "Segurança" e programe os itens conforme as telas abaixo. Após clique em “OK”



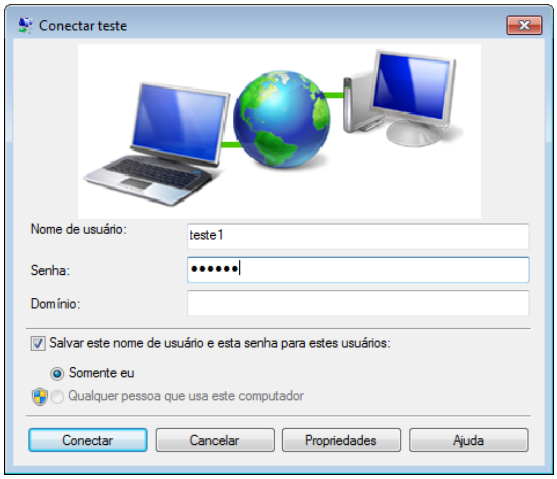
11 - Clique na aba "Opções" e programe os itens conforme as telas abaixo. Após clique em “OK”



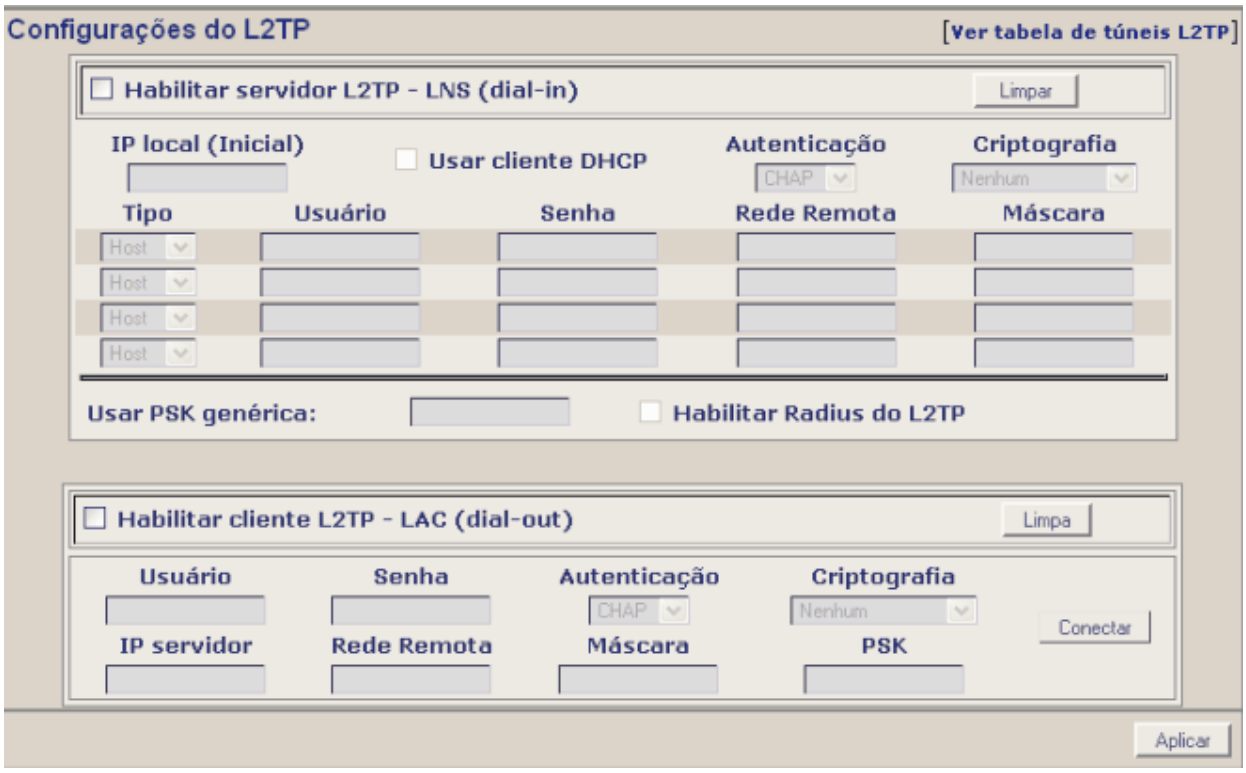
12 - Clique na aba "Rede" e programe os itens conforme as telas abaixo. Após clique em “OK”



13 - Configure usuário e senha. Após clique em “Conectar”.



3.4.2. Configurações do L2TP



A sigla L2TP significa protocolo de túnel de camada 2. É um protocolo que foi implementado pela IETF para resolver alguns problemas de segurança do PPTP e alguns problemas com o L2F. O protocolo utiliza os fundamentos do L2F, protocolo criado pelo fabricante Cisco. O L2TP tem como funcionalidade o transporte de protocolos de camada 2 do modelo OSI, como IP, IPX e NETBEUI, daí o seu nome. Também utiliza encapsulamento PPP, onde é possível utilizá-lo para fazer autenticação de usuários.

O L2TP utiliza a porta UDP 1701 para controle (RFC 2661). O L2TP não possui mecanismos de encriptação para tráfego de dados. Para resolver o problema de segurança utilizam o mesmo sobre outro protocolo seguro, o IPSEC.

No Gateway Digistar quando é utilizado o túnel IPSEC para fazer a encriptação dos dados utiliza-se o túnel IPSEC no modo túnel. (Ver mais detalhes na *“seção IPSEC”*)

Como servidor permite :

- **Sem RADIUS e sem DHCP:** Permite até 4 conexões VPN. Configura-se um IP inicial fora do range do servidor DHCP e cada usuário que se conectar irá ganhar um IP entre o IP inicial e o IP inicial + 3. Assim se eu tiver 4 usuários User1, User2, User3 e User4, com o IP inicial 192.168.10.100, quando o usuário User1 se conectar irá ganhar o IP 192.168.10.100, quando o usuário User2 se conectar ganhará o IP 192.168.10.101, e assim até o User4 com o IP 192.168.10.103. Para que não haja conflito de IPs, é necessário usar o servidor DHCP (tela Rede e DHCP) com os limites de IPs que não colidam com os endereços do L2TP. Assim, no nosso exemplo, deveria ser configurado o servidor DHCP com IP final até 192.168.10.99 ou com o IP inicial a partir de 192.168.10.104.
- **Com RADIUS e sem DHCP:** Permite até 4 conexões. Semelhante a forma acima, com a diferença que os usuários e senhas devem ser colocados no servidor RADIUS, para o mesmo fazer a autenticação. Para configurar o servidor RADIUS seção 3.5.2
- **Sem RADIUS e com DHCP:** Permite múltiplas conexões com até 4 usuários distintos. Não há mais configuração do IP inicial e os IP são fornecidos para os usuários através do servidor DHCP da rede. É a maneira mais fácil de estabelecer uma conexão L2TP. Desta forma, a cada conexão é fornecido um IP diferente, mesmo sendo o mesmo usuário. Assim, por exemplo, podemos criar um usuário "*vendedores"* e um usuário "*fornecedores"*. Todos os vendedores podem acessar a rede privada usando o mesmo login "*vendedores",* assim como todos os fornecedores o login "*fornecedores"*.
- **Com RADIUS e com DHCP.** Permite múltiplas conexões com até 4 usuários distintos. Irá usar o servidor DHCP para fornecer IPs e irá fazer autenticação usando o servidor RADIUS.

Existem duas formas de autenticação:

- PAP – (Protocolo de Autenticação por Senha) – É a forma de autenticação que envia o usuário e a senha em aberto na rede, sem nenhuma criptografia. É a maneira menos segura de autenticação.

- CHAP – (Protocolo de Autenticação de Desafio de Resposta) – Utiliza protocolo de codificação Message Digest 5 (MD5) de um só sentido. A senha é enviada de forma codificada.

  Quando é utilizada criptografia L2TP sobre IPSEC são utilizados como algoritmo de chave privada ou simétrica o 3DES, algoritmo de desafio SHA1 e como algoritmo de chave pública ou assimétrica o Diffie-Hellman Grupo 2 de 1024 bits (Ver mais detalhes na "Seção IPSEC"). Para fazer a autenticação das chaves são possíveis dois métodos:

- PSK (Pre- Shared Key, ou Chave pré-compartilhada): É o método em que as duas pontas possuem a mesma chave e que na hora de estabelecer o túnel as mesmas são verificadas. Normalmente são específicas para cada IP. Para facilitar o uso, no caso Cliente-LAN, foi criado um campo PSK genérica, que funciona para todos os usuários.

Para que se estabeleça um túnel IPSEC (no caso se usar o L2TP com criptografia) existe a necessidade de selecionar o tipo de identificador a ser usado pelo servidor. Se a empresa possuir um IP fixo (p. exemplo 200.200.200.200) e estiver selecionado o campo "Usar IP da WAN" para que a discagem funcione, a conexão deve discar exclusivamente para este número IP. Se estiver sendo usado o DNS dinâmico no Gateway Digistar podemos usar o campo "Usar FQDN do DDNS" e assim a conexão pode ser estabelecida discando para um nome ou FQDN (p. exemplo ip.do.servidor.com). Se estiver atrás de outra rede privada, ou outra máquina que faz o DNS dinâmico é possível usar a opção "Usar FQDN ou IP específico" e colocar outro identificador.

Com o L2TP é possível criar conexões do tipo Cliente-LAN ou LAN-to-LAN. A forma de uso é definida pelo campo TIPO. Se o campo estiver como *rede* irá se estabelecer uma conexão do tipo LAN-to-LAN, assim como se estiver como *host* irá se estabelecer uma conexão do tipo Cliente-LAN. Para conexão do tipo LAN-to-LAN é necessário informar o número de rede remota e a máscara da rede remota. Vale lembrar que é necessário que as redes privadas das máquinas sejam diferentes para que o túnel LAN-to-LAN se estabeleça.

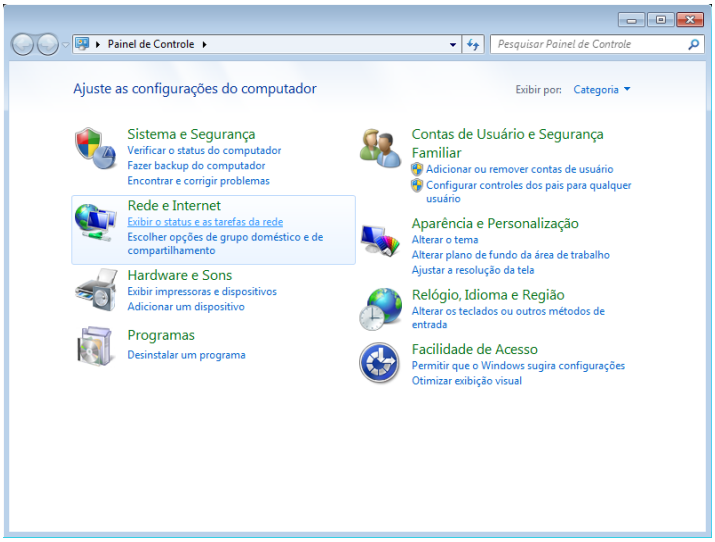
O Gateway Digistar pode funcionar como cliente L2TP, também chamado de LAC. Assim o Gateway Digistar irá fazer a discagem para outra máquina. Basta entrar com as configurações, aplicá-las e clicar no botão CONECTAR. No Gateway Digistar também pode ser habilitado como um servidor L2TP.

> **Importante:** *No Gateway Digistar somente é possível estabelecer um túnel L2TP seguro como cliente com o uso de PSK usando IPSEC como criptografia.*

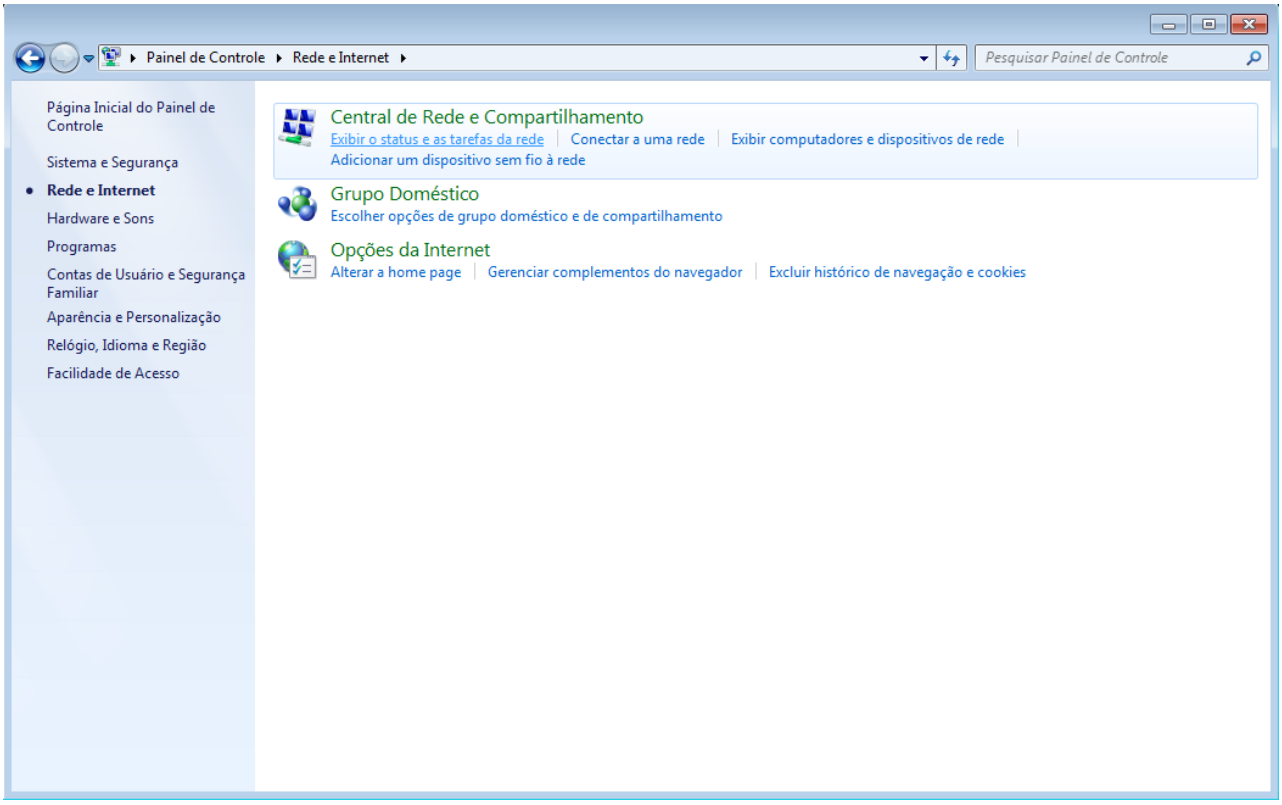
Para ver quais os túneis que estão ativos no momento, basta ir na opção ”Ver tabela de túneis L2TP”.

Os passos para fazer o túnel em ambiente Windows7 são:

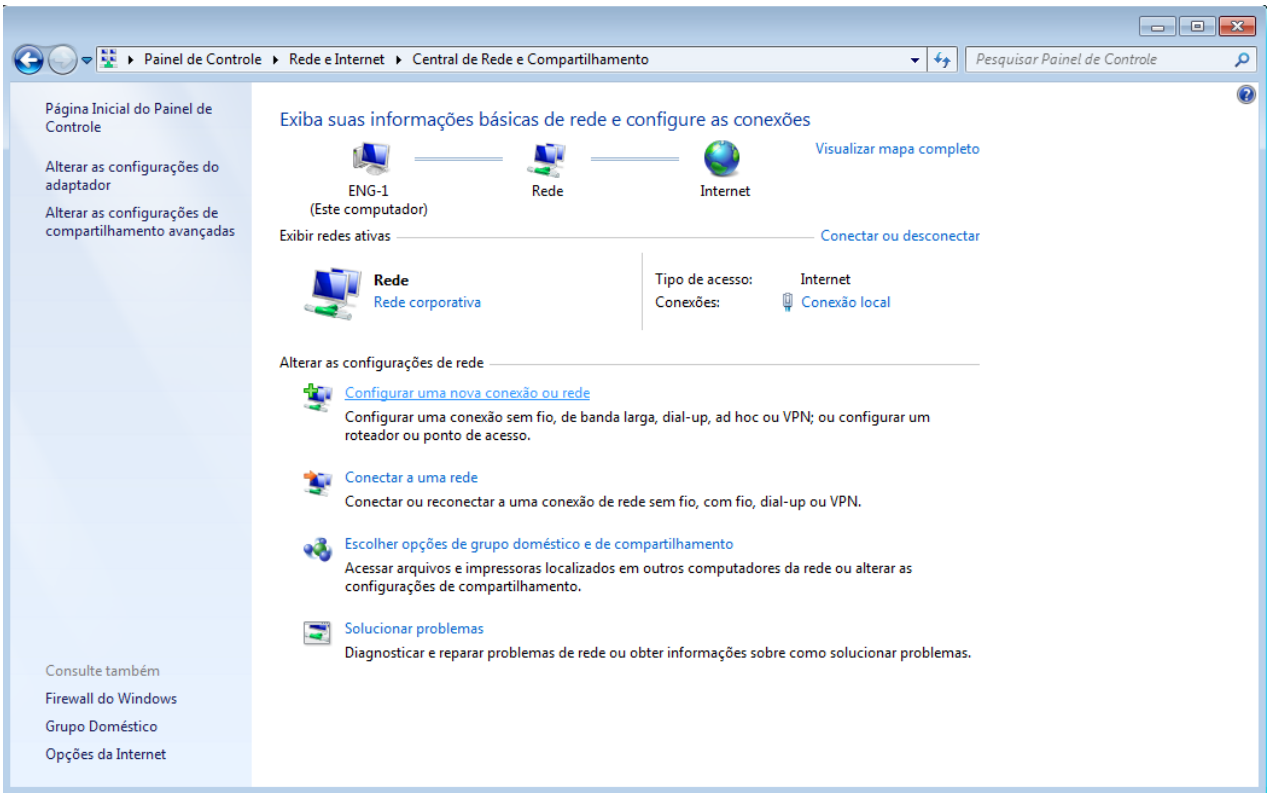
1 - Vá em "Painel de controle" e clique em "Rede e Internet"



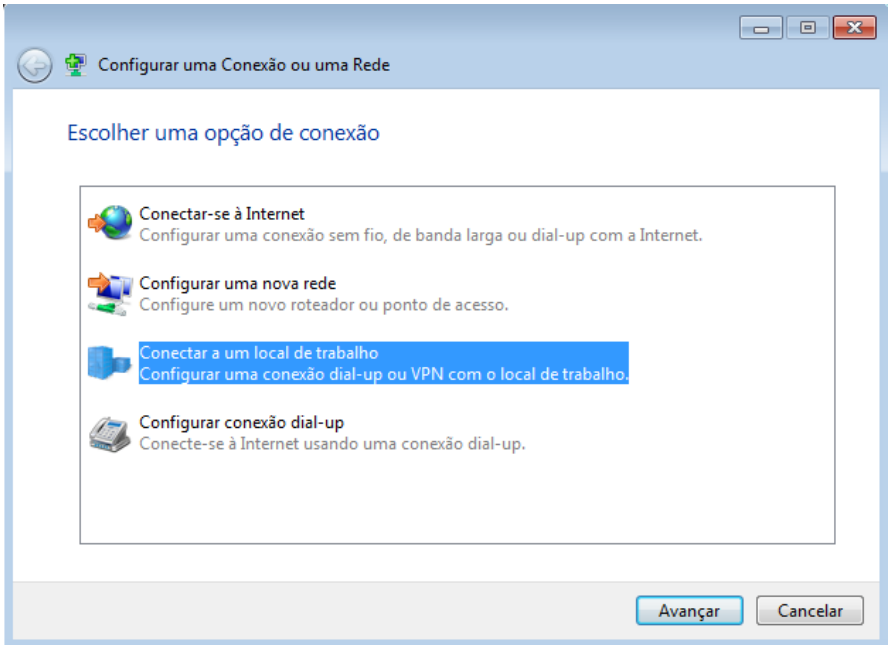
2 - Clique em "Exibir o status e as tarefas da Rede"



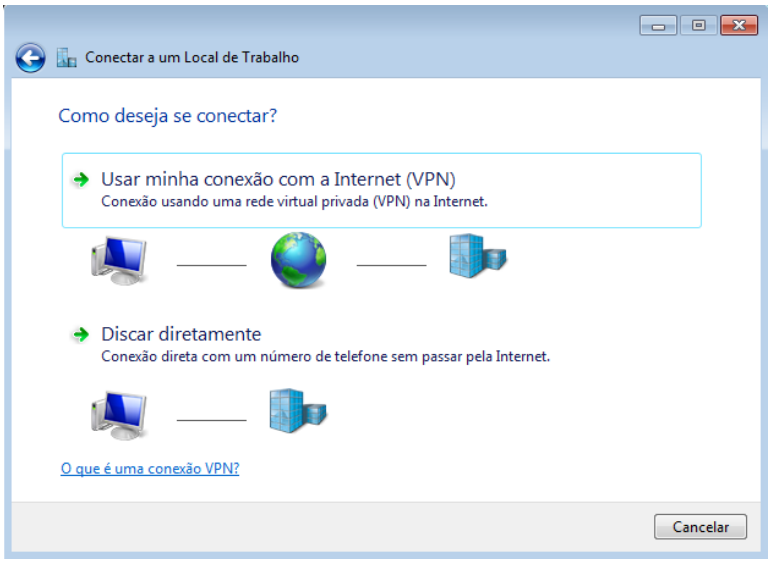
3 - Clique em "Configurar uma nova conexão ou rede"



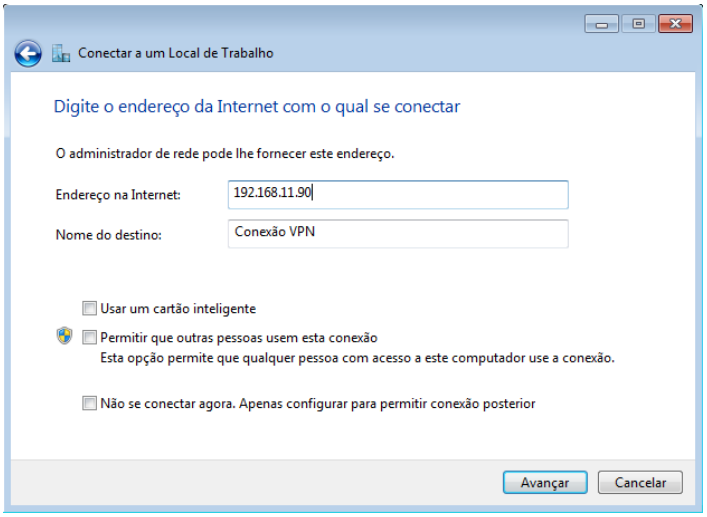
4 - Clique em "Conectar a um local de trabalho" e depois em "avançar"



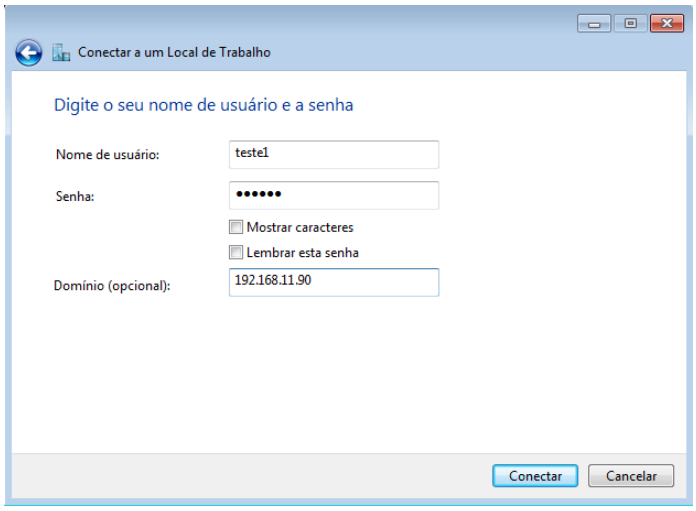
5 - Clique em "Usar minha conexão com a internet (VPN)"



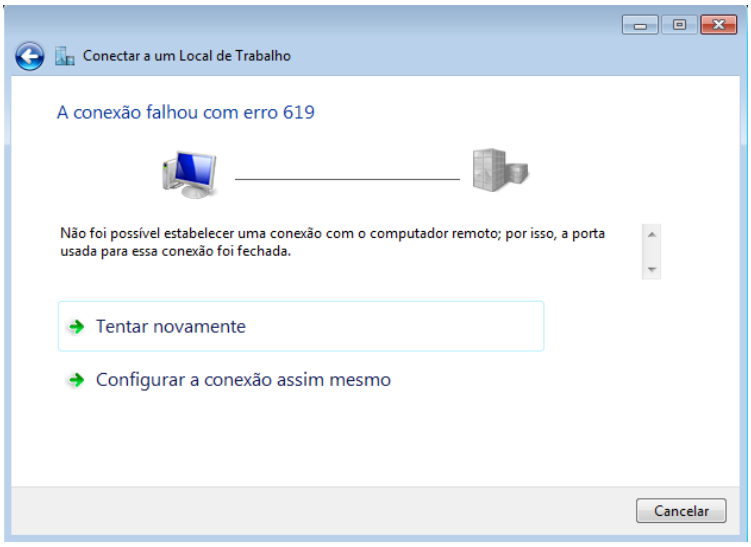
6 - Configure o IP onde será conectada a VPN e o nome da conexão e após clique em “Avançar”



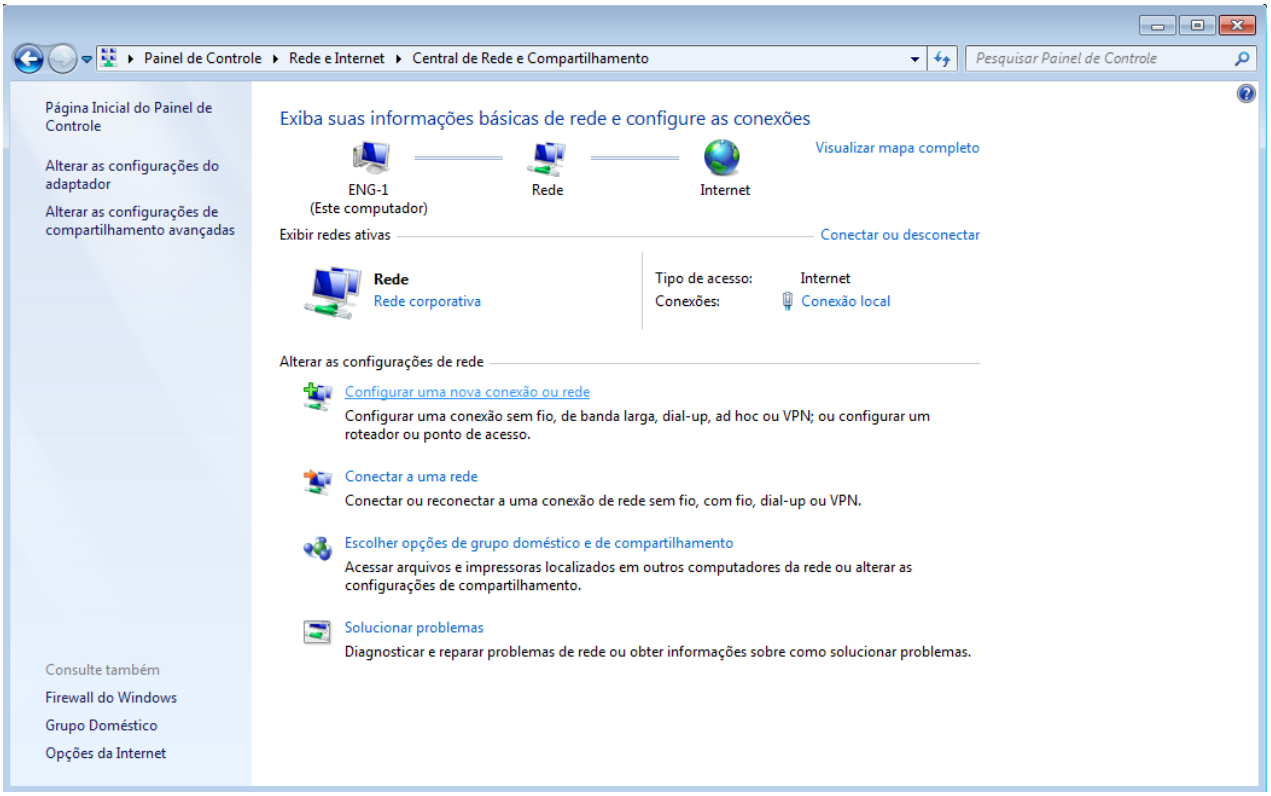
7 - Programe o usuário, a senha e o IP do destino e clique em “Conectar”.

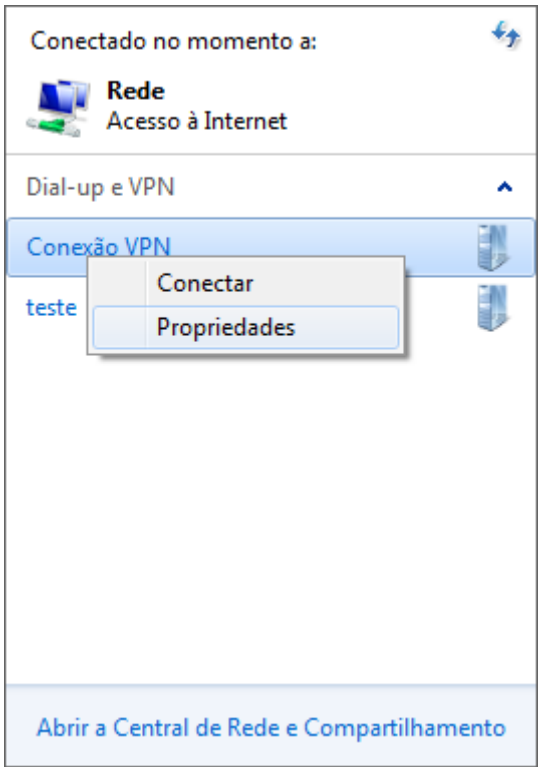


8 - Após aparecerá a conexão, mas essa conexão não irá funcionar pois será necessário configurar mais alguns itens. Clique em "Configurar a conexão assim mesmo"

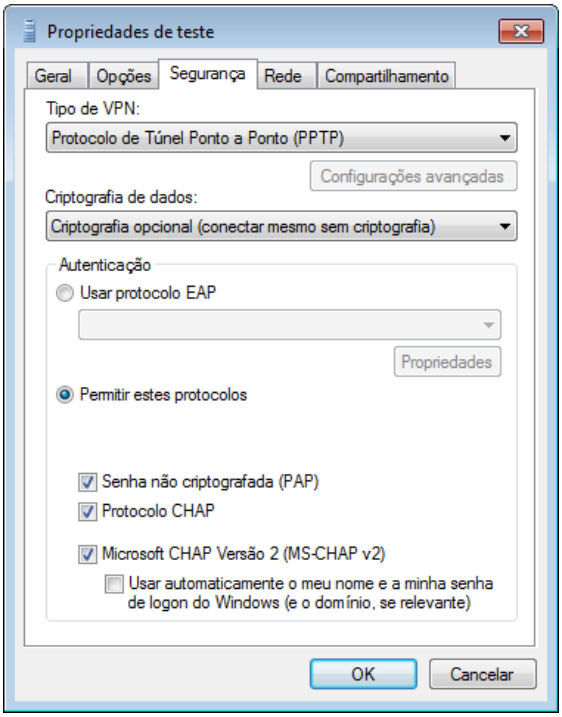


9 - Entre no item "Conectar a uma rede" e com botão direito do mouse clique sobre a conexão configurada e selecione o item “propriedades”.

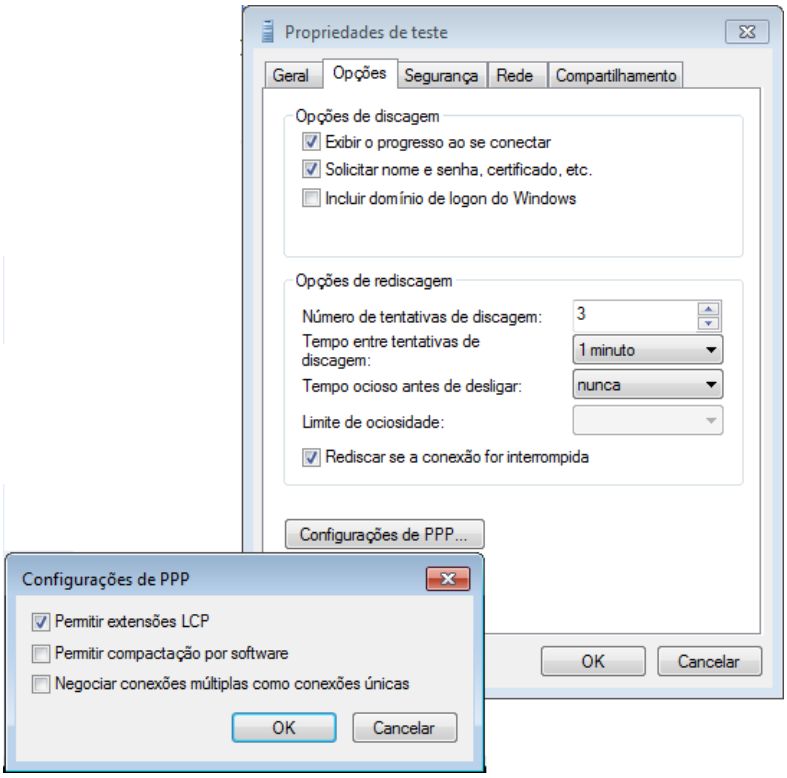




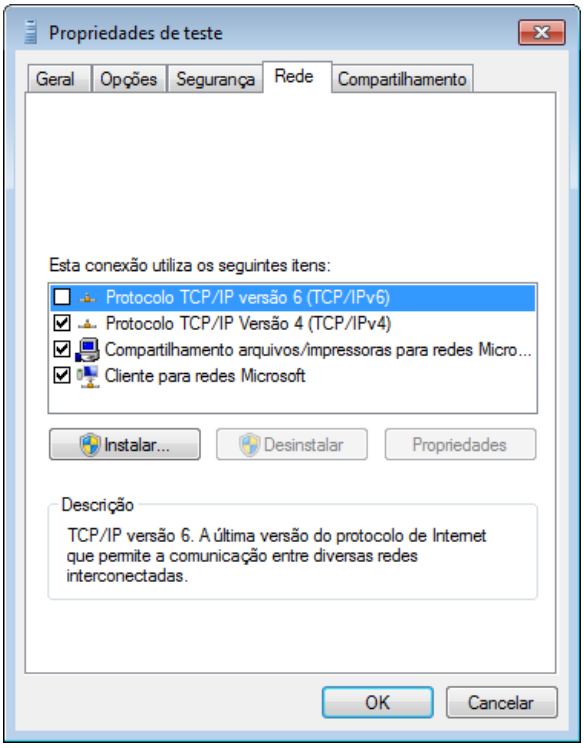
10 - Clique na aba "Segurança" e programe os itens conforme as telas abaixo. Após clique em “OK”



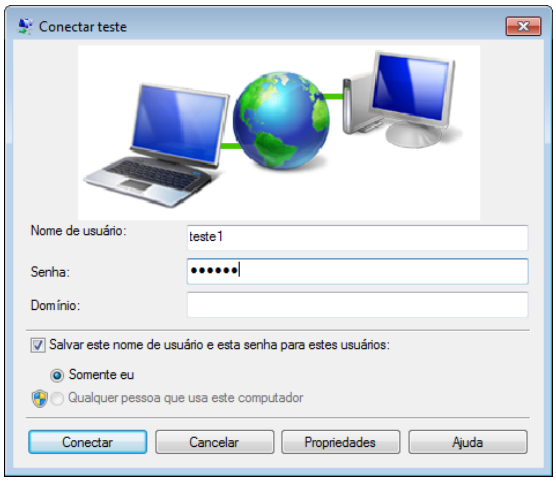
11 - Clique na aba "Opções" e programe os itens conforme as telas abaixo. Após clique em “OK”



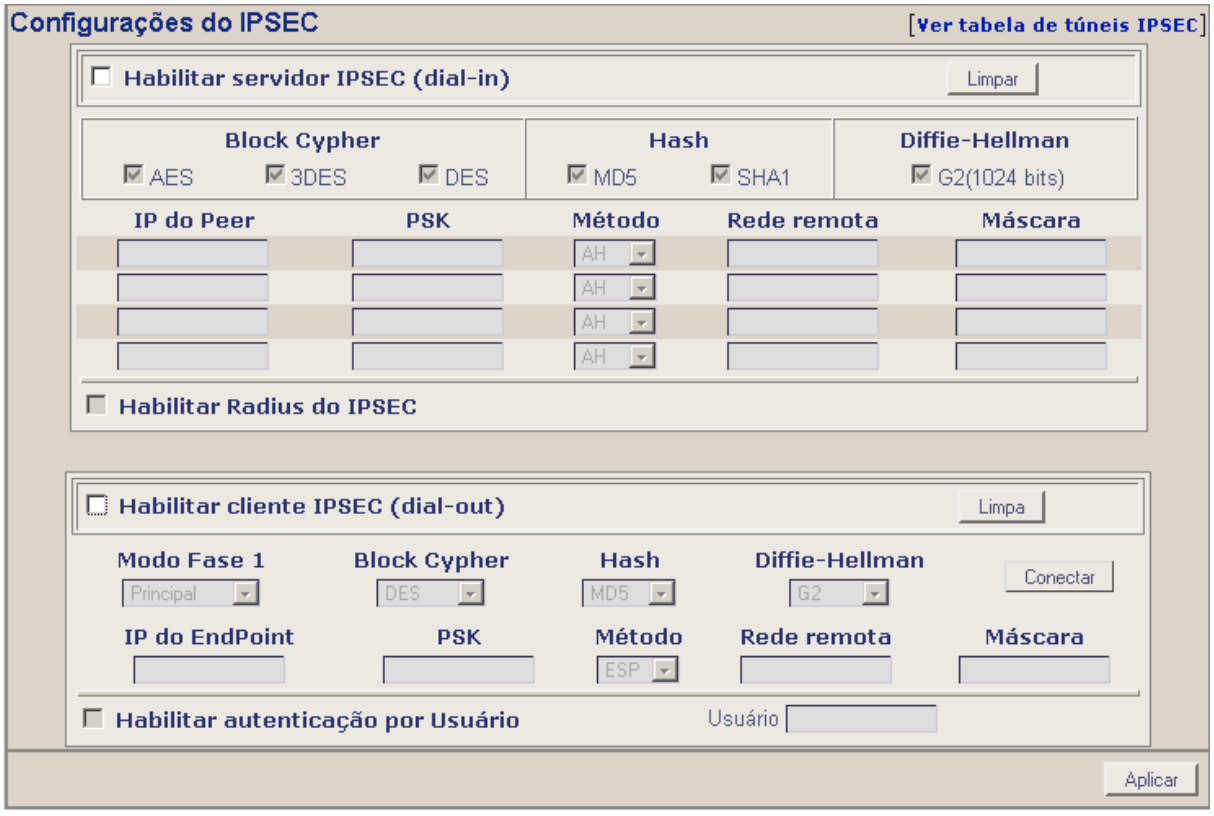
12 - Clique na aba "Rede" e programe os itens conforme as telas abaixo. Após clique em “OK”



13 - Configure usuário e senha. Após clique em “Conectar”.



3.4.3. Configurações do IPSEC



O IPSec ou IP seguro é um conjunto de protocolos desenvolvido pelo grupo de segurança do IETF para garantir autenticidade, confidenciabilidade e integridade dos dados. Os protocolos IPSec são de camada 3, ou seja, fazem IP sobre IP. Outra função do IPSec é o gerenciamento e troca de chaves IKE (Internet Key Exchange- RFC 2409).

O IPSec possui dois modos de operação:

Modo transporte: Somente os dados são criptografados. Assim a composição final do pacote IP será: Cabeçalho original + Cabeçalho IPSec + Dados criptografados.

Modo túnel: Tanto o cabeçalho quanto os dados são criptografados. Assim a composição do pacote IP será: Novo cabeçalho IP + Cabeçalho IPSec + Cabeçalho e dados criptografados.

O Gateway Digistar também permite utilizar o modo de túnel.

Como falado anteriormente o IPSec é um conjunto de protocolos, composto de:

AH (Autenticação de Cabeçalho – RFC 2402): Fornece autenticação e integridade dos dados, porém não fornece confidencialidade;
ESP (Dados encapsulados – RFC 2406): Fornece autenticação e confidencialidade dos dados através de criptografia, porém não oferece integridade.

IKE (Troca de chaves pela Internet – RFC 2409): Utilizado para troca de Associações Seguras (SA), ou seja, verifica quais os tipos de criptografia disponíveis em ambos os lados, e também gerencia os tipos de chaves disponíveis.

Existem três métodos de autenticação:

- PSK (Pre-Shared Key, ou Chave pré-compartilhada): É o método em que as duas pontas possuem a mesma chave e na hora de estabelecer o túnel as mesmas são verificadas.
- Certificados: É o método em que um certificado da maquina A é instalado na máquina B e vice-versa. Também é conhecido como uma autenticação assimétrica, pois as chaves para criptografar e para descriptografar são diferentes, garantindo maior segurança. Pela dificuldade de instalação de certificados o Gateway Digistar **não** trabalha com certificados usando IPSec.
- X-Auth ou Híbrida: Autenticação será feita usando uma chave pré-compartilhada para um usuário específico e não para um IP como na PSK.

O túnel IPSec é estabelecido sob demanda e não de forma compulsória, ou seja, quando for feito um Peer, por exemplo, *"ip.remoto"* que possui uma rede LAN 192.168.1.0, com máscara 255.255.255.0, acessando qualquer IP 192.168.1.X, o IPSec tentará criar o túnel. Se o túnel ficar em desuso o túnel deixará de existir. Vale lembrar que é necessário que as redes privadas das máquinas sejam diferentes para que o túnel LAN-to-LAN se estabeleça.

Para que se estabeleça um túnel IPSEC (caso se use o L2TP com criptografia) existe a necessidade de selecionar o tipo de identificador do servidor. Se a empresa possuir um IP fixo (p. exemplo 200.200.200.200) e estiver selecionado o campo "Usar IP da WAN" para que a discagem funcione, a conexão deve discar exclusivamente para este número IP. Se estiver sendo usado o DNS dinâmico no Gateway Digistar podemos usar o campo "Usar FQDN do DDNS" e assim a conexão pode ser estabelecida discando para um nome ou FQDN (p. exemplo ip.do.servidor.com). Se estiver atrás de outra rede privada, ou outra máquina faz o DNS dinâmico é possível usar a opção "Usar FQDN ou IP específico" e colocar outro identificador.

Como o túnel é criado sob demanda, qualquer Peer colocado no campo "Dial–in", pode ser usado para começar o túnel. Qualquer serviço que tentar acessar o IP da LAN do Peer remoto (por exemplo, ping 192.168.10.1), estabelecerá a conexão.

Se houver a necessidade de forçar a conexão, ou de usar o IPSec no modo Híbrido, existe o campo "Dial-out" , onde é possível usar o botão "Conectar" ou a autenticação por usuário..

Para ver quais os túneis que estão ativos no momento, basta ir na opção "Ver tabela de túneis IPSEC".

Os algoritmos de cryptografia (block cypher) utilizados são o DES, 3DES e AES. Os algoritmos de embaralhamento (hash) são o MD5 e o SHA1. O algoritmo de exponenciação é o Diffie-Hellman grupo 2 (1024 bits) (chave simétrica).

Para o cliente de um túnel IPSEC há a opção de definir qual o algoritmo de criptografia (block cypher) e o algoritmo de embaralhamento (hash) desejável para a conexão. Também é possível definir o modo como será feita a troca de chaves pela Internet (IKE). A conexão é estabelecida em duas fases, sendo que na primeira (Modo Fase 1) é possível mandar todas as informações (6 pacotes) ou metade delas (3 pacotes). Quando se envia todas as informações é chamado de modo principal, quando se envia metade chamamos modo agressivo. Para garantir maior segurança o modo principal é recomendado.

3.5. Serviços

3.5.1. Configurações de Data e Hora

Método de Sincronização

O relógio do Gateway Digistar pode ser sincronizado a partir de três tipos de fonte de data e hora: servidores **NTP** (RFC1305), servidores de **RDATE** (RFC868), e também o próprio **browser.**

Para que possa sincronizar data e hora através de servidores de NTP ou RDATE, o Gateway Digistar deve estar com a rede da WAN configurada e com acesso a pelo menos um dos servidores que devem ser especificados. A sincronização é realizada assim que as configurações são aplicadas e também a cada reinicialização do Gateway Digistar. Se os servidores estiverem indisponíveis por qualquer motivo então será realizada uma nova tentativa de atualização de cinco em cinco minutos até que o relógio seja sincronizado com sucesso.

Para o caso de não haver disponibilidade de alguma máquina com servidores NTP ou RDATE segue abaixo uma lista de servidores públicos na internet. Deve-se notar que estes servidores são oferecidos voluntariamente e não têm garantias de precisão de relógio nem de disponibilidade de acesso. Uma lista maior e atualizada de servidores NTP pode ser encontrada em http://ntp.isc.org.

NTP	RDATE
br.pool.ntp.org	time.nist.gov
south-america.pool.ntp.org	time-a.nist.gov
pool.ntp.org	time-b.nist.gov
0.pool.ntp.org	time-a.timefreq.bldrdoc.gov, time-b.timefreq.bldrdoc.gov, time-c.timefreq.bldrdoc.gov
1.pool.ntp.org	utcnist.colorado.edu
2.pool.ntp.org	nist1.symmetricom.com

Para atualizar a data e a hora pelo navegador basta ajustar o relógio da máquina cliente do Configurador Web Digistar e aplicar a configuração. Utilizando o ajuste de data e hora através do browser será necessário fazer a sincronização através do configurador cada vez que o Gateway Digistar for inicializado.

Fuso horário

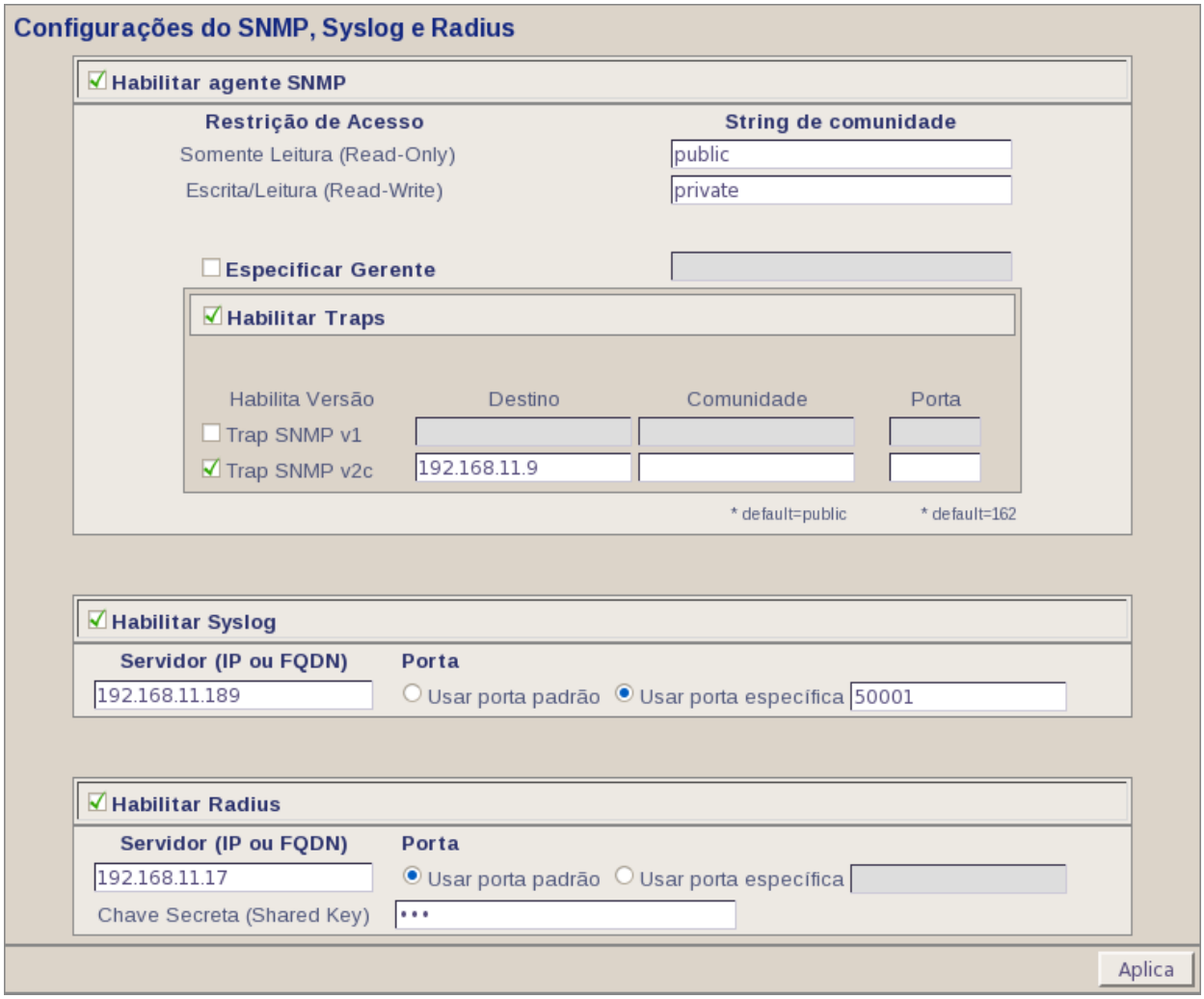
Selecione o fuso horário correspondente à sua região. Os fusos horários dos estados brasileiros são apresentados abaixo:

Acre, Amazonas (oeste)	GMT-5:00
Amazonas (leste), Mato Grosso, Mato Grosso do Sul, Pará (oeste), Rondônia, Roraima	GMT-4:00
Alagoas, Amapá, Bahia, Ceará, Distrito Federal, Espírito Santo, Goiás, Maranhão, Minas Gerais, Pará (oeste), Paraíba, Paraná, Pernambuco (oeste), Piauí, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul, Santa Catarina, São Paulo, Sergipe, Tocantins	GMT-3:00
Pernambuco (leste)	GMT-2:00

Horário de verão

As datas de início e fim do horário de verão estão sujeitas à legislação vigente na região. Para configurar duração do horário de verão corrente no Brasil consulte os decretos do governo disponíveis no site http://pcdsh01.on.br/DecHV.html

3.5.2. Configurações de SNMP, Syslog e RADIUS



Habilitar agente SNMP

O Gateway Digistar possui ferramentas convencionais de gerenciamento como o agente SNMP (Simple Network Management Protocol). O SNMP é um protocolo, na camada de aplicação, para o gerenciamento de redes TCP/IP. O agente SNMP do Gateway Digistar tem suporte às versões v1 e v2c do SNMP, implementando as MIBs:

- MIB-II (RFC 1213): permite o monitoramento de diversas informações da rede, tais como estado das interfaces de rede e estatísticas de uso dos protocolos TCP/UDP, entre outras.
- RTP-MIB (RFC 2959): possibilita monitorar o desempenho das ligações VoIP.
- DS1-MIB (RFC 4805): permite monitorar a interface E1 no Gateway Digistar

Restrições de Acesso: Por motivos de segurança é possível especificar comunidades (String de comunidade) de somente leitura ou comunidades que permitam também escritas. Caso sejam definidas comunidades equivalentes nos dois modos, prevalecerá a opção de somente leitura e a escrita não será permitida.

Especificar Gerente: Para garantir que somente uma máquina possa gerenciar é possível colocar o IP ou FQDN (nome do domínio, www.digistar.com.br, por exemplo) de um gerente específico.

Habilitar Traps: Além de consultas ao Gateway Digistar o agente SNMP também permite o envio de alarmes (Traps/Notificações) sobre determinados eventos ocorridos no equipamento. São enviadas Traps, conforme a MIB II, quando o agente é iniciado e finalizado, e quando é recebida uma requisição SNMP v1 usando uma comunidade com um nome desconhecido. Também são enviadas Traps quando é modificado o estado do tronco E1, como definido em DS1-MIB (RFC 4805). É possível habilitar o envio de Traps nas versões SNMP v1 e SNMP v2. Caso for ativada as duas opções o agente do Gateway Digistar enviará Traps em ambas as versões. Em cada versão habilitada deve-se definir o IP ou FQDN e a Porta de destino das Traps. Se não for definido um valor para a porta será utilizada a porta padrão 162. Quando necessário também é possível definir uma Comunidade específica às Traps (por padrão envia-se com a comunicada "public").

Habilitar SYSLOG

O syslog (RFC – 3164) é um protocolo de transmissão de eventos e notificações (Logs) pela internet. Foi desenvolvido inicialmente na University of Califórnia Berkeley Software Distribution (BSD). O Syslog utiliza protocolo UDP e a porta 514 como padrão de saída. Também há a opção de trocar a porta de saída.

Habilitar RADIUS

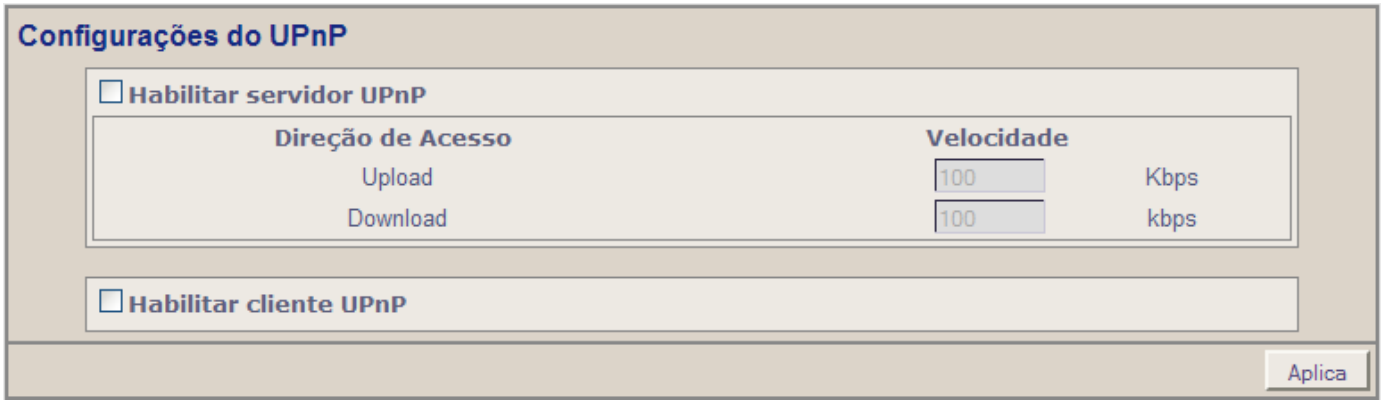
O RADIUS (Remote Authentication Dial In User Service) é um protocolo especificado pela RFC – 2865 para fazer autenticação, autorização e verificação de contas de usuários. O servidor Radius, se habilitado, será o mesmo utilizado para todos os tipos de VPN.

O servidor RADIUS deve estar em uma máquina da rede interna. A porta padrão de uso é a 1812, mas há a opção de mudar a porta de saída.

3.5.3. Configurações do UPnPTM

A UPnP™ é uma arquitetura padrão de conectividade de dispositivos que oferece suporte a anúncio e descoberta de recursos em rede. Mais informações disponíveis no site do Fórum do UPnP™ (http://www.upnp.org/).

Se o servidor UPnP™ estiver habilitado o Gateway Digistar funcionará como um dispositivo IGD (Internet Gateway Device - http://www.upnp.org/standardizeddcps/igd.asp). Os serviços oferecidos por este dispositivo podem ser utilizados por aplicações em máquinas da LAN. Bons exemplos destas aplicações são o MSN Messenger e mesmo outros Gateway Digistar que precisam de algumas adaptações para funcionar em redes privadas. Para que o tráfego multimídia destas aplicações possa ser transferido uma solução comum é requisitar redirecionamentos de porta por NAT para o dispositivo UPnP™ que tem acesso à WAN.



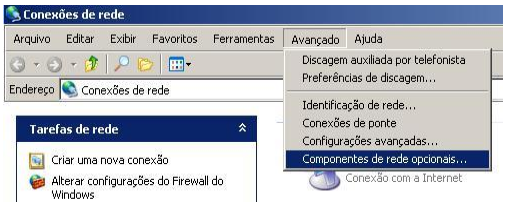
Se o cliente UPnP™ estiver habilitado então o Gateway Digistar funcionará como um controlador IGD e poderá executar ações dos serviços disponíveis caso esteja na LAN de algum outro dispositivo IGD. Nos casos em que Gateway Digistar não possui um IP público, somente um IP privado, o cliente UPnP™ pode ser habilitado para requisitar automaticamente redirecionamentos de porta por NAT para possibilitar o tráfego de voz das ligações. A página de configuração do cliente apresenta algumas informações do dispositivo IGD que for detectado na interface da WAN. Através da página de configuração também é possível requisitar e remover redirecionamentos de porta no dispositivo IGD interativamente.

ATENÇÃO: *Para funcionar o cliente UPnP™, o firewall precisa estar desabilitado.*

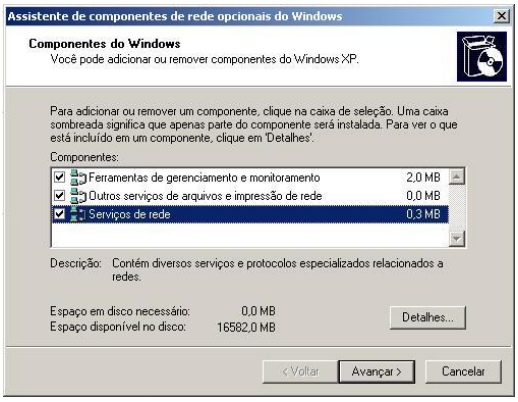
O Gateway Digistar enquanto cliente UPnP se comunica com o servidor pela interface da WAN, e o servidor UPnP do Gateway Digistar se comunica com clientes pela interface da LAN. As duas opções (cliente e servidor) são mutuamente exclusivas, portanto somente uma delas pode estar habilitada.

Se os serviços de UPnP estiverem instalados no Windows XP, um ícone de Conexão com a Internet deverá aparecer, como mostra a figura abaixo, quando o computador estiver conectado na LAN de um Gateway Digistar com o servidor UPnP habilitado.

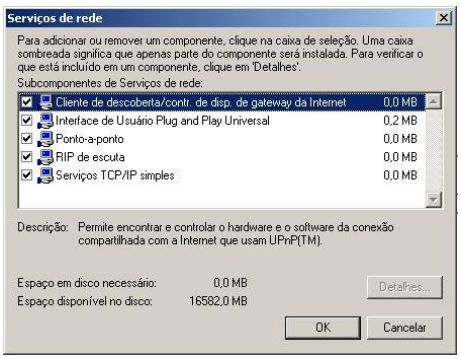
Para utilizar os recursos do UPnP no Windows XP é necessário ter os componentes de software do UPnP instalado. Na janela de diálogo de conexões de rede selecione “Componentes de rede opcionais” na aba “Avançado”.



Abra os detalhes do item “Serviços de rede”.



Selecione o item “Cliente de descoberta/controle de dispositivos de gateway da Internet” “Interface de Usuário Plug and Play Universal”.



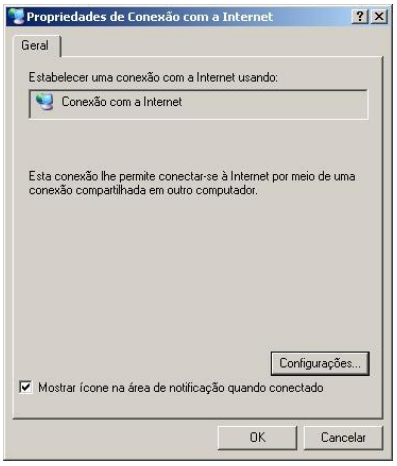
Depois de realizadas as configurações, será possível visualizar o ícone do Internet Gateway Device na janela de Conexões de Rede.

Para verificar o status do dispositivo dê um clique duplo sobre o ícone.

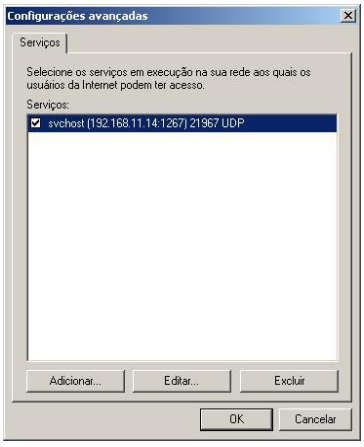
Serão apresentadas informações sobre a conexão.

É possível adicionar redirecionamentos de porta no dispositivo IGD através do Windows.

Acesse as propriedades na tela de status e na tela de propriedades entre em Configurações.



Na tela de configurações avançadas será apresentada uma lista com os redirecionamentos de porta configurados e ativos no dispositivo IGD.



Clique em adicionar para criar novos redirecionamentos de porta. Os redirecionamentos de portas criados por requisições UPnP para o Gateway Digistar funcionam da mesma maneira que os redirecionamentos de porta por NAT (PAT), contudo são perdidos após a reinicialização do Gateway Digistar.

O exemplo abaixo cria um redirecionamento TCP da porta 1022 do IP da WAN do Gateway Digistar para a porta 22 do IP 192.168.11.10 da LAN.

Os mapeamentos de porta podem ser requisitados dinamicamente por clientes através da arquitetura do UPnP. Esse recurso é utilizado por diversas aplicações para transpor a limitação que uma rede com IPs privados com NAT constitui. Dentre estas aplicações podemos citar o MSN Messenger, Microsoft's Remote Assistance, Remote Desktop e o próprio Gateway Digistar. Deve-se notar que este recurso tem um histórico de vulnerabilidades de segurança bastante negativo em plataformas Windows, portanto é recomendável que as máquinas clientes da LAN sejam mantidas com o software sempre atualizado.

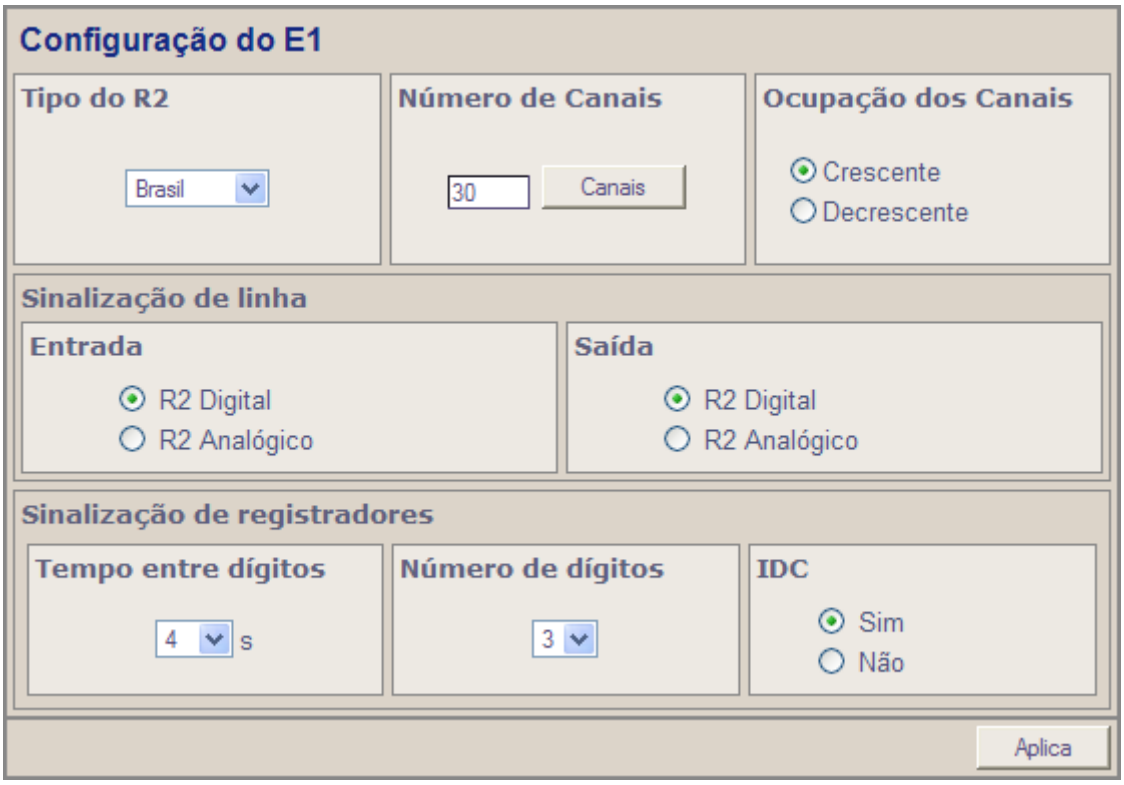
3.5.4. Troca do MAC

O Gateway Digistar vem programado de fábrica com um número MAC. Caso haja colisão do número com outro da rede, existe a possibilidade de trocar por outro MAC. Para que a operação de troca de número MAC seja feita com sucesso, após a troca, o Gateway Digistar deve ser reinicializado.

Também existe a opção de verificar a tabela ARP (Resolução de endereços com os MAC) visível nas interfaces de rede, clicando na opção *"Ver tabela de ARP"*.

3.6. TDM

3.6.1. Configuração do Tronco Digital

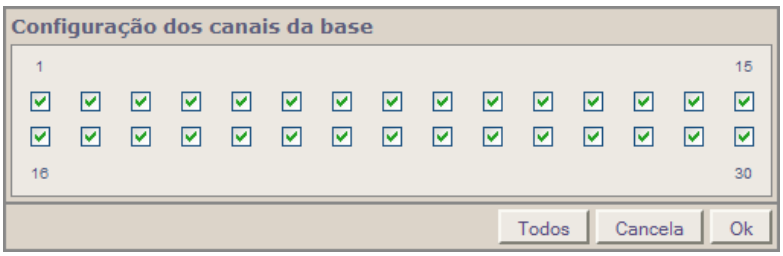


Tipo de R2

Devido às diferenças de protocolos utilizados, para o correto funcionamento da sinalização MFC e particularidades do envio de IDC, este campo deve ser selecionado.

Número de canais

Neste campo deve ser configurado o número de canais que serão utilizados para se conectar com o PABX.



Ocupação dos canais

Define se a ocupação dos canais do E1 no Gateway Digistar será crescente ou decrescente. Se for configurado como crescente, será escolhido sempre o menor canal E1 disponível para encaminhar ligações VoIP para o equipamento conectado à interface E1. Caso for escolhida a opção "decrescente", o gateway selecionará sempre o maior canal disponível. Isso permite diminuir a chance de colisões, uma vez que ao definir uma ordem diferente da utilizada no PABX conectado ao Gateway Digistar, ocorrerá uma colisão somente quando todos os canais forem ocupados.

Sinalização de Linha

Pode ser configurada tanto para entrada como para saída independentemente. A configuração pode ser feita entre R2 analógico (também conhecida como E+M contínua) ou R2 digital. A sua correta configuração deve estar de acordo com sua prestadora.

Sinalização de Registradores

Tanto na entrada quanto na saída a sinalização será do tipo MFC (utilizado para comunicação entre centrais públicas).

Tempo entre dígitos

Define o tempo máximo de espera entre os dígitos do número de destino enviados pelo PABX ao Gateway Digistar no protocolo E1 (R2/MFC). Se expirar o tempo máximo para enviar o dígito seguinte, a seqüência digitada pelo executor da chamada será considerada finalizada. Caso esta sequência não for equivalente a nenhuma regra de dígitos da Resolução 86 da Anatel, então o critério de análise para o término da seqüência será o tempo desta configuração. Ainda, se o início desta sequência atender a uma regra da Resolução 86, mas não forem fornecidos o número de dígitos esperados, também a ligação será encaminhada após expirar o tempo entre dígitos.

Número de dígitos

O Gateway Digistar quando recebe uma ligação VoIP encaminha esta para o enlace E1. Deve então ser definido o número de dígitos recebidos a serem encaminhados. Por exemplo, se forem configurados 4 dígitos e o número de destino recebido na ligação VoIP for 3590-3456, os dígitos enviados serão os últimos 4, i.e., 3456. (Obs.: a quantidade de dígitos pode ser menor dependendo das regras definidas na configuração de redirecionamento. Ver seção "Configuração do Redirecionamento de Chamadas").

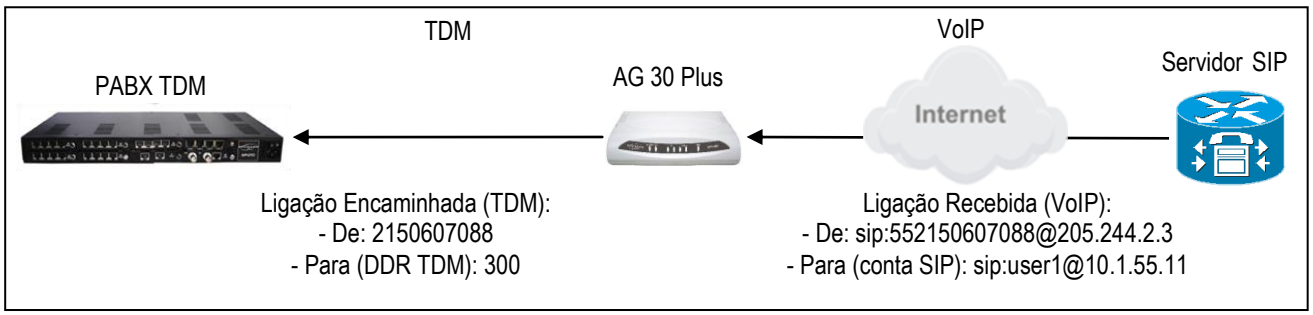
IDC - Identificador de Chamadas

Quando ativado, o Gateway Digistar irá pedir ao PABX a ele conectado o número de identificação de quem está realizando a chamada (IDC). Para o correto funcionamento, o PABX deve também ser configurado para o envio do IDC. Uma vez recebido pelo Gateway, o IDC será repassado ao destino da ligação.

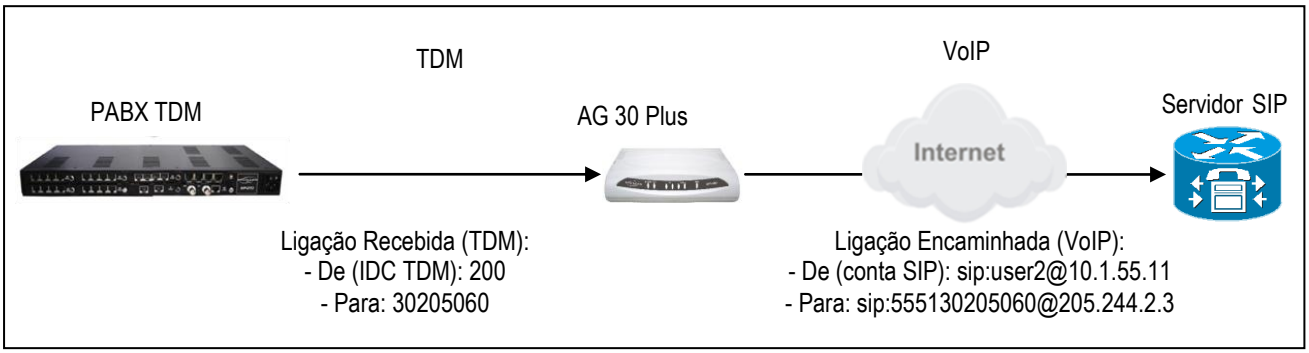
3.6.2. Configuração do Redirecionamento de Chamadas

De modo a redirecionar as ligações entre as duas interfaces (TDM e VoIP) é necessário fazer a associação dos números de DDR/IDC E1 no TDM às contas SIP no VoIP e vice-versa. Assim, uma ligação recebida ou realizada por um interface utilizará o seu par na outra interface.

As figuras abaixo ilustram exemplos de ligações nos dois sentidos e a associação entre as interfaces.



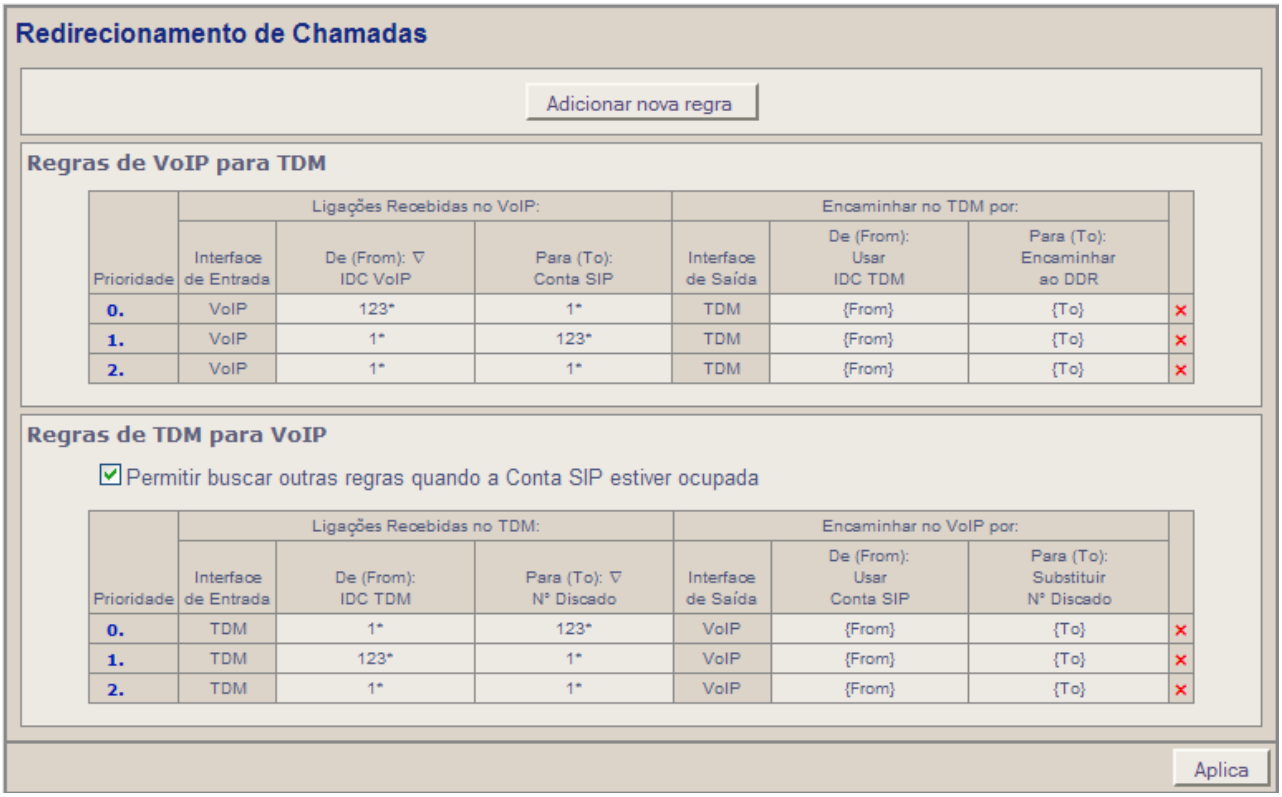
A primeira figura ilustra uma ligação recebida pelo VoIP e encaminhada ao PABX no TDM. O Gateway Digistar associa a conta SIP do VoIP ao seu DDR correspondente no TDM, nesse caso a conta "user1" ao DDR "300".



Na segunda figura ilustra-se um exemplo de uma ligação recebida pelo Gateway Digistar a partir da rede TDM, sendo encaminhada pelo VoIP. Nesse exemplo, a origem no TDM, o IDC "200", corresponde no VoIP à conta SIP "user2". O Gateway Digistar, ao receber a ligação pelo TDM, redireciona pelo VoIP utilizando o par correspondente. Observe que nesse exemplo, optou-se, por alterar o número de destino "30205060", acrescentando os prefixos "+5551" ao número discado.

Esses redirecionamentos são configurados utilizando-se de regras com expressões regulares[1], as quais permitem realizar a associação e substituições de modo flexível.

[1] Expressões regulares: provém, por meio de uma linguagem formal, uma maneira concisa e flexível para identificar cadeias de caracteres de interesse, como caracteres específicos, palavras, ou padrões de caracteres.



Caso os DDRs/IDCs e as contas SIP apresentem algum padrão de equivalência, é possível criar apenas uma regra para encaminhar diversas ligações. Do contrário, devem-se criar regras específicas para cada associação.

Observação: é necessário criar regras para os dois sentidos: chamadas de VoIP para TDM e chamadas de TDM para VoIP. Isso é preciso porque as chamadas podem ter associações diferentes entre os DDRs/IDCs E1 e as contas SIP, dependendo do sentido que são realizadas.

Regras de VoIP para TDM

Nesse cenário as ligações são originadas no VoIP por algum dos servidores SIP ou por um ponto VoIP remoto, tendo como destino alguma das contas SIP cadastradas no Gateway Digistar. Ao receber a ligação o Gateway Digistar deve identificar e encaminhar ao DDR no TDM equivalente à conta SIP. Isso é feito, por meio das regras com direção VoIP→TDM.

Primeiramente, deve-se descrever em cada regra uma ligação ou um padrão de ligações que deseja-se tratar pela regra quando for recebida na interface VoIP. Essa configuração pode ser feita apontando na regra: a conta SIP específica de destino da ligação; os endereços/números VoIP da origem; ou escrevendo uma expressão de associação (ver “Expressões de Associação”), que permite associar com várias contas SIP e endereços/números VoIP de origem.

Além disso, deve-se apontar a qual número DDR a ligação será encaminhada no TDM. Isso é feito, definindo o número exato do DDR ou por meio de uma expressão de substituição, que a partir do valor recebido no VoIP faz trocas de dígitos para definir o DDR ao qual será encaminhada a ligação (ver “Expressões de Substituição”).

Adicionalmente, pode-se definir qual o IDC a ser enviado no TDM, que pode ser um valor fixo, repassando o número provindo da origem no VoIP, ou até aplicando uma expressão de substituição para manipular a origem identificada no VoIP.

- **Ligações Recebidas:** descreve uma ou várias ligações recebidas pela interface VoIP e que serão encaminhadas à interface TDM, sendo:
  - **Interface de Entrada:** interface por onde a ligação foi recebida, nesse caso será a VoIP
  - **De (From): IDC VoIP:** expressão de associação ou identificação do originador da ligação no VoIP.
  - **Para (To): Conta SIP:** expressão de associação ou identificação da conta SIP de destino.

- **Encaminhar por:** redirecionamento da ligação pelo TDM, onde:
  - **Interface de Saída:** interface por onde a ligação será encaminhada, nesse caso o TDM.
  - **De (From'): Usar IDC TDM:** expressão de substituição ou o número exato do IDC pelo qual a ligação será feita no TDM.
  - **Para (To'): Encaminhar ao DDR:** expressão de substituição ou número exato do DDR de destino.

Regras de TDM para VoIP

Nesse cenário as ligações são originadas no TDM pelo PABX conectado ao Gateway Digistar. Ao receber a ligação o Gateway Digistar deve identificar e encaminhar, por alguma conta SIP cadastrada, para o Servidor SIP correspondente. Isso é feito por meio das regras com direção TDM →VoIP.

A descrição da ligação ou do conjunto de ligações que serão tratadas por cada regra quando recebida(s) pelo TDM pode ser feita apontando: o número exato do IDC provindo no TDM; o número discado; ou escrevendo uma expressão de associação (ver "Expressões de Associação"), que permite associar com várias origens (IDCs) e números discados.

Além disso, deve-se apontar a conta SIP para fazer a ligação no VoIP. Isso é feito selecionando uma conta SIP cadastrada ou por meio de uma expressão de substituição, que a partir do valor recebido no IDC do TDM, faz substituições para identificar qual conta SIP será usada (ver "Expressões de Substituição").

Obs.: se nenhuma conta SIP válida for identificada para encaminhar a chamada, a ligação será rejeitada.

Adicionalmente, pode-se manipular o número de destino a ser enviado ao VoIP também por meio de expressões de substituição.

- **Ligações Recebidas:** descreve uma ou várias ligações recebidas pela interface TDM, sendo:
  - **Interface de Entrada:** interface por onde a ligação foi recebida, nesse caso será a TDM.
  - **De (From): IDC TDM:** expressão de associação ou o número exato no TDM originador da ligação.
  - **Para (To): Nº Discado:** expressão de associação ou o número exato de destino discado no TDM.

- **Encaminhar por:** redirecionamento da ligação pelo VoIP, onde:
  - **Interface de Saída:** interface por onde a ligação será encaminhada, nesse caso o VoIP
  - **De (From'): Usar Conta SIP:** expressão de substituição ou a conta SIP pela qual a ligação será feita no VoIP.
  - **Para (To'): Substituir Nº Discado:** expressão de substituição ou o número do destino (opcional).

Expressões de Associação

As expressões de associação são utilizadas para descreverem as ligações de entrada. Elas são baseadas nas expressões regulares e permitem vincular com uma ou várias ligações. Para isso, pode-se combinar os seguintes comandos:

^	Início da discagem
N	Um dígito: [0-9], [a-z] ou [A-Z]
*	Nenhum ou mais dígitos N
+	Um ou mais dígitos N
?	Nenhum ou um dígito
[x-y]	Intervalos como: [1-3], [a-z]...
[1,4]	Somente dígitos: 1 e 4
$	Fim da discagem
{n,m}	De 'n' a 'm' caracteres
{n}	Exatamente 'n' caracteres

Exemplos:

^NNN Qualquer número de três dígitos (ex.: 201, 356, 999, etc)

^2NN Qualquer número de três dígitos, iniciado com 2 (ex.: 201, 205, 209, etc)

^[0-8] Qualquer número cujo o primeiro dígito esteja entre 0 e 8, isto é, excluindo os que começam com o dígito 9 (ex.:0800, 30303030, 07711.., etc)

* Qualquer número. (ex.: 201, 9090303030, 0800, etc)

Expressões de Substituição

As expressões de substituição são utilizadas no encaminhamento das ligações, trocando dígitos ou caracteres para os valores equivalentes na outra interface. A seguir tem-se a sintaxe dessas expressões:

- Expressão de substituição do originador: <num>{From:<offset>:<length>}<num>
- Expressão de substituição de destino: <num>{To:<offset>:< length >} <num>

A primeira define o modo de substituição do identificador da chamada (originador), tanto do TDM (IDC) como do VoIP (IDC VoIP). A segunda é para definir o número de destino, sendo o DDR nas ligações para o TDM e o número de saída (Nº Discado) nas ligações para o VoIP.

Com essas expressões é possível referenciar os números originais pelas palavras "From" para o originador e "TO" para o destino. Podem-se acrescentar números antes ou depois (<num>) e também referenciar somente partes dos números originais, possibilitando uma gama de combinações. A referência para parte dos números originais (From ou To) é feita apontando o primeiro digito em <offset> e quantos dígitos, a partir do primeiro, que serão considerados em <length>. Existem algumas considerações:

- O primeiro dígito está na posição zero (*offset* = 0).
- Se o *offset* for negativo, são considerados os dígitos, iniciando do *offset*, da direita para a esquerda. Se *offset* for positivo, considera-se da esquerda para a direita.
- Se a *length* for omitido, então todo o restante dos dígitos, iniciando do *offset*, será considerado.

Exemplos:

Sendo "To" igual a "30405060", têm-se os seguintes resultados com as expressões abaixo:

{To:4}	Significado: a partir do dígito na posição quatro, pega todo o resto. Resultado: 5060
{To:0:3}	Significado: a partir do dígito na posição zero, pega três dígitos. Resultado: 304
09988{To}	Significado: acrescenta o prefixo 09988. Resultado: 0998830405060

Sendo "From" igual a "2345", têm-se os seguintes resultados com as expressões abaixo:

{From:-1:2}	Significado: a partir do dígito na posição um a partir da direita, pega dois dígitos. Resultado: 45
30{From}40	Significado: acrescenta o prefixo 30 e o sufixo 40. Resultado: 30234540

Ordem de execução das regras:

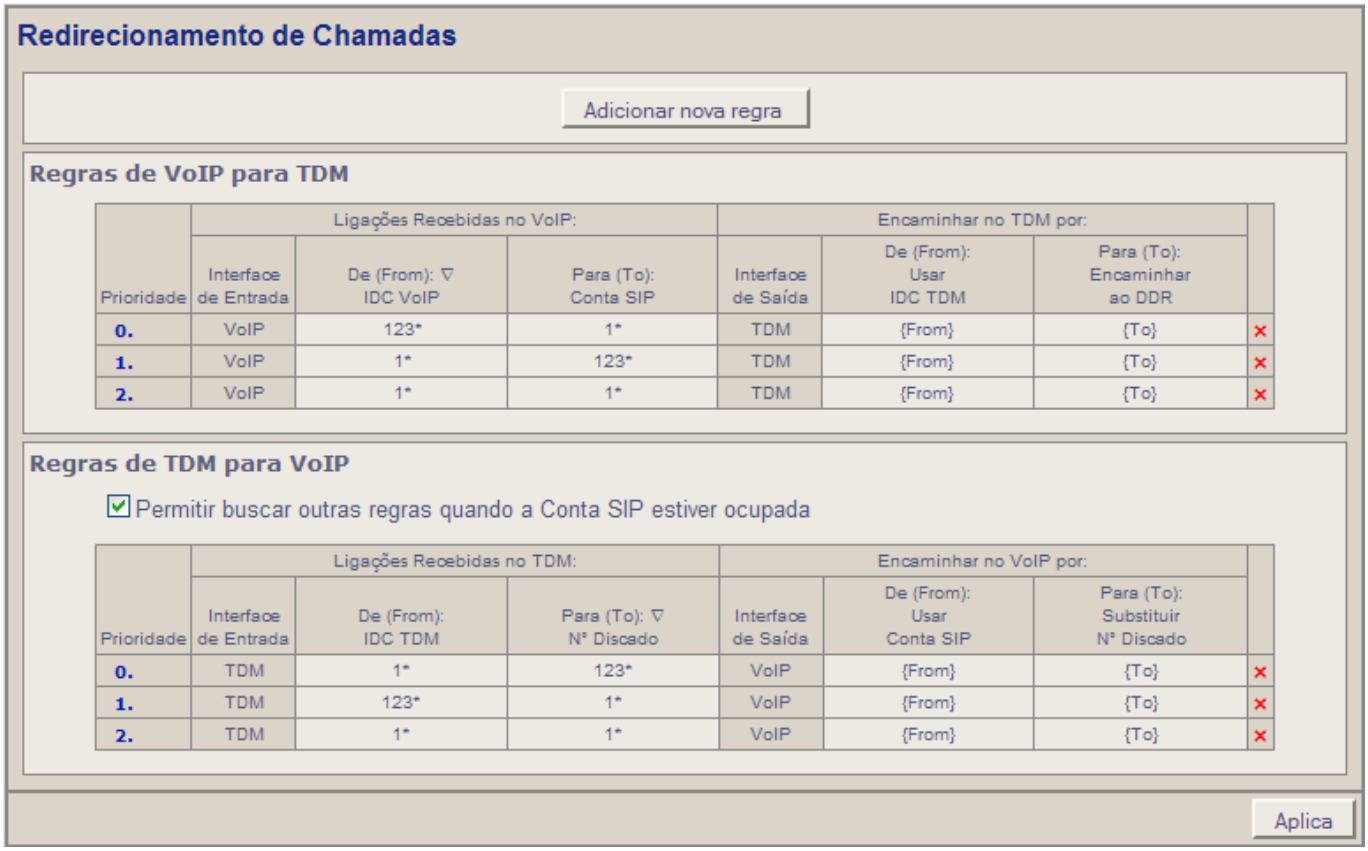
A ordem de execução das regras influência no resultado final. Assim, as regras são ordenadas, automaticamente, da mais específica para a menos, ou seja, a regra que tiver maior número de dígitos especificados será executada antes de uma regra com menos.

Exemplificando: caso em uma regra de TDM para VoIP for definido no campo de destino (Para) a expressão "1*" e em outra igual a "123*", essa última regra terá uma prioridade maior que a outra. Assim, caso chegue uma ligação com o destino igual a "1234", ela casará com a regra "123*" e se chegar uma ligação com destino igual a "1555", será verificado primeiro a regra "123*", mas casará com a regra "1*".

É possível ver a prioridade de cada regra pela coluna "Prioridade" na tela de Redirecionamento. Os campos considerados no ordenamento são diferentes nas ligações de entrada e nas de saída, sendo:

- Ordenamento nas Ligações de Entrada (VoIP para TDM): primeiro ordenado pelo campo "De" e depois pelo campo "Para" nas colunas de Ligação Recebida.
- Ordenamento nas Ligações de Saída (TDM para VoIP): primeiro ordenado pelo campo "Para" e depois pelo campo "De" nas colunas de Ligação Recebida.

Assim, se forem cadastradas as mesmas regras para ligações de VoIP para TDM e de ligações de TDM para VoIP elas ficariam ordenadas de modo diferente, tal como exemplificado na figura abaixo.



Permitir buscar outras regras quando a Conta SIP estiver ocupada.

Nas ligações de TDM para VoIP pode existir situações em que não é permitido que uma conta SIP realize ligações simultâneas, mas as regras possibilitem que dois IDCs tentem utilizar uma mesma conta SIP. Como alternativa, pode-se habilitar para que, quando a conta SIP estiver ocupada, o Gateway Digistar continue executando as demais regras para tentar encontrar outra possibilidade de encaminhar a ligação por outra conta SIP.

Esse comportamento não se aplica às ligações do VoIP para TDM, sendo que o Gateway Digistar encaminha as ligações mesmo que o destino no TDM esteja ocupado. Fica como responsabilidade do PABX no TDM rejeitar ou re-encaminhar a ligação para outro DDR.

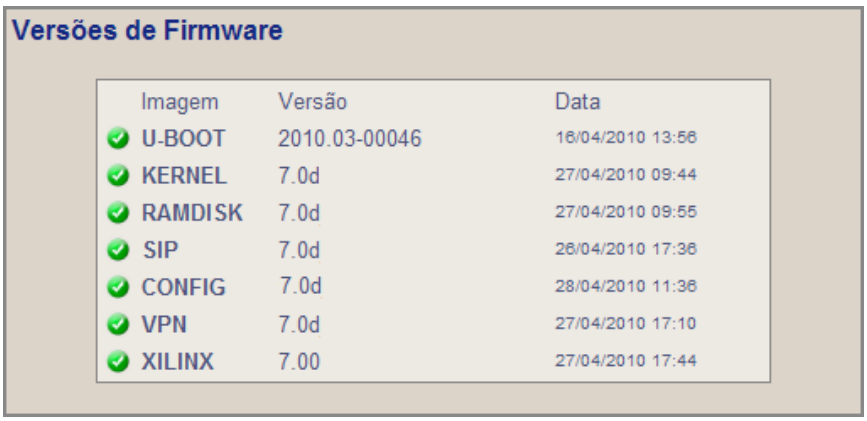
4. Manutenção

Os itens a seguir são para realizar a manutenção do sistema depois de configurado.

4.1. Firmware

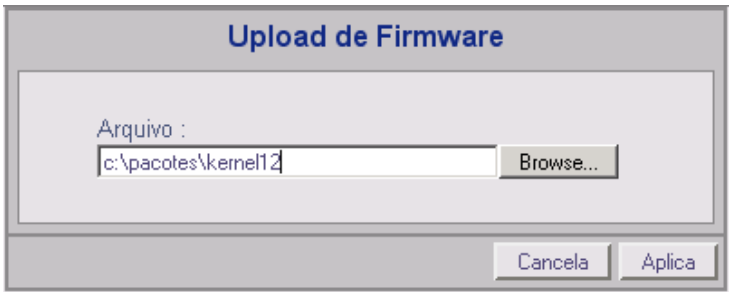
4.1.1. Versões

Tela onde são mostradas as versões de todos os pacotes instalados no Gateway Digistar.



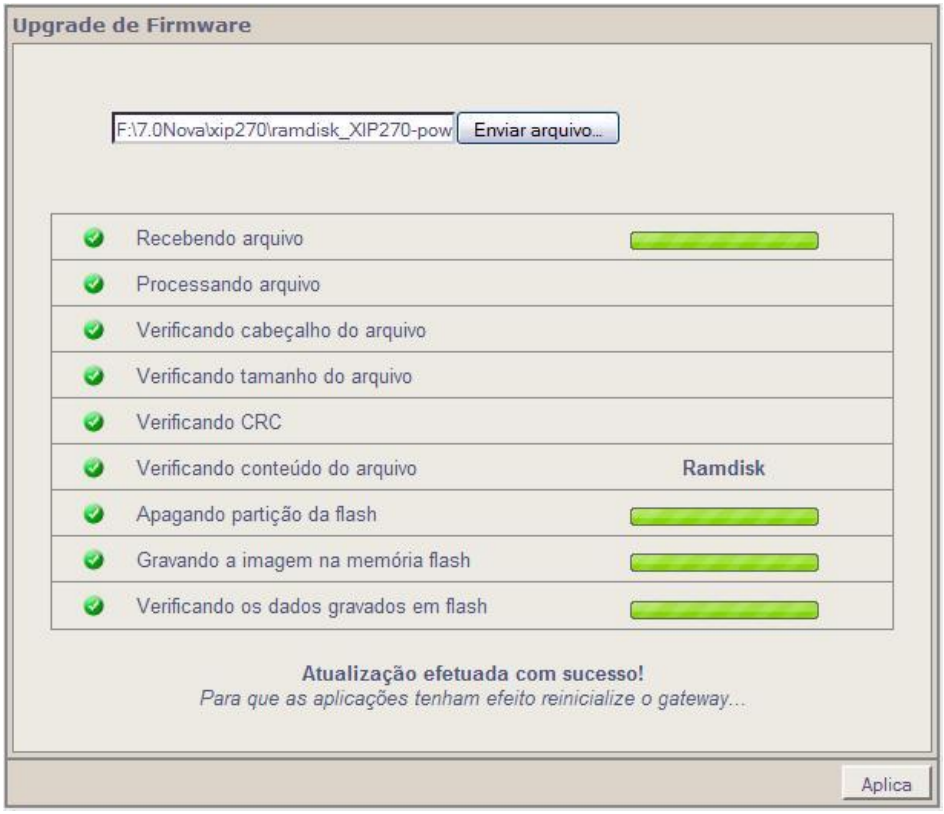
4.1.2. Upgrade de Firmware

Para manter seu Gateway Digistar sempre atualizado existe na opção upgrade de firmware, uma forma bastante simples de operação. Colocando no campo “Upgrade de Firmware”, qualquer pacote de atualização (Kernel, Ramdisk, SIP, Config, VPN ou Xilinx), o Gateway Digistar irá automaticamente identificar o pacote utilizado e efetuar a gravação do novo pacote.



Se a gravação ocorrer com sucesso, você deve reiniciar o Gateway Digistar. Caso haja algum problema, verifique se a imagem não está corrompida, e repita a operação. Para que haja mais segurança a atualização deve ser feita por uma máquina da interface LAN, embora seja possível atualizar pela interface WAN, habilitando o campo respectivo nas configurações gerais do firewall (Ver *“Seção Firewall”*).

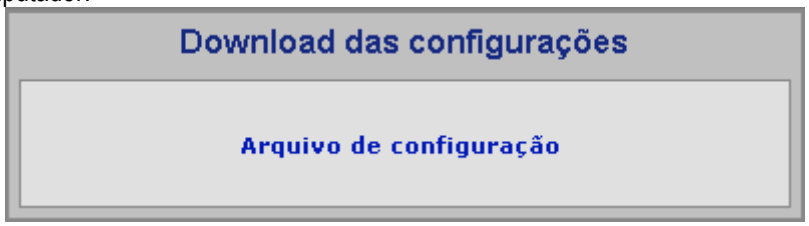
OBS.: *Durante o processo de atualização do firmware alguns serviços podem parar de funcionar. Para o restabelecimento de todas as de todas as funções, aguarde a atualização e resete o Gateway Digistar*



4.2. Configuração

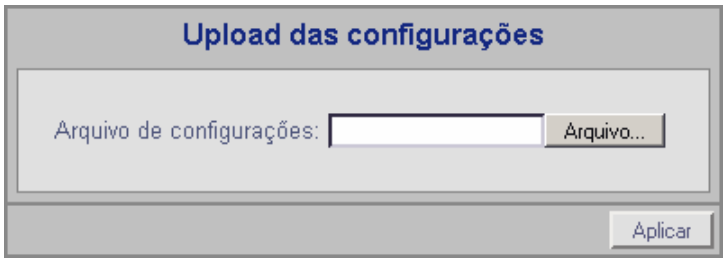
Download

Permite fazer um backup dos arquivos de configuração. Após clicar em download e digitar a senha de programação correta, aparecerá uma tela que permite realizar o download do arquivo de configuração do Gateway Digistar, para um diretório a sua escolha em seu computador.



Upload

Permite a partir de um backup do arquivo de configuração, voltar a uma configuração feita anteriormente. Após clicar em upload aparecerá uma tela que permite realizar o upload do arquivo de configuração. Procure o diretório do computador, onde está o arquivo baixado anteriormente e clique em “Aplica” para trazer o arquivo do computador para o Gateway Digistar. Para as modificações terem efeito será necessário desligar e ligar o Gateway Digistar.



4.3. Misc

4.3.1. Reset Geral

Neste caso as configurações de Gateway Digistar voltarão às configurações de fábrica, ou seja, limpará tudo que fora configurado, inclusive o que está rodando e colocará a configuração de fábrica.

5. Anexo I - Glossário

ADSL	Linha digital Assimétrica para Assinante. Utiliza a linha telefônica a dois fios e permite trafegar simultaneamente voz e dados. Tecnologia de modulação assimétrica entre download e upload (velocidades diferentes).
ARP	Protocolo de Resolução de endereços O protocolo ARP permite certo computador se comunicar com outro computador em rede quando somente o endereço de IP é conhecido pelo destinatário. Todo pacote de IP que circula na rede deve conter IP/MAC do remetente e destinatário. Para se obter o endereço MAC (Media Access Control) do computador do destinatário, o protocolo ARP envia um broadcast com o IP do destinatário requisitando o endereço do MAC do mesmo.
Backup MX	Redireciona os e-mails recebidos no mail.nome.servidor.no-ip.com, por exemplo, para um outro servidor de e-mails, caso o Gateway Digistar esteja desligado.
CHAP	Protocolo de Autenticação de Desafio de Resposta. Utiliza protocolo de codificação Message Digest 5 (MD5) de um só sentido. A senha é enviada de forma codificada
DDNS	Serviço Dinâmico de Resolução de Nomes. Veja DNS.
DDoS	Ataque do tipo DoS realizado de forma distribuída (mais um de ataque simultâneo).
DHCP	Protocolo de Configuração Dinâmica de Máquinas Em redes TCP/IP, todo computador precisa ter um número de IP diferente. Para que duas máquinas não tenham o mesmo número IP, seleciona-se uma máquina que forneça os IPs para todas as máquinas da rede.
Diffserv	Serviço diferenciado, é um tipo de QoS que marca os pacotes de acordo com classes de serviços pré-determinadas.
DMZ	Zona não Militarizada. Especifica uma máquina da rede interna para receber todos os pacotes, com exceção dos pacotes recebidos para portas abertas e portas com redirecionamento por NAT.
DNS	Serviço de resolução de nomes. DNS permite usar nomes amigáveis ao invés de endereços IP para acessar servidores, um recurso básico que existe praticamente desde os primórdios da internet. Quando você se conecta a internet e acessa o endereço http://www.digistar.com.br, é um servidor DNS que converte o "nome fantasia" no endereço IP real do servidor, permitindo que seu micro possa acessar o site.
DoS	Negação de Serviço. Ataques deste tipo comprometem a disponibilidade das máquinas atingidas, seja por alguma vulnerabilidade de segurança ou uma inundação de tráfego falso, fazendo com que estas não consigam atender a demanda de requisições dos clientes.
Download	Transferência de arquivos de uma rede (Ex.: Internet) para o computador local.
DSCP	Ponto de Código de Serviços Diferenciados. São as marcações pré-definidas para selecionar os pacotes utilizados no QoS do tipo Diffserv.
DTMF	Tons de duas freqüências. Sistema de sinalização através de freqüências de áudio (tons) usado em teclado de telefones.

ETHERNET	Ethernet é uma tecnologia de interconexão para redes locais (LAN) baseada no envio de pacotes. Ela define cabeamento e sinais elétricos para a camada física e formato de pacotes e protocolos para a camada de controle de acesso ao meio (MAC) do modelo OSI. A Ethernet foi padronizada pelo IEEE como 802.3.
Firewall	Um sistema de segurança cujo principal objetivo é filtrar o acesso a uma rede.
FQDN	Nome de Domínio Totalmente Qualificado. Combinação dos nomes de host e de domínio de um computador.
FTP	Protocolo de Transferência de Arquivos. O FTP é um protocolo geralmente usado para trocar arquivos sobre toda a rede que suportar o protocolo de TCP/IP. É uma forma bastante rápida e versátil de transferir arquivos, sendo uma das mais usadas na internet. Pode referir-se tanto ao protocolo quanto ao programa que implementa este protocolo (neste caso, tradicionalmente aparece em letras minúsculas, por influência do programa de transferência de arquivos do Unix). A transferência de dados em redes de computadores envolve normalmente transferência de arquivos e acesso a sistemas de arquivos remotos (com a mesma interface usada nos arquivos locais).
Gateway Digistar	Equipamentos de interconexão de redes da Digistar: AG 30 Plus.
GRE	Protocolo de Roteamento Genérico. O protocolo GRE é usado normalmente em conjunto com o protocolo PPTP (protocolo de tunelamento ponto a ponto) para criar VPNs. Os pacotes designados para serem enviados através do túnel (já encapsulados com um cabeçalho de um protocolo como, por exemplo, o IP) são encapsulados por um novo cabeçalho (cabeçalho GRE) e colocados no túnel com o endereço de destino do final do túnel. Ao chegar a este final, os pacotes são desencapsulados (retira-se o cabeçalho GRE) e continuarão seu caminho para o destino determinado pelo cabeçalho original.
HDSL	Tecnologia de modulação que permite a comunicação simétrica à velocidade de 2048 Kbps, utilizada nos entroncamentos digitais E1.
Host	É qualquer máquina ou computador conectado a uma rede. Os hosts variam de computadores pessoais a supercomputadores, dentre outros equipamentos, como roteadores.
HTML	Linguagem de Formatação de Hipertexto. Linguagem usada principalmente em páginas da internet, em que certos comandos são colocados no meio do texto e não aparecem na tela, sendo, entretanto, executados pelo programa de navegação ou processador de textos.
ISSO	Protocolo de Transferência de Hipertexto. É um protocolo da camada de Aplicação do modelo OSI utilizado para transferência de dados na WWW – World_Wide_Web. Ele transfere dados de hiper _xcha (imagens, sons e textos). Geralmente esse protocolo utiliza a porta 80 e ele é usado para a comunicação com sites
IAX2	IAX2 – Inter Asterisk _xchange V2. É o padrão de comunicação VoIP usado pelo Asterisk.
ICMP	Protocolo de mensagem de controle da Internet. É um protocolo integrante do Protocolo IP, definido pelo RFC 792, e utilizado para fornecer relatórios de erros à fonte original. Qualquer computador que utilize IP precisa aceitar as mensagens ICMP, e alterar o comportamento em resposta ao erro relatado. Os gateways devem estar programados para enviar mensagens ICMP quando receberem datagrama que provoquem algum erro.

IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos. Um de seus papéis mais importantes é o estabelecimento de padrões para formatos de Computadores e Dispositivo.
IETF	IETF – Internet Engineering Task Force, Órgão responsável pelo desenvolvimento de padronização para a Internet.
IGMP	Protocolo de Gerenciamento de Grupos na Internet. Usado por Hosts e Roteadores para a propagação da informação de quais hosts pertencem a um determinando grupo multicast num determinado momento.
IP	Protocolo Internet. Padrão de endereçamento dos blocos de dados enviados através da rede mundial de computadores e redes similares. Identificação numérica de um endereço na Internet. Cada domínio tem um endereço IP.
IP Options	Estes tipos de pacotes podem ser utilizados para comprometer sistemas com vulnerabilidades no protocolo IP.
IP Spoofing	Esta técnica consiste na alteração do IP de origem de pacotes fazendo que uma máquina atacante se passe por outra máquina.
IPSEC	O IPSEC ou IP seguro é um conjunto de protocolos desenvolvidos pelo grupo de segurança do IETF para garantir autenticidade, confidenciabilidade e integridade dos dados. Os protocolos IPSEC são da camada 3, ou seja, fazem IP sobre IP.
ITU	União Internacional das Telecomunicações. Órgão europeu responsável pelo desenvolvimento de padronização para telecomunicações.
L2TP	Protocolo de Túnel de Camada 2. É um protocolo que foi implementado pela IETF para resolver alguns problemas de segurança do PPTP.
LAN	Rede Local. Tipo de sistema usado para interligar computadores próximos entre si.
MAC	Controle de Acesso ao Meio. É o endereço físico da interface de rede. É um endereço de 48 bits, representado em hexadecimal. O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet. Este endereço é o utilizado na camada 2 do Modelo OSI.
NAPT	Tradução de Endereços e Portas de Rede. É utilizado para mapear endereços e/ou portas de uma rede interna para um IP público real.
NATT	NAT Transversal. É a solução para a maioria dos problemas em redes TCP/IP para estabelecimento de conexões entre máquinas que estão ligadas em redes privadas. NATT é usualmente utilizado para estabelecimento de túneis IPSEC e pacotes de áudio para VoIP. Existem várias técnicas de usar NAT Transversal como STUN e clientes UpnP.
NTP	É um protocolo desenvolvido para permitir a sincronização dos relógios dos sistemas de uma rede.
OSI	O modelo OSI define as regras e procedimentos para estabelecer compatibilidade de comunicação entre os diversos equipamentos, sistemas, software e protocolos envolvidos neste processo de comunicação.
PAP	Protocolo de Autenticação por Senha. É a forma de autenticação que envia o usuário e a senha em aberto na rede, sem nenhuma criptografia. É a maneira menos segura de autenticação.

Peer to Peer	É uma conexão que estabelece uma espécie de rede de computadores virtual, onde cada estação possui capacidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, no qual alguns computadores são dedicados a servirem dados a outros.
PCM	Modulação por Código de Pulso. É o padrão de codificação digital de voz, necessitando de 64 Kbps por canal.
Ping of Death	Pacotes icmp com tamanho muito grande. O Ping of Death pode travar ou reiniciar um grande número de computadores através do envio de uma mensagem de "ping" maior que o tamanho predefinido.
Port Scan	Técnicas que servem para encontrar portas abertas em máquinas são os passos iniciais para a maioria dos ataques.
PPP	Protocolo Ponto a Ponto. É um protocolo desenvolvido para permitir acesso autenticado e transmissão de pacotes de diversos protocolos. É utilizado nas conexões discadas à Internet. O PPP encapsula o protocolo TCP/IP, no acesso discado à Internet.
PPPoA	Point-to-Point Protocol over AAL5 ou over ATM. É uma adaptação do PPP para funcionar em redes ATM (ADSL)
PPPoE	Point-to-Point Protocol over Ethernet. É uma adaptação do PPP para funcionar em redes Ethernet.
PPTP	Protocolo de túnel ponto a ponto. É um mecanismo de encapsulamento, onde é possível fazer criptografia e autenticação de usuários, utilizado para transferir quadros PPP em VPN.
PSK	Chave de criptografia pré-compartilhada.
PSTN	Rede Pública de Telefonia Comutada
QoS	Qualidade de Serviço. Com o advento da Voz sobre o IP algumas preocupações foram tomadas para que a banda, a cadência e o atraso dos pacotes de voz sejam tratados de forma diferente.
Radius	É um protocolo para fazer autenticação, autorização e verificação de contas de usuários. O servidor Radius deve estar um uma máquina da rede interna e ocupa a porta padrão 1812.
Rdate	É um protocolo desenvolvido para permitir a sincronização dos relógios dos sistemas de uma rede.
Relay Agent	Quando o servidor DHCP encontra-se em uma sub-rede, ou seja, em outra rede local, devemos configurar um DHCP Relay Agent na rede onde não existe o servidor DHCP. O DHCP Relay Agent pega os pacotes enviados pelos clientes e encaminha para o servidor DHCP, ou seja, é um intermediário entre ambos.
RFC	Solicitação de Comentário. Documentos escritos para e pela comunidade da Internet, descrevendo protocolos da Internet, pesquisas, medições, idéias e observações.
RTP	Protocolo de Transporte em Tempo-real. O RTP promove o transporte de rede fim a fim necessário a aplicações de tempo real, tais como, áudio e vídeo.
SIP	Protocolo de Iniciação de Sessão Como o próprio nome indica, o protocolo SIP é usado para iniciar uma sessão de comunicação entre usuários.
Smurf Attack	Pings em broadcast com spoofing no IP de origem. Neste tipo de ataque o atacante envia pacotes ICMP echo-request em broadcast para uma subrede com IP de origem falsificado com o IP da

	vítima. Assim a vítima receberá tantos ICMP echo-replies quantas forem as máquinas da subrede que responderem ao ICMP echo-request.
SNMP	Protocolo de Gestão Simples de Rede. É um protocolo da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede. O SNMP possibilita aos administradores de rede gerir o desempenho da rede, encontrar e resolver problemas de rede, e planejar o crescimento desta.
SOAP	Protocolo para intercâmbio de mensagens entre programas de computador. SOAP é um dos protocolos usados na criação de Web Services.
SSL	Protocolo desenvolvido pela Netscape para promover o tráfego seguro de dados na Internet. O SSL usa um sistema de criptografia de duas chaves. Uma chave pública conhecida por todos e uma chave confidencial ou secreta conhecida somente pelo receptor da mensagem. Outro protocolo seguro para dados transmitidos sobre o WWW é https. O SSL cria uma conexão segura entre um cliente e um usuário, sobre qualquer quantidade de dados e o https é projetado para transmitir mensagens individuais.
STUN	STUN – Simple Traversal of UDP through NAT. STUN é um protocolo da camada de aplicação que possa determinar o IP público e a natureza de um dispositivo NAT.
SYN flood	Pacotes TCP com flag SYN setada são utilizados para iniciar uma conexão TCP. Como cada recebimento de pacotes SYN acompanha a alocação de estruturas de dados para posterior estabelecimento da conexão TCP, um flood destes pacotes acabaria consumindo muitos recursos do sistema. Para minimizar este problema uma solução é descartar pacotes SYN excessivos originados de uma mesma máquina.
SYSLOG	O Syslog é um protocolo de transmissão de eventos e notificações (Logs) pela Internet. O Syslog utiliza protocolo UDP e a porta 514 como padrão de saída.
TCP/IP	Protocolos utilizados no processo de comunicação entre os computadores na Internet.
Traceroute	Traceroute ou Determinação de Rota é um procedimento que permite verificar a rota que é utilizada no acesso entre computadores.
Trojan Horses	Programa que age como a lenda do cavalo de Tróia, entrando no computador, e liberando uma porta para um possível invasor.
UDP	É um protocolo sem conexão, que corresponde à camada de transporte no modelo ISSO/OSI. O UDP transforma as mensagens geradas por uma aplicação em pacotes a serem enviados via IP, mas não verifica a recepção das mensagens e nem a ordem correta dos datagramas, sendo usado para vários fins, como o SNMP, em que a confiabilidade depende da aplicação geradora da mensagem.
UpnP	Universal Plug and Play é um setor do protocolo de rede de computadores. As metas da UpnP são para conectar diretamente e para simplificar a implementação de redes em casa e em corporação. A tecnologia Plug-and-Play é para ligação direta entre o computador e o dispositivo.
UPNPC	Cliente UpnP.
URL	É o endereço de um recurso (um arquivo, uma impressora, etc.) disponível em uma rede, seja a Internet ou uma rede corporativa, uma intranet.
VAD	A detecção de atividade de voz quando em silêncio (sem conversação) não envia pacote, economizando a banda.
VLAN	Rede Local Virtual é um conceito, não um recurso, que trata de subdividir, via software (sem o uso de routers, switches, etc), o ambiente de rede em vários segmentos independentes.

VoIP	Voz Sobre IP. Tecnologia que torna possível estabelecer conversações telefônicas em uma Rede IP (incluindo a Internet), tornando a transmissão de voz mais um dos serviços suportados pela rede de dados.
VPN	Redes Virtuais Privadas. Tecnologia que consiste em criar um "túnel" de conexão entre dois ou mais routers na Internet. Somente após a criação deste túnel é que os dados são enviados/recebidos, impedindo que Hackers, "fora do túnel", consigam acessar as informações que estão sendo transmitidas.
WAN	Rede de Longa Distância. Definida por uma rede de computadores ligada por meios de comunicação de longa distância, como por exemplo, sinais de rádio, L.P.s (linhas privadas) e até mesmo satélites.
WAP	Protocolo para Aplicações Sem Fio. Protocolo de dados desenvolvido para uso em dispositivos sem fio, como celulares.
Web	"Teia" em Inglês, é um termo usado para se referir às redes de computadores. O termo surgiu devido ao formato de uma teia de aranha lembrar a disposição física de uma rede, com cabos interligando os pontos. O termo WWW significa "Word Wide Web", ou larga teia mundial e é naturalmente usado com relação à Internet.
WEP	É um padrão de encriptação de dados para redes wireless, que traz como promessa um nível de segurança equivalente à das redes cabeadas. Geralmente o WEP é ativado para não permitir que um outro dispositivo não pertencente à rede tenha acesso à mesma. Usa-se Criptografia para a proteção dos dados, esta pode ter 64 ou 128bits.
Wi-Fi	Nome comercial para os padrões 802.11b, 802.11a e 802.11g. A topologia deste tipo de rede é semelhante a das redes de par trançado, com um hub central (substituído pelo Ponto de Acesso). A diferença no caso é que simplesmente não existem os fios.
Wireless	Refere-se a aparelhos capazes de transmitir dados via rádio, infravermelho ou outra tecnologia que não envolva o uso de fios.
WLAN	Wirelles LAN, conhecida também pelo nome de Wi-Fi