intelbras

Manual do usuário
Manual del usuario

Placas base e codec ICIP 30 Impacta 68i
Tarjetas madre y codec ICIP 30 Impacta 68i

Índice

intelbras

Placas base e codec ICIP 30 Intelbras Impacta 68i

Parabéns, você acaba de adquirir um produto com a qualidade e segurança Intelbras.

A Intelbras, pensando nestas necessidades do mercado VoIP, oferece a solução ICIP 30 68i para as centrais telefônicas da linha Impacta modelos Impacta 68i aprimorando sua performance e garantindo uma alta disponibilidade de ligações.

A ICIP 30 68i é uma placa opcional baseada em uma plataforma IP com alta capacidade de customização e compatível com o protocolo de comunicação SIP. Foi projetada para ser uma solução em redes VoIP, permitindo que as comunicações telefônicas sejam realizadas através da rede de dados disponível, proporcionando, assim, uma redução significativa dos gastos com telefonia e um aumento na flexibilidade da planta para pequenas e médias empresas.

1. Especificações técnicas

Padrões	IEEE802.3 Ethernet 10BASE-T IEEE802.3 Nway Auto Negotiation IEEE802.3u Fast Ethernet 100BASE-TX IEEE802.1Q tagged VLAN IEEE802.1p Layer2/CoS Traffic Priority IEEE802.3ac VLAN tagging
Interfaces de rede	1 porta LAN UTP fast Ethernet RJ45 10/100 Mbps 1 porta WAN UTP fast Ethernet RJ45 10/100 Mbps
Protocolo de sinalização	SIP 2.0/SIP Intelbras
Interface USB	1 porta USB host tipo A Compatíveis com USB 1.1/2.0
Canais VoIP	Até 30 canais (10 canais por placa codec ICIP 30 68i)
Codificação de voz	G.711 PCM (A/u-law) até 64 kbps G.729 AB CS- ACELP até 8 kbps GSM Full Rate 6.10 até 13,2 kbps G.723, G.726-16, G.726-24, G.726-32, G.726-40 (ADPCM)
LEDs	Indicativos do status do sistema e codecs

2. Características

- » Suporte em processamento de sinais.
- » Controle adaptável e fixo de jitter buffer e tecnologia para ocultação de perda de pacotes (PLC).
- » Codificação digital de voz - GSM Full Rate 6.10, G.711 PCM (A-law e u-law) e G729AB, G.726 (ADPCM), Detecção de Atividade de Voz (VAD), Geração de Ruído de Conforto (CNG), Cancelamento de eco (LEC - G.168-2002, até 128ms) e Controle Automático de Ganho (AGC).
- » FAX (Bypass e T.38).
- » Sinalização DTMF (In-Band, RFC 2833 e SIP INFO).
- » Suporte em rede.
- » 1 ramal IP e 1 juntor IP para cada canal VoIP, sendo que cada placa codec possui 10 canais (não necessita aquisição de chave de hardware).
- » Até 30 canais VoIP (utilizando até 3 módulos do tipo placa codec ICIP 30).
- » Juntores IP: Ponto a Ponto e Proxy (operadora VoIP).
- » Suporta até 5 VLANs.
- » 2 portas UTP Fast Ethernet 10/100 Mbps para LAN e WAN.
- » Detecção automática da placa codec ICIP 30 Intelbras.
- » Monitoração do sistema via SNMP (V1/V2c/V3).
- » Atualização de firmwares do PABX (central, DISA, música, interfaces e telefone IP TIP 100 e ATA GKM 2210T da Intelbras).
- » Suporte a configuração via navegador web (HTTPS). Programação via web é compatível com o navegador Mozilla Firefox® (consulte a versão compatível na *Tabela de Compatibilidade Centrais Impacta*, disponível na seção *Downloads* do nosso site).
- » Proteção do sistema via Firewall.
- » Controle de tráfego.
- » Permite a conexão a um Bilhetador, Monitor E1, CSTA e outras aplicações via ICTI.
- » Geração de Logs locais e remoto (SysLog).
- » Registro de um endereço DNS dinâmico (DDNS).
- » Sincronização de relógios do sistema via internet (NTP).
- » Interface de acesso a rede local (LAN) e rede externa (WAN).
- » Autoprovisionamento para ramais IP com telefone Intelbras TIP 100 e ATA GKM 2210T (a partir da versão 1.3 release 32).
- » Inicialização automática de telefones IP.
- » Atualização automática do número de ramal do telefone IP/ATA Intelbras TIP 100 e ATA GKM 2210T.

» Detecção de operadora VoIP fora de serviço.
» Indicação de prioridade de mensagens em relação a outras (QoS, protocolo IP Precedence).
» Detecção de Brute Force Attack.

3. Cuidados e segurança

As informações a seguir são dirigidas a técnicos autorizados ou especializados.

Atenção: somente técnicos treinados pela Intelbras estão autorizados a instalar e configurar o PABX, bem como abrir a caixa, conectar e manusear suas interfaces.

Ler cuidadosamente todas as informações sobre o equipamento e seguir todas as informações de segurança.

» Consultar sempre um superior ou responsável imediato antes de iniciar o trabalho, informando os procedimentos necessários para realizar o serviço solicitado e as precauções de segurança necessárias.
» Desligar a alimentação do sistema durante os serviços de montagem ou retirada das interfaces.
» Conectar o condutor de aterramento no sistema envolvido antes de iniciar. Nunca operar o equipamento com o condutor de aterramento desconectado.

Para evitar danos eletrostáticos à placa ICIP, observe as seguintes precauções:

Atenção: a eletricidade estática pode danificar os componentes eletrônicos da Interface. Esse tipo de dano pode ser irreversível ou reduzir a expectativa de vida útil do dispositivo.

» Utilize uma pulseira antiestática, ou similar, para manusear as placas.
» O transporte e o armazenamento devem ser somente em embalagens à prova de eletricidade estática.
» Coloque a placa sobre uma superfície aterrada ao retirá-la da embalagem.
» Evite tocar nos pinos dos circuitos integrados ou condutores elétricos.
» Esteja sempre adequadamente aterrado ao tocar na placa ou em algum componente.

4. Proteção e segurança de dados

4.1. Tratamento de dados pessoais

Este sistema utiliza e processa dados pessoais como senhas, registro detalhado de chamadas, endereços de rede e registro dos dados de clientes, por exemplo.

5. Cuidados e segurança

5.1. Proteção e segurança de dados

Observar as leis locais relativas à proteção e uso de tais dados e as regulamentações que prevalecem no país.

O objetivo da legislação de proteção de dados é evitar infrações nos direitos individuais de privacidade baseadas no mau uso dos dados pessoais.

5.2. Diretrizes que controlam o tratamento de dados

» Assegurar que apenas pessoas autorizadas tenham acesso aos dados de clientes.
» Usar as facilidades de atribuição de senhas, sem permitir qualquer exceção. Jamais informar senhas para pessoas não autorizadas.
» Assegurar que nenhuma pessoa não autorizada tenha como processar (armazenar, alterar, transmitir, desabilitar ou apagar) ou usar dados de clientes.
» Evitar que pessoas não autorizadas tenham acesso aos meios de dados, por exemplo, discos de backup ou impressões de protocolos.
» Assegurar que os meios de dados que não são mais necessários sejam completamente destruídos e que documentos não sejam armazenados ou deixados em locais geralmente acessíveis.
» O trabalho em conjunto com o cliente gera confiança.

5.3. Uso indevido do usuário e invasão de hackers

» As senhas de acesso às informações do produto permitem o alcance e alteração de qualquer facilidade, como o acesso externo ao sistema da empresa para obtenção de dados e realizações de chamadas, portanto, é de suma importância que as senhas sejam disponibilizadas apenas àqueles que tenham autorização para uso, sob o risco de uso indevido.

» O produto possui configurações de segurança que podem ser habilitadas, e que serão abordadas neste manual, todavia, é imprescindível que o usuário garanta a segurança da rede na qual o produto está instalado, haja vista que o fabricante não se responsabiliza pela invasão do produto via ataques de hackers e crackers.

6. Produto

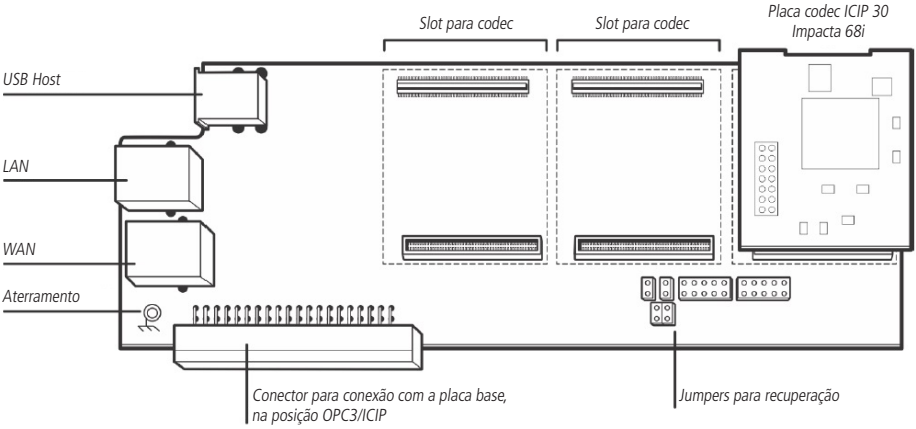
A solução de produto que permite ter acesso à tecnologia de transmissão de sinais de voz pela Internet ou por uma rede privada é composta pelo conjunto:

» **Placa base ICIP 30 68i**: responsável pelo processamento das informações de rede, protocolos de acesso e conexões a rede do cliente e internet;

» **Placa codec ICIP 30 68i**: responsável pelos canais VoIP disponíveis na placa base ICIP 30 68i e pelo processamento dos sinais de "voz" e a sua conversão em pacotes de dados dentro da rede. Cada placa codec habilita 10 canais VoIP.

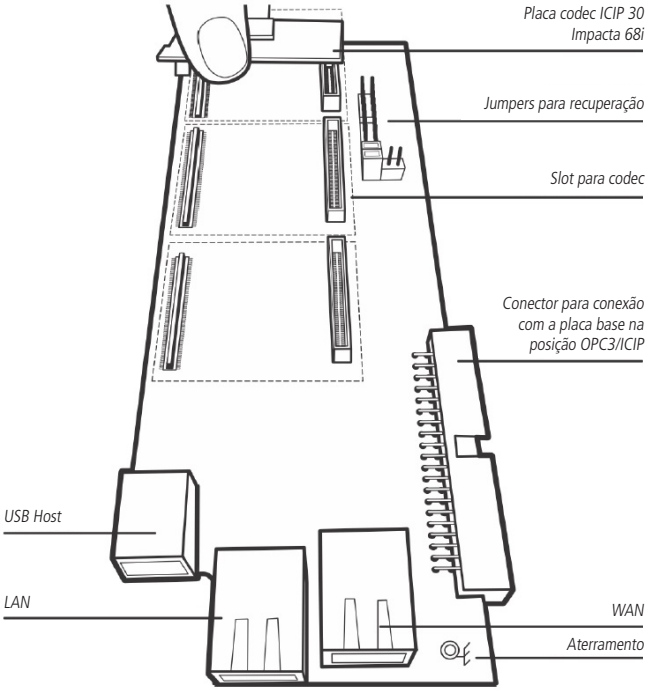
» **Chave de Hardware com licenças de ramal e troncos IP.**

6.1. Placa base ICIP 30 Impacta 68i



ICIP : Interface de Comunicação IP

6.2. Conexão placa codec ICIP 30 Impacta 68i (1 a 3)



6.3. Proteção e segurança de dados

Interface de rede LAN	Porta UTP fast Ethernet RJ45 10/100 para acesso a rede local.	
Portas USB	2 Portas USB host para conexão de periféricos	
Interface de rede WAN	Porta UTP fast Ethernet RJ45 10/100 para conexão externa de acesso a internet.	
LED indicativo do status da placa base ICIP 30 68i	**Cadência**	**Estado**
	Permanentemente aceso	Placa não inicializada
	Piscando muito rapidamente (100 ms ON/100 ms OFF)	Placa inicializando (Linux inativo)
	Piscando rapidamente (500 ms ON/500 ms OFF)	Placa inicializando (Linux ativo, e inicializando serviços)
	Piscando moderadamente (1 s ON/1 s OFF)	Placa inicializada e operando (Programador web Ativo)
	Piscando intermitente (1400 ms ON/300 ms OFF)	Falha de Inicialização da placa
Conectores para placa codec ICIP 30 68i	Existem 3 posições disponíveis para a conexão, podendo assim atingir até 30 canais VoIP	

7. Produto

7.1. Tecnologia

Visão geral

Com a placa ICIP, a central Impacta 68i continua dispondo de todos os recursos e funcionalidades já existentes, mas incorporando agora as novas funcionalidades já citadas.

Nela, as informações referentes à voz serão transmitidas pela Internet ou por uma rede privada através da tecnologia conhecida como VoIP (Voz sobre IP) usando o protocolo SIP. Então, agora, além de poder utilizar normalmente toda a estrutura da rede de telefonia instalada, sua empresa também pode utilizar a rede de dados para realizar e receber chamadas através dos telefones SIP.

Alguns dos resultados imediatos são:

- » Diminuição dos custos de ligações locais, DDD e DDI, por utilizar a internet;
- » Unificação do plano de numeração para os ramais VoIP, analógicos e digitais;
- » Acesso via web ao sistema de configuração e administração;
- » Redução dos custos de operação da rede.

7.2. VoIP

Voice Over IP (VoIP) é a tecnologia que permite que informações de voz sejam transmitidas através do protocolo Internet Protocol (IP). Este conceito consiste em digitalizar a voz, empacotá-la e transmiti-la na mesma rede que é usada para transportar os pacotes de dados IP.

O empacotamento consiste em inserir as amostras ou quadros processados pelo codificador (codec) em pacotes. Esses pacotes trafegam na rede IP através dos roteadores, que tomam a decisão recebendo os pacotes e escolhendo rotas mais convenientes até os destinatários.

7.3. Protocolo SIP

É um protocolo utilizado para estabelecer chamadas e conferências através de redes via IP. Foi projetado tendo como foco a simplicidade, e, como um mecanismo de estabelecimento de sessão, ele apenas inicia, termina e modifica a sessão, o que o torna um protocolo que se adapta confortavelmente em diferentes arquiteturas.

O SIP possui um papel cada vez mais importante na telefonia IP, principalmente devido a sua simplicidade, flexibilidade, segurança, facilidade de mobilidade e, principalmente, devido à grande aceitação de fabricantes de IP PBX, Gateways e telefones IP.

8. Instalação

Para montagem da placa base e codec ICIP 30 68i, siga o procedimento:

1. Em uma superfície aterrada conecte a pulseira antiestática;
2. Retire a placa base ICIP 30 68i e a(s) placa(s) codec ICIP 30 68i das embalagens e coloque-as sobre a superfície aterrada;
3. Confira o estado das placas e seus conectores;
4. Apoie de maneira estável a placa base ICIP 30 68i sobre a superfície e insira a(s) placa(s) codec ICIP 30 nas posições disponíveis, seguindo o esquema a seguir;
5. Insira o conjunto montado em uma embalagem antiestática até a central estar pronta para recebê-lo;
6. Informe a um responsável pela central Impacta que será necessário desligá-la;
7. Localize o administrador de rede ou técnico de informática para auxiliá-lo a reconhecer em que cenário a placa ICIP será configurada, anote os endereços IP, servidores de banda larga, servidor SIP Proxy, usuários e senhas, assim como a localização física dos cabos de rede LAN e WAN (deve-se, preferencialmente, utilizar a porta WAN para conectar-se na rede interna do cliente e a porta LAN para conectar-se na rede interna da operadora provedora do SIP Trunk);
8. Desligue a alimentação AC da central Impacta 68i e retire a tampa;
9. A placa base ICIP 30 68i deve ser conectada somente na posição OPC3/ICIP (CN2);
10. Conecte os cabos da rede LAN e WAN nos respectivos conectores;
11. Organize e identifique os cabos de rede junto com os demais cabos no DG da central;

12. Antes de colocar em serviço o sistema, deve-se efetuar a conferência visual de todas as conexões de cabos, módulos, placas e alimentação AC, corrigindo qualquer eventual falha. A conferência visual deve ser efetuada com o sistema desligado;
13. Recoloque a tampa e ligue a alimentação AC da central Impacta;
14. Após a inicialização do sistema, confira, através do Programador web/Menu Interfaces/Disposição placas, se nenhuma placa está programada para utilizar aquele slot;
15. Programe os dados necessários através do Programador web.

8.1. Recomendações técnicas

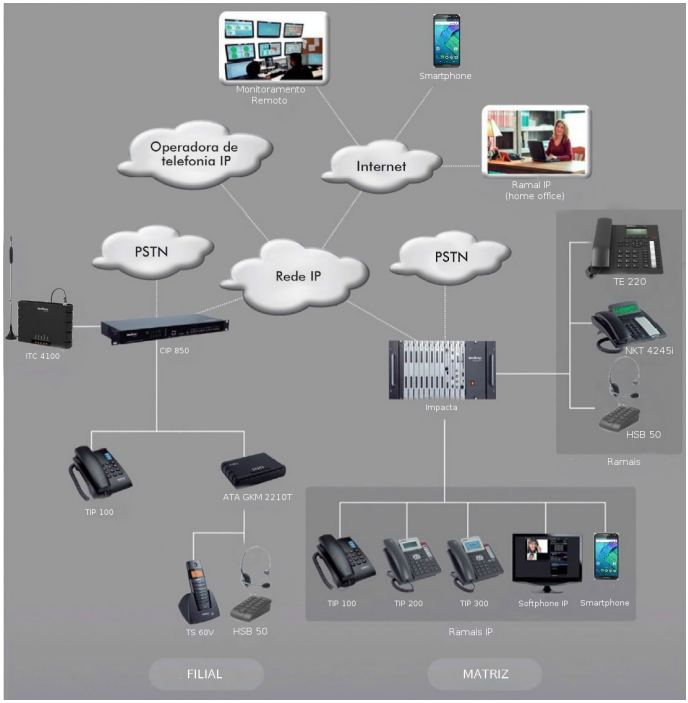
Esse sistema utiliza a tecnologia VoIP (voz sobre IP) e a qualidade do funcionamento depende das condições de tráfego e priorização da rede à qual o produto está conectado. Para que a qualidade de áudio da central seja excelente, a rede onde todo o tráfego de pacotes é transmitido/recebido deve ter banda suficiente. Em caso de anormalidades nas ligações estabelecidas, como problemas de áudio, verifique antes a situação da rede com o provedor VoIP.

As informações que deverão ser analisadas junto ao provedor de internet são:

- Garantia mínima (%) da Largura Banda em contrato: a velocidade contratada representa a velocidade máxima configurada dentro da rede do seu provedor de internet. A maioria dos provedores de internet garantem velocidade mínima de 10% da banda contratada (entre usuário e provedor) dentro de sua rede.
- Latência de rede: é o tempo que um pacote leva para trafegar pela rede, desde a origem até o destino.
- Velocidade de Download: é a velocidade com que os pacotes são recebidos da internet.
- Velocidade de Upload: é a velocidade com que os pacotes são enviados para a internet. Os provedores de internet oferecem, na maioria das vezes, velocidade de Upload menor ou igual a velocidade de Download.
- Verificar o número de computadores na rede.
- Consulte o provedor VoIP sobre quais codecs (codificador/decodificador de voz) utilizar e sobre as configurações necessárias no sistema para uma melhor qualidade de voz.
- O envio ou recebimento de Fax depende da qualidade do sinal da sua internet Banda Larga, da latência, da taxa de perda de pacote e da presença dos protocolos necessários no destino. Assim sendo, só se pode garantir o funcionamento correto do Fax se essas condições forem favoráveis.
- Recomenda-se configurar o sistema de maneira que não haja transcodificação nos ramais SIP. (ver guia *Codec*)
- Para que os ramais IP funcionem adequadamente o modo de envio DTMF deve ser SIP INFO (ver guia *VoIP Geral* no Programador web*)*.
- O endereço do servidor DNS configurado deve ser, de preferência, de um equipamento pertencente a mesma rede. Acessar um DNS externo à rede pode causar problemas de registro de juntores e ramais, deixando o sistema lento. É recomendado utilizar servidores DNS com tempo de resposta rápido.

8.2. Cenário

Existem muitos cenários de aplicação desta nova tecnologia VoIP/SIP em conjunto com as centrais Impacta 68i. Veja a seguir um cenário clássico, no qual podemos visualizar diversos ambientes se conectando através da placa ICIP, com placa codec e Licenças.



Cenário

9. Gerenciamento via navegador web

Com a instalação da placa ICIP nas centrais Impacta, o gerenciamento de todo o sistema pode ser acessado via navegador web Mozilla Firefox ® (consulte a versão compatível na Tabela de Compatibilidade Centrais Impacta, disponível na seção Downloads do nosso site).

Atenção: para acessar a interface do Programador web, configure o computador de gerenciamento com um endereço IP e máscara de sub-rede que estejam na mesma rede LAN da central.

Padrão de fábrica LAN:

- Endereço IP: 10.0.0.2
- Máscara de sub-rede: 255.255.255.0
- Gateway padrão: 10.0.0.1
- Envio de Log: 10.0.0.3

9.1. Ouvir os endereços IP

A placa ICIP pode ser configurada para obter o endereço IP automaticamente, via DHCP. Nesse caso o PABX disponibiliza uma forma de o usuário escutar o endereço IP obtido. O usuário, usando um telefone, deve digitar os seguintes comandos:

- *60993*, para ouvir o endereço IP WAN
- *60992*, para ouvir a máscara de rede WAN
- *60991*, para ouvir o endereço IP LAN
- *60990*, para ouvir a máscara de rede LAN
- *60989*, para ouvir o endereço IP VLAN1
- *60988*, para ouvir a máscara de rede VLAN1
- *60987*, para ouvir o endereço IP VLAN2
- *60986*, para ouvir a máscara de rede VLAN2
- *60985*, para ouvir o endereço IP VLAN3
- *60984*, para ouvir a máscara de rede VLAN3
- *60983*, para ouvir o endereço IP VLAN4
- *60982*, para ouvir a máscara de rede VLAN4
- *60981*, para ouvir o endereço IP VLAN5
- *60980*, para ouvir a máscara de rede VLAN5

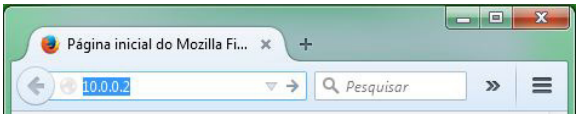
Para configuração manual do número IP e máscara de rede, para LAN e WAN, via telefone comum:

- LAN - *14 + IP(10*1*30*17) + # + Mask (255*255*255*0) + # + GW(10*1*30*1) + #
- WAN - *15 + IP(10*1*30*17) + # + Mask (255*255*255*0) + # + GW(10*1*30*1) + #

Obs.: *a configuração do GW (gateway) não é obrigatória. Pode-se configurar apenas o IP e a Máscara. Para isso, basta parar no # após digitar a máscara e aguardar a mensagem de programação aceita.*

Atenção: a central será reiniciada logo após a aceitação do comando.

Abra seu navegador web e digite o endereço da placa ICIP no campo de endereço, por exemplo, IP 10.0.0.2.



Endereço IP no navegador

Será aberta uma janela pop-up de login (caso não abra, limpe o cache do navegador ou verifique se há algum tipo de bloqueador de pop-ups ou outro produto do gênero ativo em seu computador). Digite o nome de Usuário e Senha para a autenticação. O padrão de fábrica é:

- **Usuário**: admin
- **Senha**: admin

9.2. Programador web

Após o procedimento de autenticação a tela inicial estará acessível ao administrador. Selecione o item desejado no menu do lado esquerdo e para acessar cada uma das opções de gerenciamento.

Atenção: o processo de criação e configuração de ramais e juntores IP é semelhante ao dos ramais e troncos analógicos, no mesmo menu de *Configuração>Portas*.

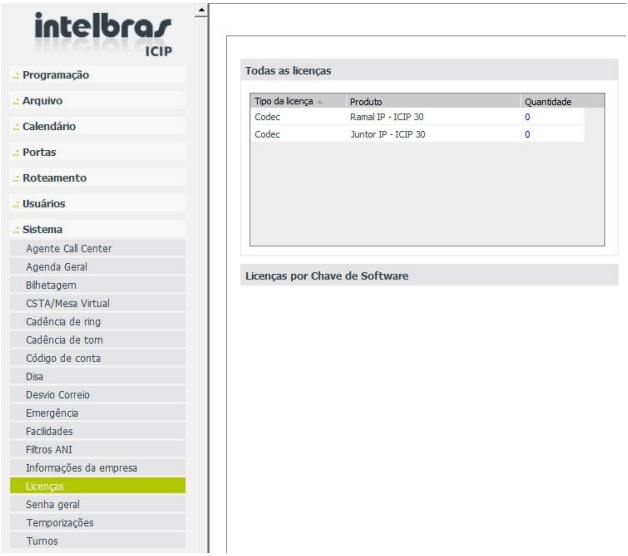
A mesma analogia ocorre para a configuração de Roteamento de ramais e troncos IP, no menu de *Configuração>Roteamento*.

Os menus do Programador web continuam os mesmos já conhecidos no Programador PC, entretanto foram criados novos menus para a configuração da placa ICIP, que seguem:

9.3. Sistema

Licenças

Acessando este submenu são exibidos o status e o número de licenças válidas para ramais IP e juntores IP.



Visualização/confirmação das licenças

9.4. Histórico

Acessando este submenu serão exibidos os registros de logs de algumas operações realizadas pelos usuários.

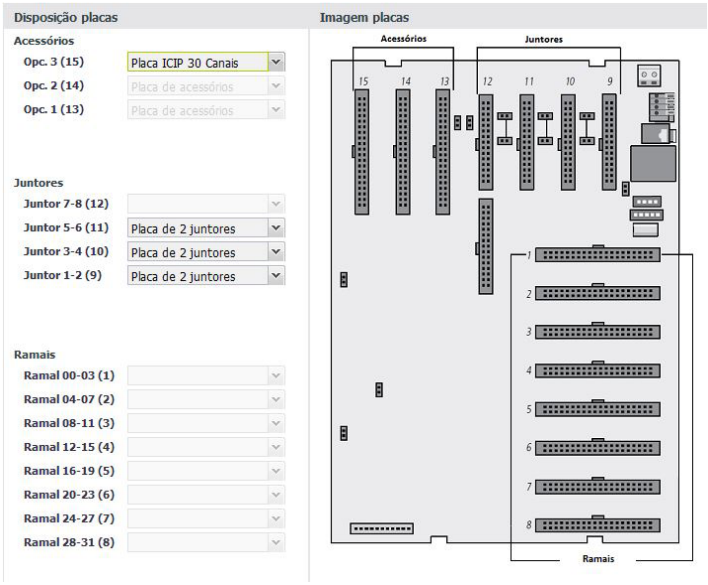
- » **Data:** apresenta a data e a hora em que ocorreu a operação.
- » **Usuário:** nome do usuário que realizou a operação.
- » **Navegador e versão:** nome do navegador e a versão usada para realizar a operação.
- » **Descrição:** descreve a operação realizada. As operações que geram log são: Enviar e Receber programações, Enviar firmware, Enviar reset e Enviar banco de dados.

9.5. Interfaces

Disposição placas

Acessando este submenu será exibido um esquema com a quantidade e os dispositivos conectados nos slots do backplane. Verifique se o tipo da placa ICIP instalada esta sendo exibida no slot correto, caso não, será necessário configurá-la.

1. Selecione no menu de placas a opção "Vazio" ou pressione o botão Limpar para deixar todos os slots como "Vazio".
2. Confirme esta operação;
3. Selecione a placa base ICIP 30 para aquele slot (neste exemplo 30 canais).



Localização/atualização para placa base ICIP 30 68i

9.6. Rede

Permite configurar os dados de endereçamento, parâmetros de segurança e serviços necessários para que a placa ICIP possa se comunicar e ser reconhecida pela rede local , assim como as informações para a conexão IP com a internet.

Atenção: algumas destas informações podem ser obtidas junto ao administrador de rede ou técnico de informática.

Menu Rede e suas configurações

Geral

Este submenu apresenta as informações gerais sobre a rede e os parâmetros disponíveis para a configuração, distribuídos nas seguintes guias:

Menu Rede/SubMenu Geral

Geral

Apresenta as informações físicas da placa para o administrador.

Menu Rede/Submenu Geral/Geral

- Tipo de placa: informa qual o tipo de placa que esta instalada no sistema.
- Slot: informa em qual slot do backplane a placa se localiza.

Habilitar VLAN

Esta seção permite habilitar a configuração da VLAN. A habilitação deste item irá ter um reflexo direto no Menu Rede, onde será habilitado o submenu equivalente para configuração. Para saber mais detalhes deste serviço, consulte a seção VLAN neste manual.

Menu Rede/Submenu Geral/Habilitar VLAN

- **Habilitar:** habilita o item VLAN para configuração do serviço e permite selecionar quantas VLANs estarão disponíveis na rede da ICIP.
- **Número de VLANs**: define o número de VLANs que estará disponível para a rede do sistema. São possíveis até 5 VLANs.

Interface de saída para os tráfegos

Define-se qual interface de rede (LAN, WAN ou VLAN) será usada para tráfego de saída do sistema como rota default.

Menu Rede/Submenu Geral/Interface de saída para os tráfegos

No menu suspenso, selecione a interface de rede que será utilizada para os tráfegos de saída.

Servidor externo de resolução NAT

O STUN (*Simple Traversal of User Datagram Protocol (UDP)*, por meio da *Network Address Translators* (*NATs*)), é um servidor que permite que clientes NAT (ex.: computadores protegidos por firewall) realizem chamadas telefônicas a um provedor VoIP que se encontra fora da rede local. O servidor STUN permite que os clientes descubram seu endereço público, o tipo de NAT utilizado, e o lado da porta da internet associada à NAT com uma porta local específica. Essas informações são usadas para permitir a comunicação UDP entre o cliente e o provedor VoIP, e então, estabelecer a chamada. Espera conexões somente na Interface WAN, na porta 3478/UDP e 3479/UDP (portas Default). O servidor STUN é habilitado no menu *Rede>Geral>Habilitar Serviços>Servidor STUN.*

Menu Rede/Submenu Geral/Servidor externo de resolução NAT

- **Servidor STUN:** habilita o uso desta facilidade.
- **IP ou FQDN do servidor (STUN, TURN, ICE):** define o endereço IP de servidores que auxiliam a central a manter a comunicação com dispositivos que estejam fora da rede local.
- **Porta do servidor:** define a porta do servidor STUN.

Configuração de NAT por gateway

Obs.: *as configurações de NAT estão disponíveis somente para interface de rede WAN, não sendo permitido configurar NAT em outras interfaces que não sejam a WAN. Dê preferência para configurar a interface LAN para acessar operadora proxy e evitar problemas de conexão, em cenário que use NAT.*

É possível configurar as opções de NAT para todos os possíveis gateways da ICIP, como, por exemplo, LAN e WAN primária e secundária, 3G. É possível fazer configurações diferentes de NAT para cada gateway, não só os das rotas padrões, mas também os das rotas estáticas.

Menu Rede/Submenu Geral/Configuração de NAT por gateway

Para cada gateway é possível definir:

Regra:

- **Sem:** não faz o tratamento do NAT.
- **STUN/TURN/ICE:** utiliza o servidor externo de STUN/TURN/ICE, caso esteja configurado.
- **NAT:** habilita a configuração do campo IP Público do NAT.
- **IP Público do NAT:** define o endereço, de IP ou FQDN, que o roteador está utilizando na Internet.

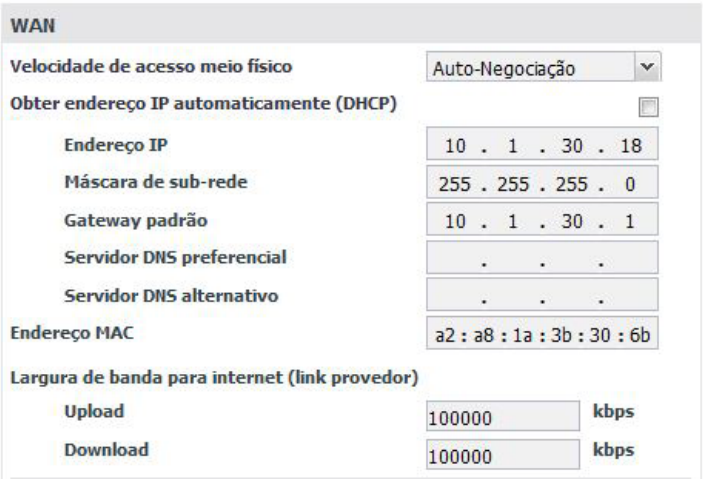
WAN

Este submenu apresenta as informações da conexão da interface WAN e os parâmetros necessários para a sua configuração dentro da rede, distribuídos nas seguintes guias:

Menu Rede/Submenu WAN

WAN

Permite a configuração dos parâmetros de conexão física e endereçamento, referentes à interface WAN, portanto é importante consultar o administrador de rede e o provedor de internet para obter os dados necessários.



Rede/Submenu WAN

- **Velocidade de acesso meio físico**: define a velocidade do modo de transmissão (Auto, Full Duplex ou Half Duplex) dos pacotes de dados na rede, possuindo uma relação direta com os dispositivos existentes na rede (cabos, hubs etc). Assim recomenda-se a opção de *Autonegociação*, caso não exista nenhuma indicação do administrador de rede.
- **Obter endereço IP automaticamente (DHCP)**: disponibiliza duas opções de acesso a rede WAN:
  - Selecionado, o acesso à rede WAN será dinâmico, isto é, informações como, endereço IP, máscara de rede, IP do gateway e IP do servidor DNS, serão fornecidas pelo primeiro dispositivo de rede que implemente um servidor DHCP. Esse equipamento pode ser um modem, roteador, switch ou um computador/servidor conectado na rede.
  - Sem seleção, o acesso à rede WAN será estático, isto é, será necessário preencher os campos Endereço IP, Máscara de Rede, IP do Gateway, IP dos servidores DNS e velocidades de upload e download, de acordo com as especificações do administrador de rede.
- **Endereço IP**: define o endereço IP da porta WAN na rede onde será conectada a placa.
- **Máscara de sub-rede**: define o valor da máscara de sub-rede onde será conectada a placa.
- **Gateway padrão**: informe o endereço IP do roteador de saída da rede (equipamento que interliga mais de uma rede física).
- **Servidor DNS preferencial e alternativo**: informe os endereços IPs dos servidores de DNS (Domain Name System - Sistema de Nomes de Domínios) de sua escolha.

  ***Obs.*:** é bastante comum em redes de pequeno e médio portes que este endereço IP seja o mesmo do endereço de gateway (roteador de saída).

» **Endereço MAC**: informe o endereço de MAC para interface WAN, caso seja necessário. Isto é tipicamente útil pois alguns provedores de internet somente permitem a autenticação com o endereço MAC previamente especificado. Em outros casos deve-se utilizar o mesmo endereço MAC do computador que estava autenticado no provedor de Internet.

» **Upload e Download**: são definidas as taxas máximas para a conexão com o provedor em função do link contratado. É importante saber as taxas de upload e download com a interface WAN disponível, para poder manter o equilíbrio na conexão do link e evitar qualquer saturação e consequente perda de qualidade.

Habilitar tráfego

São habilitados os tráfegos de pacotes de sinalização SIP, RTP (relativos ao tráfego de voz) e tráfego administrativo na rede WAN.

Menu Rede/SubMenu WAN/Habilitar tráfego

» **SIP**: habilita o tráfego dos pacotes de sinalização SIP junto a rede WAN configurada.

» **RTP**: habilita o tráfego dos pacotes de sinalização RTP junto a rede WAN fornecendo um meio uniforme para transmitir dados sujeitos a "problemas" de tempo real (áudio, vídeos,…).

» **Administração**: habilita o tráfego de administração na rede WAN. Isto pode ser utilizado para evitar o acesso as configurações de administração por pessoas não autorizadas.

QoS

Permite especificar prioridades para pacote ou classe de tráfego. O QoS busca uma melhoria da qualidade da comunicação priorizando alguns tipos de dados em detrimento de outros, de acordo com uma classificação prévia dos mesmos, e se torna extremamente útil em condições de congestionamento de tráfego na interface de saída destes dados (por exemplo, a porta de conexão com o roteador para a Internet).

Atenção: a placa ICIP marca os pacotes de dados, cabendo aos ativos de rede (switchs e roteadores) dar prioridade ao tráfego de voz.

Menu Rede/SubMenu WAN/QoS

Habilitar QoS de camada 3

Nos campos indicados nesta tela existe a opção de selecionar dois modos de sinalização dos pacotes (DSCP ou TOS) e a sua prioridade. Estes parâmetros serão utilizados para QoS e são inseridos no cabeçalho IP de todos os pacotes SIP, RTP e de administração transmitidos.

A escolha entre um dos modos depende de uma análise da rede, da compatibilidade dos dispositivos com o modo selecionado e da forma como estão configurados os roteadores e switchs para priorizar o tráfego.

O modo DSCP (Differentiated Services Code Point) prioriza o pacote de acordo com a marcação no pacote recebido. Esses pacotes se distinguem em classe de tráfego de acordo com as informações de atraso, taxa de processamento e confiabilidade anexadas ao pacote. Para isto, utiliza 6 bits do cabeçalho, dando 64 diferentes possibilidades para códigos de prioridade.

No modo TOS (Type of Service), pacotes que entram na rede por meio da ICIP são encaminhados de acordo com a prioridade definida. Para isto, utiliza 3 bits do cabeçalho dando 8 diferentes possibilidades para códigos de prioridade, sendo 0 a prioridade mais baixa.

Quanto maior o valor, maior será a prioridade no tratamento e uso dos recursos da rede.

Atenção:

- » Os modos DSCP e TOS entrarão em operação, conforme o comportamento definido pela IETF.
- » Quando a taxa de tráfego entrante em um equipamento de rede é superior à taxa de tráfego sainte do mesmo (largura de banda), ocorre um congestionamento na rede. Durante estas condições, os quadros marcados com maior prioridade recebem tratamento preferencial e são entregues antes dos quadros com menor prioridade.
- » Lembre-se que é baseado nestes parâmetros que os equipamentos de rede priorizam o tráfego de voz frente ao tráfego de dados.

SIP

Ao lado do campo *SIP* é possível selecionar o modo de QoS:

- » TOS com valor de 0 a 7, que representa a prioridade do pacote.
- » DSCP com valor de 0 a 63, que representa a prioridade do pacote.

RTP

Ao lado do campo *RTP* é possível selecionar o modo de QoS:

- » TOS com Valor de 0 a 7, que representa a prioridade do pacote.
- » DSCP com Valor de 0 a 63, que representa a prioridade do pacote.

Administração

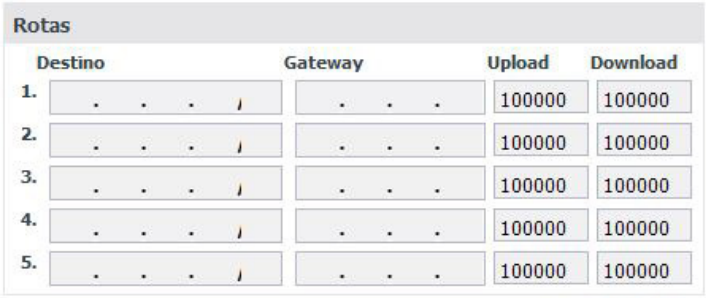
Ao lado do campo *Administração* é possível selecionar o modo de QoS:

- » TOS com Valor de 0 a 7, que representa a prioridade do pacote.
- » DSCP com Valor de 0 a 63, que representa a prioridade do pacote.

Atenção: as alterações efetuadas terão validade somente em equipamentos que forem configurados do mesmo modo, caso contrário, o tráfego será encaminhado de acordo com o comportamento padrão da IETF ou conforme alguma configuração específica no equipamento seguinte.

Rotas

Esta configuração permite definir rotas específicas para sub-redes na rede WAN, criando caminhos pré-determinados, onde as informações podem ser direcionadas até um host ou uma outra rede específica.



Menu Rede/Submenu WAN/Rotas

- » **Destino**: são informados os endereços IPs e a máscara (endereços IP/net-mask tipo CIDR) do destino do roteamento.
- » **Gateway**: informe o endereço IP do roteador, por meio do qual o tráfego vai fluir para a sub-rede de destino
- » **Upload e Download**: são definidas as taxas máximas para a conexão com a interface de destino. É importante saber as taxas de upload e download com a interface de destino disponível, para poder manter o equilíbrio na conexão do link e evitar qualquer saturação e consequente perda de qualidade.

LAN

Este submenu apresenta as informações da conexão da interface LAN e os parâmetros necessários para sua configuração dentro da rede (iguais aos da WAN), distribuídos nas seguintes guias:

Menu Rede/SubMenu LAN

Configuração de IP secundário para LAN e WAN

A configuração de IP Secundário permite configurar uma rede diferente da principal, tanto para a interface LAN quanto para a WAN. Com isso é possível alternar entre redes diferentes apenas mudando a porta em que está conectado o cabo da ICIP no switch.

Obs.: *estas redes não funcionam simultaneamente. Por exemplo: a interface LAN principal está configurada com uma rede A e a interface LAN secundária está configurada com uma rede B. Se o cabo de rede estiver conectado à rede A, valem as configurações da interface LAN principal. Se o cabo de rede estiver conectado à rede B, valem as configurações da interface LAN secundária.*

Configuração de IP secundário para LAN e WAN

DDNS

Com o DDNS (Dynamic Domanin Name System) é possível vincular a central a um nome de domínio na Internet (endereço DNS). Esse recurso é útil, por exemplo, quando a central não possui um endereço fixo na internet.

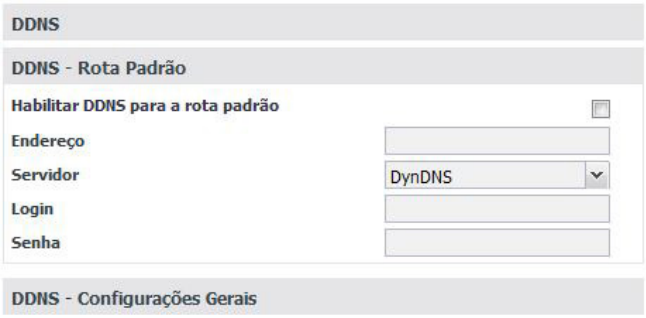
Antes de configurar este serviço, crie uma conta de serviço DDNS em um provedor de DDNS como o *www.no-ip.com*.

O provedor de serviço DDNS fornecerá um login e senha após o cadastro.

Menu Rede/SubMenu DDNS

DDNS - Rota Padrão

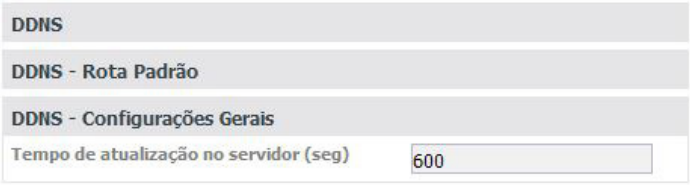
Permite a configuração dos parâmetros do servidor de DDNS. Para o correto funcionamento é necessário que todos os campos estejam configurados. Portanto é importante consultar o administrador de rede para obter os dados necessários.



Menu Rede/SubMenu DDNS/DDNS

- » **Endereço**: informe o endereço IP ou nome cadastrado nos servidores DDNS, ex: icip.dyndns.org.
- » **Servidor:** define o servidor que será utilizado (No-IP, DynDNS).
- » **Habilitar DDNS para a rota padrão**: habilita a atualização do servidor DDNS para a interface de saída para a internet.
- » **Login**: digite o login de usuário no servidor DDNS.
- » **Senha**: digite a senha de usuário no servidor DDNS.

DDNS - Configurações gerais



DDNS - Configurações gerais

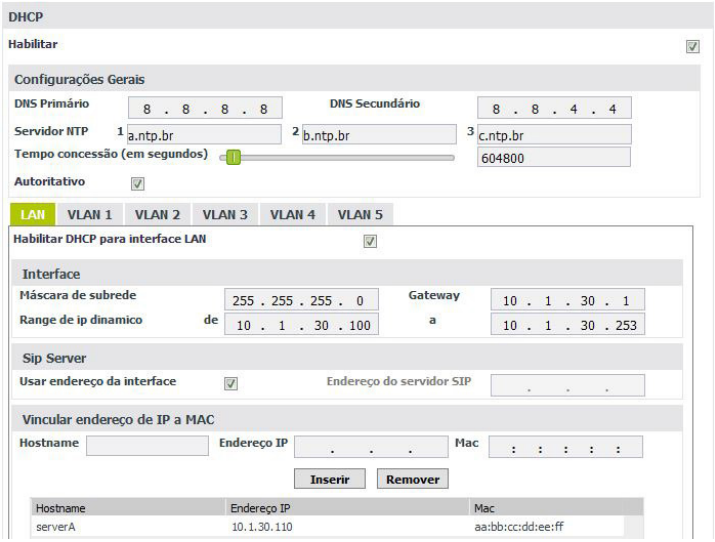
- » **Tempo de atualização no servidor (seg):** define o tempo de atualização das informações no servidor DDNS.

Atenção: para buscar o endereço IP que a placa tem disponível na internet, este serviço consulta via HTTP um servidor na Internet que retorna o endereço IP que a placa acessou a internet. Por isto é necessário que a ICIP tenha acesso a internet sem filtros na porta 80, isto inclui filtros como firewall e proxy autenticado.

Servidor DHCP

O DHCP, *Dynamic Host Configuration Protocol* (Protocolo de Configuração Dinâmica de Host), é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host, Máscara de sub-rede, *Default Gateway* (Gateway Padrão), entre outros. A placa ICIP possui um servidor DHCP embarcado. O principal motivo é ser possível fazer o auto provisionamento do endereço do servidor SIP para os telefones IP.

Esta funcionalidade não sai habilitada de fábrica.



Servidor DHCP

- » **Habilitar:** habilita o servidor DHCP.
- » **DNS Primário:** define o endereço IP do servidor DNS primário.
- » **DNS Secundário:** define o endereço IP do servidor DNS secundário.
- » **Servidor NTP 1:** define o endereço IP do servidor NTP 1.
- » **Servidor NTP 2:** define o endereço IP do servidor NTP 2.
- » **Servidor NTP 3:** define o endereço IP do servidor NTP 3.
- » **Tempo concessão (em segundos):** define o tempo em segundos da concessão dos endereços IP.
- » **Autoritativo:** define se o servidor é autoritativo.
- » **Habilitar DHCP para interface LAN:** habilita o servidor DHCP para a interface LAN.

Interface

- » **Máscara de subrede:** define a máscara da subrede.
- » **Gateway:** define o endereço IP do Gateway.
- » **Range de IP dinâmico:** define qual a faixa de endereços IP o servidor irá conceder aos dispositivos da rede.

Sip Server

- » **Usar endereço da interface:** com esta opção marcada, utiliza o mesmo endereço da interface para o servidor SIP.
- » **Endereço do servidor SIP:** se a opção anterior não estiver marcada, o endereço IP do servidor SIP deverá ser informado neste campo.

Vincular endereço de IP a MAC

- **Hostname:** nome do dispositivo na rede.
- **Endereço IP:** endereço IP que será concedido ao dispositivo.
- **MAC:** endereço MAC do dispositivo para o qual será concedido o endereço IP.
- **Inserir e Remover:** utilize estes botões para inserir os registros na tabela.

Obs.: *considere estas mesmas informações se quiser configurar as interfaces VLAN 1 à 5.*

NTP

O NTP (Network Time Protocol) é um protocolo de sincronização de relógios na internet, com isto é possível manter a hora da central correta e sincronizada com os principais sistemas da internet.

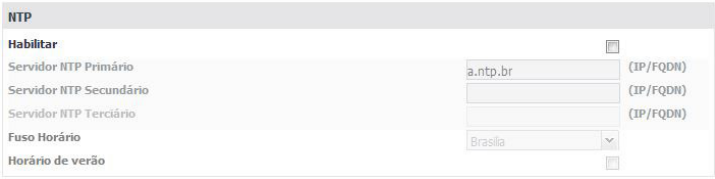
Atenção: a configuração do serviço de NTP só será possível após a habilitar este submenu no item Habilitar serviços.

Menu Rede/SubMenu NTP

NTP

Nesta guia é possível configurar os servidores NTP que irão manter atualizadas as informações de hora e data do sistema.

Atenção: ao inserir os servidores de NTP certifique-se de que as configurações de fuso-horário e horário de verão estão corretas.



Menu Rede/SubMenu NTP/NTP

- **Habilitar:** habilita ou desabilita o servidor NTP.
- **Servidor NTP Primário**: informe o endereço IP ou o nome do servidor NTP primário.
- **Servidor NTP Secundário**: informe o endereço IP ou o nome do servidor NTP secundário.
- **Servidor NTP Terciário**: informe o endereço IP ou o nome do servidor NTP terciário.
- **Fuso Horário:** define o fuso horário.
- **Horário de verão:** define se utiliza ou não horário de verão.

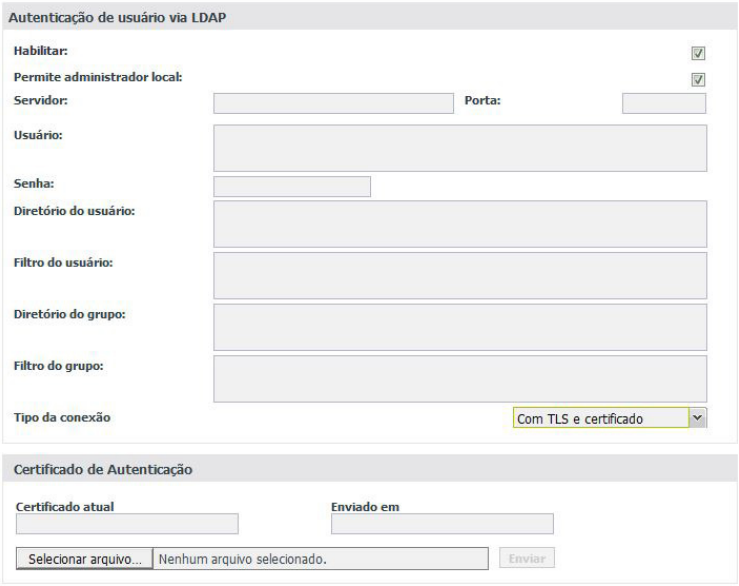
Atenção: o endereço registro.br mantém servidores NTP disponíveis para a sincronização com a hora legal brasileira. Os endereços destes servidores NTP são: a.ntp.br, b.ntp.br e c.ntp.br. Caso não possua servidores NTP em sua rede, utilize-os. Para maiores informações visite *http://www.ntp.br*.

Autenticação LDAP

A autenticação de usuário via LDAP (*Lightweight Directory Access Protocol*) serve para centralizar o controle de senhas de usuário, utilizando um servidor de autenticação que disponibiliza um acesso via LDAP. Esse servidor pode ser o mesmo que a empresa utiliza para fazer a autenticação de seus usuários. Ao ativar a autenticação via LDAP, o acesso via usuário e senha existente no PABX é desabilitado e, a depender da configuração realizada, passa a ser executado somente por meio do usuário *admin*.

Cada usuário que se autentica via LDAP deve ser criado também no PABX ou deve ser criado um usuário com o nome de um grupo a qual um ou vários usuários LDAP pertençam e habilitar a opção *Grupo LDAP*, acessando o menu *Sistema>Acesso de usuário*. O nome do usuário no PABX deve ser idêntico ao usuário do servidor LDAP e a senha deve ser diferente do PABX, esta senha, por sua vez não será utilizada quando a autenticação via LDAP estiver habilitada e sim somente será utilizada para acesso sem LDAP. A senha do usuário LDAP é armazenada somente no servidor LDAP. Para o funcionamento correto, é necessário configurar o PABX com os dados do servidor de autenticação e definir as permissões e categoria de cada usuário.

A configuração de autenticação do servidor via LDAP pode ser realizada acessando no programador WEB menu *Rede> Autenticação LDAP.*



Autenticação de usuário via LDAP

- **Habilitar:** habilita a autenticação do usuário em um servidor LDAP. Ao habilitar, os demais campos existentes devem ser preenchidos.
- **Permitir administrador local:** permite que o usuário padrão *admin* se autentique no PABX mesmo com o LDAP habilitado. A senha utilizada é a senha definida no PABX. Essa configuração deve ser utilizada enquanto estamos configurando o LDAP, permitindo a autenticação no PABX e alteração da configuração errada.
- **Servidor:** contém o nome ou o IP do servidor para autenticação.
- **Porta:** contém a porta do servidor LDAP, valor padrão é *389*.
- **Usuário:** usuário necessário para acessar o servidor de LDAP. O campo não é obrigatório, dependendo de como o servidor foi configurado.
- **Senha:** senha do usuário necessário para acessar o servidor de LDAP. O campo não é obrigatório, dependendo de como o servidor foi configurado.
- **Diretório do usuário:** deve conter o nome do diretório raiz onde os usuários que se autenticam estão armazenados. Os usuários podem ser organizados em outras pastas a partir deste diretório.
- **Filtro do usuário:** deve conter um campo que é utilizado para filtrar o nome do usuário.

» **Diretório do grupo:** deve conter o nome do diretório raiz onde os grupos que se autenticam estão armazenados. Os grupos podem ser organizados em outras pastas a partir deste diretório.
» **Filtro do grupo:** deve conter um campo que é utilizado para filtrar o nome do grupo.
» **Habilitar TLS:** habilita a utilização de encriptação dos dados LDAP. O servidor deve ser configurado para utilizar a encriptação.

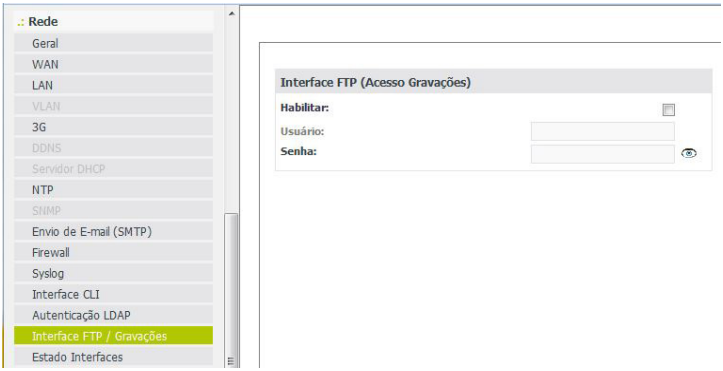
Grupo de usuários LDAP

Caso o método de autenticação utilize um grupo de usuários, deve-se cadastrar um usuário e marcar a opção *Grupo LDAP* em *Usuários>Acesso de usuário*.

Grupo de usuários LDAP

Interface FTP/Gravações

Permite que o aplicativo *Gravador de chamadas* conecte-se ao PABX.

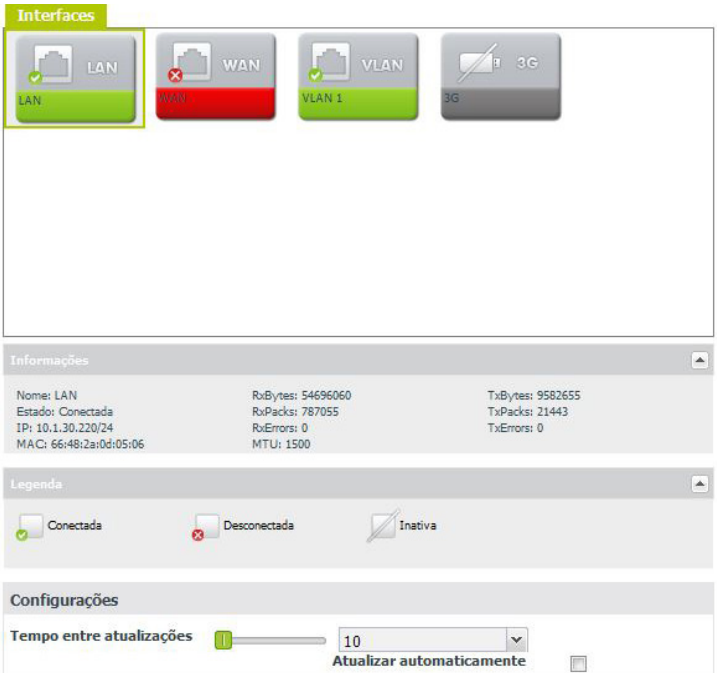


Interface FTP/gravações

» **Habilitar:** habilita ou desabilita o acesso FTP para o aplicativo de gravação.
» **Usuário:** define o nome do usuário.
» **Senha:** define a senha do usuário.

Estado das interfaces

Esta tela apresenta as informações de todas as interfaces de rede da central.



Estado das Interfaces

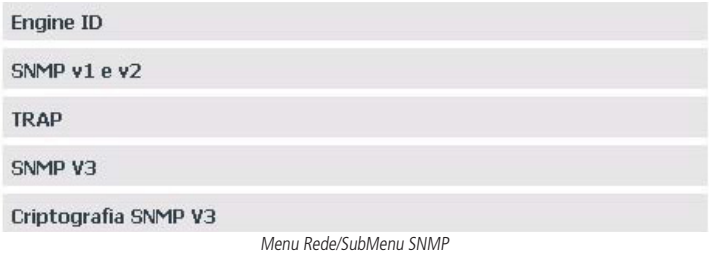
- » **Informações:** apresenta as informações da interface selecionada: Nome, Estado, IP, MAC, RxBytes, RxPacks, RxErrors, MTU, TxBytes, TxPacks, TxErrors.
- » **Legenda:** apresenta a legenda das imagens: Conectada, Desconectada ou Inativa.
- » **Tempo entre atualizações:** define o tempo para atualizações automáticas da página.
- » **Atualizar automaticamente:** habilita ou desabilita a atualização automática da página.

SNMP

O SNMP (Simple Network Management Protocol) é um protocolo de gerência de redes TCP/IP, da camada de aplicação, que facilita o intercâmbio de informações entre os dispositivos de rede. A utilização deste protocolo na ICIP possibilita aos administradores monitorar e gerenciar seu desempenho na rede, assim como, localizar e solucionar eventuais problemas, através de softwares dedicados a este fim.

Este submenu permite configurar os parâmetros necessários para o gerenciamento da ICIP através deste protocolo.

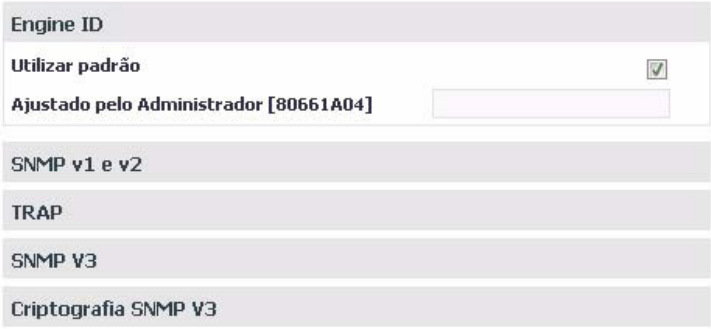
Atenção: a configuração do serviço SNMP para o sistema só será possível após a habilitar este submenu no item *Habilitar serviços*.



Menu Rede/SubMenu SNMP

Engine ID

Define que Engine ID será utilizado pelo sistema, se o padrão ou um personalizado. O Engine ID é um identificador único para cada equipamento de rede e é utilizado somente para identificação, não para endereçamento.



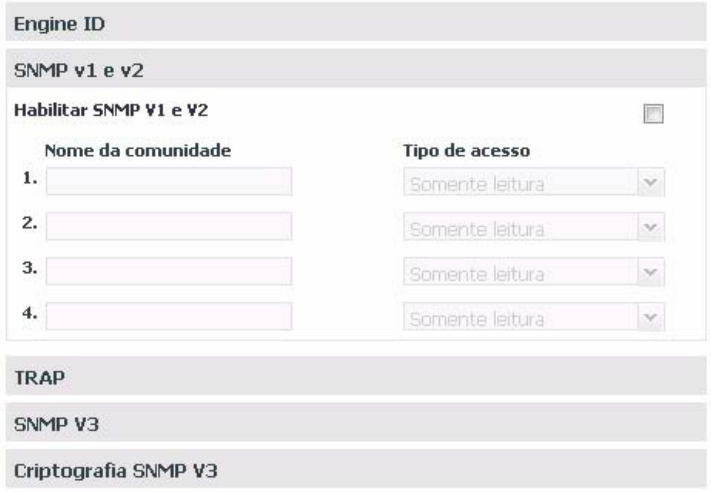
Menu Rede/SubMenu SNMP/Engine ID

» **Utilizar padrão**: selecionado, o Engine ID utilizado será o padrão do sistema.

» **Ajustado pelo Administrador [80661A04]**: estará acessível caso a opção de Engine ID padrão não esteja. O administrador deve informar o Engine ID personalizado (apenas caracteres hexadecimais).

SNMP v1 e v2

Nesta guia são configuradas as comunidades e os privilégios de acesso às informações dos dados e desempenho da ICIP dentro da rede. Assim o administrador, através de um software de gerenciamento SNMP, pode ter acesso a comunidades com diferentes níveis de informações.



Menu Rede/SubMenu SNMP/SNMP v1 e v2

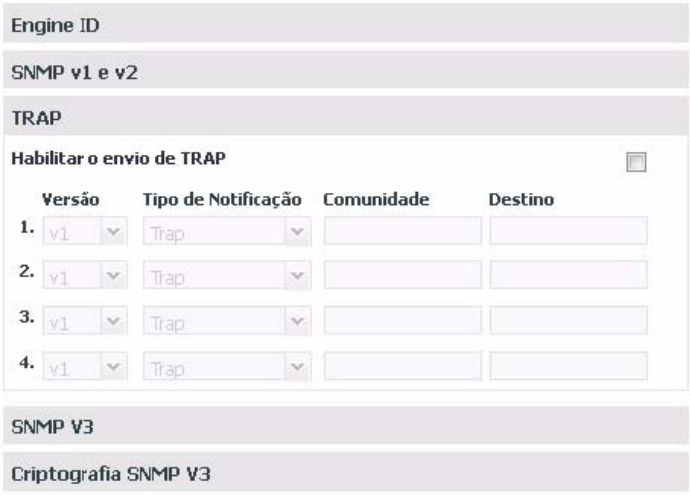
» **Habilitar SNMP V1 e V2**: habilita a criação de comunidades e a configuração dos privilégios.

» **Nome da comunidade**: é definido o nome da comunidade para acesso do gerenciador SNMP.

» **Tipo de acesso**: são definidos os privilégios relativos a leitura e escrita da comunidade pelo gerenciador SNMP.

TRAP

Nesta guia são configurados o envio de mensagens com informações de alerta relativas a eventos ocorridos na ICIP através das comunidades associadas. O administrador então, através de um software de gerenciamento SNMP, poderá tratar o evento adequadamente.



Menu Rede/SubMenu SNMP/TRAP

- **Habilitar o envio de TRAP:** habilita o envio de traps do sistema para o gerenciador SNMP.
- **Versão:** é definida a versão de SNMP que os traps utilizarão: V1 ou V2c.
- **Tipo de notificação:** apresenta as opções de notificação para a versão de SNMP selecionada:
- **Trap**: mensagens de alerta aos administradores (gerentes de rede) sobre eventos que ocorreram na ICIP;
- **Inform**: utilizado para notificar quando um evento foi confirmado.
- **Comunidade:** entre com o nome da comunidade para acesso do gerenciador SNMP ao evento ocorrido.
- **Destino:** é definido o responsável por receber as notificações dos traps do sistema.

SNMP V3

Nesta guia o SNMP V3 disponibiliza os serviços de segurança, através das opções de autenticação por *Usuário* e privacidade, além dos privilégios de acesso (como nas versões v1 e v2) e as informações dos dados e desempenho da ICIP dentro da rede.

Assim, o administrador deve utilizar um usuário e uma senha para ter acesso às informações.

Menu Rede/SubMenu SNMP/SNMP V3

» **Habilitar SNMP v3**: habilita os serviços de autenticação e privacidade por usuário.
» **Usuário**: é definido um usuário como identificador para o controle de acesso ao gerenciamento da base de dados MIB (Management Information Base).
» **Tipo de acesso**: são definidos os privilégios relativos a leitura e escrita do usuário pelo gerenciador SNMP.
» **Modo**: selecione o nível de segurança de autenticação e encriptação:
  » **noAuthNoPriv**: sem autenticação e sem privacidade;
  » **authNoPriv**: autenticado e sem privacidade;
  » **authPriv**: autenticado e privacidade;
» **Tipo Senha**: selecione o algorítmo de criptografia MD5 (128 bit) ou o SHA (160 bit) para autenticar os usuários.
» **Senha**: é definida a senha de acesso do usuário.

Criptografia SNMP V3

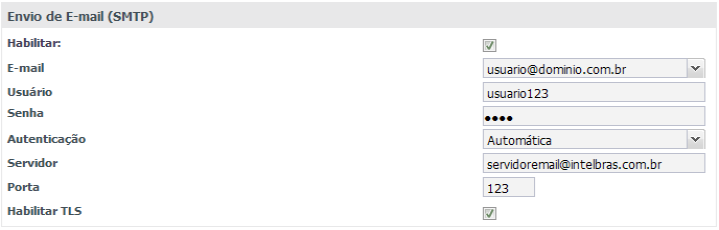
Nesta guia o SNMP V3 disponibiliza o serviço de segurança das mensagens através da seleção de um algoritmo criptográfico. Isto garante a privacidade das informações e evita o acesso por fontes não autorizadas.

Menu Rede/SubMenu SNMP/Criptografia SNMP V3

- » **Tipo de criptografia**: selecione o algoritmo de privacidade com o qual deseja encriptar as mensagens SNMP:
  - » **AES (Advanced Encryption Standard)**: algoritmo mais recente.
  - » **DES (Data Encryption Standard)**: algoritmo antigo.
- » **Senha de criptografia**: é definida a senha chave para a criptografia.

Envio de e-mail (SMTP)

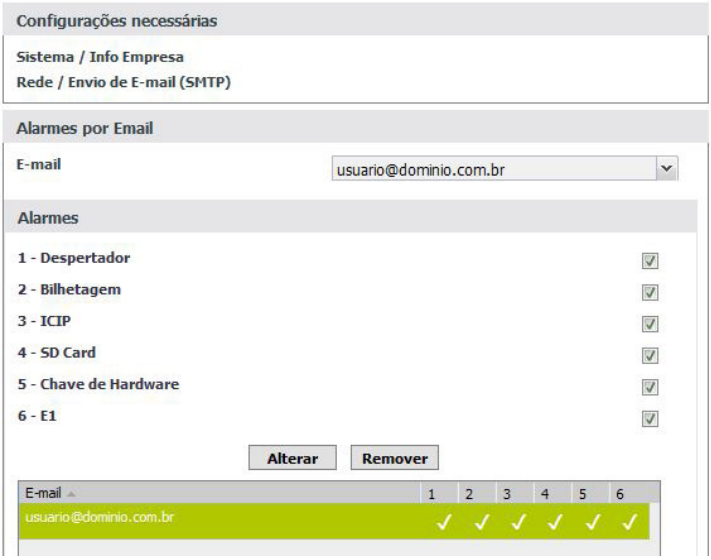
Esta tela apresenta as configurações para que a central possa enviar e-mails:



Envio de e-mail (SMTP)

- » **Habilitar:** habilita ou desabilita envio de e-mail.
- » **E-mail:** define o endereço de e-mail que será usado para enviar e-mails.
- » **Usuário:** define o nome do usuário da conta de e-mail.
- » **Senha:** define a senha da conta de e-mail.
- » **Autenticação:** define o tipo da autenticação no servidor de e-mail:
  - » Nenhuma
  - » Automática
  - » Senha normal
- » **Servidor:** endereço do servidor de e-mail.
- » **Porta:** porta do servidor de e-mail.
- » **Habilitar TLS:** habilita ou desabilita a criptografia TLS.

Uma aplicação para este serviço de envio de e-mail é a notificação de alguns alarmes ocorridos na central. Sua configuração pode ser realizada em *Manutenção>Alarmes por e-mail.*



Menu Manutenção/Alarmes por e-mail

- » **Despertador:** despertou/não despertou/não atendeu/não ficou livre.
- » **Bilhetagem:** buffer de bilhetagem atingindo a capacidade máxima.
- » **ICIP:** placa ICIP inicializada/não inicializada
- » **E1: perda de sincronismo**

Obs.: necessário configurar as informações da empresa em Sistema>Informações da empresa.

Menu Sistema/Informações da empresa

Segurança

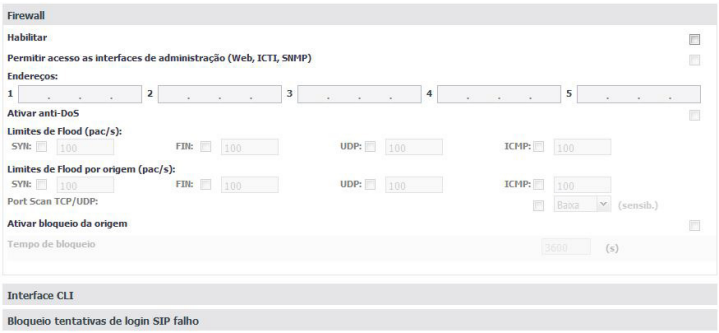
Neste menu podem ser encontradas as configurações de segurança da placa ICIP

Menu Rede - SubMenu Segurança

Firewall

Este submenu possibilita restringir o acesso de determinados IPs às funções de administração do PABX, como o acesso ao SNMP, Programador web e ICTI, e também a detecção e bloqueio de tentativas de DDoS (Distributed Denial of Service) e Port Scan.

Menu Rede - Submenu Segurança - Firewall



Menu Rede/SubMenu Firewall/Firewall

- **Habilitar:** habilita ou desabilita o Firewall.
- **Permitir acesso as interfaces de administracao (web, ICTI, SNMP)**: permite a configuração de acesso às funções de administração por determinados IPs.
- **Endereço**: define quais endereços IPs podem acessar os serviços de administração do PABX.
- **Ativar anti-DoS**: habilita alguns filtros com os quais é possível prevenir alguns tipos comuns de ataque de negação de serviço, em que pessoas mal intencionadas podem tentar negar o serviço da ICIP, por exaurirem os recursos, como quantidade de conexões simultâneas ou ataques em massa (flood). Além disso é possível configurar o bloqueio de tentativas de portscan.
- **Campo**:
  - Limite de SYN Flood.
  - Limite de FIN Flood.
  - Limite de UDP Flood.
  - Limite de ICMP Flood.

Estes campos dos filtros, podem ser selecionados e configurados para limitar o número máximo de pacotes de cada tipo que a ICIP irá aceitar por segundo, sendo estes pacotes de qualquer origem. Quando a quantidade instantânea de pacotes estiver além do valor definido, a ICIP iniciará a função de bloqueio imediatamente. O valor padrão é 100.

- **Campo**:
  - Limite de SYN Flood por origem.
  - Limite de FIN Flood por origem.
  - Limite de UDP Flood por origem.
  - Limite de ICMP Flood por origem.

Estes campos dos filtros podem ser selecionados e configurados para limitar o número máximo de conexões de cada tipo que a ICIP irá aceitar por segundo de um determinado IP. Quando a quantidade instantânea de conexões estiver além do valor definido, a ICIP iniciará a função de bloqueio imediatamente. O valor padrão é 100.

» **Port Scan TCP/UDP**: ativa a detecção de tentativas de portscan na ICIP. Portscan é o nome dado a técnica de escanear as portas abertas em um dispositivo de rede para determinar quais serviços este dispositivo disponibiliza. Com esta opção é possível detectar um dispositivo fazendo portscan na ICIP. A sensibilidade diz respeito a quão rápido o firewall irá identificar um possível portscan. Com a sensibilidade Alta o firewall irá considerar um portscan ao menor sinal de uma tentativa, já a sensibilidade Baixa fará o firewall ser mais conservador ao determinar um portscan. Caso um endereço seja identificado por fazer um portscan, a ICIP irá bloquear as tentativas de conexão deste endereço. Caso a opção "Ativar bloqueio da origem" esteja selecionada o endereço identificado será bloqueado pelo tempo determinado em "Tempo de bloqueio".

» **Ativar bloqueio da origem**: selecionado, os endereços IP que caírem na regra de limite de pacotes por origem, terão todas as tentativas de conexão bloqueadas durante o tempo especificado em Tempo de bloqueio.

Interface CLI

A interface CLI é um meio de se conectar à ICIP via SSH. Esta interface é a mesma utilizada anteriormente, onde o usuário conseguia se conectar via SSH à porta 16022 com o usuário icip e a senha icip1.0. Agora é possível configurar o usuário e a senha via programador web.

Menu Rede/SubMenu Segurança - Interface CLI

» **Habilitar:** habilita ou desabilta a interface CLI.

» **Usuário:** define o nome do usuário.

» **Senha:** define a senha do usuário.

Após configurar usuário e senha e enviar a programação, abra o terminal SSH, informe o IP da central e a porta 16022. Para autenticar, digite o usuário e senha cadastrados anteriormente. Digite o comando help para visualizar os comandos disponíveis:

ICIP>help

hardware_status

call_status

version

config

log

dns_latency

ping

traceroute

interfaces

route

top

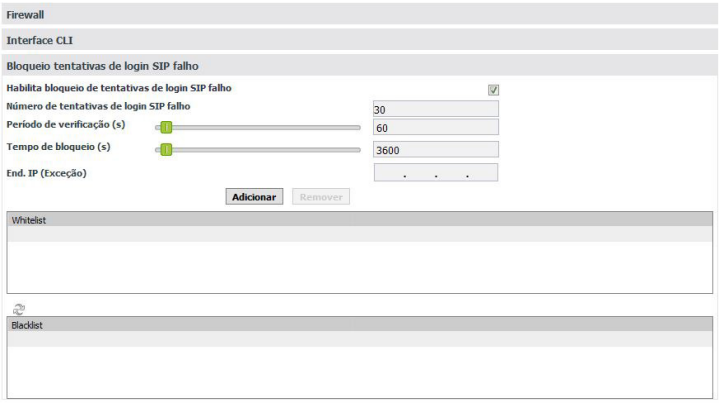
ps

enable_debug

exit

Bloqueio tentativas de login SIP falho

Esta é uma ferramenta de segurança dos dados para acessos não autorizados, implantada no sistema para garantir sua confiabilidade. Se durante a autenticação do login este não for reconhecido pelo sistema, o usuário poderá ter mais algumas tentativas antes de receber uma mensagem de bloqueio ou ainda, pode ser configurada uma lista de IPs que não serão analizados por esta regra, ficando livres de bloqueio.



Menu Rede/SubMenu Segurança/Bloqueio tentativas de login SIP falho

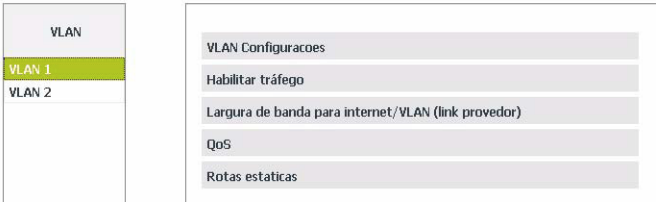
- » **Habilita bloqueio de tentativas de login SIP falho:** habilita o serviço de verificação da autenticação dos logins dos usuários no sistema.
- » **Número de tentativas de login SIP falho:** define o número máximo de tentativas com login incorreto.
- » **Período de verificação (segundos):** define um período de tempo dentro do qual será analisado o número de tentativas de login. Caso o número exceda o valor configurado no campo Número de tentativas de login falho, o endereço IP que está tentando login será bloqueado.
- » **Tempo de bloqueio (segundos):** define o período pelo qual será mantido o bloqueio do IP origem dos logins incorretos.
- » **End. IP (Exceção):** permite definir um endereço IP que não será analisado pelas regras, ficando livre do bloqueio. Informe os endereços IPs desejados e utilize os botões Adicionar e Remover para administrá-los.
- » **Whitelist:** apresenta a lista dos endereços IP, configurada por meio do campo End. IP (Exceção), que não será analisado pelas regras de bloqueio.
- » **Blacklist:** apresenta a lista dos endereços IP bloqueados.

VLAN

Este submenu apresenta as informações das múltiplas interfaces VLAN suportadas e os parâmetros necessários para a sua configuração dentro da rede.

Com esta função, a interface de rede pode ser segmentada em múltiplas VLANs (1 a 5) para reduzir as colisões por broadcast e melhorar a eficiência.

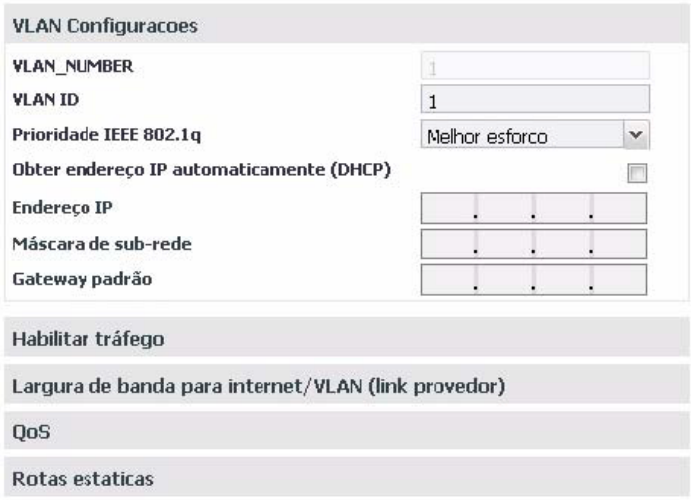
Atenção: a configuração da VLAN só será possível após habilitar este submenu no item *Habilitar serviços*.



Menu Rede/VLAN

VLAN Configurações

Permite a configuração dos parâmetros de prioridade de conexão e endereçamento, referentes a interface VLAN com a rede local. Portanto é importante consultar o administrador de rede para obter os dados necessários.



Menu Rede/SubMenu VLAN/VLAN Configurações

» **VLAN_NUMBER**: apresenta o número da VLAN na rede.

» **VLAN ID**: permite a inclusão de um identificador para a VLAN. Os valores válidos são de 1 a 4096.

» **Prioridade IEEE 802.1q**: dispõe de 8 níveis de prioridade ordenados da menor prioridade (Background) para a maior prioridade (Gerenciamento de rede). Estes níveis são utilizados para definir a prioridade do tráfego de acordo com as tags (rótulos) de prioridade adicionadas aos quadros (frames) das VLANs durante seu encaminhamento em um segmento de rede (sub-rede). Quando a taxa de tráfego entrante em um equipamento de rede é superior à taxa de tráfego sainte do mesmo (largura de banda), ocorre um congestionamento na rede. Durante estas condições, os quadros marcados com maior prioridade recebem tratamento preferencial e são entregues antes dos quadros com menor prioridade.

Atenção: para que este serviço seja implementado, os dispositivos conectados a ICIP devem possuir suporte à marcação (tag) de prioridade no rótulo de VLAN 802.1q do quadro Ethernet, para que sejam analisados, classificados, priorizados e enfileirados de acordo com sua marcação de prioridade.

» **Obter endereço IP automaticamente (DHCP)**: disponibiliza 2 opções de acesso a rede VLAN:

  » Selecionado, o acesso à rede VLAN será dinâmico, isto é, informações como endereço IP, máscara de rede e IP do gateway, serão fornecidas pelo primeiro dispositivo de rede que implemente um servidor DHCP. Esse equipamento pode ser um modem, roteador, switch ou um computador/servidor conectado na rede.

  » Sem seleção, o acesso à rede VLAN será estático, isto é, será necessário preencher os campos: Endereço IP, Máscara de Rede e IP do Gateway, de acordo com as especificações do administrador de rede.

» **Obter endereço IP automaticamente (DHCP)**: sem seleção.

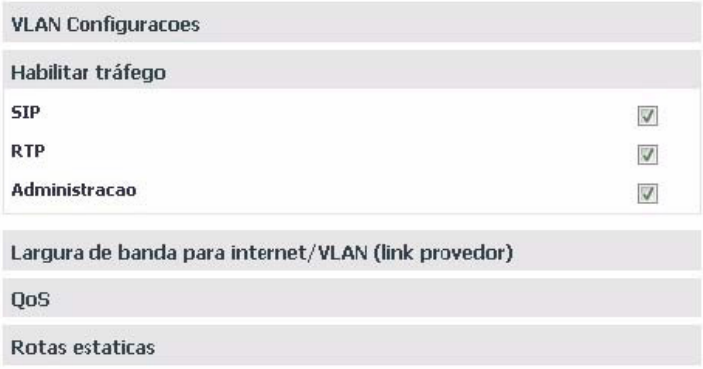
» **Endereço IP**: define o endereço IP da interface VLAN.

» **Máscara de sub-rede**: define os valores da máscara de sub-rede da interface VLAN.

» **Gateway padrão**: informe o endereço IP do roteador de saída da rede (equipamento que interliga mais de uma rede física).

Habilitar tráfego

Aqui são habilitados os tráfegos de administração e o de pacotes de sinalização SIP e RTP (relativos ao tráfego de voz) na interface VLAN.

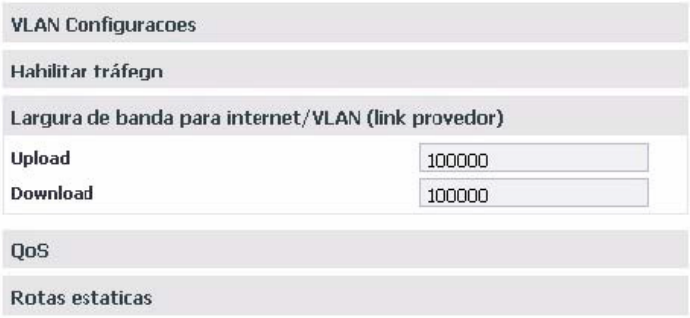


Menu Rede/SubMenu VLAN/Habilitar tráfego

- **SIP**: habilita o tráfego dos pacotes de sinalização SIP junto a rede VLAN configurada.
- **RTP**: habilita o tráfego dos pacotes de sinalização RTP junto a rede VLAN, fornecendo um meio uniforme para transmitir dados sujeitos a problemas de tempo real (áudio, vídeos,…).
- **Administração**: habilita o tráfego de administração na rede VLAN. Isto pode ser utilizado para evitar acesso às configurações de administração por pessoas não autorizadas.

Largura de banda para internet/VLAN (link provedor)

Nesta guia são configuradas as velocidades contratadas da banda do provedor dentro da rede.



Menu Rede/SubMenu VLAN/Largura de banda para internet/VLAN (link provedor)

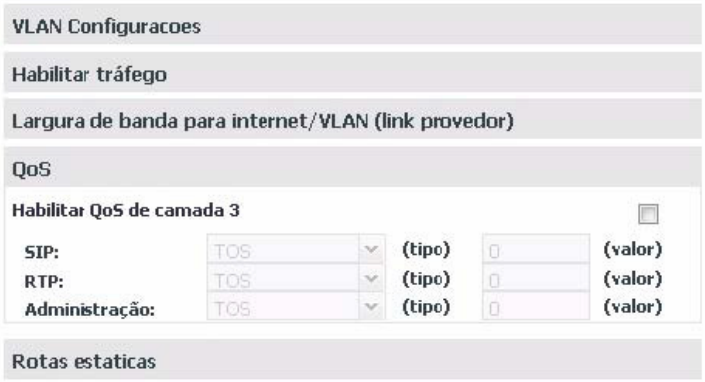
- **Upload e Download**: são definidas as taxas máximas para a conexão com o link provedor em função dos equipamentos conectados.

É importante saber as taxas de upload e download com a interface VLAN disponível, para poder manter o equilíbrio na conexão e evitar qualquer saturação e consequente perda de qualidade.

QoS

Permite especificar prioridades para pacote ou classe de tráfego. O QoS busca uma melhoria da qualidade da comunicação priorizando alguns tipos de dados em detrimento de outros, de acordo com uma classificação prévia dos mesmos, e se torna extremamente útil em condições de congestionamento de tráfego na interface de saída destes dados (por exemplo, a porta de conexão com o roteador para a Internet).

Atenção: a placa ICIP marca os pacotes de dados, cabendo aos ativos de rede (switchs e roteadores) dar prioridade ao tráfego de voz.



Menu Rede/SubMenu VLAN/QoS

Habilitar QoS de camada 3 Selecionado

Nos campos indicados nesta tela existe a opção de selecionar dois modos de sinalização dos pacotes (DSCP ou TOS) e a sua prioridade. Estes parâmetros serão utilizados para QoS e são inseridos no cabeçalho IP de todos os pacotes SIP, RTP e de administração transmitidos.

A escolha entre um dos modos depende de uma análise da rede, da compatibilidade dos dispositivos com o modo selecionado e da forma como estão configurados os roteadores e switchs para priorizar o tráfego.

- **Modo DSCP (Differentiated Services Code Point)**: prioriza o pacote de acordo com a marcação no pacote recebido. Esses pacotes se distinguem em classe de tráfego de acordo com as informações de atraso, taxa de processamento e confiabilidade anexadas ao pacote. Para isto, utiliza 6 bits do cabeçalho, dando 64 diferentes possibilidades para códigos de prioridade.
- **Modo TOS (Type of Service)**: os pacotes que entram na rede por meio da ICIP são encaminhados de acordo com a prioridade definida. Para isto, utiliza 3 bits do cabeçalho dando 8 diferentes possibilidades para códigos de prioridade, sendo 0 a prioridade mais baixa.

Atenção: quanto maior o valor, maior será a prioridade no tratamento e uso dos recursos da rede. Os modos DSCP e TOS entrarão em operação, conforme comportamento definido pela IETF.

Quando a taxa de tráfego entrante em um equipamento de rede é superior à taxa de tráfego sainte do mesmo (largura de banda), ocorre um congestionamento na rede. Durante estas condições, os quadros marcados com maior prioridade recebem tratamento preferencial e são entregues antes dos quadros com menor prioridade.

Lembre-se de que é baseado nestes parâmetros que os equipamentos de rede priorizam o tráfego de voz frente ao tráfego de dados.

SIP

Ao lado do campo *SIP* é possível selecionar o modo de QoS:

- TOS com valor de 0 a 7, que representa a prioridade do pacote.
- DSCP com valor de 0 a 63, que representa a prioridade do pacote.

RTP

Ao lado do campo *RTP* é possível selecionar o modo de QoS:

» TOS com valor de 0 a 7, que representa a prioridade do pacote.

» DSCP com valor de 0 a 63, que representa a prioridade do pacote.

Administração

Ao lado do campo *Administração* é possível selecionar o modo de QoS:

» TOS com valor de 0 a 7, que representa a prioridade do pacote.

» DSCP com valor de 0 a 63, que representa a prioridade do pacote.

Atenção: as alterações efetuadas terão validade somente em equipamentos que forem configurados do mesmo modo, caso contrário, o tráfego será encaminhado de acordo com o comportamento padrão da IETF ou conforme alguma configuração específica no equipamento seguinte.

Rotas estáticas

Esta configuração permite definir rotas específicas para sub-redes do lado da rede VLAN, criando caminhos pré-determinados, onde as informações podem ser direcionadas até um host ou uma outra rede específica.

Menu Rede/SubMenu VLAN/Rotas estáticas

» **Destino:** são informados os endereços IPs e a máscara (endereços IP/net-mask tipo CIDR) do destino do roteamento.

» **Gateway:** informe o endereço IP do roteador, por meio do qual o tráfego vai fluir para a sub-rede de destino

» **Upload e Download:** são definidas as taxas máximas para a conexão com a interface de destino. É importante saber as taxas de upload e download com a interface de destino disponível, para poder manter o equilíbrio na conexão do link e evitar qualquer saturação e consequente perda de qualidade.

9.7. VoIP - Placa ICIP 30 canais

Permite configurar os parâmetros gerais do provedor de serviço de telefonia, assim como as conexões e todos parâmetros necessários para que a central possa realizar as chamadas pela internet via VoIP.

Atenção: algumas destas informações podem ser obtidas junto ao administrador de rede e Provedor VoIP.

Menu VoIP/Placa ICIP e seus componentes

Geral

Este submenu permite configurar algumas características do VoIP, codecs e esquema de canais VoIP do sistema.

Menu VoIP/Placa ICIP/SubMenu Geral

VoIP Geral

Possibilita a configuração dos parâmetros relacionados a sinalização e melhoria de qualidade de aúdio. Esses parâmetros valem para ramais IP e conexões ponto a ponto.

Menu VoIP/Placa ICIP/SubMenu Geral/ VoIP Geral

- **SIP keep alive**: quando habilitado, o sistema envia periodicamente uma mensagem SIP ao destino da ligação, com o intuito de manter a sessão da NAT (Network Address Translation) disponível. Padrão 60s.
- **Jitter buffer adaptáve**l: quando habilitado, é possível especificar uma faixa de tempo de atraso para acomodar os pacotes que chegam da rede, permitindo que o sistema adapte o buffer, tendendo ao seu valor mínimo quando a rede está boa e ao máximo quando ruím. Dessa forma o sistema evita perdas e provê uma melhora na qualidade de áudio, o que torna esta opção a mais utilizada. A faixa padrão é entre 40ms e 100 ms.
- **Jitter buffer fixo**: quando habilitado, é possível especificar um tempo fixo de atraso para os pacotes. Nessa opção o tempo de "represamento" dos pacotes que chegam da rede, antes de "tocá-los", é sempre o mesmo. Técnicamente é mais simples porém, apresenta desempenho inferior pois não consegue acompanhar o comportamento da rede. O padrão é 40 ms.

Reserva Canais VoIP

Possibilita a configuração dos parâmetros relacionados a distribuição dos canais VoIP em relação aos ramais e juntores. O sistema permite reserva para ramais, juntores e livre acesso (sem reserva).

Menu VoIP/Placa ICIP/SubMenu Geral/Reserva Canais VoIP

- **Reservar canais VoIP**: habilitado, o administrador do sistema pode fazer a reserva de um número específico de canais VoIP para Juntores e/ou Ramais IP e disponibilizar os canais restantes para serem utilizados conforme demanda da central. Se não estiver habilitado os canais são alocados livremente, por demanda.
- **Canais para Juntores IP**: define o número de canais VoIP que ficarão reservados para Juntores IP.
- **Canais para Ramais IP**: define o número de canais VoIP que ficarão reservados para Ramais IP.
- **Canais sem reserva**: define o número de canais VoIP a serem usados livremente por troncos ou ramais IP, conforme demanda.
- **Habilitar economia de canal VoI**P: selecionado, o sistema economiza canais quando os dois dispositivos IP envolvidos na ligação forem ramais IP.

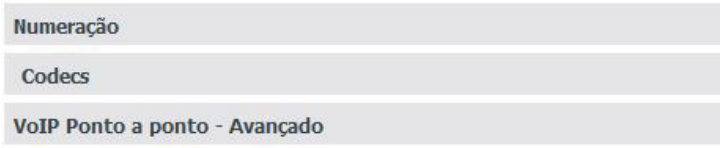
***Obs.*:** algumas situações fogem a essa regra, ou seja, a economia não será possível se:

- Pelo menos um dos ramais IP estiver atrás de NAT.
- Houver conferência envolvendo os ramais IP.
- O telefone, logado no ramal IP, não estiver preparado para funcionar com a ICIP de forma plena.

Atenção: funciona corretamente com TIP100 e ATA 2210T.

Ponto a ponto

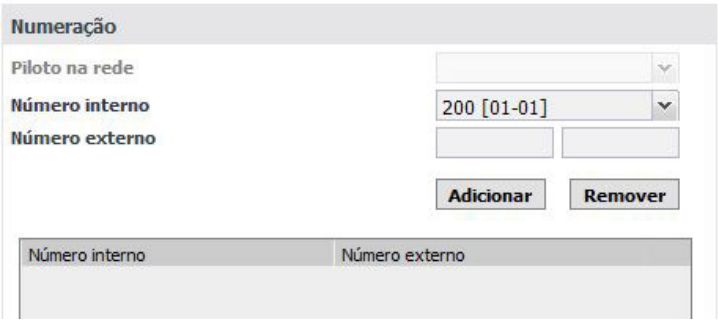
Este submenu permite configurar uma conexão entre a central Impacta e uma outra central IP, sem utilizar um provedor VoIP.



Menu VoIP/Placa ICIP/SubMenu Ponto a ponto

Numeração

Nesta guia são cadastrados todos os ramais que irão gerar e receber ligações VoIP ponto a ponto envolvendo filiais.



Menu VoIP/Placa ICIP/SubMenu Ponto a ponto/Numeração

» **Piloto na rede:** define o número externo que será usado como assinante chamador caso o ramal originador da ligação não esteja cadastrado na tabela.

» **Número interno:** selecione o ramal que poderá encaminhar e receber ligação VoIP envolvendo as filiais.

» **Número externo:** informe o número VoIP pelo qual o ramal interno é conhecido na rede.

Utilize os botões *Adicionar* e *Remover* para administrar os números internos/externos desejados.

Ponto a ponto filial

Nesta guia são cadastradas todas as filiais que irão gerar e receber ligações VoIP.

É ativada através do botão *Filiais* com as opções de criar uma nova Filial (botão *Novo*) ou consultar/modificar uma já existente (seleção direta do nome na guia).

Menu VoIP/Placa ICIP/SubMenu Ponto a ponto/Botão Filiais

SubMenu Ponto a ponto filial/Ponto a ponto filial

» **Localidade:** entre com um nome que seja significativo para identificar a Filial (ex.: nome da cidade, etc)

» **Endereço (IP ou FQDN):** informe o endereço IP ou FQDN da central ou dispositivo VoIP da Filial.

Numeração

Nesta guia são cadastrados todos os ramais da filial que irão gerar e receber ligações VoIP.

SubMenu Ponto a ponto filial/Numeração

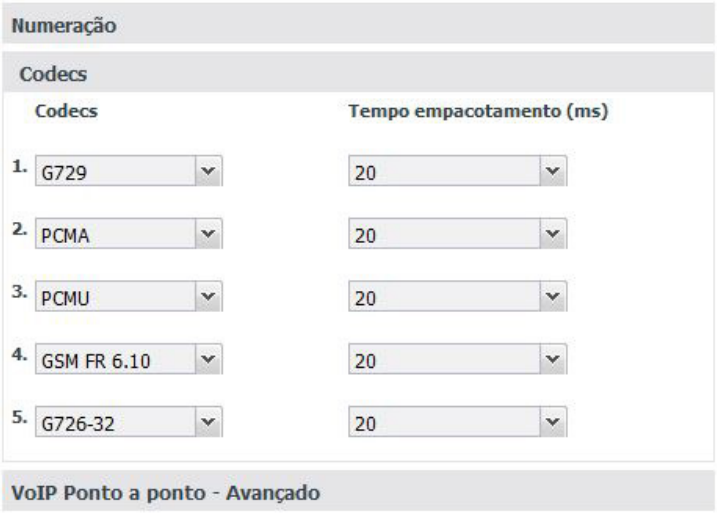
» **Número interno**: informe o ramal da filial para o qual será encaminhada a ligação VoIP. Esse número é aquilo que se disca, portanto não deve haver duplicidade com outro ramal ou facilidade.

» **Número externo**: informe o número VoIP pelo qual o ramal interno da filial é conhecido na rede.

Utilize os botões *Adicionar* e *Remover* para administrar os números internos/externos desejados.

Codecs

A função dos codecs é reduzir a largura de banda necessária para transmissão dos sinais de voz sobre a rede de pacotes. Isso é alcançado utilizando-se técnicas de compressão de voz, que, em maior ou menor grau, atuam no sentido de reduzir a redundância característica presente nos sinais de fala.



Menu VoIP/Placa ICIP/Submenu Ponto a Ponto/Codecs

» **Opção de 1 a 5:** definem a ordem de preferência dos codecs e o período do pacote RTP, quando se realiza ou se recebe uma ligação.

» **Codecs:** possuem diferentes relações de compressão, qualidade de aúdio e ocupação de largura de banda. A ICIP suporta os codecs: G.729AB, GSM FR 6.10, G.723, G.726-16, G.726-24, G.726-32, G.726-40 e G.711 PCMa e u.

» **Tempo empacotamento (ms):** em ligações VoIP, o áudio é transformado em pacotes de dados e este campo apresenta o tempo que a ICIP aguardará para envio dos pacotes RTP para a rede.

Obs.: *pelo menos uma das opções deve estar configurada como PCMA.*

VoIP ponto a ponto – Avançado

Nesta guia é possível configurar os dados VoIP ponto a ponto mais específicos.

VoIP ponto a ponto - Avançado

- **Porta de escuta SIP:** define a porta de escuta do protocolo SIP.
- **Porta do servidor:** define a porta usada no servidor.
- **Porta RTP Mín e Porta RTP Máx:** definem a faixa de portas que poderão ser utilizadas na transmissão e recepção do áudio. A faixa de portas RTP do provedor VoIP deve estar contida nesta faixa. Caso exista um Firewall, verificar se estas portas estão liberadas.
- **Enviar eventos DTMF:** define com qual método os dígitos DTMF serão enviados na rede após a chamada ter sido completada.
  - **SIP INFO:** envia os eventos DTMF como sinalização SIP.
  - **Out-of-band (RFC2833):** envia os eventos DTMF como uma sinalização de carga RTP, usando RFC 2833.
  - **In-Band:** envia os eventos DTMF no pacote de voz.
- **Formatação para envio de eventos SIP Info:** caso o método de DTMF escolhido seja SIP Info, estarão disponíveis as opções DTMF-Relay, DTMF e Telephone Event.

  Obs.: *utilize o método definido pela operadora.*
- **Valor do payload se RFC2833:** configure o tipo de carga (payload) do DTMF quando selecionado o evento DTMF Out-of-band (RFC2833). O valor varia de 96 até 127, sendo o padrão *101*.
- **Tempo de pausa entre dígitos (ms):** define o tempo da pausa inserido entre os dígitos discados.

» **Cancelamento de eco:** quando habilitado, o sistema evita que o eco na híbrida (quando se passa de 4 para 2 fios) retorne para a rede IP. Ou seja, o cancelador de eco de rede atua em ligações provenientes da rede IP, com destino a algum dispositivo TDM, eliminando o sinal refletido na híbrida, garantindo qualidade de áudio e conforto ao originador da chamada.

» **FEC:** habilita o uso do FEC (Forward Error Correction), algoritmo para correção adiantado de erros. Envia pacotes adicionais que permitem reconstruir, no receptor, pacotes de áudio perdidos na transmissão. Em redes com perda de pacotes, mantém a qualidade do áudio.

Obs.: *opção disponível apenas para a placa codec ICIP 30 - B).*

» **ANS:** habilita o uso do ANS (Adaptive Noise Suppressor), algoritmo de redução de ruído. Reduz ruídos nos sinais de voz provenientes da rede TDM, proporcionando uma melhora no conforto e inteligibilidade da comunicação.

Obs.: *opção disponível apenas para a placa codec ICIP 30 - B).*

» **VAD/CNG:** habilita o uso do VAD (Voice Activity Detection/(Confort Noise Generation): os algoritmos VAD e CNG formam um esquema de para identificar segmentos de voz ou ruído (VAD) em uma conversação e codificar os segmentos de ruído (CNG). Este esquema é ultilizado para reduzir o uso de banda em uma ligação telefônica quando o sinal transmitido contém somente silêncio/ruído.

Categoria para acesso VoIP a ramal externo (ramal de filial)

Esta configuração permite definir se o ramal possui categoria para fazer chamadas para ramais externos como, por exemplo, ramais de outras filiais conectadas via ponto-a-ponto VoIP. Padrão de fábrica *desabilitado*. Para habilitar, acesse R*amal>Categoria>Categoria para chamada interna*.

Categoria para acesso VoIP a ramal externo (ramal de filial)

Proxy

Este submenu permite configurar a conexão entre a central Impacta e o provedor VoIP através do qual poderão ser geradas e recebidas chamadas externas VoIP. É possível cadastrar até 50 servidores de registro Proxy.

Ao selecionar este submenu, é apresentada uma guia onde é/está cadastrada a(s) operadora(s) VoIP do sistema.
Para cadastrar um Provedor VoIP, utilize o botão *Novo* ou selecione um já existente para consultar/modificar (seleção direta do nome na guia).

Menu VoIP - Placa ICIP/SubMenu Proxy

VoIP proxy

Aqui são configuradas as informações repassadas pela Operadora para acesso do sistema.

Obs.: *dê preferência para configurar a interface LAN para acessar operadora proxy e evitar problemas de conexão, em cenário que use NAT.*

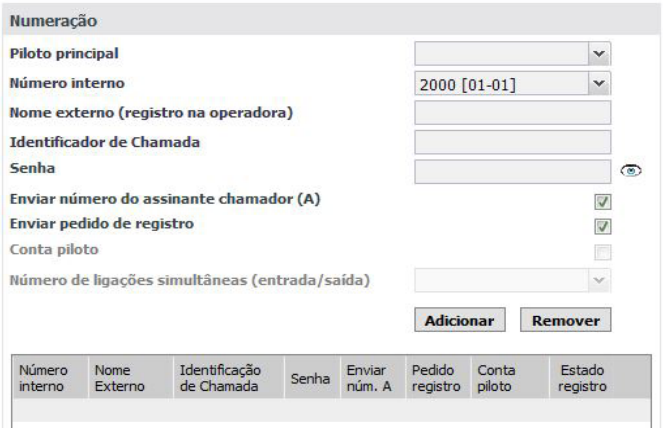
Atenção: algumas destas informações podem ser obtidas junto ao administrador de rede ou diretamente com a Operadora VoIP.

Menu VoIP/Placa ICIP/SubMenu Proxy/VoIP proxy

- **Estado da Operadora**: podemos visualizar se a operadora está operacional perante o sistema (Operadora contatável).
  - **Verde:** com pedido de registro *OK*.
  - **Vermelho:** com pedido de registro negado.
  - **Cinza:** com pedido de registro sem resposta.
  - **Azul:** sem pedido de registro.
- **Operadora**: entre com o nome da Operadora VoIP.
- **Localidade:** informe um nome que faça referência a localidade onde a central esta instalada.
- **Endereço do servidor (IP ou FQDN)**: informe o endereço IP ou nome de domínio da operadora VoIP, de acordo com as informações repassadas pela Operadora VoIP (ex.: operadora.net.br).
- **Porta do servidor**: defina a porta por onde o servidor VoIP irá transmitir e receber as mensagens SIP. O valor padrão de fábrica é 5060.
- **Bloquear DDC**: quando selecionado, as chamadas identificadas como "a cobrar" serão bloqueadas.
- **Considerar DDC se assinante origem iniciar com**: define os caracteres alfanuméricos que, se estiverem presentes no início do assinante chamador, classificarão a chamada como a cobrar.

Numeração

Nesta guia são cadastrados todos os ramais que irão gerar e receber ligações VoIP.



Menu VoIP/Placa ICIP/SubMenu Proxy/Numeração

» **Piloto principal:** define o número que será usado como assinante chamador caso o ramal originador da ligação não esteja cadastrado na tabela.
» **Número interno:** selecione o ramal interno que poderá encaminhar/receber ligação VoIP via operadora.
» **Nome externo (registro na operadora):** informe o número externo equivalente, que será registrado na operadora (conta).
» **Identificador de chamada:** define o nome do assinante no serviço VoIP. O valor deste campo será exibido no visor do identificador de chamadas do usuário que estiver recebendo uma chamada. Em alguns casos, o provedor VoIP pode sugerir a identidade real do chamador.
» **Senha:** informe a senha de registro do número externo, para autenticação junto à operadora VoIP. A senha deve ser de até 24 dígitos.
» **Enviar número do assinante chamador (A):** se essa opção estiver marcada o que será enviado como identificação para o destinatário será o valor preenchido no campo Identificador de chamada. Se estiver desmarcada será enviado o valor *Anônimo*.
» **Enviar pedido de registro:** define se a conta enviará pedidos de registro.
» **Conta piloto:** define se a conta é piloto.
» **Número de ligações simultâneas (entrada/saída):** define quantas ligações simultâneas poderão ser feitas por esta conta piloto.
» **Utilize os botões Adicionar e Remover:** administre os números internos/nomes desejados.

Portabilidade

Nesta guia são configurados os parâmetros para integração com servidores de portabilidade.

Portabilidade

» **Habilita portabilidade:** define se a portabilidade será habilitada ou desabilitada.
» **Tempo para aguardar servidor responder (ms):** define o tempo que será aguardado pela resposta do servidor em ms.
» **Em caso de falha na consulta:** define a ação a ser tomada caso a consulta ao servidor não consiga ser realizada. A chamada pode ser derrubada ou não.
» **Enviar aviso de falha:** define se enviará aviso em caso de falha.
» **Por e-mail:** envia o aviso para o e-mail informado.
» **Período para envio (em minutos):** define o período em minutos para que seja enviado o aviso.

Atenção: para obter as informações de portabilidade o usuário deverá contratar uma empresa que fornece este serviço. Vale ressaltar que é necessário verificar se o serviço de portabilidade da empresa é compatível com a Impacta antes de realizar a contratação do serviço.

O método utilizado pela Impacta para transmissão de informação com o servidor de portabilidade segue o seguinte padrão:

» A placa ICIP 30 envia uma mensagem de INVITE padrão SIP com o número de destino contendo o código de área para o servidor de portabilidade. No exemplo a seguir e realizada uma ligação para o número (48) 9932-8721 através do servidor servidordeportabilidade.com, registrado com a conta usuário.

U 2014/11/06 17:51:50.037471 201.3.239.120:5060 -> 10.252.68.161:5060
INVITE sip:4899328721@servidordeportabilidade.com:5060 SIP/2.0.
Via: SIP/2.0/UDP 201.3.239.120:5060;rport;branch=z9hG4bKPjKuwdcQlJfEvXhk61aNFfLCIC3fJYD63E.
Max-Forwards: 70.
From: "Usuario" <sip:contadousuario@servidordeportabilidade.com:5060>;tag=ZEJA-DHg3mfbIZ87ONa7.Jn8BJcKPqQ2.
To: <sip:4899328721@servidordeportabilidade.com:5060>.
Contact: "Usuario" <sip:contadousuario@201.3.239.120:5060>;+sip.account.user=usuario.
Call-ID: -DP1cbYwuBYbZFNmXQCTzXVWbYogqVGX.
CSeq: 32398 INVITE.
Allow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, REFER, OPTIONS, SUBSCRIBE, NOTIFY.
Supported: 100rel.
User-Agent: icip_intelbras /PBX_IMPACTA - v1.9.41_I30_MD.
Proxy-Authorization: Digest username="intelbras", realm="servidordeportabilidade.com",
nonce="545bb55000017a04a2065e61e331b532363a43f81c67e135", uri="sip:4899328721@servidordeportabilidade.com:5060",
response="b6aaa477cf4cfdc8ecaf50142dcd0a3e", cnonce="udlUghuKruOzUZTm14QXBKpCtDcs0g4C", qop=auth, nc=00000001.
Content-Type: application/sdp.
Content-Length: 358.
.
v=0.
o=icip_intelbras 3624288554 3624288554 IN IP4 201.3.239.120.
s=Intelbras.
c=IN IP4 201.3.239.120.
t=0 0.
m=audio 6000 RTP/AVP 18 8 0 3 2 101.
a=rtpmap:18 G729/8000.
a=fmtp:18 annexb=yes.
a=rtpmap:8 PCMA/8000.
a=rtpmap:0 PCMU/8000.
a=rtpmap:3 GSM/8000.
a=rtpmap:2 G726-32/8000.
a=sendrecv.
a=rtpmap:101 telephone-event/8000.
a=fmtp:101 0-15.
a=ptime:20.

» O servidor de portabilidade deverá retornar uma resposta do tipo 304-Moved Temporarily. Conforme informacao a seguir.

U 2014/11/06 17:51:50.037917 10.252.68.161:5060 -> 201.3.239.120:5060
SIP/2.0 302 Moved Temporarily.
Via: SIP/2.0/UDP 201.3.239.120:5060;received=201.3.239.120;rport=5060;branch=z9hG4bKPjKuwdcQlJfEvXhk61aNFfLCIC3fJYD63E.
From: "usuario" <sip:usuario@servidordeportabilidade.com:5060>;tag=ZEJA-DHg3mfbIZ87ONa7.Jn8BJcKPqQ2.
To: <sip:4899328721@servidordeportabilidade.com:5060>;tag=9e202574851715a2900e0fc5c60433e0-7825.
Call-ID: -DP1cbYwuBYbZFNmXQCTzXVWbYogqVGX.
CSeq: 32398 INVITE.
Contact: <sip:553204899328721@servidordeportabilidade.com>.
Server: IAO 1.1.
Content-Length: 0.

Note que é retornado na mensagem 304-Moved Temporarily, um número adicional que corresponde ao código da operadora do número solicitado, chamado RN1, no qual deverá estar cadastrado no menu roteamento>Portabilidade.

Atenção: para obter as informações de portabilidade o usuário deverá contratar uma empresa que fornece este serviço. Vale ressaltar que é necessário verificar se o serviço de portabilidade da empresa e compatível com a Impacta antes de realizar a contratação do serviço.

Codecs

A função dos codecs é reduzir a largura de banda necessária para transmissão dos sinais de voz sobre a rede de pacotes. Isso é alcançado utilizando-se técnicas de compressão de voz, que, em maior ou menor grau, atuam no sentido de reduzir a redundância característica presente nos sinais de fala.

Menu VoIP/Placa ICIP/SubMenu Proxy/Codec

» **Opção de 1 a 5**: definem a ordem de preferência dos codecs e o período (Tempo empacotamento) do Pacote RTP, quando se realiza ou se recebe uma ligação.

» **Codecs**: possuem diferentes relações de compressão, qualidade de aúdio e ocupação de largura de banda. A ICIP suporta os codecs: G.729AB, GSM FR 6.10, G.723, G.726-16, G.726-24, G.726-32, G.726-40 e G.711 PCMa e u.

» **Tempo empacotamento (ms)**: em ligações VoIP, o áudio é transformado em pacotes de dados e este campo apresenta o tempo que o sistema aguardará para envio dos pacotes RTP para a rede.

Obs.: *pelo menos uma das opções deve estar configurada como PCMA.*

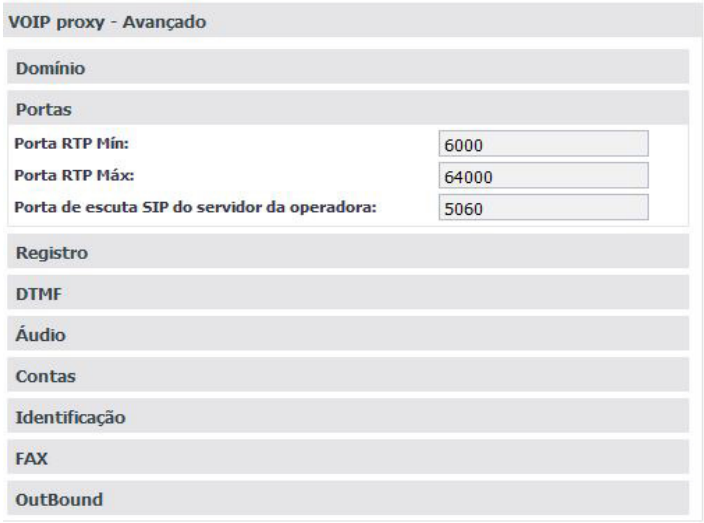
VoIP proxy - Avançado

Nesta guia é possível configurar os dados VoIP proxy mais específicos.

Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado

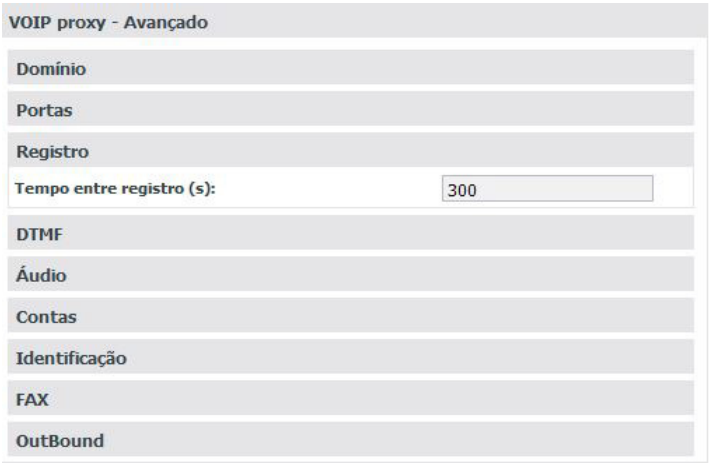
Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/Domínio

» **Domínio**
  » Nome de domínio.



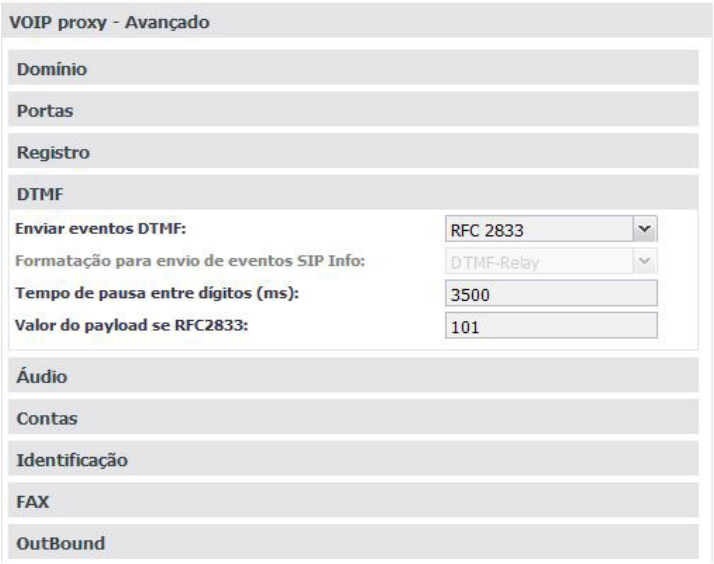
Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/Portas

» **Portas**
  » Porta RTP Mín. e Porta RTP Máx.
  » Porta de escuta SIP do servidor da operadora.



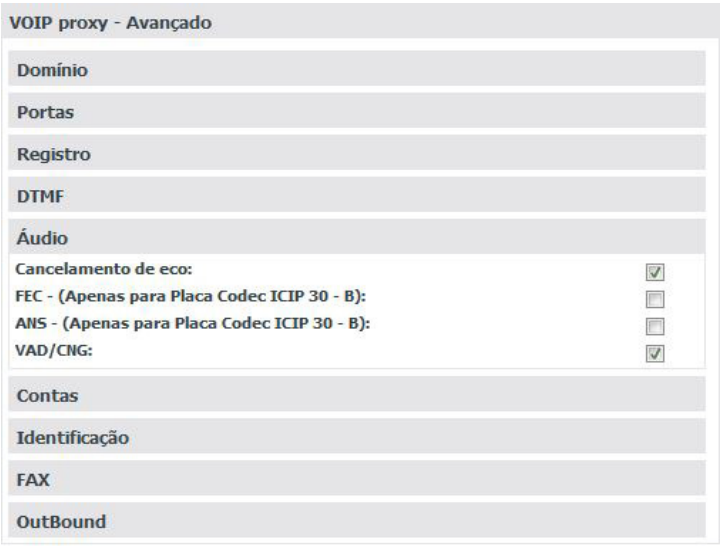
Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/Registro

» **Registro**
  » Tempo entre registro(s).



Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/DTMF

» **DTMF**
  » Enviar eventos DTMF.
    » SIP INFO.
    » Out-of-band (RFC2833).
    » In-Band.
  » Tempo de pausa entre dígitos (ms).
  » Valor do payload se RFC2833.

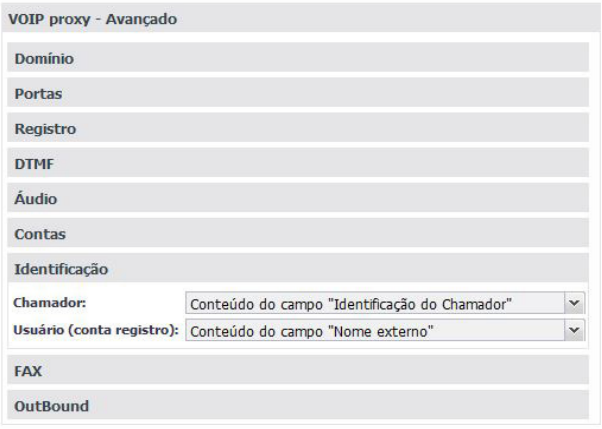


Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/Áudio

» **Áudio**
  » Cancelamento de eco.
  » FEC.
  » ANS.
  » VAD/CNG.

Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/Contas

» **Contas**
  » **Habilitar múltiplas contas piloto:** habilita a configuração de contas piloto.
  » **Subsistema (conta no destino é ramal IP):** habilita o modo Subsistema caso a conta no servidor destino seja um ramal IP.
  » **Originar ligação sempre usando o piloto:** as ligações serão originadas sempre usando o piloto.

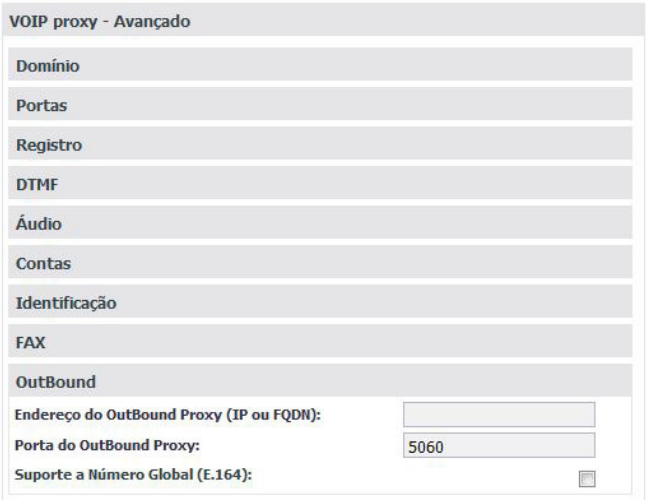


Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/Identificação

» **Identificação**
  » Enviar como Identificação do chamador.
    » Conteúdo do campo *Identificação do Chamador.*
    » Núm. do ramal originador (interno).
    » Núm. do chamador externo se a ligação vem de juntor.
  » Enviar como usuário (conta de registro).
    » Conteúdo do campo *Nome externo.*
    » Núm. do ramal originador (interno).
    » Núm. do chamador externo (bina) se ligação vem de juntor.

Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/Fax

» **FAX**
  » Desabilitado.
  » Bypass.
  » Data Bypass.
  » T.38.



Menu VoIP/Placa ICIP/SubMenu Proxy/Avançado/OutBound

» **OutBound**

É um serviço implementado por alguns servidores SIP que obriga todos os pacotes, incluindo pacotes de voz, a viajar através desse servidor em troca de uma melhor supervisão sobre suas funcionalidades.

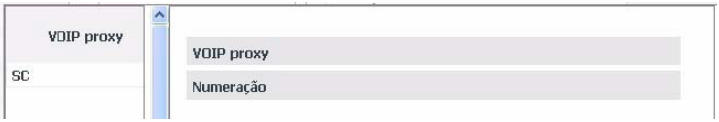
» **Endereço do OutBound Proxy:** pode ser endereço IP ou FQDN- Porta do OutBound Proxy: porta do servidor.

» **Suporte a número global (E.164):** E.164 é uma recomendação da ITU-T (*Telecommunication Standardization Sector*), que define, internacionalmente, a utilização da numeração na rede de telecomunicações pública (PSTN) e em algumas outras redes de dados. Também define o formato de números de telefone. Os números E.164 podem ter um máximo de quinze dígitos e são geralmente escritos com um prefixo +. Para discar os números corretamente a partir de uma linha de telefone fixa normal deve-se utilizar o prefixo internacional adequado.

VoIP Proxy Filial

Nesta guia são cadastrados todas as filiais que irão gerar e receber ligações VoIP. Utilize esta tabela quando houver comunicação com filiais e se ocorrer via operadora.

É ativada através do botão *Filiais* com as opções de criar uma nova Filial (botão *Novo*) ou consultar/modificar uma já existente (seleção direta do nome na guia).



Menu VoIP/Placa ICIP/SubMenu Proxy/Botão Filiais

VoIP proxy

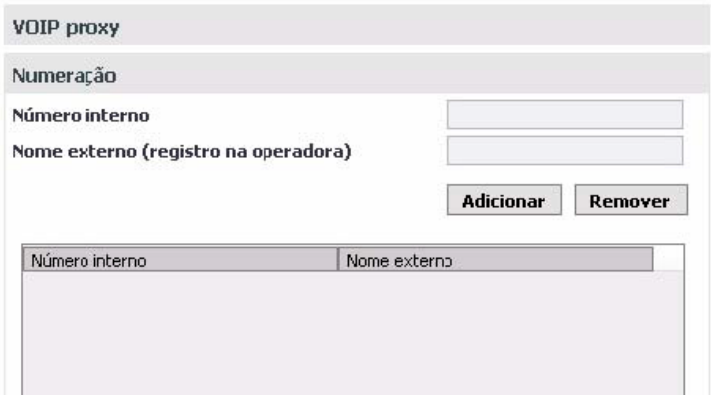
Nesta guia é cadastrada a identificação da filial que irá gerar e receber ligações VoIP.

SubMenu Proxy/VoIP proxy filial

» **Localidade filial:** entre com um nome que seja significativo para identificar a filial.

Numeração

Nesta guia são cadastrados todos os números da filial que irão gerar e receber ligações VoIP.



SubMenu Proxy/Numeração filial

» **Número interno:** informe o ramal da filial para o qual será encaminhada a ligação VoIP.
» **Nome externo (registro na operadora):** informe o nome ou número VoIP pelo qual o número interno da filial é conhecido na rede.
  » Utilize os botões *Adicionar* e *Remover* para administrar os números internos/nome desejados.

Ramais IP - Global

Nesta guia são configurados os parâmetros gerais dos ramais VoIP.

Ramais IP - Global

» **Porta de escuta SIP:** define a porta de escuta do protocolo SIP.
» **Porta RTP Mín:** define a porta mínima do protocolo RTP.
» **Porta RTP Máx:** define a porta máxima do protocolo RTP.

Auto configuração ramais IP

Esse submenu é extremamente útil quando se está instalando os ramais IP pela primeira vez. É possível inserir uma faixa de ramais IP na lista de diponíveis para obter login/senha. Dessa forma, ao *plugar* o telefone IP ele busca seu endereço IP automaticamente (se configurado para obter via DHCP). Na resposta o servidor informa também o endereço IP da central. De posse do endereço IP o telefone requisita seu login/senha. O serviço envia o primeiro disponível na lista e marca como atribuído. Na sequencia o administrador pluga o próximo ramal.

Menu VoIP/Placa ICIP/SubMenu Auto configuração ramais IP

O ATA GKM 2210T e os telefones TIP 100, TIP 120 e TIP 125 ao inicializarem pela primeira vez ou após uma restauração de configuração, estará apto a buscar, via DHCP, o endereço da central ICIP. Para isso, após ter inicializado, o Terminal IP irá requisitar via DHCP um endereço de IP, nesta requisição o terminal IP irá embutir o header "sip-servers" de código 120. Esta header tem a função de informar o endereço de um servidor SIP na rede. O servidor de DHCP da rede, na qual o terminal IP estiver conectado, poderá retornar junto com os outros headers, o header "sip-servers" com o valor do endereço IP da central ICIP. Com isso, o terminal IP irá se configurar para realizar uma requisição, com o intuito de adquirir configurações básicas para se registrar na central ICIP, como Número do Ramal e senha do ramal. Se houver número de ramal disponível na ICIP para este serviço, o servidor web da ICIP irá responder com um arquivo com informações necessárias para o registro. Se houver sucesso no registro com a ICIP, o Terminal IP irá seguir o fluxo normal e irá requisitar o arquivo de configuração armazenado na ICIP.

Para prover este serviço, a central ICIP deve ser configurada, via web, para liberar a faixa de ramais disponíveis para a configuração automática. Ou seja, na central determina-se os números/ramais que serão disponibilizados nas requisições automáticas do Terminal IP. Toda vez que um terminal IP adquirir um número da central, o ramal correspondente sairá da lista de disponíveis e não será mais oferecido a outro terminal IP.

Caso o número de ramais disponíveis esteja esgotado, a central ICIP irá retornar uma configuração inválida e o terminal IP não registrará na ICIP.

Em servidores Linux a configuração do serviço DHCP é editável no arquivo "/etc/dhcpd/ dhcpd.conf". O terminal IP irá avaliar se o parâmetro 120, na requisição DHCP, para autoconfigurar com a ICIP. Exemplo de configuração com a rede 10.1.30.xxx:

option sip-servers code 120 = {integer 8, ip-address};.

subnet 10.1.30.0 netmask 255.255.255.0 {

option sip-servers 1 10.1.30.61;

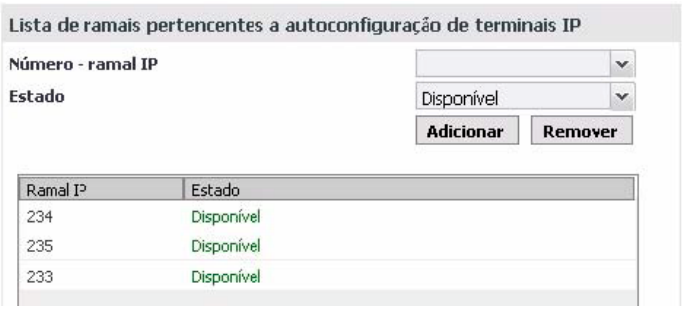
range 10.1.30.10 10.1.30.100;

range 10.1.30.150 10.1.30.200;

O endereço IP 10.1.30.61 é o IP da placa ICIP.

Lista de ramais pertencentes a auto configuração de terminais IP

Nesta guia são configurados os ramais IP que poderão ser auto configurados através da central. Este recurso permite uma configuração rápida dos terminais IP e o seu gereciamento.



Menu VoIP/Placa ICIP/SubMenu Auto configuração ramais IP/Ramais

» **Número - ramal IP:** informe o ramal IP que irá pertencer a auto configuração.

» **Estado:** define se o ramal está disponível ou utilizado para o sistema. Utilize os botões *Inserir* e *Remover* para administrar os ramais IP desejados.

Envio de alertas da central via e-mail

É possível programar envio automático de e-mail na ocorrência dos seguintes alertas:

» **Despertador:** despertou/não despertou/não atendeu/não ficou livre.

» **Bilhetagem:** buffer de bilhetagem atingindo a capacidade máxima.

Para isto, acesse *Sistema>Informações da empresa* e configure as informações solicitadas.

Menu Sistema/Informações da empresa

Envio de mensagens SMS apartir de terminais IP

Esta facilidade permite que aparelhos terminais IP TIP 200 e 300, assim como a TI NKT 4245i, possam enviar mensagens SMS redigidas no próprio aparelho.

***Obs.:** é pré-requisito que a placa GSM esteja configurada e possua chip registrado na operadora. É necessário também configurar as categorias de acesso do ramal e do juntor para envio de SMS.*

Suporte a BLF para ramal e juntor

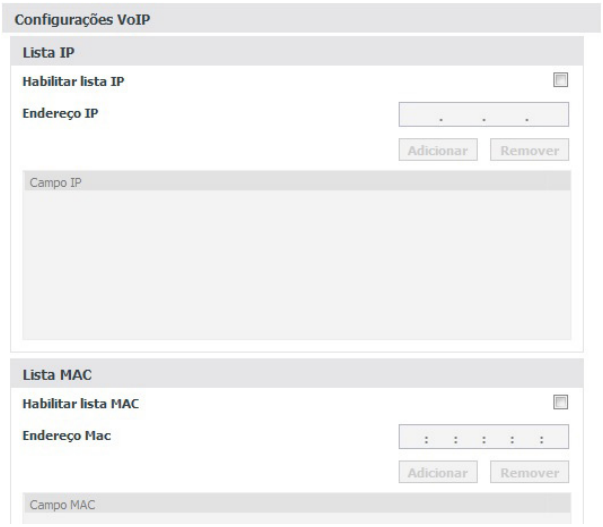
Alguns telefones IP possuem teclas de função BLF. BLF é o acrônimo de "*Busy Lamp Field*", que são as luzes sobre um telefone IP que indicam o estado de outros ramais ou juntores do PABX. Por meio desta indicação é possível saber se estão livres, recebendo chamadas ou ocupados. Por convenção, o LED aceso na cor verde indica que o ramal/juntor está livre. Se estiver piscando vermelho o ramal/juntor está recebendo uma chamada e se estiver vermelho, significa que o ramal/juntor está ocupado em uma chamada.

Filtro MAC/IP para ramal IP

Existem situações em que o endereço IP de um determinado dispositivo muda automaticamente, sem a intervenção do usuário. Isso acontece com certa frequência em dispositivos móveis, como aparelhos celulares por exemplo. Se o usuário utiliza um softphone IP nesse dispositivo, a mudança do endereço IP pode provocar a perda de registro da conta IP deste softphone.

Para resolver esse problema o administrador da central pode configurar o número MAC do dispositivo móvel na lista de MACs aceitos.

Nessa situação, a placa ICIP aceitará o pedido de registro independente do endereço IP origem, mas desde que o MAC seja igual ao configurado.



Filtro MAC/IP para ramal IP

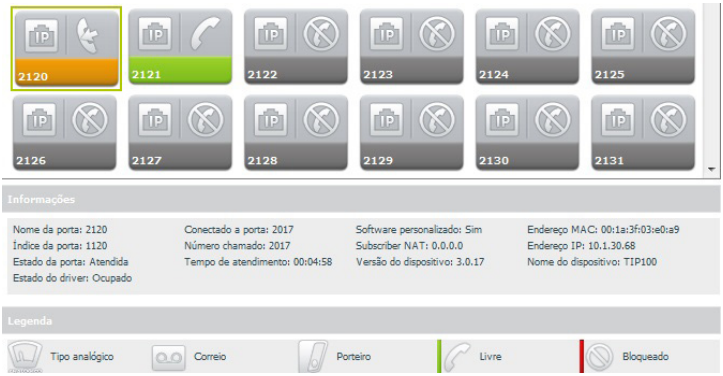
- » **Habilitar lista IP:** habilita a configuração da lista de endereços IP.
- » **Endereço IP:** define qual endereço IP será inserido na lista.
- » **Adicionar e Remover:** utilize estes botões para adicionar ou remover os registros na tabela.

Obs.: *o dispositivo precisa enviar o número MAC no pedido de registro.*

9.8. Manutenção

Estado das portas

Na tela *Estado* das portas é possível selecionar qualquer um dos ramais e consultar informações como, por exemplo, se a porta está em uma chamada, com qual ramal e a duração desta chamada. Para os ramais IP, algumas informações adicionais sobre o aparelho telefônico podem ser visualizadas: nome, versão, endereço IP, se está em um cenário NAT e se o aparelho é personalizado para funcionar com a placa ICIP de forma plena.



Informações sobre os ramais IP

Syslog

O Syslog é o protocolo de envio de mensagens de Logs. Os logs registram as informações do funcionamento do sistema, como eventos e erros ocorridos, para uso posterior.

Estes registros possuem formato de mensagem e, através do Syslog, podem ser armazenados internamente na ICIP ou enviados a um servidor de Syslog externo, tanto na rede local como na internet, seguindo o padrão do IETF para a RFC 5424.

Menu Manutenção/SubMenu Syslog

Syslog

Nesta guia é possível configurar o servidor de Syslog.

Menu Manutenção/SubMenu Syslog/Syslog

- **Habilitar:** habilita ou desabilita o syslog.
- **Tamanho máximo do arquivo de log:** define o tamanho do log armazenado na ICIP, em KB.
- **Habilitar servidor syslog remoto:** habilita o envio de log, via rede, para um servidor Syslog.
- **Endereço do servidor syslog:** informe o endereço IP ou o nome do servidor Syslog que receberá as mensagens de log do sistema.
- **Nível do log:** define níveis de informações nos logs. Quanto mais para baixo na lista, mais informações serão exibidas.
- **Emergency:** mensagens de emergência
- **Alert:** mensagens de alerta
- **Critical:** mensagens críticas
- **Error:** mensagens de erro

» **Warning:** mensagens de advertência
» **Notice:** mensagens de aviso
» **Info:** mensagens de informação
» **Debug:** mostra todas as mensagens

Suporte a sinalização de correio de voz MWI

A configuração MWI (*Message Waiting Indicator*), ou seja, indicador de mensagem em espera, é um recurso que permite à central avisar os aparelhos terminais que estes possuem mensagens de voz novas ou não ouvidas. Os aparelhos terminais comumente repassam essa informação aos usuários acendendo uma das teclas ou botões no próprio aparelho.

Obs.: *este recurso está presente em dispositivos compatíveis com a sinalização MWI e pode ser encontrada nos aparelhos terminais TIP 100, TIP 200/300.*

Atualização automática de senha para ramais IP

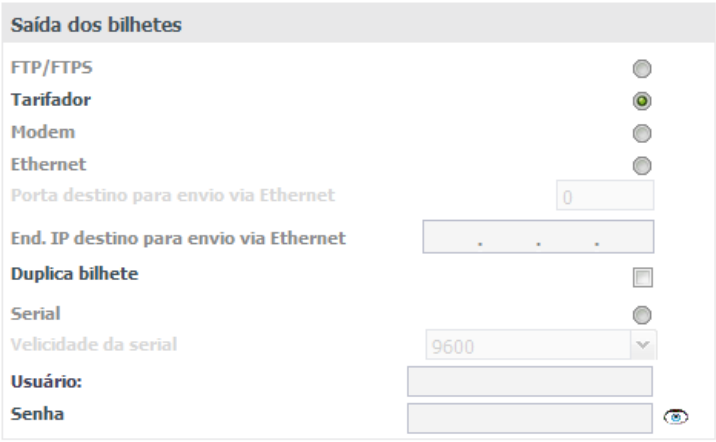
Ao realizar a alteração de senha em um ramal IP via programador, a placa ICIP enviará automaticamente a nova senha para o telefone registrado neste ramal.

Obs.: *alguns requisitos são necessários para que isto funcione:*

» *Somente telefones preparados para funcionar com a ICIP de forma plena. Funciona corretamente com telefone IP TIP 100 e ATA 2210T.*
» *O telefone deve estar registrado na conta no momento da alteração da senha.*

Coleta de bilhetes via FTP/FTPS

A coleta dos bilhetes das chamadas realizadas na central poderão ser coletados através do serviço FTP disponibilizado pela ICIP.



Coleta de bilhetes via FTP/FTPS

Para configurar, basta acessar *Sistema>Bilhetagem* e configurar a saída dos bilhetes como FTP/FTPS e criar o usuário e senha que serão utilizados para o acesso via FTP.

Atualização de firmware

Para atualizar a versão de firmware da placa ICIP, acesse o menu Gravação - Enviar, selecione a opção Firmware ICIP, selecione o arquivo de firmware e pressione Enviar. É recomendado que o equipamento seja atualizado com as versões de firmware mais atuais disponibilizadas em nosso site.

Termo de garantia

Fica expresso que esta garantia contratual é conferida mediante as seguintes condições:

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo: Nº de série:

Revendedor:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano, sendo este prazo de 3 (três) meses de garantia legal mais 9 (nove) meses de garantia contratual –, contado a partir da data da compra do produto pelo Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem vício de fabricação, incluindo as despesas com a mão de obra utilizada nesse reparo. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.
2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.
3. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.
4. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.
6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.
7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.

Sendo estas as condições deste Termo de Garantia complementar, a Intelbras S/A se reserva o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

O processo de fabricação deste produto não é coberto pelos requisitos da ISO 14001.

Todas as imagens deste manual são ilustrativas.

Produto beneficiado pela Legislação de Informática.

intelbras

Tarjeta madre y codec ICIP 30 Intelbras
Modelo Impacta 68i

¡Felicitaciones! Usted acaba de adquirir un producto con la calidad y seguridad Intelbras.

Intelbras, pensando en las necesidades del mercado VoIP, ofrece la solución ICIP 30 68i para las centrales telefónicas de la línea Impacta, modelo Impacta 68i, mejorando su desempeño y garantizando una alta disponibilidad de llamadas.

La ICIP 30 68i es una tarjeta opcional basada en una plataforma IP con alta capacidad de personalización y compatible con el protocolo de comunicación SIP. Fue proyectada para ser una solución en redes VoIP, permitiendo que las comunicaciones telefónicas se realicen a través de la red de datos disponible, proporcionando, así, una reducción significativa de los costos con telefonía y un aumento en la flexibilidad para pequeñas y medianas empresas.

Antes de usar (o ensamblar) el producto lea cuidadosamente este instructivo y las características eléctricas del producto.

1. Especificaciones técnicas

Estándares	IEEE802.3 Ethernet 10BASE-T
	IEEE802.3 Nway Auto Negotiation
	IEEE802.3u Fast Ethernet 100BASE-TX
	IEEE802.1Q tagged VLAN
	IEEE802.1p Layer2/CoS Traffic Priority
	IEEE802.3ac VLAN tagging
Interfaces de red	1 puerta LAN UTP fast Ethernet RJ45 10/100 Mbps
	1 puerta WAN UTP fast Ethernet RJ45 10/100 Mbps
Protocolo de señalización	SIP 2.0/SIP Intelbras
Interfaz USB	1 puerta USB host tipo A
	Compatibles con USB 1.1/2.0
Canales VoIP	Hasta 30 canales (10 canales por tarjeta codec ICIP 30 68i)
Codificación de voz	G.711 PCM (A/u-law) hasta 64 kbps
	G.729 AB CS- ACELP hasta 8 kbps
	GSM Full Rate 6.10 hasta 13,2 kbps
	G.723, G.726-16, G.726-24, G.726-32, G.726-40 (ADPCM)
LEDs	Indicadores de estatus, sistema y codecs

2. Características

» Soporte en procesamiento de señales.

» Control adaptable y fijo de jitter buffer y tecnología para ocultación de pérdida de paquetes (PLC).

» Codificación digital de voz - GSM Full Rate 6.10, G.711 PCM (A-law y u-law) y G729AB, G.726 (ADPCM), Detección de Actividad de Voz (VAD), Generación de Ruido de Confort (CNG), Cancelación de eco (LEC - G.168-2002, hasta 128ms) y Control Automático de Ganancia (AGC).

» FAX (Bypass y T.38).

» Señalización DTMF (In-Band, RFC 2833 y SIP INFO).

» Soporte en red.

» 1 extensión IP y 1 línea IP para cada canal VOIP, siendo que cada tarjeta codec posé 10 canales (no necesita llave de hardware).

» Hasta 30 canales VoIP (utilizando hasta 3 submódulos del tipo tarjeta codec ICIP 30).

» Troncales IP: Punto a Punto y Proxy (operador VoIP).

» Soporta hasta 5 VLANs.

» 2 puertos Fast Ethernet (10/100Mbps) 1 LAN, 1 WAN.

» Detección automática de la tarjeta codec ICIP 30 Intelbras.

» Monitoreo del sistema vía SNMP (V1/V2c/V3).

» Actualización de firmwares del PABX (central, DISA, música, interfaces y teléfono IP TIP 100 y ATA GKM 2210T de Intelbras).

» Soporte a configuración vía navegador web (HTTPS). Programación vía web es plenamente compatible con el navegador Mozilla Firefox® (consulte la versión compatible en la *Tabla de Compatibilidad Centrales Impacta* disponible en la sección *Descargas* de nuestra página web).

» Protección del sistema vía Firewall.

» Control de tráfico.

» Permite conectar a un Tarificador, Monitor E1, CSTA y otras aplicaciones vía ICTI.

» Generación de Logs locales y remoto (SysLog).

» Registro de una dirección DNS dinámica (DDNS).

» Sincronización de relojes del sistema vía Internet (NTP).

» Interfaz de acceso a red local (LAN) y red externa (WAN).

» Auto aprovisionamiento de extensiones/internos IP con teléfono Intelbras TIP 100 y ATA GKM 2210T (a partir de la versión 1.3 release 32).

» Inicialización automática de teléfonos IP.

» Actualización automática del número de extensión/interno del teléfono IP/ATA Intelbras TIP 100 y ATA GKM 2210T.
» Detección de Operador VoIP fuera de servicio.
» Indicación de prioridad de mensajes en relación a otras (QoS, protocolo IP Precedente).
» Detección de Brute Force Attack.

3. Cuidados y seguridad

Las informaciones a continuación se destinan a técnicos autorizados o expertos.

Atención: solamente técnicos capacitados por Intelbras están autorizados a instalar y configurar el PABX, bien como abrir la caja, conectar y operar sus interfaces.

Leer cuidadosamente todas las informaciones sobre el equipo y seguir todas las informaciones de seguridad.

» Consultar siempre un superior o responsable inmediato antes de iniciar el trabajo, informando los procedimientos necesarios para realizar el servicio solicitado y las precauciones de seguridad necesarias.
» Retirar la alimentación del sistema durante los servicios de montaje o retirada de las interfaces.
» Conectar el conductor a tierra al sistema involucrado antes de iniciarlo. Nunca operar el equipo con el conductor a tierra desconectado.

Para evitar daños electrostáticos a la tarjeta ICIP, observe las siguientes precauciones:

Atención: la electricidad estática puede dañar los componentes electrónicos de la Interfaz. Ese tipo de daño puede ser irreversible o reducir la expectativa de vida útil del dispositivo.

» Utilice una pulsera antiestática, o similar, para manipular las tarjetas.
» El transporte y el almacenaje deben ser solamente en embalajes a prueba de electricidad estática.
» Coloque la tarjeta sobre una superficie conectada a tierra al retirarla del embalaje.
» Evite tocar en las patillas de los circuitos integrados o conductores eléctricos.
» Esté siempre adecuadamente conectado a tierra al tocar en la tarjeta o en algún componente.

4. Protección y seguridad de datos

4.1. Tratamiento de datos personales

Este sistema utiliza y procesa datos personales como claves, registro detallado de llamadas, direcciones de red y registro de los datos de clientes, por ejemplo.

5. Cuidados y seguridad

5.1. Protección y seguridad de datos

Observar las leyes locales respecto a la protección y uso de dichos datos y las reglamentaciones que prevalecen en el país.

El objetivo de la legislación de protección de datos es evitar infracciones en los derechos individuales de privacidad basadas en el uso inadecuado de los datos personales.

5.2. Directrices que controlan el tratamiento de datos

» Asegurar que solo personas autorizadas tengan acceso a los datos de clientes.
» Usar las facilidades de atribución de claves, sin permitir cualquier excepción. Nunca informar claves a personas no autorizadas.
» Asegurar que ninguna persona no autorizada tenga como procesar (almacenar, modificar, transmitir, deshabilitar o borrar) o usar datos de clientes.
» Evitar que personas no autorizadas tengan acceso a los medios de datos, por ejemplo, discos de backup o impresos de protocolos.
» Asegurar que los medios de datos que no son más necesarios sean completamente destruidos y que documentos no sean almacenados o dejados en locales generalmente accesibles.
» El trabajo en conjunto con el cliente genera confianza.

5.3. Uso indebido del usuario e invasión de hackers

» Las contraseñas de acceso a la información del producto permiten el alcance y alteración de cualquier facilidad, como el acceso externo al sistema de la empresa para obtener datos y realizar llamadas, por lo que es muy importante que las contraseñas solamente estén disponibles para aquellos que tengan autorización para su uso, bajo el riesgo de uso indebido.

» El producto posee configuraciones de seguridad que pueden ser habilitadas, y que serán abordadas en este manual. También es imprescindible que el usuario garantice la seguridad de la red en la que el producto está instalado, teniendo en cuenta que el fabricante no se responsabiliza por la invasión del producto por medio de hackers y crackers.

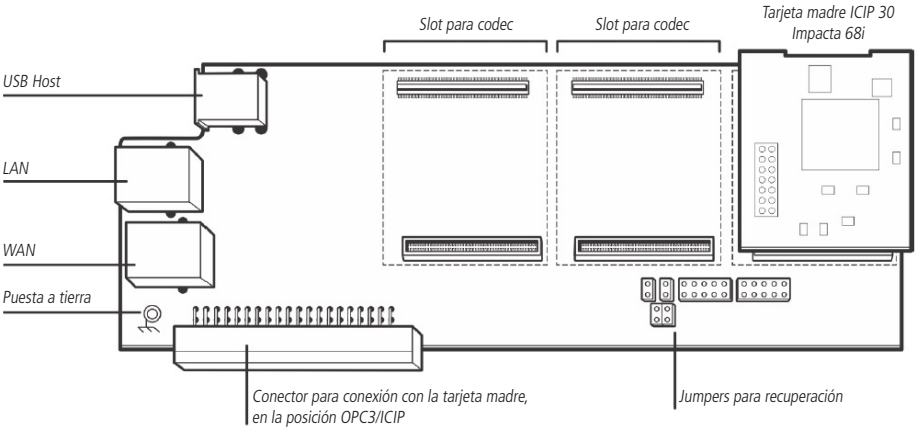
6. Producto

La solución de producto que permite acceder a la tecnología de transmisión de señales de voz por Internet o por una red privada está compuesta por el conjunto:

» **Tarjeta madre ICIP 30 68i**: responsable por el procesamiento de las informaciones de red, protocolos de acceso y conexiones a red del cliente e Internet;

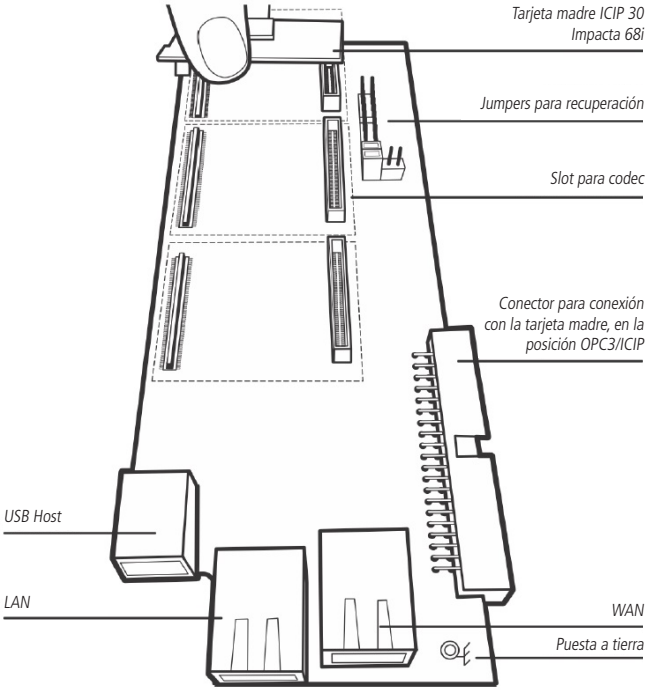
» **Tarjeta codec ICIP 30 68i**: responsable por los canales VoIP disponibles en la tarjeta madre ICIP 30 68i y por el procesamiento de las señales de "voz" y su conversión en paquetes de datos dentro de la red. Cada tarjeta codec habilita 10 canales VoIP.

6.1. Tarjeta madre ICIP 30 Impacta 68i



ICIP: Interfaz de Comunicación IP

6.2. Posiciones de conexión tarjeta madre ICIP 30 Impacta 68i (1 a 3)



6.3. Protección y seguridad de datos

Interfaz de red LAN	Puerto RJ45 Fast Ethernet 10/100 para acceso a red local	
Puertos USB	2 puertos USB host para conexión de periféricos	
Interfaz de red WAN	Puerto RJ45 Fast Ethernet 10/100 para conexión externa de acceso a Internet	
LED indicador del estatus de la tarjeta madre ICIP 30 68i	**Cadencia**	**Estado**
	Permanentemente encendido	Tarjeta no inicializada
	Parpadeando muy rápidamente (100 ms ON/100 ms OFF)	Tarjeta inicializando (Linux inactivo)
	Parpadeando rápidamente (500 ms ON/500 ms OFF)	Tarjeta inicializando (Linux activo, e inicializando servicios)
	Parpadeando moderadamente (1 s ON/1 s OFF)	Tarjeta inicializada y operando (Programador web activo)
	Parpadeando intermitente (1400 ms ON/300 ms OFF)	Falla de Inicialización de la tarjeta
Conectores para tarjeta codec ICIP 30 68i	Existen 3 posiciones disponibles para la conexión, pudiendo así alcanzar hasta 30 canales VoIP.	

7. Producto

7.1. Tecnología

Vista general

Con la tarjeta ICIP, la central Impacta 68i sigue disponiendo de todos los recursos y funcionalidades ya existentes, además de las nuevas funcionalidades anteriormente mencionadas.

En ella, las informaciones referentes a voz serán transmitidas por Internet o por una red privada, a través de la tecnología conocida como VoIP (Voz sobre IP), usando el protocolo SIP. Así, además de poder utilizar normalmente toda la estructura de la red de telefonía instalada, su empresa también puede utilizar la red de datos para realizar y recibir llamadas a través de los teléfonos IP.

Algunos de los resultados inmediatos son:

- » Reducción de los costos con llamadas locales, LDN y LDI, por utilizar Internet;
- » Unificación del plan de numeración para las extensiones/internos VoIP, analógicas y digitales;
- » Acceso vía web al sistema de configuración y administración;
- » Reducción de los costos de operación de la red.

7.2. VoIP

Voice Over IP (VoIP) es la tecnología que permite que informaciones de voz sean transmitidas a través del protocolo Internet Protocol (IP). Este concepto consiste en digitalizar la voz, empaquetarla y transmitirla en la misma red que es usada para transportar los paquetes de datos IP.

El empaquetamiento consiste en insertar las muestras o cuadros procesados por el codificador (codec) en paquetes. Estos paquetes trafican en la red IP a través de los ruteadores, que toman la decisión recibiendo los paquetes y eligiendo rutas más convenientes hasta los destinatarios.

7.3. Protocolo SIP

Es un protocolo utilizado para establecer llamadas y conferencias a través de redes vía IP. Fue proyectado con enfoque en la simplicidad, y, como un mecanismo de establecimiento de sesión, en el que solo se inicia, modifica y termina la sesión, lo que lo vuelve un protocolo que se adapta tranquilamente en diferentes arquitecturas.

El protocolo SIP posee un papel cada vez más importante en la telefonía IP, principalmente debido a su sencillez, flexibilidad, seguridad, facilidad de movilidad y, especialmente, debido a la gran aceptación de fabricantes de IP PBX, Gateways y teléfonos IP.

8. Instalación

Para el montaje de la tarjeta madre y codec ICIP 30 68i, siga el procedimiento:

1. En una superficie conectada a tierra conecte la pulsera antiestática;
2. Retire la tarjeta madre ICIP 30 68i y la(s) tarjeta(s) codec ICIP 30 68i de los embalajes y póngalas sobre la superficie conectada a tierra;
3. Verifique el estado de las tarjetas y sus conectores;
4. Apoye de manera estable la tarjeta madre ICIP 30 68i sobre la superficie e inserte la(s) tarjeta(s) codec ICIP 30 68i en las posiciones disponibles, siguiendo el esquema del item *6.2 Posiciones;*
5. Inserte el conjunto montado en un embalaje antiestático hasta que la central esté lista para recibirlo;
6. Informe a un responsable de la central Impacta que será necesario apagarla;
7. Localice el administrador de red o técnico de informática para auxiliarlo a reconocer en cuál escenario la tarjeta ICIP será configurada, anote las direcciones IP, servidores de banda ancha, servidor SIP Proxy, usuarios y claves, así como la localización física de los cables de red LAN y WAN (se debe utilizar preferentemente el puerto WAN para conectar la red interna del cliente y el puerto LAN para conectarse a la red interna del proveedor del SIP Trunk);

8. Retire la alimentación CA de la central Impacta y retire la tapa;
9. La tarjeta madre ICIP 30 68i debe conectarse solamente en la posición OPC3/ICIP (CN2);
10. Conecte los cables de la red LAN y WAN en los respectivos conectores;
11. Organice e identifique los cables de red junto con los demás cables en el DG de la central;
12. Antes de la puesta en marcha del sistema, se debe realizar la confirmación visual de todas las conexiones de cables, módulos, tarjetas y alimentación AC, corrigiendo cualquier eventual falla. La confirmación visual debe efectuarse con el sistema apagado;
13. Recoloque la tapa y conecte la alimentación CA de la central Impacta;
14. Tras la inicialización del sistema, verifique a través del *Programador web/Menú Interfaces/Disposición de placas*, si ninguna tarjeta está programada para utilizar aquel slot;
15. Programe los datos necesarios a través del *Programador web*.

8.1. Recomendaciones técnicas

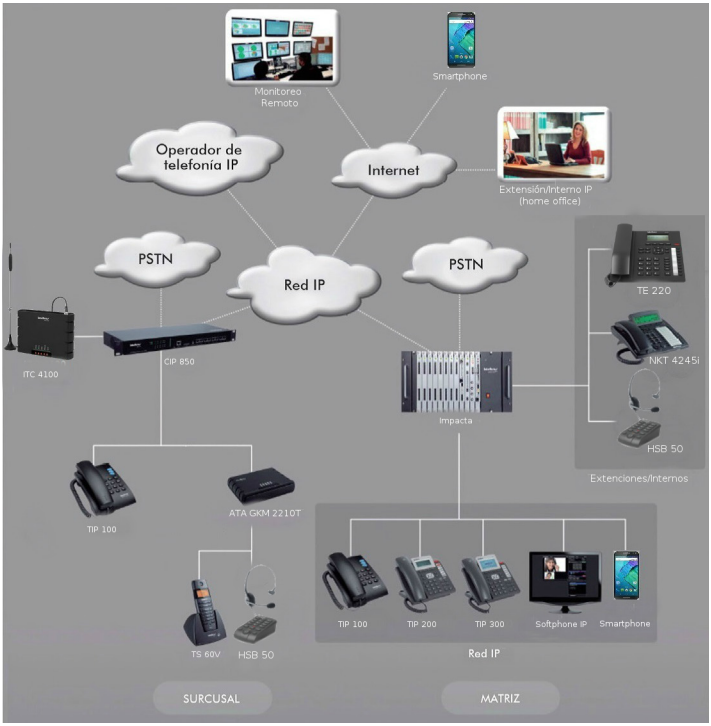
Este sistema utiliza la tecnología VoIP (voz sobre IP) y la calidad del funcionamiento depende de las condiciones de tráfico y priorización de la red a la que el producto está conectado. Para que la calidad de audio de la central sea excelente, la red en la que todo el tráfico de paquetes es transmitido/recibido debe tener banda suficiente. En el caso de anormalidades en las llamadas establecidas, como problemas de audio, verifique antes la situación de la red con el proveedor VoIP.

Las informaciones que deben ser analizadas junto al proveedor de internet son:

- » Garantía mínima (%) del Ancho de Banda en contrato: la velocidad contratada representa la velocidad máxima configurada dentro de la red de su proveedor de Internet. La mayoría de los proveedores de Internet garantizan velocidad mínima del 10% de la banda contratada (entre usuario y proveedor) dentro de su red.
- » Latencia de red: es el tiempo que un paquete lleva para traficar por la red, desde el origen hasta el destino.
- » Velocidad de Descarga: es la velocidad con que los paquetes son recibidos desde Internet.
- » Velocidad de Carga: es la velocidad con que los paquetes son enviados a Internet. Los proveedores de Internet ofrecen, en la mayoría de las veces, velocidad de Carga menor o igual a la velocidad de Descarga.
- » Verificar el número de computadoras en la red.
- » Consultar al proveedor VoIP respecto de cuáles codecs (codificador/decodificador de voz) utilizar y respecto a las configuraciones necesarias en el sistema para una mejor calidad de voz.
- » El envío o recibimiento de Fax depende de la calidad de la señal de su Internet Banda ancha, de la latencia, de la tasa de pérdida de paquetes y de la presencia de los protocolos necesarios en el destino. Así, sólo se puede garantizar el funcionamiento correcto del Fax si esas condiciones son favorables.
- » Se recomienda configurar el sistema de manera que no haya transcodificación en las extensiones/internos SIP (ver *pestaña codec*).
- » Para que las extensiones/internos IP funcionen adecuadamente, el modo de envío DTMF debe ser SIP INFO (ver *pestaña "VoIP General" en el Programador web*).
- » La dirección del servidor DNS configurado debe ser, de preferencia, de un equipo perteneciente a la misma red. El acceso a un DNS externo a la red puede causar problemas de registro de troncales y extensiones/internos, dejando el sistema lento. Se recomienda utilizar servidores DNS con tiempo de respuesta rápido.

8.2. Escenario

Existen muchos escenarios de aplicación de esta nueva tecnología VoIP/SIP en conjunto con las centrales Impacta 68i. Vea a continuación un escenario clásico, en el donde podemos visualizar diversos ambientes conectándose a través de la tarjeta ICIP, con tarjeta codec y Licencias.



Escenario

9. Administración vía navegador web

Con la instalación de la tarjeta ICIP en las centrales Impacta, es posible acceder a la administración de todo el sistema vía navegador web Mozilla Firefox® (consulte la versión compatible en la *Tabla de Compatibilidad Centrales Impacta* disponible en la sección *Descargas* de nuestra página web).

Atención: para acceder a la interfaz del Programador web, configure la computadora de administración con una dirección IP y máscara de subred que estén en la misma red LAN de la central.

Estandar de fábrica LAN:

- Dirección IP: 10.0.0.2
- Máscara de subred: 255.255.255.0
- Gateway por defecto: 10.0.0.1
- Envío de Log: 10.0.0.3

9.1. Escuchar las direcciones IP

La tarjeta ICIP puede ser configurada para obtener la dirección IP automáticamente, vía DHCP. En ese caso, el PABX posibilita una manera del usuario escuchar la dirección IP obtenida. El usuario, desde un teléfono, debe marcar los siguientes comandos:

- *60993*, para escuchar la dirección IP WAN
- *60992*, para escuchar la máscara de red WAN
- *60991*, para escuchar la dirección IP LAN
- *60990*, para escuchar la máscara de red LAN
- *60989*, para escuchar la dirección IP VLAN1
- *60988*, para escuchar la máscara de red VLAN1
- *60987*, para escuchar la dirección IP VLAN2
- *60986*, para escuchar la máscara de red VLAN2
- *60985*, para escuchar la dirección IP VLAN3
- *60984*, para escuchar la máscara de red VLAN3
- *60983*, para escuchar la dirección IP VLAN4
- *60982*, para escuchar la máscara de red VLAN4
- *60981*, para escuchar la dirección IP VLAN5
- *60980*, para escuchar la máscara de red VLAN5

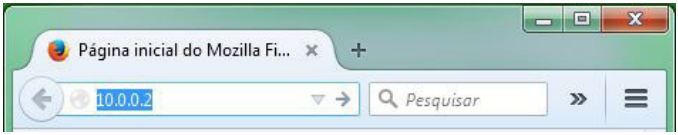
Para configuración manual del número IP y máscara de red, para LAN y WAN, vía teléfono analógico:

- LAN - *14 + IP(10*1*30*17) + # + Mask (255*255*255*0) + # + GW(10*1*30*1) + #
- WAN - *15 + IP(10*1*30*17) + # + Mask (255*255*255*0) + # + GW(10*1*30*1) + #

Obs.: *la configuración del GW (gateway) no es obligatoria. Se puede configurar sólo la IP y la Máscara. Para ello, basta parar en el # después de escribir la máscara y aguardar el mensaje de programación aceptada.*

Atención: la central será reiniciada después de la aceptación del comando.

Abra su navegador web e inserte la dirección de la Placa ICIP en el campo de dirección, por ejemplo, IP 10.0.0.2.



Dirección IP en el navegador

Se abrirá una ventana pop-up de login (si no abre, limpie el caché del navegador o compruebe si hay algún tipo de bloqueador de pop-ups u otro producto similar activo en su ordenador). Inserte el nombre de Usuario y Clave para la autenticación. El estándar de fábrica es:

- **Usuario:** admin
- **Clave:** admin

9.2. Programador web

Tras el procedimiento de autenticación, la pantalla inicial estará accesible al administrador. Seleccione el ítem deseado en el menú a la izquierda y para acceder a cada una de las opciones de administración.

Atención: el proceso de creación y configuración de extensiones/internos y troncales IP es semejante al de las extensiones/internos y troncales analógicas, en el mismo menú de *Configuración >Puertos*.

La misma analogía ocurre para la configuración de Enrutamiento de extensiones/internos y troncales IP, en el menú de *Configuración >Enrutamiento*.

Los menús del *Programador web* son los mismos ya conocidos en el Programador PC, sin embargo fueron creados nuevos menús para la configuración de la tarjeta ICIP, como siguen:

9.3. Sistema

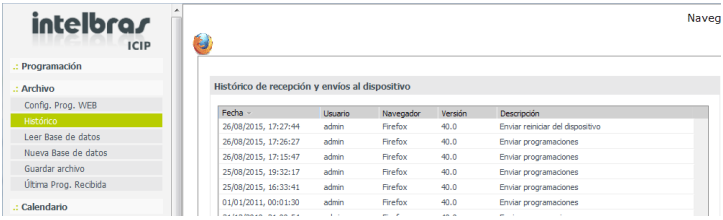
Licencias

Al acceder a este submenú se muestran el estatus y el número de licencias válidas para extensiones/internos IP y troncales IP.

Visualización/confirmación de las licencias

9.4. Historial

Cuando se accede a este submenú, se muestran los registros de logs de algunas operaciones realizadas por los usuarios.



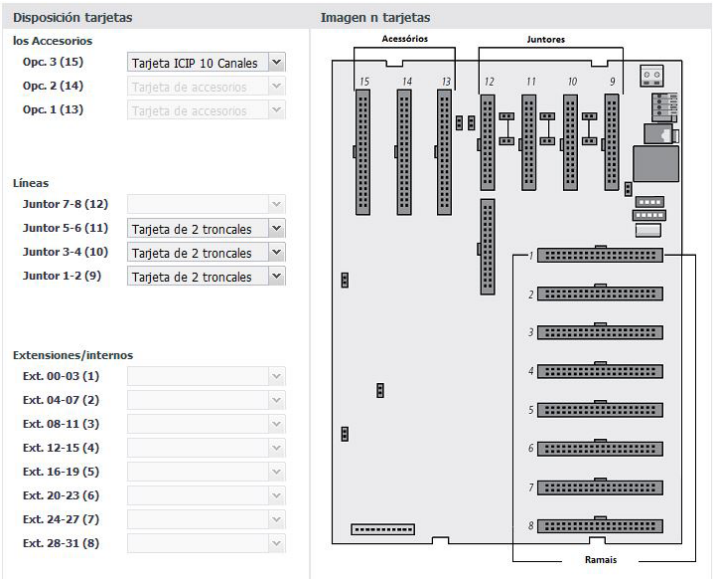
- **Fecha:** presenta la fecha y la hora en la que se produjo la operación.
- **Usuario:** nombre del usuario que realizo la operación.
- **Navegador y versión:** nombre del navegador y la versión utilizada para realizar la operación.
- **Descripción:** describe la operación realizada. Las operaciones que generan log son: Enviar y Recibirr programaciones, Enviar firmware, Enviar reset y Enviar base de datos.

9.5. Interfaces

Disposición de las tarjetas

Al acceder a este submenú se exhibirá un esquema con la cantidad y los dispositivos conectados en los slots del backplane. Verifique si se exhibe el tipo de la tarjeta ICIP instalada en el slot correcto, en caso de no estar exhibida, será necesario realizar la configuración.

1. Seleccione en el menú de tarjetas la opción "Vacío" o presione el botón Limpiar para dejar todos los slots como "Vacío";
2. Confirme esta operación;
3. Seleccione la placa base ICIP 30 para aquel slot (en este ejemplo 30 canales).



Localización/actualización para placa base ICIP 30 68i

9.6. Red

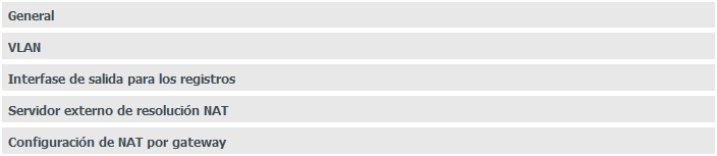
Permite configurar los datos de direccionamiento, parámetros de seguridad y servicios necesarios para que la Placa ICIP pueda comunicarse y ser reconocida por la red local, así como las informaciones para la conexión IP con Internet.

Atención: algunas de estas informaciones pueden obtenerse junto al administrador de red o técnico de informática.

Menú red y sus componentes

General

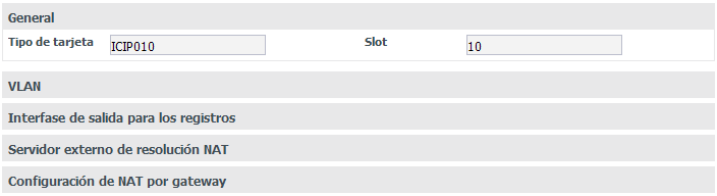
Este submenú presenta las informaciones generales sobre la red y los parámetros disponibles para la configuración, distribuidos en las siguientes pestañas:



Menú Red/Submenú General

General

Presenta las informaciones físicas de la tarjeta para el administrador.

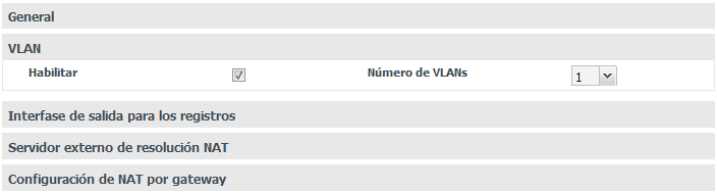


Menú red - General

- » **Tipo de tarjeta:** informa el tipo de placa que está instalada en el sistema.
- » **Slot:** informa en cuál slot del backplane se localiza la tarjeta.

Habilitar VLAN

Esta sección permite habilitar la configuración de la VLAN. La selección de este ítem se reflejará directamente en el menú RED, donde será habilitado un submenú equivalente para configuración. Para saber mas detalles de este servicio consulte la sección VLAN de este manual.



Menú red/Submenú General/Habilitar VLAN

- » **Habilitar:** habilita el ítem VLAN para configurar el servicio y permite seleccionar las VLAN disponibles en la red de la ICIP.
- » **Número de VLAN:** define el número de VLAN que estará disponible para la red del sistema. Son posibles hasta 5 VLAN.

Interfaz de salida para los registros

Se define cual interfaz de red (LAN, WAN o VLAN) será utilizada para el tráfico de salida del sistema como ruta default.

Menú red/Submenú General/Interfaz de salida para los tráficos

En el menú desplegable, seleccione la interfaz de red que será utilizada para los tráficos de salida.

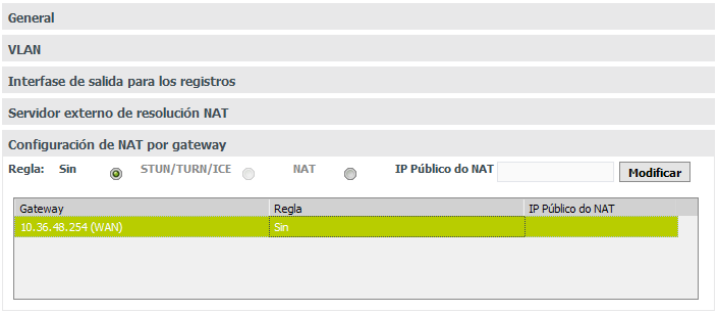
Servidor externo de resolución NAT

El STUN (Session Traversal Utilities for NAT), es un servidor que permite que clientes NAT (ej.: computadoras protegidas por firewall) realicen llamadas telefónicas a un proveedor VoIP que se encuentra fuera de la red local. El servidor STUN permite que los clientes descubran su dirección pública, el tipo de NAT utilizado, y el puerto de Internet asociado al NAT con un puerto local específico. Esta información se utiliza para permitir la comunicación UDP entre el cliente y el provedor VoIP, y entonces establecer la llamada. Sólo espera conexiones en la Interfaz WAN, en el puerto 3478/UDP y 3479/UDP (puertos Default). El servidor STUN es habilitado en el menu Red>General>Habilitar Servicios>Servidor STUN.

- **Servidor STUN:** habilita el uso de esta facilidad.
- **IP o FQDN del servidor ((STUN, TURN, ICE):** define la dirección IP de servidores que auxilian a la central a mantener la comunicación con dispositivos que estén fuera de la red local.
- **Puerto del servidor:** define el puerto del servidor STUN.

Configuración de NAT por gateway

Es posible configurar las opciones de NAT para todos los posibles gateways de la ICIP, como por ejemplo, LAN y WAN primaria y secundaria, 3G. Es posible hacer configuraciones diferentes de NAT para cada gateway, no solo de las rutas estándar, sino también de las rutas estáticas.



Para cada gateway es possible definir:

Regla:

- **Sin:** no realiza el tratamiento del NAT.
- **STUN/TURN/ICE:** utiliza el servidor externo de STUN/TURN/ICE, si está configurado.
- **NAT:** habilita la configuración del campo IP Pública del NAT.
- **IP Pública del NAT:** define la dirección, de IP o FQDN, que el router está utilizando en Internet.

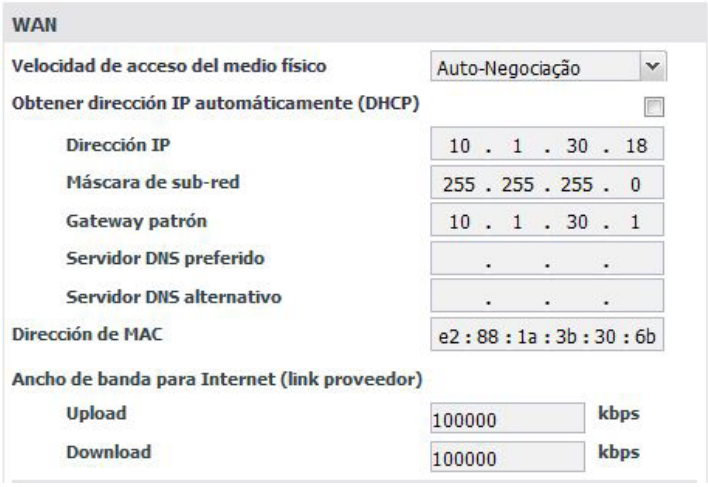
WAN

Este submenú presenta las informaciones de la conexión de la interfaz WAN y los parámetros necesarios para su configuración dentro de la red, distribuidos en las siguientes guías:

Menú Red/Submenú WAN

WAN

Permite la configuración de los parámetros de conexión física y direccionamiento, referentes a interfaz WAN, por tanto es importante consultar el administrador de red y el proveedor de Internet para obtener los datos necesarios.



Red - submenú WAN

» **Velocidad de acceso medio físico:** define la velocidad del modo de transmisión (Auto, Full Duplex o Half Duplex) de los paquetes de datos en la red, posee una relación directa con los dispositivos existentes en la red (cables, hubs, etc.). Se recomienda la opción de Auto negociación, en caso que no haya ninguna indicación del administrador de red.

» **Obtener dirección IP automáticamente (DHCP):** posibilita dos opciones de acceso a red WAN:

  » Seleccionado, el acceso a red WAN será dinámico, es decir, informaciones como, dirección IP, máscara de red, IP del gateway e IP del servidor DNS, serán suministradas por el primer dispositivo de red que implemente un servidor DHCP. Ese equipo puede ser un módem, ruteador, switch o una computadora/servidor conectada en la red.

  » Sin selección, el acceso a la red WAN será estático, es decir, será necesario llenar los campos Dirección IP, Máscara de Red, IP del Gateway, IP de los servidores DNS y velocidades de carga y descarga, de acuerdo con las especificaciones del administrador de red.

» **Dirección IP:** define la dirección IP del puerto WAN en la red en la que se conectará la tarjeta.

» **Máscara de subred:** define el valor de la máscara de subred en la que se conectará la tarjeta.

» **Gateway patrón:** ingrese la dirección IP del ruteador de salida de la red (equipo que interconecta más de una red física).

» **Servidor DNS preferencial y alternativo:** ingrese las direcciones IPs de los servidores de DNS (Domain Name System - Sistema de Nombres de Dominios) de su elección.

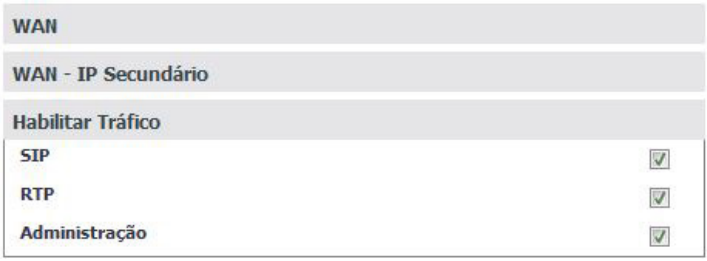
***Obs.:** es bastante común en redes de pequeño y mediano portes que esta dirección IP sea la misma de la dirección de gateway (ruteador de salida).*

» **Dirección MAC:** informe la dirección de MAC para interfaz WAN, si es necesario. Esto es indispensable, cuando no se tiene una MAC configurada el PBX o la tarjeta ICIP se comportan inestables perdiendo comunicación incluso para la programación, en las últimas versiones de FW esta MAC se "auto programa", pues algunos proveedores de Internet solamente permiten la autenticación con la dirección MAC previamente especificada. En otros casos, debe utilizarse la misma dirección MAC de la computadora que estaba autenticada en el proveedor de Internet.

» **Carga y Descarga:** se definen las tasas máximas para la conexión con el proveedor de acuerdo con el enlace contratado. Es importante saber las tasas de carga y descarga con la interfaz WAN disponible, para mantener equilibrada la conexión del enlace y evitar cualquier saturación y consecuente pérdida de calidad.

Habilitar tráfico

Son habilitados los tráficos de paquetes de señalización SIP, RTP (relativos al tráfico de voz) y tráfico administrativo en la red WAN.



Menú Red/Submenú WAN/Habilitar tráfico

- **SIP:** habilita el tráfico de los paquetes de señalización SIP junto a la red WAN configurada.
- **RTP:** habilita el tráfico de los paquetes de señalización RTP junto a la red WAN suministrando un medio uniforme para transmitir datos sujetos a "problemas" de tiempo real (audio, vídeos,…).
- **Administración:** habilita el tráfico de administración en la red WAN. Esto puede ser utilizado para evitar el acceso a las configuraciones de administración por personas no autorizadas.

QoS

Permite especificar prioridades para el paquete o clase de tráfico. El QoS busca una mejoría de la calidad de la comunicación priorizando algunos tipos de datos en detrimento de otros, de acuerdo con una clasificación previa de los mismos, y se vuelve extremamente útil en condiciones de embotellamiento de tráfico en la interfaz de salida de estos datos (por ejemplo, el puerto de conexión con el ruteador para Internet).

Atención: la tarjeta ICIP marca los paquetes de datos, tocando a los activos de red (switches y ruteadores) dar prioridad al tráfico de voz.

Menú Red/Submenú WAN/QoS

Habilitar QoS de llamada 3

En los campos indicados en esta pantalla hay la opción de seleccionar dos modos de señalización de los paquetes (DSCP o TOS) y su prioridad. Estos parámetros serán utilizados para QoS y son insertados en el encabezado IP de todos los paquetes SIP, RTP y de administración transmitidos.

La elección entre uno de los modos depende de un análisis de la red, de la compatibilidad de los dispositivos con el modo seleccionado y de la forma como están configurados los ruteadores y switches para priorizar el tráfico.

El modo DSCP (Differentiated Services Code Point) prioriza el paquete de acuerdo con la marcación en el paquete recibido. Esos paquetes se distinguen en clase de tráfico de acuerdo con las informaciones de retraso, tasa de procesamiento y confiabilidad anexadas al paquete. Para esto, utiliza 6 bits del encabezado, dando 64 diferentes posibilidades para códigos de prioridad.

En el modo TOS (Type of Service), paquetes que entran en la red por medio de la ICIP son encaminados de acuerdo con la prioridad definida. Para esto, utiliza 3 bits del encabezado dando 8 diferentes posibilidades para códigos de prioridad, siendo 0 la prioridad más baja.

Cuanto mayor el valor, mayor será la prioridad en el tratamiento y uso de los recursos de la red.

Atención:

- Los modos DSCP y TOS entrarán en operación, conforme el comportamiento definido por la IETF.
- Cuando la tasa de tráfico entrante en un equipo de red es superior a la tasa de tráfico saliente del mismo (Ancho de banda), ocurre un embotellamiento en la red. Durante estas condiciones, los cuadros marcados con mayor prioridad reciben tratamiento preferencial y son entregados antes de los cuadros con menor prioridad.
- Hay que recordar que es con base en estos parámetros que los equipos de red priorizan el tráfico de voz frente al tráfico de datos.

SIP

Al lado del campo SIP es posible seleccionar el modo de QoS:

- TOS con valor de 0 a 7, que representa la prioridad del paquete.
- DSCP con valor de 0 a 63, que representa la prioridad del paquete.

RTP

Al lado del campo RTP es posible seleccionar el modo de QoS:

- TOS con Valor de 0 a 7, que representa la prioridad del paquete.
- DSCP con Valor de 0 a 63, que representa la prioridad del paquete.

Administración

Al lado del campo Administración es posible seleccionar el modo de QoS:

- TOS con Valor de 0 a 7, que representa la prioridad del paquete.
- DSCP con Valor de 0 a 63, que representa la prioridad del paquete.

Atención: las modificaciones efectuadas serán válidas solamente en equipos que se configuren del mismo modo, de lo contrario, el tráfico será encaminado de acuerdo con el comportamiento patrón de la IETF o conforme alguna configuración específica en el equipo siguiente.

Rutas

Esta configuración permite definir rutas específicas para subredes en la red WAN, creando caminos predeterminados, donde las informaciones pueden ser direccionadas hasta un host u otra red específica.

Menú Red/Submenú WAN/Rutas

- **Destino:** son informadas las direcciones IPs y la máscara (direcciones IP/net-mask tipo CIDR) del destino del enrutamiento.
- **Gateway:** ingrese la dirección IP del ruteador, por medio del cual el tráfico fluirá para la subred de destino.
- **Carga y Descarga:** se definen las tasas máximas para la conexión con la interfaz de destino. Es importante saber las tasas de carga y descarga con la interfaz de destino disponible, para mantener equilibrada la conexión del enlace y evitar cualquier saturación y consecuente pérdida de calidad.

LAN

Este submenu presenta la información de la conexión de la interfaz LAN y los parámetros necesarios para su configuración dentro de la red (iguales a los de la WAN), distribuidos en las siguientes pestañas:

Menú Red/Submenú LAN

Configuración de la IP secundaria para LAN y WAN

La configuración de la IP Secundaria permite configurar una red diferente de la principal, tanto para la interfaz LAN como para la WAN. Con ello es possible alternar entre redes diferentes simplemente cambiando el puerto en el que está conectado el cable de la ICIP en el switch.

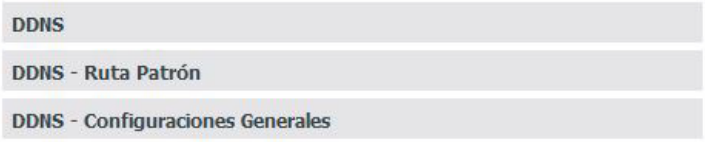
Obs.: *estas redes no funcionan al mismo tiempo. Por ejemplo: la interfaz LAN principal está configurada con una red A y la interfaz LAN secundaria está configurada con una red B. Si el cable de red está conectado a la red A, valen las configuraciones de la interfaz LAN principal. Si el cable de red está conectado a la red B, valen las configuraciones de la interfaz LAN secundaria.*

DDNS

Con el DDNS (Dynamic Domain Name System) es posible vincular la central a un nombre de dominio en Internet (dirección DNS). Ese recurso es útil, por ejemplo, cuando la central no posee una dirección fija en Internet.

Antes de configurar este servicio, hay que crear una cuenta de servicio DDNS en un proveedor de DDNS como el *www.no-ip.com.*

El proveedor de servicio DDNS suministrará un login y una clave tras el registro.



Menú Red/Submenú DDNS

DDNS - Ruta patrõn

Permite la configuración de los parámetros del servidor de DDNS. Para el correcto funcionamiento es necesario que todos los campos estén configurados. Por tanto es importante consultar el administrador de red para obtener los datos necesarios.

Menú Red/Submenú DDNS/DDNS

- » **Dirección**: ingrese la dirección IP o el nombre registrado en el DDNS, ej.: icip.dyndns.org.
- » **Servidor:** define el servidor que será utilizado (No-IP, DynDNS).
- » **Habilitar DDNS para ruta patrón:** habilita la actualización del DDNS para la interfaz de salida para Internet.
- » **Login**: inserte el login de usuario en el DDNS.
- » **Clave**: inserte la clave de usuario en el DDNS.

Menú Red/Submenú DDNS/Configuraciones Generales

Configuraciones generales

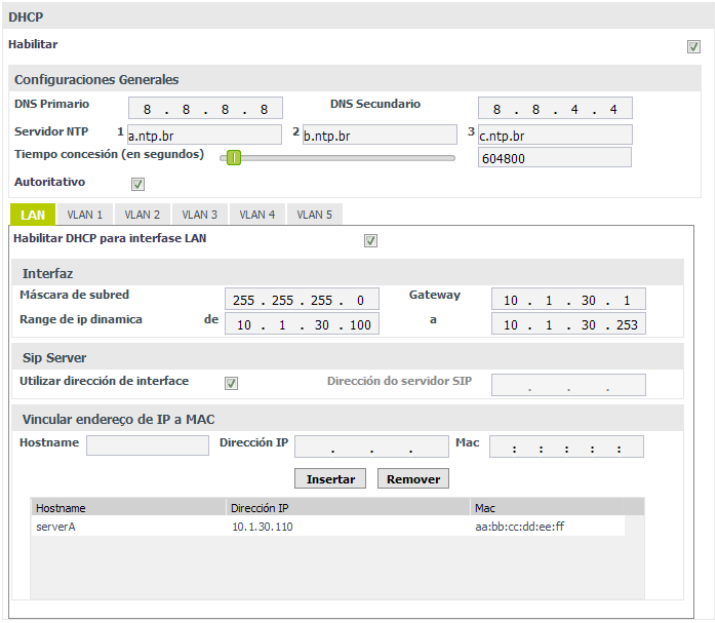
» **Tiempo de actualización en el servidor (seg):** define el tiempo de actualización de la información en el servidor.

Atención: para buscar la dirección IP que la tarjeta tiene disponible en Internet, este servicio consulta vía HTTP un servidor en Internet que retorna la dirección IP que la tarjeta ha accedido a Internet. Por esto es necesario que la ICIP tenga acceso a Internet sin filtros en el puerto 80, esto incluye filtros como firewall y proxy autenticado.

Servidor DHCP

El DHCP, Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host), es un protocolo de servicio TCP/IP que ofrece una configuración dinámica de terminales, con concesión de direcciones IP de host, Máscara de subred, Default Gateway (Gateway Estándar), entre otros. La tarjeta ICIP posee un servidor DHCP embebido. El principal motivo es que es posible hacer el autoaprovisionamiento de la dirección del servidor SIP para los teléfonos IP.

Esta funcionalidad no sale habilitada de fábrica.



Configuraciones generales (mismo estilo de Interfaz, Sip Server, Vincular dirección IP a MAC)

Configuraciones generales

- **Habilitar:** habilita el servidor DHCP.
- **DNS Primario:** define la dirección IP del servidor DNS primario.
- **DNS Secundario**: define la dirección IP del servidor DNS secundario.
- **Servidor NTP 1:** define la dirección IP del servidor NTP 1.
- **Servidor NTP 2**: define la dirección IP del servidor NTP 2.
- **Servidor NTP 3:** define la dirección IP del servidor NTP 3.
- **Tiempo concesión (en segundos):** define el tiempo en segundos de la concesión de las direcciones IP.
- **Autoritativo:** define si el servidor es autoritativo.
- **Habilitar DHCP para interfaz LAN:** habilita el servidor DHCP para la interfaz LAN.

Interfaz

- **Máscara de subred:** define la máscara de la subred.
- **Gateway:** define la dirección IP del Gateway.
- **Range de IP dinámica:** define el intervalo de direcciones IP que el servidor concederá a los dispositivos de la red.

Sip Server

- **Utilizar la dirección de la interfaz:** con esta opción marcada, utiliza la misma dirección de la interfaz para el servidor SIP.
- **Dirección del servidor SIP:** si la opción anterior no está marcada, la dirección IP del servidor SIP deberá ser informada en este campo.

Vincular dirección IP a MAC

- **Hostname:** nombre del dispositivo en la red.
- **Dirección IP:** dirección IP que será concedida al dispositivo.
- **MAC:** dirección MAC del dispositivo para el que se concederá la dirección IP.
- **Introducir y Eliminar:** utilice estos botones para introducir los registros en la tabla.

Obs.: *considere esta misma información si quiere configurar las interfaces VLAN de 1 a 5.*

NTP

El NTP (Network Time Protocol) es un protocolo de sincronización de relojes en Internet, con esto es posible mantener la hora de la central correcta y sincronizada con los principales sistemas de Internet.

Atención: la configuración del servicio de NTP sólo será posible tras habilitar este submenú en el ítem Habilitar servicios.

Menú Red/Submenú NTP

NTP

En este sub-menú es posible configurar los servidores NTP que van a mantener actualizadas las informaciones de hora y fecha del sistema.

Atención: al introducir los servidores de NTP compruebe que las configuraciones de huso horario y horario de verano son correctas.

Menú Red/Submenú NTP/NTP

» **Habilitar:** habilita o deshabilita el servidor NTP.
» **Servidor NTP Primario:** ingrese la dirección IP o el nombre del servidor NTP primario.
» **Servidor NTP Secundario:** ingrese la dirección IP o el nombre del servidor NTP secundario.
» **Servidor NTP Terciario:** ingrese la dirección IP o el nombre del servidor NTP terciario.
» **Huso Horario:** define el huso horario.
» **Horario de verano:** define si utiliza o no el horario de verano.

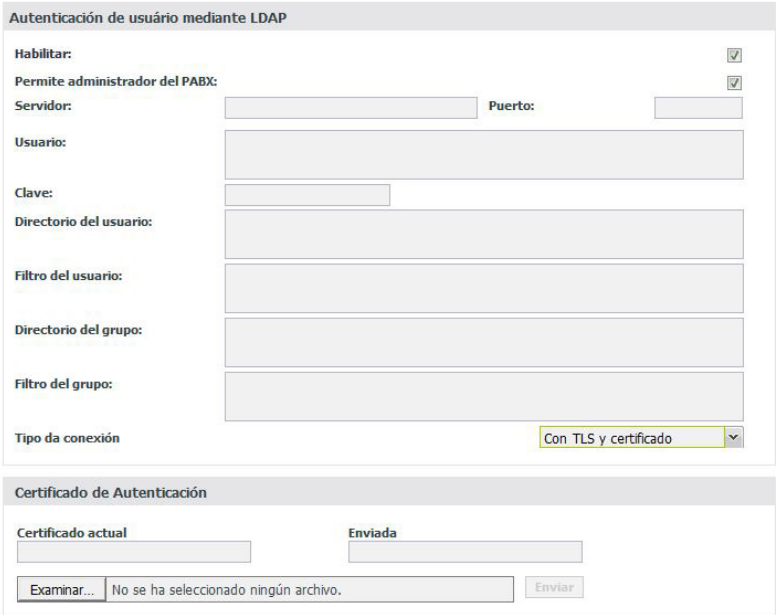
Atención: la dirección registro.br mantiene servidores NTP disponibles para la sincronización con la hora oficial brasileña. Las direcciones de estos servidores NTP son: *a.ntp.br, b.ntp.br* y *c.ntp.br.* En caso de no contar con servidores NTP en su red, utilícelos. Para mayores informaciones visite la dirección *http://www.ntp.br.*

Autenticación LDAP

La autenticación de usuarios a través de LDAP (*Lightweight Directory Access Protocol*) se utiliza para centralizar el control de las contraseñas de usuario, utilizando un servidor de autenticación que proporciona acceso a través de LDAP. Este servidor puede ser el mismo que la empresa utiliza para autenticar sus usuarios. Así que se active la autenticación vía LDAP, el acceso Via usuario y contraseña existente en el PABX será deshabilitado y, dependiendo de la configuración realizada, pasará a ser ejecutado solamente por medio del usuario *admin*.

Cada usuario que se autentica a través de LDAP también se debe crear en la PBX o se debe crear un usuario con el nombre de un grupo en el que uno o más usuarios LDAP pertenecen y habilitar la opción de grupo LDAP, accediendo al menú Sistema> Acceso de usuario. El nombre de usuario en la central debe ser idéntico al nombre de usuario del servidor LDAP y la contraseña debe ser diferente de la central, esta contraseña a su vez no será utilizada cuando la autenticación a través de LDAP está habilitada, pero sólo se utiliza para el acceso sin LDAP. La contraseña para el usuario de LDAP se almacena sólo en el servidor LDAP. Para un correcto funcionamiento, debe configurar la central con los datos del servidor de autenticación y establecer permisos y la categoría de cada usuario.

La configuración de autenticación del servidor LDAP puede ser realizada accediendo programador Web al menú *Red > Autenticación LDAP.*



Autenticación de usuarios a través de LDAP

» **Habilitar:** habilita la autenticación de usuario en un servidor LDAP. Al habilitar los otros campos existentes deben ser llenados.
» **Permitir administrador del PABX:** permite al usuario por defecto "*admin*" autenticar al PBX incluso con LDAP habilitado. La contraseña utilizada es la contraseña establecida en la central. Este ajuste se debe utilizar mientras estamos configurando el LDAP, que permite la autenticación en el PBX y cambiar la configuración incorrecta.
» **Servidor:** contiene el nombre o IP del servidor para la autenticación.
» **Puerto:** contiene el puerto del servidor LDAP, valor por defecto es 389.
» **Usuario:** usuario necesario para acceder al servidor LDAP. La opción no es obligatoria, dependiendo de cómo se haya configurado el servidor.
» **Clave:** clave de usuario requerida para acceder al servidor LDAP. La opción no es obligatoria, dependiendo de cómo se haya configurado el servidor.
» **Directorio del usuario:** debe contener el nombre del directorio raíz donde se autentican los usuarios almacenados. Los usuarios pueden ser organizados en otras carpetas desde este directorio.
» **Filtro del usuario:** debe contener una opción que se utiliza para filtrar el nombre de usuario.
» **Directorio del grupo:** debe contener el nombre del directorio raíz donde Son almacenados los grupos que se autentican. Los grupos pueden ser organizados en otras carpetas desde este directorio.
» **Filtro del grupo:** debe contener un campo que se utiliza para filtrar el nombre del grupo.
» **Habilitar TLS:** habilitar el uso de encriptación de datos LDAP. El servidor debe estar configurado para utilizar encriptación.

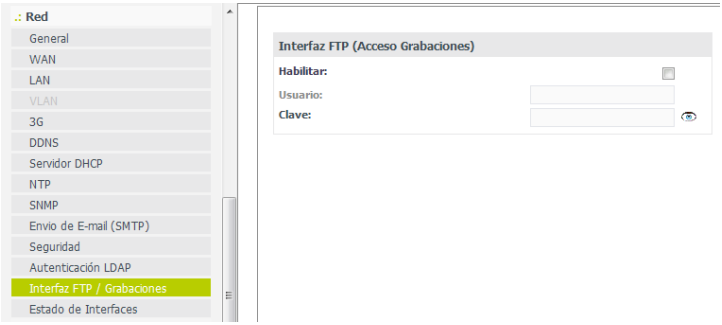
Grupo de usuarios LDAP

Si el método de autentificación utiliza un grupo de usuarios, se debe registrar un usuario y marcar la opción Grupo LDAP en Usuarios>Acceso de usuario.

Menú Usuarios/Submenú Acceso de usuarios

Interfaz FTP/Grabaciones

Permite que la aplicación Grabador de llamadas se conecte al PABX.

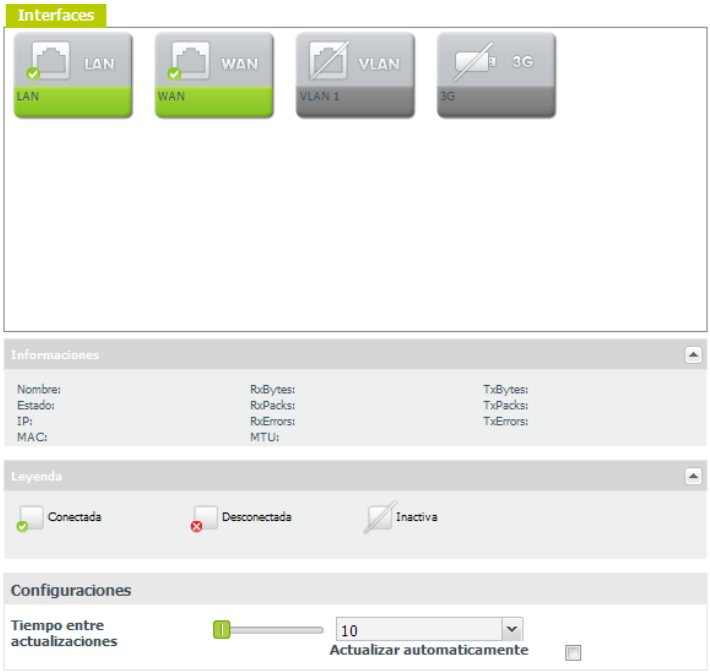


Menú Red/Submenú Interfaz FTP/Grabaciones

» **Habilitar:** habilita o deshabilita el acceso FTP para la aplicación de grabación.
» **Usuario:** define el nombre del usuario.
» **Contraseña:** define la contraseña del usuario.

Estado de las interfaces

Esta pantalla presenta la información de todas las interfaces de red de la central.



Menú Red/Submenú Estado de Interfaces

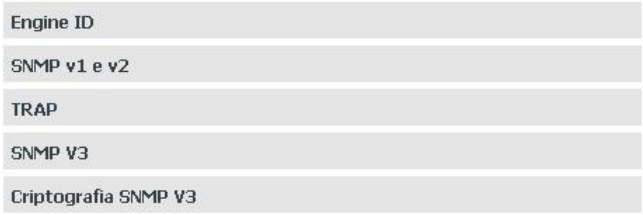
- » **Información:** presenta la información de la interfaz seleccionada: Nombre, Estado, IP, MAC, RxBytes, RxPacks, RxErrors, MTU, TxBytes, TxPacks, TxErrors.
- » **Leyenda:** presenta la leyenda de las imágenes: Conectada, Desconectada o Inactiva.
- » **Tiempo entre actualizaciones:** define el tiempo para actualizaciones automáticas de la página.
- » **Actualizar automáticamente:** habilita o deshabilita la actualización automática de la página.

SNMP

El SNMP (Simple Network Management Protocol) es un protocolo de administración de redes TCP/IP, de la capa de aplicación, que facilita el intercambio de informaciones entre los dispositivos de red. La utilización de este protocolo en la ICIP posibilita a los administradores monitorear y administrar su desempeño en la red, así como, localizar y solucionar eventuales problemas, a través de softwares dedicados a esta finalidad.

Este submenú permite configurar los parámetros necesarios para la administración de la ICIP a través de este protocolo.

Atención: la configuración del servicio SNMP para el sistema sólo será posible tras habilitar este submenú en el ítem *Habilitar servicios*.



Menú Red/Submenú SNMP

Engine ID

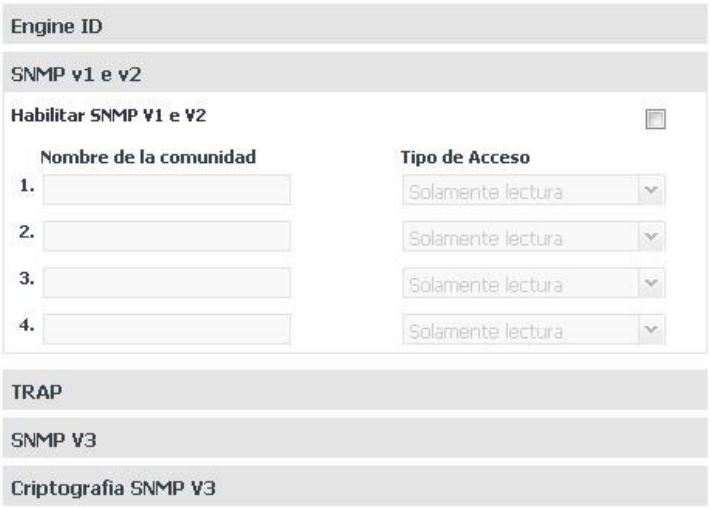
Define que *Engine ID* será utilizado por el sistema, si el estandar o un personalizado. El *Engine ID* es un identificador único para cada equipo de red y es utilizado solamente para identificación, no para direccionamiento.

Menú Red/Submenú SNMP/Engine ID

» **Utilizar estandar:** seleccionado, el Engine ID utilizado será el patrón del sistema.
» **Ajustado por el Administrador [80661A04]:** estará accesible cuando la opción de *Engine ID* estandar no esté. El administrador debe informar el Engine ID personalizado (solo caracteres hexadecimales).

SNMP v1 y v2

En este sub-menú se configuran las comunidades y los privilegios de acceso a las informaciones de los datos y desempeño de la ICIP dentro de la red. Así, el administrador, a través de un software de administración SNMP, puede acceder a comunidades con diferentes niveles de informaciones.



Menú Red/Submenú SNMP/SNMP v1 y v2

» **Habilitar SNMP V1 y V2:** habilita la creación de comunidades y la configuración de los privilegios.
» **Nombre de la comunidad:** se define el nombre de la comunidad para acceso del administrador SNMP.
» **Tipo de acceso:** se definen los privilegios relativos a la lectura y escrita de la comunidad por el administrador SNMP.

TRAP

En este sub-menú se configuran el envío de mensajes, con informaciones de alerta relativas a eventos ocurridos en la ICIP, a través de las comunidades asociadas. El administrador entonces, a través de un software de administración SNMP, podrá tratar el evento adecuadamente.

Menú Red/Submenú SNMP/TRAP

- » **Habilitar el envío de TRAP:** habilita el envío de traps del sistema para el administrador SNMP.
- » **Versión:** se define la versión de SNMP que los traps utilizarán: V1 o V2c.
- » **Tipo de notificación:** presenta las opciones de notificación para la versión de SNMP seleccionada:
- » **Trap:** mensajes de alerta a los administradores (gerentes de red) sobre eventos que han ocurrido en la ICIP;
- » **Inform:** utilizado para notificar cuando un evento fue confirmado.
- » **Comunidad:** entre con el nombre de la comunidad para acceso del administrador SNMP al evento ocurrido.
- » **Destino:** se define el responsable por recibir las notificaciones de los traps del sistema.

SNMP V3

En este sub-menú el SNMP V3 dispone los servicios de seguridad, a través de las opciones de autenticación por *Usuario* y *privacidad*, además de los privilegios de acceso (como en las versiones v1 y v2) y las informaciones de los datos y desempeño de la ICIP dentro de la red.

Así, el administrador debe utilizar un usuario y una clave para acceder a las informaciones.

Menú Red/Submenú SNMP/SNMP V3

- **Habilitar SNMP v3**: habilita los servicios de autenticación y privacidad por usuario.
- **Usuario:** se define un usuario como identificador para el control de acceso a la administración de la base de datos MIB (Management Information Base).
- **Tipo de acceso:** se definen los privilegios relativos a lectura y escritura del usuario por el administrador SNMP.
- **Modo:** seleccione el nivel de seguridad de autenticación y encriptación:
  - **noAuthNoPriv:** sin autenticación y sin privacidad;
  - **authNoPriv:** autenticado y sin privacidad;
  - **authPriv:** autenticado y con privacidad;
- **Tipo de Clave:** seleccione el algoritmo de criptografía MD5 (128 bit) o el SHA (160 bit) para autenticar los usuarios.
- **Clave:** se define la clave de acceso del usuario.

Encriptación SNMP V3

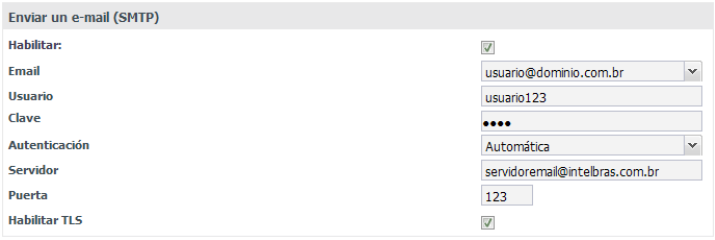
En este sub-menú el SNMP V3 dispone el servicio de seguridad de los mensajes a través de la selección de un algoritmo criptográfico. Esto garantiza la privacidad de las informaciones y evita el acceso por fuentes no autorizadas.

Menú Red/Submenú SNMP/Criptografía SNMP V3

- **Tipo de encriptación:** seleccione el algoritmo de privacidad con el que desea cifrar los mensajes SNMP:
  - **AES (Advanced Encryption Standard):** algoritmo más reciente.
  - **DES (Data Encryption Standard):** algoritmo antiguo.
- **Clave de encriptación:** se define la clave llave para la criptografía.

Envío de email (SMTP)

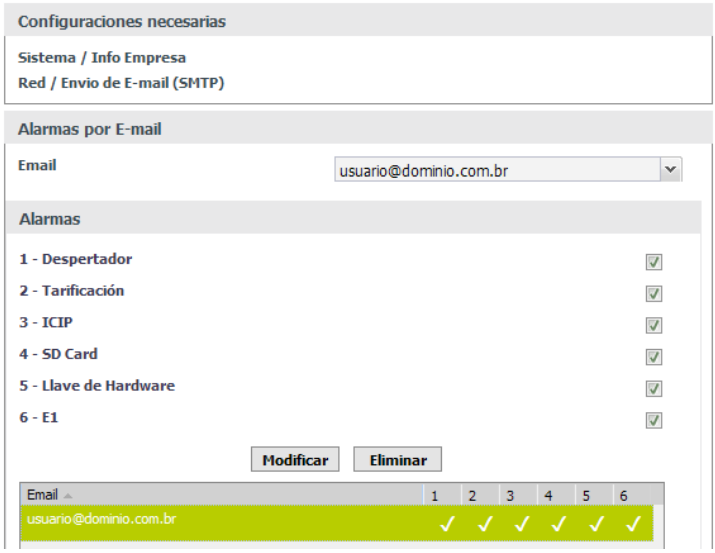
Esta pantalla presenta las configuraciones para que la central pueda enviar emails:



Menú Red/Submenú Envio de E-mail (SMTP)

- **Habilitar:** habilita o deshabilita el envío de emails.
- **Email:** define la dirección de email que será utilizada para enviar emails.
- **Usuario:** define el nombre de usuario de la cuenta de email.
- **Contraseña:** define la contraseña de la cuenta de email.
- **Autenticación:** define el tipo de la autenticación en el servidor de email:
  - Ninguna
  - Automática
  - Contraseña normal
- **Servidor:** dirección del servidor de email.
- **Puerto:** puerto del servidor de email.
- **Habilitar TLS:** habilita o deshabilita la criptografía TLS.

Una aplicación para este servicio de envío de email es la notificación de algunas alarmas producidas en la central. Su configuración se puede realizar en Mantenimiento>Alarmas por email.



Menú Mantenimiento/Submenú Alarmas por email

» **Despertador:** despertó/no despertó/no atendió/no estaba libre.
» **Registro de Llamadas:** buffer de registro de llamadas consiguiendo la capacidad máxima.
» **ICIP:** Tarjeta ICIP inicializada/no inicializada.
» **E1:** pérdida de sincronismo.
Obs.: *es necesario configurar la información de la empresa en Sistema>Información de la empresa.*

Menú Sistema/Información de la empresa

Seguridad

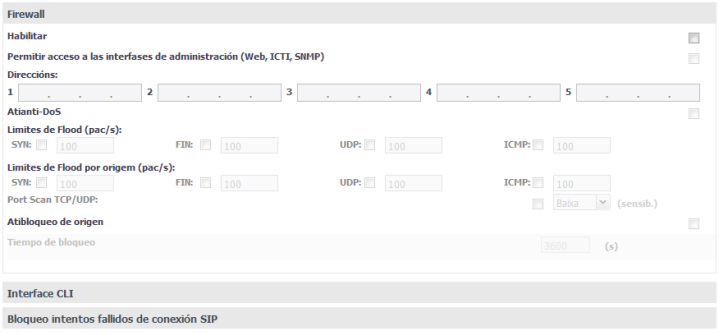
En este menú se pueden encontrar las configuraciones de seguridad de la tarjeta ICIP.

Menú Red - Submenú Seguridad

Firewall

Este sub-menú posibilita restringir el acceso de determinados IPs a funciones de administración del PABX, como el acceso al SNMP, Programador web e ICTI, y también la detección y bloqueo de intentos de DDoS (Distributed Denial of Service) y Port Scan.

Menú Red/Submenú Seguridad/Firewall



Menú Red/Submenú Seguridad/Firewall

» **Habilitar:** habilita o deshabilita el Firewall.
» **Permitir acceso a interfaces de administración (web, ICTI, SNMP):** permite la configuración de acceso a las funciones de administración por determinados IPs.
» **Dirección:** define cuáles direcciones IPs pueden acceder a los servicios de administración del PABX.

» **Activar anti-DoS:** habilita algunos filtros con los cuales es posible prevenir algunos tipos comunes de ataque de denegación de servicio, en que personas mal intencionadas pueden intentar denegar el servicio de la ICIP, por agotamiento de recursos, como cantidad de conexiones simultáneas o ataques en masa (flood). Además es posible configurar el bloqueo de intentos de portscan.

» **Campo:**
  » Límite de SYN Flood.
  » Límite de FIN Flood.
  » Límite de UDP Flood.
  » Límite de ICMP Flood.

Estos campos de los filtros, pueden ser seleccionados y configurados para limitar el número máximo de paquetes de cada tipo que la ICIP aceptará por segundo, siendo estos paquetes de cualquier origen. Cuando la cantidad instantánea de paquetes haya sobrepasado el valor definido, la ICIP iniciará inmediatamente la función de bloqueo. El valor patrón es 100.

» **Campo:**
  » Límite de SYN Flood por origen.
  » Límite de FIN Flood por origen.
  » Límite de UDP Flood por origen.
  » Límite de ICMP Flood por origen.

Estos campos de los filtros pueden ser seleccionados y configurados para limitar el número máximo de conexiones de cada tipo que la ICIP aceptará por segundo de un determinado IP. Cuando la cantidad instantánea de conexiones haya sobrepasado el valor definido, la ICIP iniciará inmediatamente la función de bloqueo. El valor patrón es 100.

» **Port Scan TCP/UDP:** activa la detección de intentos de portscan en la ICIP. Portscan es el nombre dado a la técnica de escanear los puertos abiertos en un dispositivo de red, para determinar cuales servicios este dispositivo dispone. Con esta opción, es posible detectar un dispositivo realizando portscan en la ICIP. La sensibilidad indica la rapidez con que el firewall identificará un posible portscan. Con la sensibilidad Alta, el firewall considerará un portscan a la menor señal de un intento, ya la sensibilidad Baja hará el firewall más conservador al determinar un portscan. En el caso se identifique una dirección por hacer un portscan, la ICIP bloqueará los intentos de conexión de esta dirección. En el caso la opción "Activar bloqueo del origen" esté seleccionada, la dirección identificada será bloqueada por el tiempo determinado en "Tiempo de bloqueo".

» **Activar bloqueo del origen:** seleccionada, las direcciones IP que caigan en la regla de límite de paquetes por origen, tendrán todos los intentos de conexión bloqueados durante el tiempo especificado en Tiempo de bloqueo.

Interfaz CLI

La interfaz CLI es un medio de conectarse a la ICIP vía SSH. Esta interfaz es la misma utilizada anteriormente, donde el usuario consigue conectarse vía SSH al puerto 16022 con el usuario icip y la contraseña icip1.0. Ahora es posible configurar el usuario y la contraseña vía programador web.

Menú Red/Submenú Seguridad - Interfaz CLI

» **Habilitar:** habilita o deshabilita la interfaz CLI.
» **Usuario:** define el nombre de usuario.
» **Contraseña:** define la contraseña de usuario.

Después de configurar el usuario y la contraseña y enviar la programación, abra el terminal SSH, informe la IP de la central y el puerto 16022. Para autentificar, escriba el usuario y contraseña registrados anteriormente. Escriba el comando help para visualizar los comandos disponibles:

ICIP>help

hardware_status

call_status

version

config

log

dns_latency

ping

traceroute

interfaces

route

top

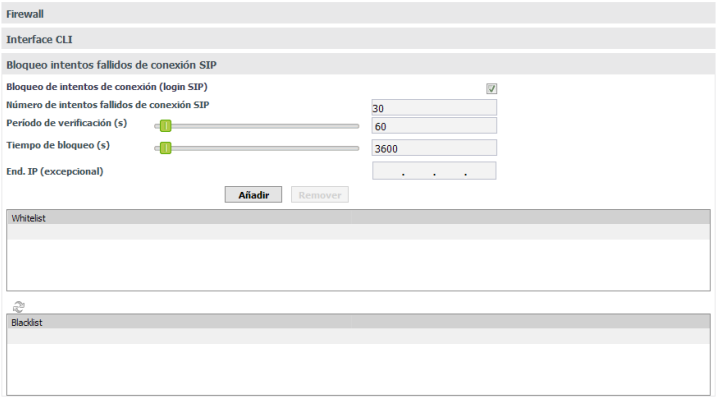
ps

enable_debug

exit

Bloqueo intentos de login SIP fallo

Esta es una herramienta de seguridad de datos para accesos no autorizados, implantada en el sistema para garantizar su fiabilidad. Si durante la autentificación del login, éste no es reconocido por el sistema, el usuario puede tener algunos intentos más antes de recibir un mensaje de bloqueo, o también puede ser configurada una lista de IP que no serán analizadas por esta regla, estando libres de bloqueo.



Menú Red/Submenú Seguridad/Bloqueo intentos de login SIP fallo

» **Habilita bloqueo de intentos de login SIP fallo:** habilita el servicio de verificación de la autentificación de los logins de los usuarios en el sistema.

» **Número de intentos de login SIP fallo:** define el número máximo de intentos con login incorrecto.

» **Periodo de verificación (segundos):** define un período de tiempo dentro del que se analiza el número de intentos de login. Si el número excede el valor configurado en el campo Número de intentos de login fallo, la dirección IP que está intentando el login será bloqueada.

» **Tiempo de bloqueo (segundos):** define el período en el que se mantiene el bloqueo de la IP origen de los logins incorrectos.

» **Dir. IP (Excepción):** permite definir una dirección IP que no es analizada por las reglas, estando libre de bloqueo. Informe las direcciones IP deseadas y utilice los botones Añadir y Eliminar para administrarlos.

» **Whitelist:** presenta la lista de las direcciones IP, configurada por medio del campo Dir. IP (Excepción), que no será analizada por las reglas de bloqueo.

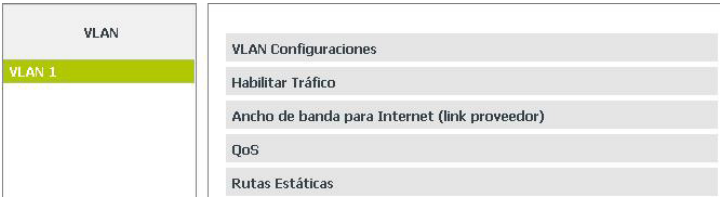
» **Blacklist:** presenta la lista de las direcciones IP bloqueadas.

VLAN

Este submenú presenta las informaciones de las múltiples interfaces VLAN soportadas y los parámetros necesarios para su configuración dentro de la red.

Con esta función, la interfaz de red puede ser segmentada en múltiples VLANs (1 a 5) para reducir las colisiones por broadcast y mejorar la eficiencia.

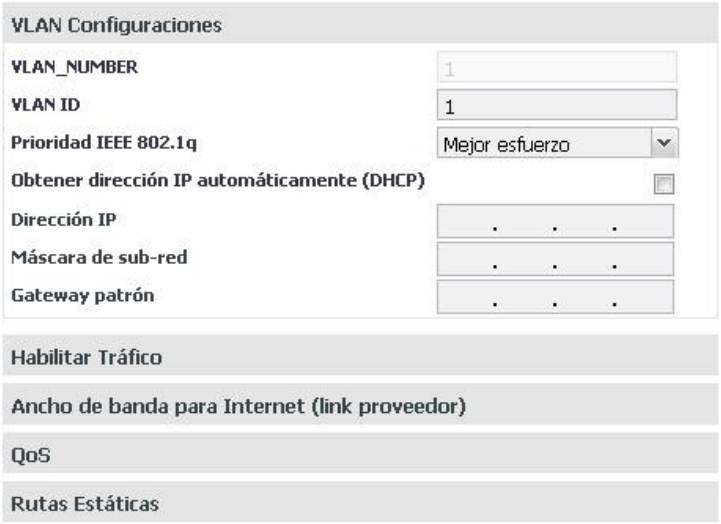
Atención: la configuración de la VLAN sólo será posible tras habilitar este submenú en el ítem Habilitar servicios.



Menú red - VLAN

VLAN Configuraciones

Permite la configuración de los parámetros de prioridad de conexión y direccionamiento, referentes a interfaz VLAN con la red local. Por lo tanto, es importante consultar al administrador de red para obtener los datos necesarios.



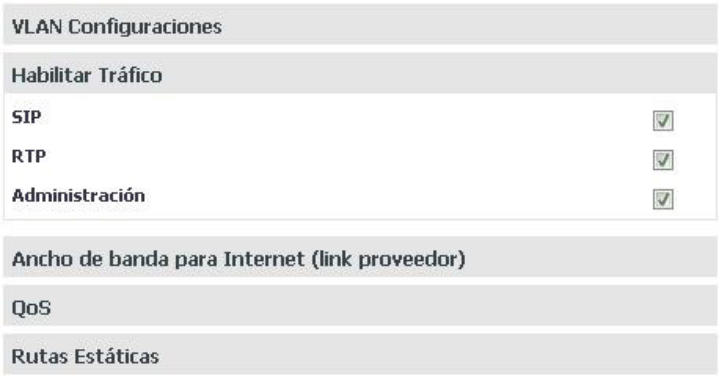
Menú Red/Submenú VLAN/VLAN Configuraciones

- **VLAN_NUMBER:** presenta el número de la VLAN en la red.
- **VLAN ID:** permite la inclusión de un identificador para la VLAN. Los valores válidos son del 1 al 4096.
- **Prioridad IEEE 802.1q:** dispone de 8 niveles de prioridad ordenados de la menor prioridad (Background) hacia la mayor prioridad (Administración de red). Estos niveles son utilizados para definir la prioridad del tráfico, de acuerdo con los tags (etiquetas) de prioridad, añadidas a los cuadros (frames) de las VLANs, durante su direccionamiento en un segmento de red (subred). Cuando la tasa de tráfico entrante en un equipo de red es superior a la tasa de tráfico saliente del mismo (ancho de banda), ocurre un embotellamiento en la red. Durante estas condiciones, los cuadros marcados con mayor prioridad reciben tratamiento preferencial y son entregados antes de los cuadros con menor prioridad.

  Atención: para que se implemente este servicio, los dispositivos conectados a la ICIP deben poseer soporte a marcación (tag) de prioridad en el rótulo de VLAN 802.1q del cuadro Ethernet, para que sean analizados, clasificados, priorizados y puestos en cola, de acuerdo con su marcación de prioridad.
- **Obtener dirección IP automáticamente (DHCP):** dispone 2 opciones de acceso a red VLAN:
  - Seleccionado, el acceso a la red VLAN será dinámico, es decir, informaciones como dirección IP, máscara de red e IP del gateway, serán suministradas por el primer dispositivo de red que implemente un servidor DHCP. Ese equipo puede ser un módem, ruteador, switch o una computadora/servidor conectado en la red.
  - No seleccionado, el acceso a la red VLAN será estático, es decir, será necesario llenar los campos: Dirección IP, Máscara de red e IP del Gateway, de acuerdo con las especificaciones del administrador de red.
- **Obtener dirección IP automáticamente (DHCP):** sin selección.
- **Dirección IP:** define la dirección IP de la interfaz VLAN.
- **Máscara de subred:** define los valores de la máscara de subred de la interfaz VLAN.
- **Gateway por defecto:** ingrese la dirección IP del ruteador de salida de la red (equipo que interconecta más de una red física).

Habilitar tráfico

Aquí son habilitados los tráficos de administración y el de paquetes de señalización SIP y RTP (relativos al tráfico de voz) en la interfaz VLAN.

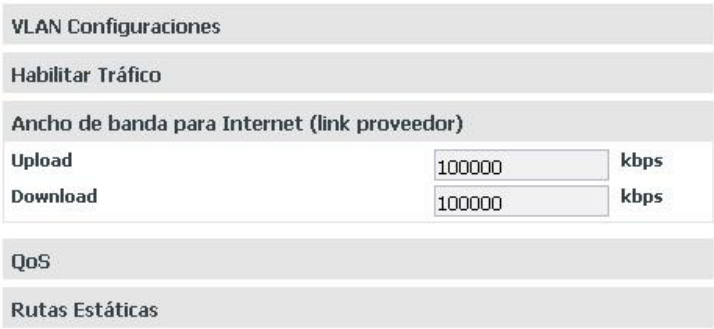


Menú Red/Submenú VLAN/Habilitar tráfico

- **SIP:** habilita el tráfico de los paquetes de señalización SIP junto a la red VLAN configurada.
- **RTP:** habilita el tráfico de los paquetes de señalización RTP junto a la red VLAN, suministrando un medio uniforme para transmitir datos sujetos a problemas de tiempo real (audio, videos,…).
- **Administración:** habilita el tráfico de administración en la red VLAN. Esto puede ser utilizado para evitar el acceso a las configuraciones de administración por personas no autorizadas.

Ancho de banda para Internet/VLAN (enlace proveedor)

En este sub-menú se configuran las velocidades contratadas de la banda del proveedor dentro de la red.



Menú Red/Submenú VLAN/Ancho de banda para Internet /VLAN (enlace proveedor)

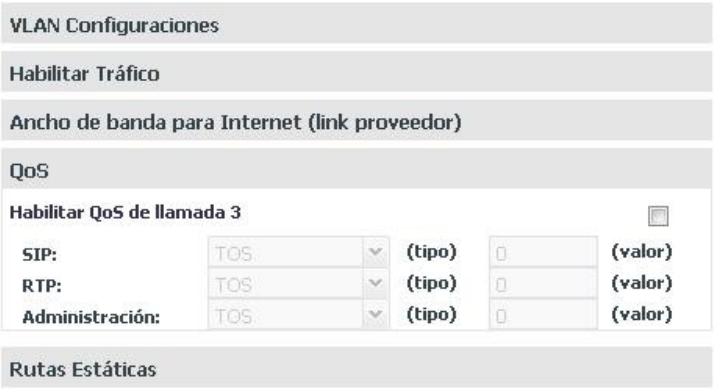
» **Carga y Descarga:** se definen las tasas máximas para la conexión con el enlace proveedor de acuerdo con los equipos conectados.

Es importante saber las tasas de carga y descarga con la interfaz VLAN disponible, para mantener el equilibrio en la conexión y evitar cualquier saturación y consecuente pérdida de calidad.

QoS

Permite especificar prioridades para el paquete o clase de tráfico. El QoS busca una mejoría de la calidad de la comunicación priorizando algunos tipos de datos en detrimento de otros, de acuerdo con una clasificación previa de los mismos, y se vuelve extremamente útil en condiciones de embotellamiento de tráfico en la interfaz de salida de estos datos (por ejemplo, el puerto de conexión con el ruteador para Internet).

Atención: la tarjeta ICIP marca los paquetes de datos, tocando a los activos de red (switches y ruteadores) dar prioridad al tráfico de voz.



Menú Red/Submenú VLAN/QoS

Habilitar QoS de capa 3 Seleccionado

En los campos indicados en esta pantalla hay la opción de seleccionar dos modos de señalización de los paquetes (DSCP o TOS) y su prioridad. Estos parámetros serán utilizados para QoS y son insertados en el encabezado IP de todos los paquetes SIP, RTP y de administración transmitidos.

La elección entre uno de los modos, depende de un análisis de la red, de la compatibilidad de los dispositivos con el modo seleccionado y de la forma como están configurados los ruteadores y switches para priorizar el tráfico.

» **Modo DSCP (Differentiated Services Code Point):** prioriza el paquete de acuerdo con la marcación en el paquete recibido. Esos paquetes se distinguen en clase de tráfico, de acuerdo con las informaciones de retraso, tasa de procesamiento y confiabilidad anexadas al paquete. Para esto, utiliza 6 bits del encabezado, dando 64 diferentes posibilidades para códigos de prioridad.

» **Modo TOS (Type of Service):** los paquetes que entran en la red por medio de la ICIP son encaminados de acuerdo con la prioridad definida. Para esto, utiliza 3 bits del encabezado dando 8 diferentes posibilidades para códigos de prioridad, siendo 0 la prioridad más baja.

Atención: cuanto mayor el valor, mayor será la prioridad en el tratamiento y uso de los recursos de la red. Los modos DSCP y TOS entrarán en operación, conforme comportamiento definido por la IETF.

Cuando la tasa de tráfico entrante en un equipo de red es superior a la tasa de tráfico saliente del mismo (ancho de banda), ocurre un embotellamiento en la red. Durante estas condiciones, los cuadros marcados con mayor prioridad reciben tratamiento preferencial y son entregados antes de los cuadros con menor prioridad.

Hay que recordar que es con base en estos parámetros que los equipos de red priorizan el tráfico de voz frente al tráfico de datos.

SIP

Al lado del campo SIP es posible seleccionar el modo de QoS:

» TOS con valor de 0 a 7, que representa la prioridad del paquete.

» DSCP con valor de 0 a 63, que representa la prioridad del paquete.

RTP

Al lado del campo RTP es posible seleccionar el modo de QoS:

» TOS con valor de 0 a 7, que representa la prioridad del paquete.

» DSCP con valor de 0 a 63, que representa la prioridad del paquete.

Administración

Al lado del campo Administración es posible seleccionar el modo de QoS:

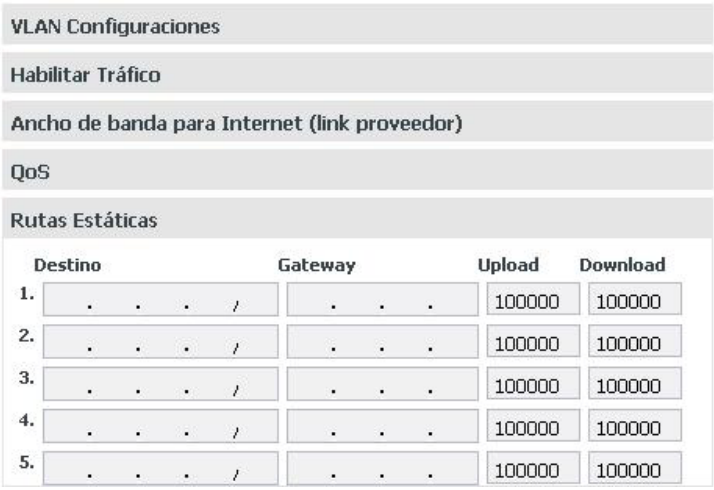
» TOS con valor de 0 a 7, que representa la prioridad del paquete.

» DSCP con valor de 0 a 63, que representa la prioridad del paquete.

Atención: las modificaciones efectuadas serán válidas solamente en equipos que se configuren del mismo modo, de lo contrario, el tráfico será encaminado de acuerdo con el comportamiento patrón de la IETF, o conforme alguna configuración específica en el equipo siguiente.

Rutas estáticas

Esta configuración permite definir rutas específicas para subredes al lado de la red VLAN, creando caminos predeterminados, donde las informaciones pueden ser direccionadas hasta un host o a otra red específica.



Menú Red/Submenú VLAN/Rutas estáticas

- **Destino:** son informadas las direcciones IPs y la máscara (direcciones IP/net-mask tipo CIDR) del destino del enrutamiento.
- **Gateway:** ingrese la dirección IP del ruteador, por medio del cual el tráfico fluirá para la subred de destino
- **Carga y Descarga:** se definen las tasas máximas para la conexión con la interfaz de destino. Es importante saber las tasas de carga y descarga con la interfaz de destino disponible, para mantener el equilibrio en la conexión del enlace y evitar cualquier saturación y consecuente pérdida de calidad.

9.7. Menú VoIP - Tarjeta ICIP 30 canales

Permite configurar los parámetros generales del proveedor de servicio de telefonía, así como las conexiones y todos parámetros necesarios para que la central pueda realizar las llamadas desde internet vía VoIP.

Atención: algunas de estas informaciones pueden obtenerse junto al administrador de red y Proveedor VoIP.

Menú VoIP - Tarjeta ICIP y sus componentes

General

Este submenú permite configurar algunas características del VoIP, codecs y esquema de canales VoIP del sistema.

Menú VoIP - Tarjeta ICIP/Submenú General

VoIP General

Posibilita la configuración de los parámetros relacionados a la señalización y mejoría de calidad de audio. Esos parámetros valen para extensiones/internos IP y conexiones punto a punto.

Menú VoIP - Tarjeta ICIP/Submenú General/VoIP General

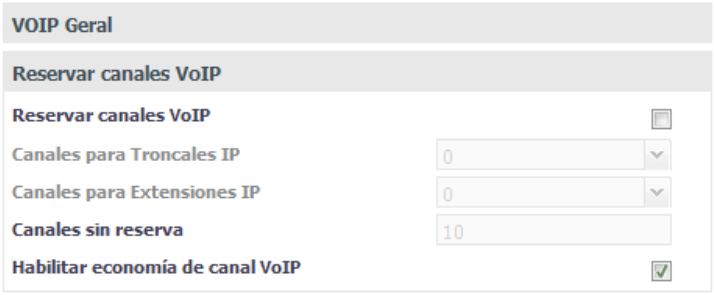
» **SIP keep alive:** cuando está habilitado, el sistema envía periódicamente un mensaje SIP al destino de la llamada, con el objetivo de mantener la sesión del NAT (Network Address Translation) disponible. Estándar 60s.

» **Jitter buffer adaptable:** cuando esta habilitado, es posible especificar un rango de tiempo de retardo para acomodar los paquetes que llegan desde la red, permitiendo que el sistema adapte el buffer, tendiendo a su valor mínimo cuando la red está buena y al máximo cuando está mala. De esa manera, el sistema evita pérdidas y provee una mejora en la calidad de audio, lo que vuelve esta opción la más utilizada. El rango estandar está entre 40ms y 100 ms.

» **Jitter buffer fijo:** cuando esta habilitado, es posible especificar un tiempo fijo de retardo para los paquetes. En esa opción, el tiempo de "re-procesamiento" de los paquetes que llegan desde la red, antes de "éjecutarlos", es siempre el mismo. Técnicamente es más sencillo, aunque presente desempeño inferior, pues no consigue acompañar el comportamiento de la red. El estándar es 40 ms.

Reserva canales VoIP

Posibilita la configuración de los parámetros relacionados a distribución de los canales VoIP en relación a las extensiones/internos y troncales. El sistema permite reserva para extensiones/internos, troncales y libre acceso (sin reserva).



Menú VoIP - Tarjeta ICIP/Submenú General/Reserva canales VoIP

» **Reservar canales VoIP:** habilitado, el administrador del sistema puede reservar un número específico de canales VoIP para Troncales y/o Extensiones/internos IP y disponer los canales restantes para que se utilicen conforme demanda de la central. Si no estuviere habilitado, los canales son ajustados libremente, por demanda.

» **Canales para Troncales IP:** define el número de canales VoIP que estarán reservados para Troncales IP.

» **Canales para Extensiones/internos IP:** define el número de canales VoIP que estarán reservados para Extensiones/internos IP.

» **Canales sin reserva:** define el número de canales VoIP a ser usados libremente por troncales o extensiones/internos IP, conforme demanda.

» **Habilitar Ahorro de canal VoIP:** seleccionado, el sistema ahorra canales cuando los dos dispositivos IP involucrados en la llamada sean extensiones/internos IP.

***Obs.:** algunas situaciones no consideran esa regla, es decir, ahorro no será posible si:*

» Al menos una de las extensiones/internos IP estuviere atrás de NAT.
» Haya conferencia involucrando las extensiones/internos IP.
» El teléfono, conectado en la extensión/interno IP, no estuviere preparado para funcionar con la ICIP de forma plena.

Atención: funciona correctamente con TIP100 y ATA 2210T.

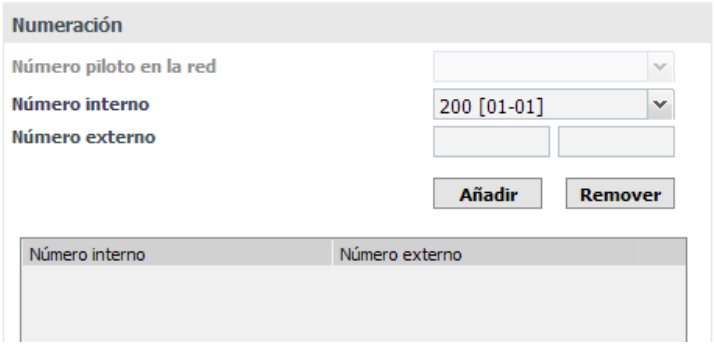
Punto a punto

Este submenú permite configurar una conexión entre la central Impacta y otra central IP, sin utilizar un proveedor VoIP.

Menú VoIP - Tarjeta ICIP/Submenú Punto a punto

Numeración

En este sub-menú son registradas todas las extensiones/internos que van a generar y recibir llamadas VoIP punto a punto involucrando sucursales.



Menú VoIP - Tarjeta ICIP/Submenú Punto a punto/Numeración

» **Piloto en la red:** define el número externo que será usado como abonado llamador en caso que la extensión/interno que origina la llamada no esté registrada en la tabla.
» **Número interno:** seleccione la extensión/interno que podrá encaminar y recibir llamada VoIP involucrando las sucursales.
» **Número externo:** ingrese el número VoIP por el que la extensión/interno interna es conocida en la red.

Utilice los botones *Añadir* y *Remover* para administrar los números internos/externos deseados.

Punto a punto sucursal

En este sub-menú se registran todas las sucursales que van a generar y recibir llamadas VoIP.

Se activa utilizando el botón Sucursales con las opciones de crear una nueva Sucursal (*botón Nuevo*) o consultar/modificar una ya existente (selección directa del nombre en el sub-menú).

Menú VoIP - Tarjeta ICIP/Submenú Punto a punto/Botón Sucursales

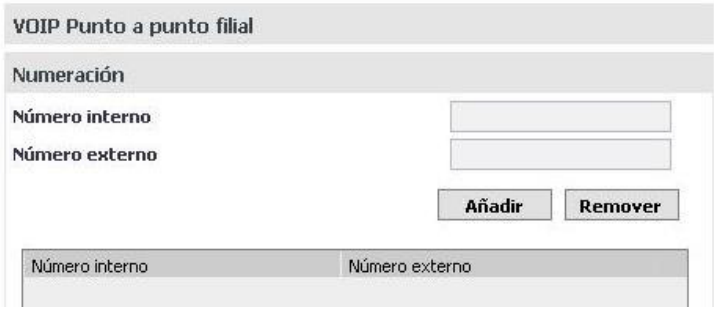
Submenú Punto a punto Sucursal/Punto a punto Sucursal

» **Localidad:** ingrese un nombre que sea significativo para identificar la Sucursal (ej.: nombre de la ciudad, etc.)

» **Dirección (IP o FQDN):** ingrese la dirección IP de la central o dispositivo VoIP de la Sucursal.

Numeración

En esta guía son registradas todas las extensiones/internos de la sucursal que van a generar y recibir llamadas VoIP.



Submenú Punto a punto sucursal/Numeración

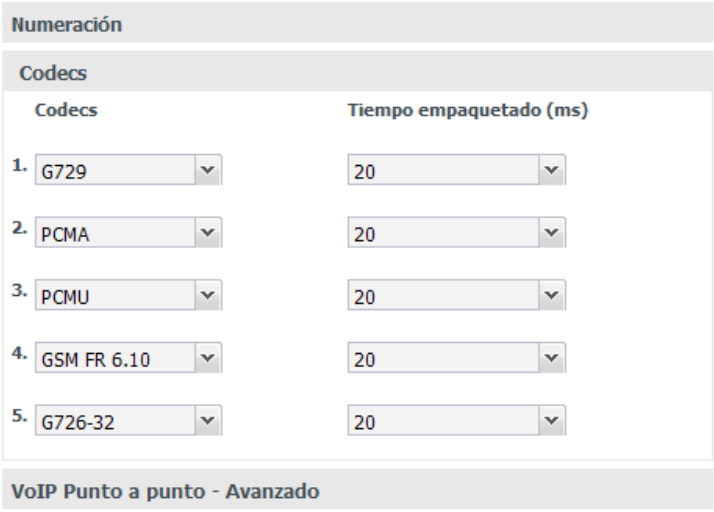
» **Número interno:** ingrese la extensión/interno de la sucursal para la cual se encaminará la llamada VoIP. Ese número será el que se marca, por tanto no debe haber duplicidad con otra extensión/interno o facilidad.

» **Número externo:** informe el número VoIP por el cual la extensión/interno interna de la sucursal es conocida en la red.

Utilice los botones *Añadir* y *Remover* para administrar los números internos/externos deseados.

Codecs

La función de los codecs es reducir el ancho de banda necesario para transmisión de las señales de voz sobre la red de paquetes. Eso se alcanza utilizándose técnicas de compresión de voz, que, en mayor o menor grado, actúan en el sentido de reducir la redundancia característica presente en las señales del habla.



Menú VoIP - Tarjeta ICIP/Submenú General/Codecs

» **Opción de 1 a 5:** definen el orden de preferencia de los codecs (7 opciones) y el período del Paquete RTP, cuando se realiza o se recibe una llamada.

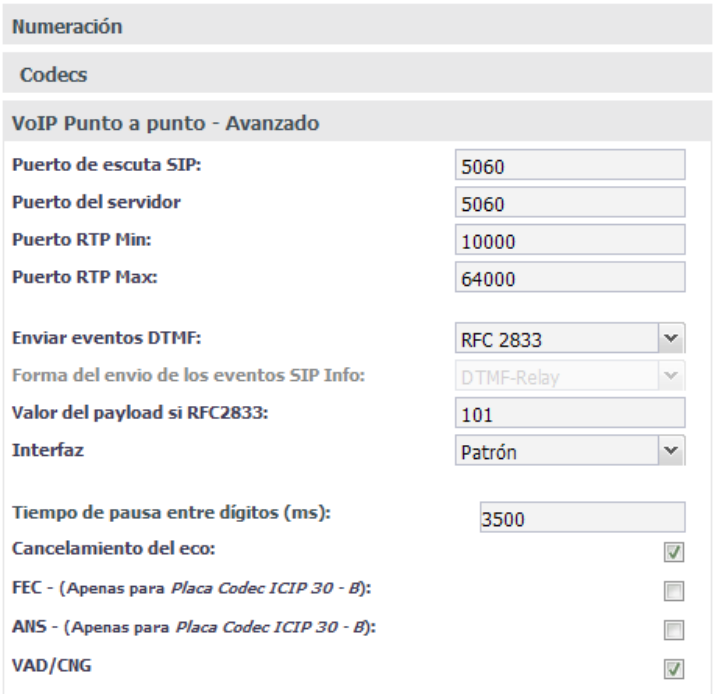
» **Codecs:** poseen diferentes relaciones de compresión, calidad de audio y ocupación de ancho de banda. La ICIP soporta los codecs: G.729AB, GSM FR 6.10, G.723, G.726-16, G.726-24, G.726-32, G.726-40 y G.711 PCMa y u.

» **Período del paquete RTP:** en llamadas VoIP, el audio es transformado en paquetes de datos y este campo presenta el tiempo que la ICIP aguardará para envío de los paquetes RTP para la red.

Obs.: *por lo menos una de las opciones debe estar configurada como PCMA*

VoIP punto a punto – Avanzado

En esta pestaña es posible configurar los datos VoIP punto a punto más específicos.



VoIP punto a punto – Avanzado

- » **Puerto de escucha SIP:** define el puerto de escucha del protocolo SIP.
- » **Puerto del servidor:** define el puerto utilizado en el servidor.
- » **Puerto RTP Mín y Puerto RTP Máx:** definen el intervalo de puertos que pueden ser utilizados en la transmisión y recepción de audio. El intervalo de puertos RTP del proveedor VoIP debe estar contenido aquí. Si existe un Firewall, verificar si estos puertos están liberados.
- » **Enviar eventos DTMF:** define el método con el que se envían los dígitos DTMF a la red después de completar la llamada.
- » **SIP INFO:** envía los eventos DTMF como señalización SIP.
- » **Out-of-band (RFC2833):** envía los eventos DTMF como una señalización de carga RTP, utilizando RFC 2833.
- » **In-Band:** envía los eventos DTMF en el paquete de voz.
- » **Formateo para envío de eventos SIP Info:** si el método de DTMF escogido es SIP Info, estarán disponibles las opciones DTMF-Relay, DTMF y Telephone Event.

  Obs.: utilice el método definido por la operadora.
- » **Valor del payload si RFC2833:** configure el tipo de carga (payload) del DTMF cuando está seleccionado el evento DTMF Out-of-band (RFC2833). El valor varía entre 96 y 127, y el estándar es 101.
- » **Tiempo de pausa entre dígitos (ms):** define el tiempo de la pausa introducido entre los dígitos marcados.
- » **Eliminación de eco:** cuando está habilitado, el sistema evita que el eco en la híbrida (cuando se pasa de 4 a 2 cables) retorne a la red IP. Es decir, el eliminador de eco de red actúa en llamadas provenientes de la red IP, con destino a algún dispositivo TDM, eliminando la señal reflejada en la híbrida y garantizando calidad de audio y comodidad al originador de la llamada.
- » **FEC:** habilita el uso del FEC (Forward Error Correction), algoritmo para la corrección anticipada de errores. Envía paquetes adicionales que permiten reconstruir en el receptor, paquetes de audio perdidos en la transmisión. En redes con pérdida de paquetes mantiene la calidad del audio.

  Obs.: opción solamente disponible para la tarjeta codec ICIP 30 - B).

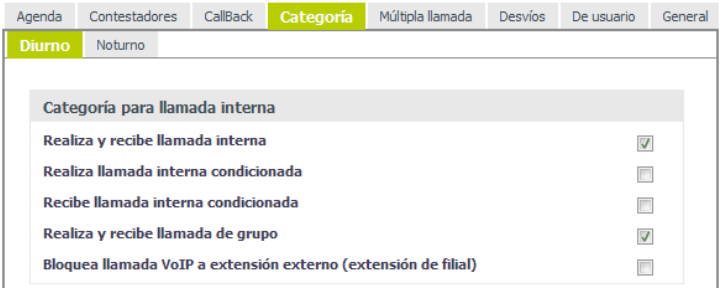
» **ANS:** habilita el uso del ANS (Adaptive Noise Suppressor), algoritmo de reducción de ruido. Reduce ruidos en las señales de voz provenientes de la red TDM, proporcionando una mejora en la comodidad e inteligibilidad de la comunicación.

Obs.: opción solamente disponible para la tarjeta codec ICIP 30 - B).

» **VAD/CNG:** habilita el uso del VAD (Voice Activity Detection/(Confort Noise Generation): los algoritmos VAD y CNG forman un esquema para identificar segmentos de voz o ruido (VAD) en una conversación y codificar los segmentos de ruido (CNG). Este esquema es utilizado para reducir el uso de banda en una llamada telefónica cuando la señal transmitida contiene solamente silencio/ruido.

Categoría para acceso VoIP a extensión externa (extensión de sucursal)

Esta configuración permite definir si la extensión posee categoría para realizar llamadas a extensiones externas como por ejemplo, extensiones de otras sucursales conectadas vía punto a punto VoIP. Estándar de fábrica deshabilitado. Para habilitar, acceda a Extensión>Categoría >Categoría para llamada interna.



Categoría para acceso VoIP a extensión externa (extensión de filial)

Proxy

Este submenú permite configurar la conexión entre la central Impacta y el proveedor VoIP, a través del cual será posible generar y recibir llamadas externas VoIP. Es posible registrar hasta 50 servidores de registro Proxy.

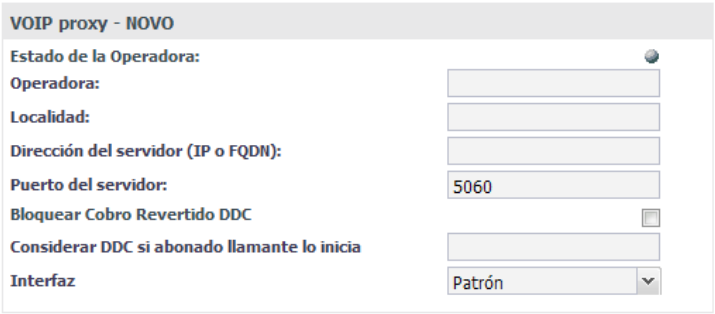
Al seleccionar esta opcion, se presentará un sub-menú donde está(n) registrada(s) el (los) operador(es) VoIP del sistema. Para registrar un Proveedor VoIP, utilice el botón *Nuevo* o seleccione uno ya existente para consultar/modificar (selección directa del nombre el menú.

Menú VoIP - Tarjeta ICIP/Submenú Proxy

VoIP proxy

Aquí son configuradas las informaciones proporcionadas por el Operador para acceso del sistema.

Atención: algunas de estas informaciones pueden obtenerse junto al administrador de red o directamente con el Operador VoIP.

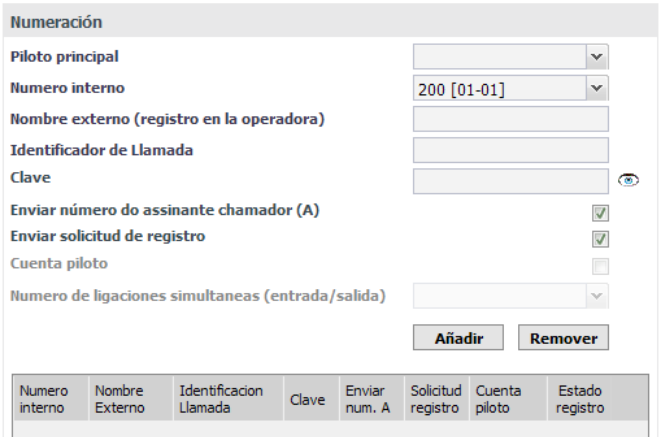


Menú VoIP - Tarjeta ICIP/Submenú Proxy/VoIP Proxy

- **Estado del operador:** es posible visualizar si el operador está activo ante el sistema (Operador localizable).
  - **Verde:** con pedido de registro OK.
  - **Rojo:** con pedido de registro negado.
  - **Gris:** con pedido de registro sin respuesta.
  - **Azul:** sin pedido de registro.
- **Operador:** introduzca el nombre del Operador VoIP.
- **Localidad:** ingrese un nombre que referencie la localidad donde la central esta instalada.
- **Dirección del servidor (IP o FQDN):** informe la dirección IP o nombre de dominio del operador VoIP, de acuerdo con las informaciones proporcionadas por el Operador VoIP (ej.: operadora.net.br).
- **Puerto del servidor:** defina el puerto por el que el servidor VoIP transmitirá y recibirá los mensajes SIP. El valor por defecto de fábrica es 5060.
- **Bloquear DDC (Llamada Directa de Cobro Revertido):** cuando seleccionado, las llamadas identificadas como "a cobro revertido" serán bloqueadas.
- **Considerar DDC si abonado origen iniciar con:** define los caracteres alfanuméricos que, si estuvieren presentes en el inicio del número del abonado llamador, clasificarán la llamada como de cobro revertido.

Numeración

En este sub-menú son registradas todas las extensiones/internos que van a generar y recibir llamadas VoIP.



Menú VoIP - Tarjeta ICIP/Submenú Proxy/Numeración

» **Nombre Piloto:** define el número que será usado como abonado llamador cuando la extensión/interno originadora de la llamada no esté registrada en la tabla.
» **Número interno:** seleccione la extensión/interno que podrá encaminar/recibir llamada VoIP vía operador.
» **Nombre externo (registro en el operador):** ingrese el número externo equivalente, que será registrado en el operador (cuenta).
» **Identificador de Llamada:** define el nombre del abonado en el servicio VoIP. El valor de este campo será exhibido en la pantalla del identificador de llamadas del usuario que esté recibiendo una llamada. En algunos casos, el proveedor VoIP puede sugerir la identidad real del llamador.
» **Clave:** ingrese la clave de registro del número externo, para autenticación junto al operador VoIP. La clave debe contener hasta 12 dígitos.
» **Enviar número del abonado (A):** si esta opción está marcada, lo que será enviado como identificación al destinatario será el valor informado en el campo Identificador de llamada. Si está desmarcada, será enviado el valor Anónimo.
» **Enviar pedido de registro:** define si la cuenta enviará pedidos de registro.
» **Cuenta piloto:** define si la cuenta es piloto.
» **Número de llamadas simultáneas (entrada/salida):** define las llamadas simultáneas que esta cuenta piloto podrá realizar.
» **Utilice los botones Añadir y Remover:** administre los números internos/nombres deseados.

Portabilidad

En este apartado se configuran los parámetros para la integración con servidores de portabilidad.

Menú VoIP - Tarjeta ICIP/Submenú Proxy/Portabilidad

» **Habilita portabilidad:** define si la portabilidad será habilitada o deshabilitada.
» **Tiempo para esperar al servidor responder (ms):** define el tiempo esperado por la respuesta del servidor en ms.
» **En caso de fallo en la consulta:** define la acción a ser tomada si no se consigue realizar la consulta al servidor. La llamada puede ser terminada o no.
» **Enviar aviso de fallo:** define si envía aviso en caso de fallo.
» **Por email:** envía el aviso al email informado.
» **Periodo para envío (en minutos):** define el período en minutos para que sea enviado el aviso.

Atención: para obtener la información de portabilidad, el usuario debe contratar una empresa que proporcione este servicio. Cabe destacar que es necesario comprobar si el servicio de portabilidad de la empresa es compatible con Impacta antes de realizar la contratación del servicio.

El método utilizado por Impacta para transmitir información con el servidor de portabilidad sigue el siguiente proceso:

» La tarjeta ICIP 30 envía un mensaje de INVITE estándar SIP con el número de destino que contiene el código del área para el servidor de portabilidad. En el siguiente ejemplo, se realiza una llamada al número (48) 9932-8721 a través del servidor sevidordeportabilidade.com, registrado con la cuenta usuario.

U 2014/11/06 17:51:50.037471 201.3.239.120:5060 -> 10.252.68.161:5060
INVITE sip:4899328721@servidordeportabilidade.com:5060 SIP/2.0.
Via: SIP/2.0/UDP 201.3.239.120:5060;rport;branch=z9hG4bKPjKuwdcQlJfEvXhk61aNFfLCIC3fJYD63E.
Max-Forwards: 70.
From: "Usuario" <sip:contadousuario@servidordeportabilidade.com:5060>;tag=ZEJA-DHg3mfblZ87ONa7.Jn8BJcKPqQ2.
To: <sip:4899328721@servidordeportabilidade.com:5060>.
Contact: "Usuario" <sip:contadousuario@201.3.239.120:5060>;+sip.account.user=usuario.
Call-ID: -DP1cbYwuBYbZFNmXQCTzXVWbYogqVGX.
CSeq: 32398 INVITE.
Allow: PRACK, INVITE, ACK, BYE, CANCEL, UPDATE, REFER, OPTIONS, SUBSCRIBE, NOTIFY.
Supported: 100rel.
User-Agent: icip_intelbras /PBX_IMPACTA - v1.9.41_I30_MD.
Proxy-Authorization: Digest username="intelbras", realm="servidordeportabilidade.com",
nonce="545bb55000017a04a2065e61e331b532363a43f81c67e135", uri="sip:4899328721@servidordeportabilidade.com:5060",
response="b6aaa477cf4cfdc8ecaf50142dcd0a3e", cnonce="udlUghuKruOzUZTm14QXBKpCtDcs0g4C", qop=auth, nc=00000001.
Content-Type: application/sdp.
Content-Length: 358.
.
v=0.
o=icip_intelbras 3624288554 3624288554 IN IP4 201.3.239.120.
s=Intelbras.
c=IN IP4 201.3.239.120.
t=0 0.
m=audio 6000 RTP/AVP 18 8 0 3 2 101.
a=rtpmap:18 G729/8000.
a=fmtp:18 annexb=yes.
a=rtpmap:8 PCMA/8000.
a=rtpmap:0 PCMU/8000.
a=rtpmap:3 GSM/8000.
a=rtpmap:2 G726-32/8000.
a=sendrecv.
a=rtpmap:101 telephone-event/8000.
a=fmtp:101 0-15.
a=ptime:20.

» El servidor de portabilidad debe devolver una respuesta de tipo 304-Moved Temporarily. Conforme la siguiente información.

U 2014/11/06 17:51:50.037917 10.252.68.161:5060 -> 201.3.239.120:5060
SIP/2.0 302 Moved Temporarily.
Via: SIP/2.0/UDP 201.3.239.120:5060;received=201.3.239.120;rport=5060;branch=z9hG4bKPjKuwdcQlJfEvXhk61aNFfLCIC3fJYD63E.
From: "usuario" <sip:usuario@servidordeportabilidade.com:5060>;tag=ZEJA-DHg3mfblZ87ONa7.Jn8BJcKPqQ2.
To: <sip:4899328721@servidordeportabilidade.com:5060>;tag=9e202574851715a2900e0fc5c60433e0-7825.
Call-ID: -DP1cbYwuBYbZFNmXQCTzXVWbYogqVGX.
CSeq: 32398 INVITE.
Contact: <sip:553204899328721@servidordeportabilidade.com>.
Server: IAO 1.1.
Content-Length: 0.

Note que en el mensaje 304-Moved Temporarily, se devuelve número adicional que corresponde con el código de la operadora del número solicitado, llamado RN1, que debe estar registrado en el menú enrutamiento>Portabilidad.

Atención: para obtener la información de portabilidad, el usuario debe contratar una empresa que proporcione este servicio. Cabe destacar que es necesario comprobar si el servicio de portabilidad de la empresa es compatible con Impacta antes de realizar la contratación del servicio.

Codecs

La función de los codecs es reducir el ancho de banda necesaria para la transmission de las señales de voz sobre la red de paquetes. Esto se logra utilizando técnicas de compresión de voz, que en mayor o menor grado actúan en el sentido de reducir la redundancia característica presente en las señales del habla.

Menú VoIP Tarjeta ICIP/Submenú Proxy/Codec

» **Opción de 1 a 5:** definen el orden de preferencia de los codecs y el periodo del paquete RTP, cuando se realiza o se recibe una llamada.

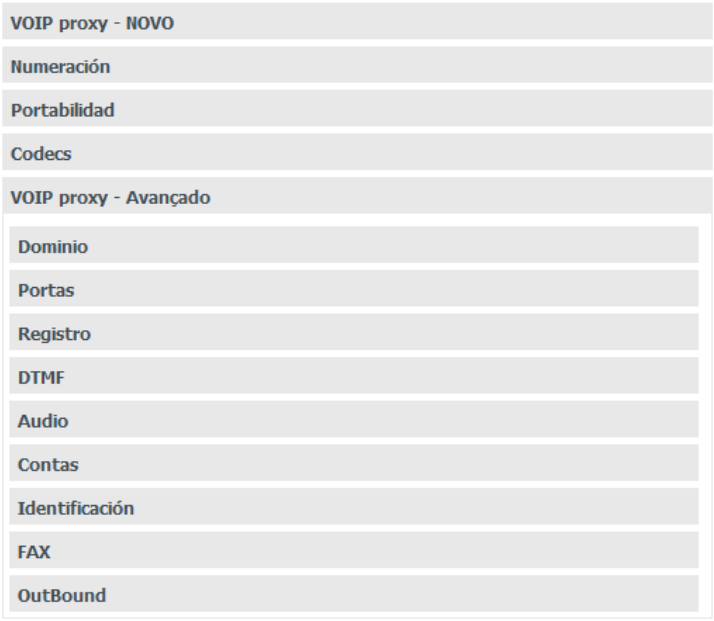
» **Codecs:** poseen diferentes relaciones de compresión, calidad de aúdio y ocupación de ancho de banda. La ICIP soporta los codecs: G.729AB, GSM FR 6.10, G.723, G.726-16, G.726-24, G.726-32, G.726-40 y G.711 PCMa y u.

» **Periodo del paquete RTP**: en llamadas VoIP, el áudio es transformado en paquetes de datos, y este campo presenta el tiempo que la ICIP esperará para enviar los paquetes RTP a la red.

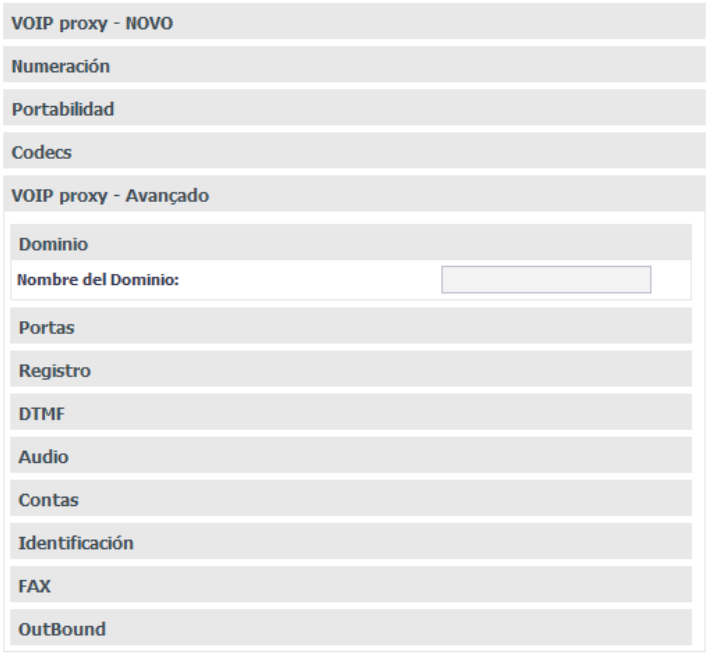
Obs.: *por lo menos una de las opciones debe estar configurada como PCMA*

VoIP Proxy – Avanzado

En esta pestaña es posible configurar los datos VoIP Proxy más específicos.

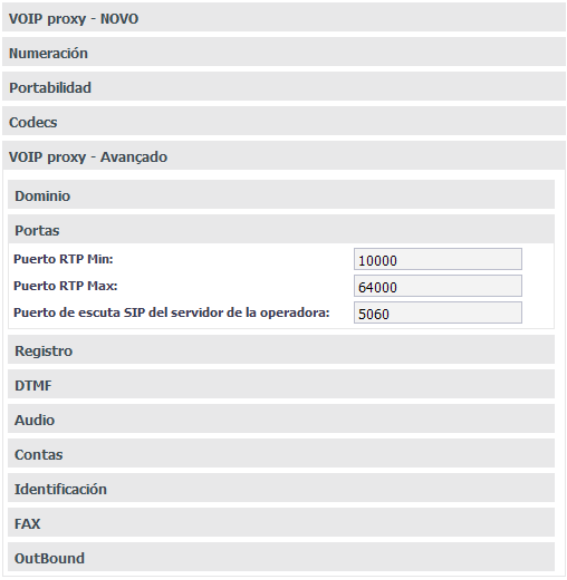


Menú VoIP - Tarjeta ICIP/Submenú Proxy/Avanzado



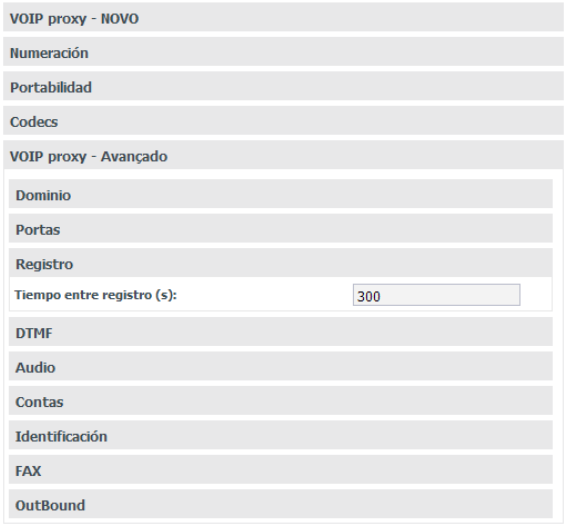
Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/Dominio

» **Dominio**
  » Nombre de dominio.



Menú VoIP/Tarjeta ICIP/SubmenúProxy/Avanzado/Puertos

» **Puertos**
  » Puerto RTP Mín. y Puerto RTP Máx.
  » Puerto de escucha SIP del servidor de la operadora.



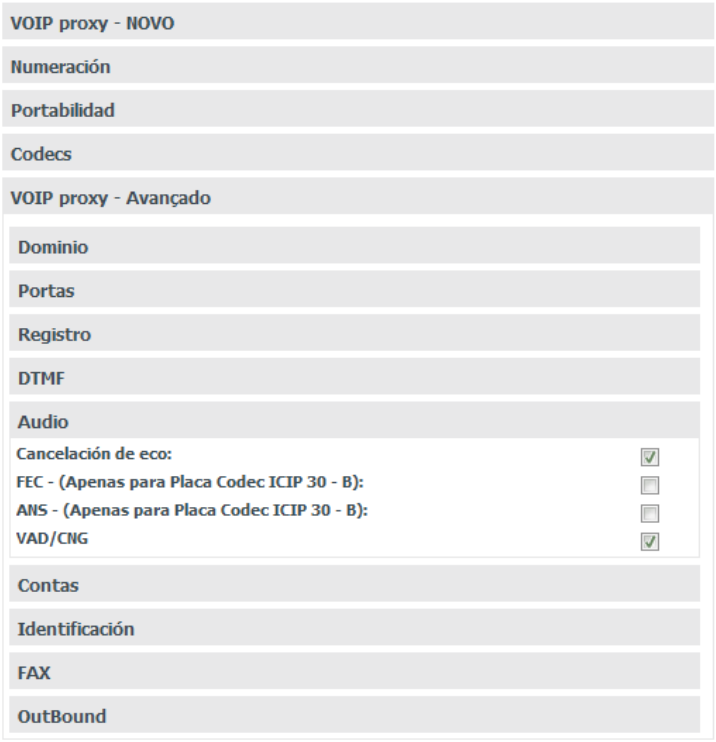
Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/Registro

» **Registro**

» Tiempo entre registro(s)

Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/DTMF

» **DTMF**
  » Enviar eventos DTMF
  » SIP INFO
  » Out-of-band (RFC2833)
  » In-Band
  » Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/DTMF
  » Tiempo de pausa entre dígitos (ms)
  » Valor del payload si RFC2833



Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/Audio

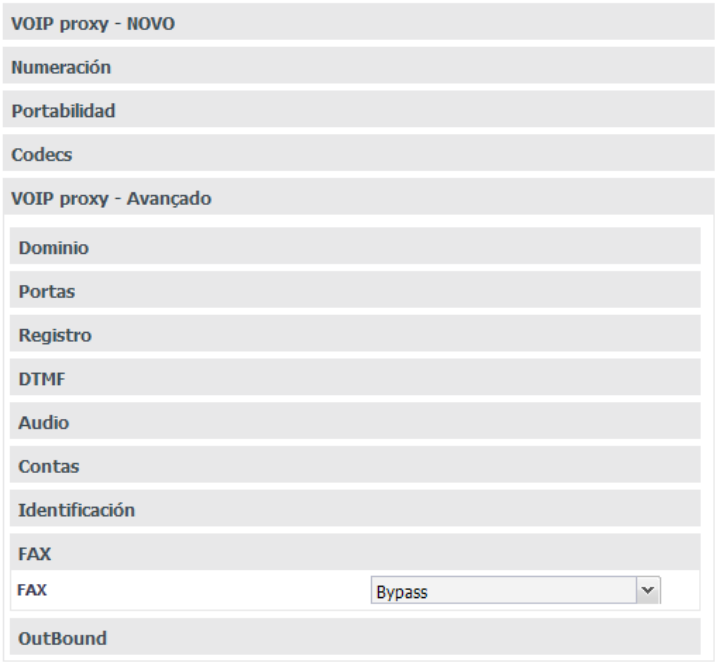
» **Audio**
  » Eliminación de eco
  » FEC
  » ANS
  » VAD/CNG

Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/Cuentas

» **Cuentas**
  » **Habilitar múltiples cuentas piloto:** habilita la configuración de cuentas piloto.
  » **Subsistema (cuenta en el destino extensión IP):** habilita el modo Subsistema si la cuenta en el servidor destino es una extensión IP.
  » **Originar llamada siempre utilizando el piloto:** las llamadas son originadas siempre utilizando el piloto

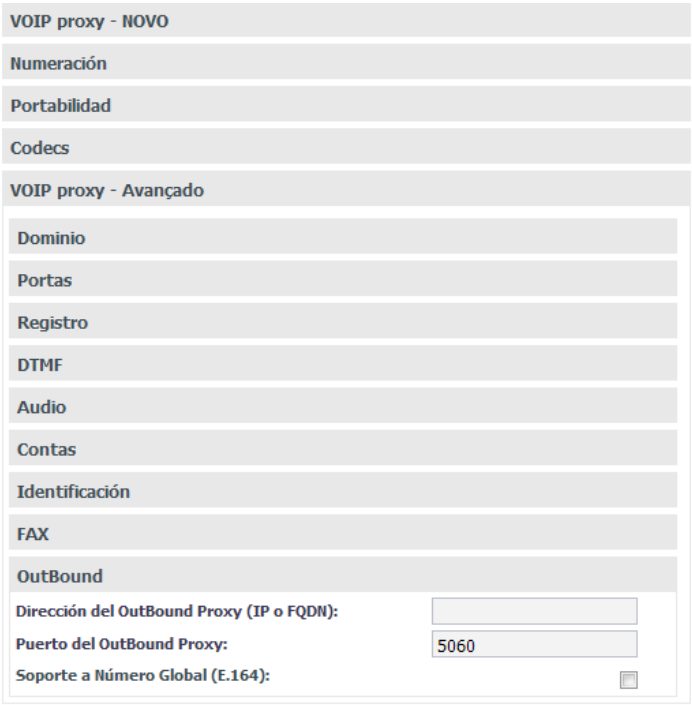
Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/Identificación

» **Identificación**
  » Enviar como Identificación del llamador.
    » Contenido del campo Identificación del Llamador.
    » Núm. de la extensión originadora (interna).
    » Núm. Del llamador externo si la llamada viene de la troncal.
  » Enviar como usuario (cuenta de registro).
    » Contenido del campo Nombre externo.
    » Núm. de la extensión originadora (interna).
    » Núm. del llamador externo (bina) si la llamada viene de la troncal.



Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/Fax

» **FAX**
  » Deshabilitado
  » Bypass
  » Data Bypass
  » T.38.



Menú VoIP/Tarjeta ICIP/Submenú Proxy/Avanzado/OutBound

» **OutBound**

Es un servicio implantado por algunos servidores SIP que obliga a todos los paquetes, incluyendo los paquetes de voz, a viajar a través de este servidor a cambio de una supervisión mejorada sobre sus funcionalidades.

  » **Dirección del OutBound Proxy:** puede ser la dirección IP o FQDN- Puerto del OutBound Proxy: puerto del servidor.
  » **Soporte a número global (E.164):** E.164 es una recomendación de la ITU-T (Telecommunication Standardization Sector), que define internacionalmente el uso de la numeración en la red de telecomunicaciones pública (PSTN) y en otras redes de datos. También define el formato de números de teléfono. Los números E.164 pueden tener un máximo de quince dígitos y generalmente se escriben con un prefijo +. Para marcar los números correctamente a partir de una línea de teléfono fija normal, se debe utilizar el prefijo internacional adecuado.

VoIP Proxy Sucursal

En este sub-menú se registran todas las sucursales que van a generar y a recibir llamadas. Utilice esta tabla cuando haya comunicación con sucursales y si ocurre vía operador.

Es activada a través del botón *Sucursales* con las opciones de crear una nueva Sucursal (botón *Nuevo*) o consultar/modificar una ya existente (selección directa del nombre en el menú).

Menú VoIP - Tarjeta ICIP/Submenú Proxy/Botón Sucursales

VoIP proxy

En este sub-menú se registra la identificación de la sucursal que va a generar y a recibir llamadas VoIP.

Submenú Proxy/VoIP proxy sucursal

» **Localidad Sucursal:** ingrese un nombre que sea significativo para identificar la sucursal.

Numeración

En este sub-menú se registran todos los números de la sucursal que van a generar y recibir llamadas VoIP.

Submenú Proxy/Numeración sucursal

» **Número interno:** ingrese la extensión/interno de la sucursal para la cual se encaminará la llamada VoIP.

» **Nombre externo (registro en el operador):** ingrese el nombre o número VoIP por el que el número interno de la sucursal es conocido en la red.

Utilice los botones *Añadir* y *Remover* para administrar los números internos/nombre deseados.

Extensiones IP - Global

En esta guía son configurados los parámetros generales de las extensiones VoIP.

Extensiones IP - Global

» **Puerto de escucha SIP:** define el puerto de escucha del protocolo SIP.
» **Puerto RTP Mín:** define el puerto mínimo del protocolo RTP.
» **Puerto RTP Máx:** define el puerto máximo del protocolo RTP

Auto configuración extensiones/internos IP

Ese submenú es extremamente útil cuando van a instalarse las extensiones/internos IP por primera vez. Es posible insertar un rango de extensiones/internos IP en la lista de disponibles para obtener login/clave. De esa manera, al "enchufar" el teléfono IP, él busca su dirección IP automáticamente (si está configurado para obtener vía DHCP). En la respuesta, el servidor informa también la dirección IP de la central. Estando con la dirección IP, el teléfono solicita su login/clave. El servicio envía el primer disponible en la lista y marca como atribuido. A continuación el administrador enchufa la próxima extensión/interno.

Menú VoIP - Tarjeta ICIP/Submenú Autoconfiguración extensiones/internos IP

El ATA GKM 2210T y el teléfonos TIP 100, TIP 125 y TIP 200 al inicializar por primera vez o tras una restauración de configuración, estará apto a buscar, vía DHCP, la dirección de la central ICIP. Para eso, tras haber inicializado, el terminal IP solicitará vía DHCP una dirección de IP, en esta requisición, el terminal IP incluirá en el header "sip-servers" de código 120. Esta header tiene la función de informar la dirección de un servidor SIP en la red. El servidor de DHCP de la red, en la que el terminal IP esté conectado, podrá retornar junto con los otros headers, el header "sip-servers" con el valor de la dirección IP de la central ICIP. Con eso, el terminal IP será configurado para realizar una solicitud, con el objetivo de adquirir configuraciones básicas para registrarse en la central ICIP, como Número de la Extensión/interno y clave de la extensión/interno. Si hubiere número de extensión/interno disponible en la ICIP para este servicio, el servidor web de la ICIP responderá con un archivo con informaciones necesarias para el registro. Si hay éxito en el registro con la ICIP, el terminal IPseguirá el flujo normal y solicitará el archivo de configuración almacenado en la ICIP.

Para proveer este servicio, la central ICIP debe ser configurada, vía web, para liberar el rango de extensiones/internos disponibles para la configuración automática. Es decir, en la central se determinan los números/extensiones/internos que serán ofrecidos en las solicitudes automáticas del Terminal IP. Toda vez que un Terminal IP adquiriera un número de la central, la extensión/interno correspondiente sale de la lista de disponibles y no será más ofrecida a otro Terminal IP.

En caso de que el número de extensiones/internos disponibles esté agotado, la central ICIP retornará una configuración inválida y el Terminal IP no se registrará en la ICIP.

En servidores Linux la configuración del servicio DHCP es editable en el archivo "*/etc/dhcpd/ dhcpd.conf*". El Terminal IP analizará si existe el parámetro 120, en la solicitud DHCP, para autoconfigurar con la ICIP. Ejemplo de configuración con la red *10.1.30.xxx*:

option sip-servers code 120 = {integer 8, ip-address};.

subnet 10.1.30.0 netmask 255.255.255.0 {

option sip-servers 1 10.1.30.61;

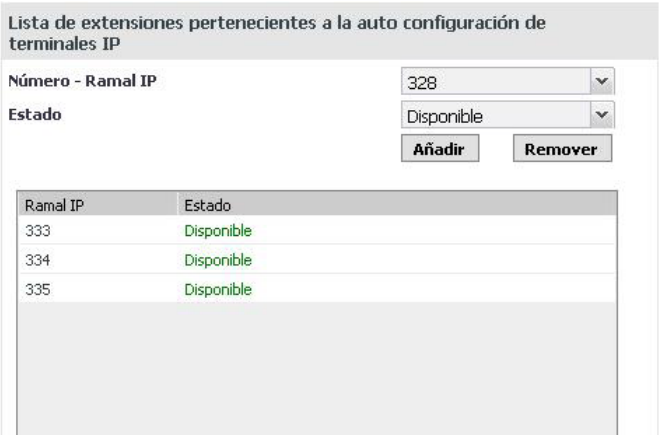
range 10.1.30.10 10.1.30.100;

range 10.1.30.150 10.1.30.200;

La dirección IP 10.1.30.61 es el IP de la tarjeta ICIP.

Lista de extensiones/internos pertenecientes a autoconfiguración de terminales IP

En este sub-menú se configuran las extensiones/internos IP que podrán ser autoconfiguradas a través de la central. Este recurso permite una configuración rápida de los terminales IP y su administración.



Menú VoIP - Tarjeta ICIP/Submenú Autoconfiguración extensiones/internos IP/Extensiones/internos

» **Número - extensión/interno IP:** ingrese la extensión/interno IP que va a pertenecer a autoconfiguración.

» **Estado:** define si la extensión/interno está disponible o utilizada para el sistema. Utilice los botones *Insertar* y *Remover* para administrar las extensiones/internos IP deseadas.

Envío de alertas de la central vía email

Es posible programar el envío automático de e-mails cuando se producen las siguientes alertas:

» **Despertador:** despertó/no despertó/no atendió/no quedó libre.

» **Registro de llamadas:** buffer de registro de llamadas alcanzando la capacidad máxima.

» **Tarjeta SD:** tarjeta con la capacidad máxima/tarjeta introducida/tarjeta extraída.

» **Llave de Hardware:** llave introducida/llave extraída.

Para ello, acceda a Sistema>Información de la empresa y configure la información solicitada.

Menú Sistema/Información de la empresa

Envío de mensajes SMS a partir de terminales IP

Esta facilidad permite que aparatos terminales IP TIP 200 y 300, así como TI NKT 4245i, puedan enviar mensajes SMS escritos en el propio aparato.

Obs.: *es requisito previo que la tarjeta GSM esté configurada y tenga un chip registrado en la operadora. También es necesario configurar las categorías de acceso de la extensión y de la troncal para enviar SMS.*

Soporte a BLF para extensión y troncal

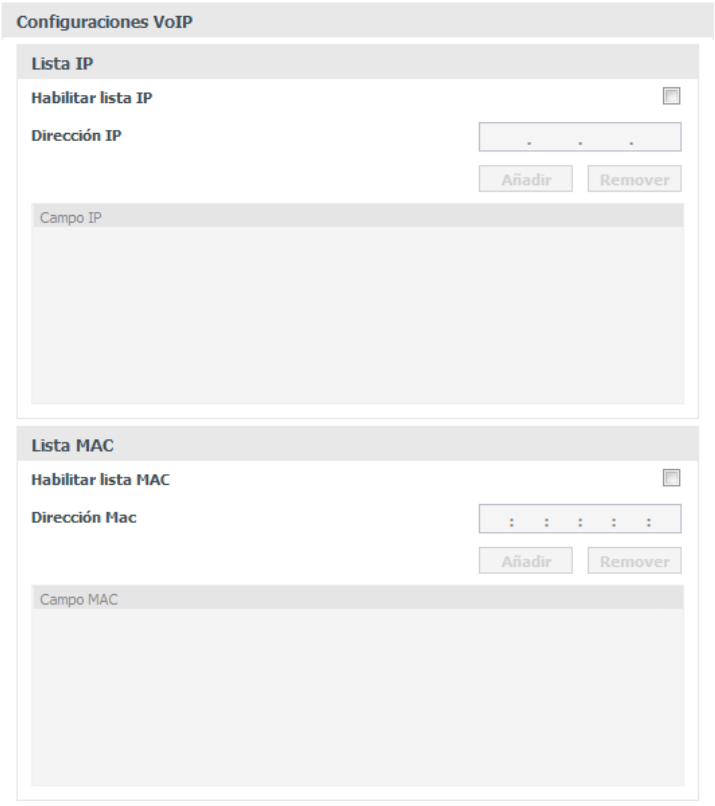
Algunos teléfonos IP tienen teclas de función BLF. BLF es el acrónimo de "Busy Lamp Field", que son las luces en un teléfono IP que indican el estado de otras extensiones o troncales del PABX. Por medio de esta indicación es posible saber si están libres, recibiendo llamadas u ocupados. El LED encendido verde indica que la extensión/troncal está libre. Si está parpadeando rojo o la extensión/troncal está recibiendo una llamada y si está rojo, significa que la extensión/juntor está ocupado con una llamada.

Filtro MAC/IP para extensión IP

Hay situaciones en las que la dirección IP de un determinado dispositivo cambia automáticamente sin la intervención del usuario. Esto pasa con cierta frecuencia en dispositivos móviles, como teléfonos móviles por ejemplo. Si el usuario utiliza un softphone IP en este dispositivo, el cambio de dirección IP puede provocar la pérdida de registro de la cuenta IP de este softphone.

Para resolver este problema, el administrador de la central puede configurar el número MAC del dispositivo móvil en la lista de MAC aceptados.

En esta situación, la tarjeta ICIP aceptará el pedido de registro independientemente de la dirección IP de origen, pero siempre y cuando el MAC sea igual al configurado.



Filtro MAC/IP para extensión IP

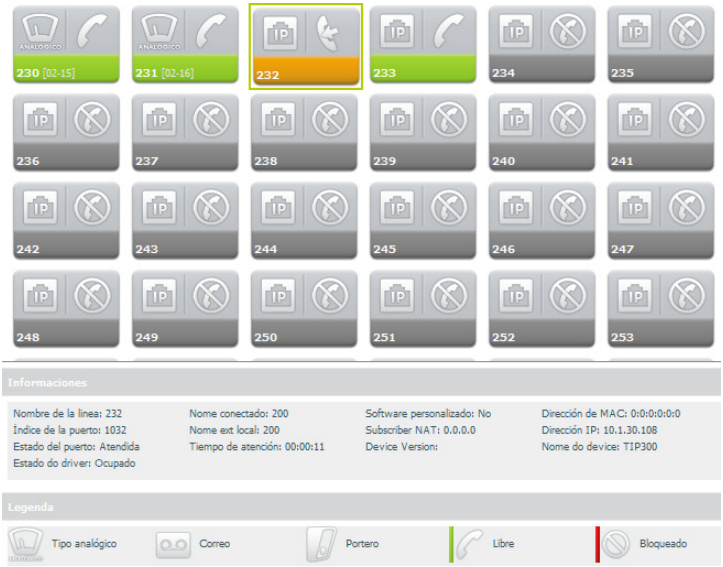
- » **Habilitar lista IP:** habilita la configuración de la lista de direcciones IP.
- » **Dirección IP:** define la dirección IP que será introducida en la lista.
- » **Añadir y Eliminar:** utilice estos botones para añadir o eliminar registros en la tabla.

***Obs.:** el dispositivo tiene que enviar la dirección MAC en la solicitud de registro.*

9.8. Mantenimiento

Estado de los puertos

En la pantalla Estado de los puertos es posible seleccionar cualquier extensión y consultar información, como por ejemplo, si el puertos está en una llamada, con qué extensión y la duración de dicha llamada. Para las extensiones IP, se puede visualizar alguna información adicional sobre el aparato telefónico: nombre, versión, dirección IP, si está en un escenario NAT y si el aparato está personalizado para funcionar con la tarjeta ICIP de forma plena.



Menú Mantenimiento/Sub-Menú Estado de los puertos

Syslog

Syslog es el protocolo de envío de mensajes de Logs. Los logs registran la información del funcionamiento del sistema, como eventos y errores producidos, para su uso posterior.

Estos registros tienen formato de mensaje y, a través del Syslog, pueden ser almacenados internamente en la ICIP o enviados a un servidor de Syslog externo, tanto en la red local como en Internet, de acuerdo con el estándar del IETF para la RFC 5424.

Menú Mantenimiento/Submenú Syslog

Syslog

En esta guía es posible configurar el servidor de Syslog.

Menú Mantenimiento/Submenú Syslog/Syslog

- » **Habilitar:** habilita o deshabilita el syslog.
- » **Tamaño máximo del archivo de log:** define el tamaño del log almacenado en la ICIP, en KB.
- » **Habilitar servidor syslog remoto**: habilita el envío de log vía red a un servidor Syslog.
- » **Dirección del servidor syslog:** informe la dirección IP o el nombre del servidor Syslog que recibirá los mensajes de log del sistema.
- » **Nivel del log:** define niveles de información en los logs. Cuando más bajo en la lista, se mostrará más información.
- » **Emergency:** mensajes de emergencia
- » **Alert:** mensajes de alerta
- » **Critical:** mensajes críticos
- » **Error:** mensajes de error
- » **Warning:** mensajes de advertencia
- » **Notice:** mensajes de aviso
- » **Info:** mensajes de información
- » **Debug:** muestra todos los mensajes

Soporte a la señalización de correo de voz MWI

La configuración MWI (Message Waiting Indicator), es decir, indicador de mensaje en espera, es un recurso que permite a la central avisar a los aparatos terminales que tienen mensajes de voz nuevos o no escuchados. Los aparatos terminales normalmente transfieren esta información a los usuarios encendiendo una de las teclas o botones en el propio aparato.

***Obs.:** este recurso está presente en dispositivos compatibles con la señalización MWI y se puede encontrar en los aparatos terminales TIP 100, TIP 200/300.*

Actualización automática de contraseña para extensiones IP

Al realizar la alteración de contraseña en una extensión IP vía programador, la tarjeta ICIP envía automáticamente la nueva contraseña al teléfono registrado en esta extensión.

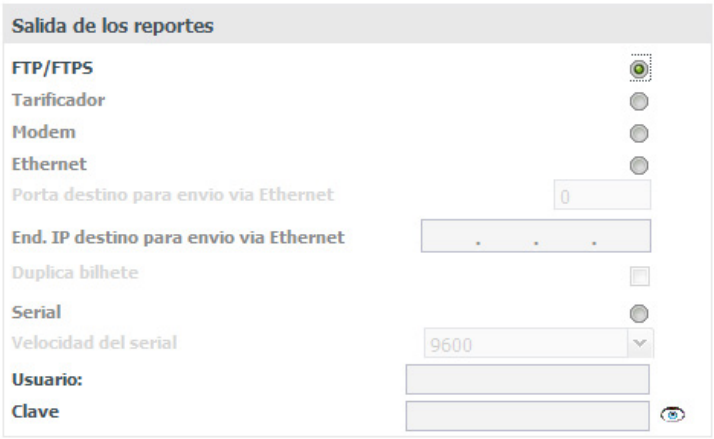
***Obs.:** algunos requisitos son necesarios para que esto funcione:*

Solamente teléfonos preparados para funcionar con la ICIP de forma plena. Funciona correctamente con teléfono IP TIP 100 y ATA 2210T.

El teléfono debe estar registrado en la cuenta en el momento de la modificación de la contraseña.

Colecta de billetes vía FTP/FTPS

La tarificación de las llamadas realizadas en la central puede ser recopilada a través del servicio FTP puesto a disposición por la ICIP.



Colecta de billetes vía FTP/FTPS

Para configurar, basta acceder a Sistema>Registro de Llamadas y configurar la salida de los billetes como FTP/FTPS y crear el usuario y contraseña que se van a utilizar para acceder vía FTP.

Actualización de firmware

Para actualizar la versión de firmware de la tarjeta ICIP, acceda al menú Grabación - Enviar, seleccione la opción Firmware ICIP, seleccione el archivo de firmware y presione Enviar. Se recomienda que el equipo sea actualizado con las versiones de firmware más actuales disponibles en nuestra página web.

Póliza de garantía

Este documento solamente es válido en el territorio de la República Mexicana.

Importado por:

Industria de Telecomunicación Electrónica Brasileña de México S.A. de C.V.

Avenida Félix Cuevas, 301 - 205 - Colonia Del Valle

Delegación Benito Juarez - C.P. 03100 - México - D.F.

Teléfono: + 52 (55) 56 87 74 84

soporte.tec@intelbras.com.mx | www.intelbras.com

Industria de Telecomunicación Electrónica Brasileña de México S.A. de C.V, se compromete a reparar o cambiar las piezas y componentes defectuosos del producto, incluyendo la mano de obra, o bien, el producto entero por un período de 1 año (3 meses por norma y 9 meses adicionales otorgados por el fabricante) a partir de la fecha de compra. Para hacer efectiva esta garantía, solamente deberá presentarse el producto en el Centro de Servicio, acompañado por: esta póliza debidamente sellada por el establecimiento en donde fue adquirido, o la factura, o el recibo, o el comprobante de compra, en donde consten los datos específicos del producto. Para las ciudades en donde no hay un centro de servicio, deberá solicitarse una recolección mediante el servicio de paquetería asignado por Intelbras, sin ningún costo adicional para el consumidor. El aparato defectuoso debe ser revisado en nuestro Centro de Servicio para evaluación y eventual cambio o reparación. Para instrucciones del envío o recolección favor comunicarse al Centro de Servicio:

Centro de Servicio y Distribuidor Autorizado

Intelbras

Avenida Félix Cuevas, 301 - 205 - Colonia Del Valle

Delegación Benito Juarez - C.P. 03100 - México - D.F.

56 87 74 84 Ciudad de México

01800 000 7484 Larga Distancia Nacional Sin Costo

soporte.tec@intelbras.com.mx

El tiempo de reparación en ningún caso será mayor de 30 días naturales contados a partir de la fecha de recepción del producto en el Centro de Servicio.

ESTA GARANTÍA NO ES VÁLIDA EN LOS SIGUIENTES CASOS:

a. Cuando el producto ha sido utilizado en condiciones distintas a las normales.
b. Cuando el producto no ha sido instalado o utilizado de acuerdo con el Manual de Usuario proporcionado junto con el mismo.
c. Cuando el producto ha sido alterado o reparado por personas no autorizadas por Industria de Telecomunicación Electrónica Brasileña de México S.A de C.V.
d. Cuando el producto ha sufrido algún daño causado por: accidentes, siniestros, fenómenos naturales (rayos, inundaciones, derrumbes, etc.), humedad, variaciones de voltaje en la red eléctrica, influencia de naturaleza química, electromagnética, eléctrica o animal (insectos, etc.).
e. Cuando el número de serie ha sido alterado.

Con cualquier Distribuidor Autorizado, o en el Centro de Servicio podrá adquirir las partes, componentes, consumibles y accesorios.

Datos del producto y distribuidor.

Producto:	Colonia:
Marca:	C.P.:
Modelo:	Estado:
Número de serie:	Tipo y número de comprobante de compra:
Distribuidor:	Fecha de compra:
Calle y número:	Sello:

Término de garantía

Queda expreso que esta garantía contractual es entregada mediante a las siguientes condiciones:

Nombre del cliente:

Firma del cliente:

Nº de la nota fiscal:

Fecha de la compra:

Modelo: Nº de serie:

Revendedor:

1. Todas las partes, piezas y componentes del producto están garantizados contra eventuales vicios de fabricación, que puedan presentarse, por el plazo de 1 (un) año, siendo este plazo de 3 (tres) meses de garantía legal más 9 (nueve) meses de la garantía contractual, contados a partir de la fecha de la compra del producto por el Señor Consumidor, conforme consta en la factura de compra del producto, que es parte integrante de este Término en todo el territorio nacional. Esta garantía contractual comprende el cambio gratuito de partes, piezas y componentes que presentan vicio de fabricación, incluyendo los gastos con la mano de obra utilizada en esta reparación. En el caso que no sea constatado vicio de fabricación, y si vicio(s) proveniente(s) de uso inadecuado, el Señor Consumidor será responsable de estos gastos.
2. La instalación del producto debe ser hecha de acuerdo con el Manual del Producto y/o Guía de Instalación. En el caso que su producto necesite la instalación y configuración por un técnico capacitado, busque a un profesional idóneo y especializado, siendo que los costos de estos servicios no están incluidos en el valor del producto.
3. Constatado el vicio, el Señor Consumidor deberá inmediatamente comunicarse con el Servicio Autorizado más cercano que conste en la relación ofrecida en el sitio *www.intelbras.com*, pues que exclusivamente estos están autorizados a examinar y sanar el defecto durante el plazo de garantía aquí previsto. Si esto no es respetado, esta garantía perderá su validez, ya que estará caracterizada la violación del producto.
4. En la eventualidad que el Señor Consumidor solicite atención domiciliaria, deberá enviarse al Servicio Autorizado más cercano para consulta de la tasa de visita técnica. En el caso sea constatada la necesidad de la retirada del producto, los gastos derivados, como las de transporte y seguridad de ida y vuelta del producto, quedan bajo la responsabilidad del Señor Consumidor.
5. La garantía perderá totalmente su validez en la ocurrencia de cualesquiera de las hipótesis a continuación: a) si el vicio no es de fabricación, pero si causado por el Señor Consumidor o por terceros extraños al fabricante; b) si los daños al producto son oriundos de accidentes, siniestros, agentes de la naturaleza (rayos, inundaciones, desprendimientos, etc.), humedad, tensión en la red eléctrica (sobretensión provocada por accidentes o fluctuaciones excesivas en la red), instalación/uso en desacuerdo con el manual del usuario o derivados del desgaste natural de las partes, piezas y componentes; c) si el producto ha sufrido influencia de naturaleza química, electromagnética, eléctrica o animal (insectos, etc.); d) si el número de serie del producto ha sido adulterado o rayado; e) si el aparato ha sido violado.
6. Esta garantía no cubre la pérdida de datos, por lo tanto, se recomienda, si es el caso específicamente del producto, que el Consumidor haga una copia de seguridad regularmente de los datos que constan en el producto.
7. Intelbras no se hace responsable por la instalación de este producto, y también por eventuales intentos de fraudes y/o sabotajes en sus productos. Se recomienda que el Señor Consumidor mantenga las actualizaciones del software y aplicaciones utilizadas en día, si es el caso, así como las protecciones de red necesarias para protección contra invasiones (hackers). El equipamiento está garantizado contra vicios dentro de sus condiciones normales de uso, siendo importante que se tenga consciencia de que, por ser un equipamiento electrónico, no está libre de fraudes y violaciones que puedan interferir en su correcto funcionamiento.

Siendo estas las condiciones de este Término de Garantía complementaria, Intelbras S/A se reserva el derecho de alterar las características generales, técnicas y estéticas de sus productos sin previo aviso.

El proceso de fabricación de este producto no está cubierto por los requisitos de la norma ISO 14001.

Todas las imágenes de este manual son ilustrativas.

Linux es una marca registrada de Linus Torvalds. Firefox es una marca registrada de Mozilla Foundation.

intelbras

fale com a gente / *hable con nosotros*

Brasil
Suporte a clientes: (48) 2106 0006
Fórum: forum.intelbras.com.br
Suporte via chat: intelbras.com.br/suporte-tecnico
Suporte via e-mail: suporte@intelbras.com.br
SAC: 0800 7042767
Onde comprar? Quem instala?: 0800 7245115

México
Contactos para clientes en México:
soporte.tec@intelbras.com.mx

Otros países
soporte@intelbras.com

Produzido por: / Producido por:
Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br | www.intelbras.com

04.19
Indústria brasileira
Fabricado en Brasil