



Manual do usuário
Manual del usuario

Placas Base e Codec ICIP 30
Placas Base y Codec ICIP 30

Índice

Português	5
1. Especificações técnicas	6
2. Características	6
3. Cuidados e segurança	7
4. Proteção e segurança de dados	7
4.1. Tratamento de dados pessoais	7
5. Cuidados e segurança	7
5.1. Proteção e segurança de dados	7
5.2. Diretrizes que se aplicam aos funcionários da Intelbras	7
5.3. Diretrizes que controlam o tratamento de dados	8
6. Produto	8
6.1. Placa Base ICIP 30	8
6.2. Posições de conexão Placa Codec ICIP 30 (1 a 3)	9
6.3. Proteção e segurança de dados	9
7. Produto	9
7.1. Tecnologia	9
7.2. VoIP	10
7.3. Protocolo SIP	10
8. Instalação	10
8.1. Recomendações técnicas	11
8.2. Chave de hardware ICIP	11
8.3. Licenças	11
9. Instalação	12
9.1. Cenário	12
10. Gerenciamento via navegador web	12
10.1. Ouvir os endereços IP	13
10.2. Programador Web	13
10.3. Sistema	14
10.4. Interfaces.	14
10.5. Rede	15
10.6. Administração	20
10.7. Menu VoIP - Placa ICIP 30 canais	37
10.8. Codec	44
Termo de garantia	48
Español	49
1. Especificaciones técnicas	50
2. Características	50
3. Cuidados y seguridad	51

4. Protección y seguridad de datos	51
4.1. Tratamiento de datos personales	51
5. Cuidados y seguridad	51
5.1. Protección y seguridad de datos	51
5.2. Directrices que se aplican a los funcionarios de Intelbras	51
5.3. Directrices que controlan el tratamiento de datos	52
6. Producto	52
6.1. Placa Base ICIP 30	52
6.2. Posiciones de conexión Placa Codec ICIP 30 (1 a 3)	53
6.3. Protección y seguridad de datos	53
7. Producto	53
7.1. Tecnología	53
7.2. VoIP	54
7.3. Protocolo SIP	54
8. Instalación	54
8.1. Recomendaciones técnicas	55
8.2. Llave de Hardware ICIP	55
8.3. Licencias	55
9. Instalación	56
9.1. Escenario	56
10. Administración vía navegador web	56
10.1. Escuchar las direcciones IP	56
10.2. Programador Web	57
10.3. Sistema	58
10.4. Interfaces	58
10.5. Red	59
10.6. Administración	64
10.7. Menú VoIP - Placa ICIP 30 canales	82
10.8. Codecs	83
Poliza de garantía	93
Término de garantía	94



Placas Base e Codec ICIP 30 Intelbras Impacta 94/140/220

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 para as centrais telefônicas da linha Impacta modelos Impacta 94, 140 e 220, aprimorando sua performance e garantindo uma alta disponibilidade de ligações.

A ICIP 30 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
Interface USB	2 portas USB host tipo A Compatíveis com USB 1.1/2.0
Canais VoIP	Até 30 canais (10 canais por Placa Codec ICIP 30/licenças liberadas na <i>Chave de Hardware ICIP</i>)
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.726 (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 G.729AB, 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.
- » Até 4 ramais IP e 1 juntor IP para cada canal VoIP (aquisição de licenças com Chave de Hardware ICIP).
- » Até 30 canais VoIP (utilizando até 3 submódulos do tipo Placa Codec ICIP 30).
- » Juntadores 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 plenamente compatível com os browsers Mozilla Firefox® 3.6 ou posterior.
- » Proteção do sistema via Firewall.
- » Controle de licenças via *Chave de Hardware ICIP*.
- » 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).
- » Acesso a banda larga via modem 3G. (modem não incluso).
- » 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 um técnico autorizado pode abrir a tampa do PABX, bem como 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 se aplicam aos funcionários da Intelbras

Os funcionários da Intelbras estão sujeitos a práticas de comércio seguro e confidencialidade de dados sob os termos dos procedimentos de trabalho da companhia.

É imperativo que as regras a seguir sejam observadas para assegurar que as provisões estatutárias relacionadas a serviços (sejam eles serviços internos ou administração e manutenção remotas) sejam estritamente seguidas. Isto preserva os interesses do cliente e oferece proteção pessoal adicional.

5.3. Diretrizes que controlam o tratamento de dados

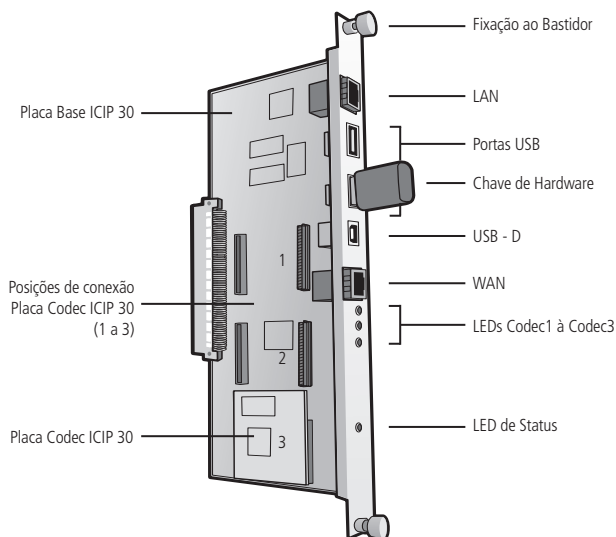
- » Assegurar que apenas pessoas autorizadas tenham acesso aos dados de clientes.
- » Usar as facilidades de atribuição de senhas, sem permitir qualquer exceção. Jamais informar senhas para pessoas não autorizadas.
- » Assegurar que nenhuma pessoa não autorizada tenha como processar (armazenar, alterar, 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.

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:

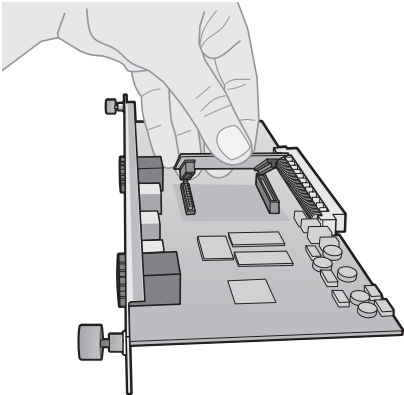
- » **Placa Base ICIP 30:** responsável pelo processamento das informações de rede, protocolos de acesso e conexões a rede do cliente e internet;
- » **Placa Codec ICIP 30:** responsável pelos canais VoIP disponíveis na Placa Base ICIP 30 e pelo processamento dos sinais de "voz" e a sua conversão em 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



ICIP : Interface de Comunicação IP

6.2. Posições de conexão Placa Codec ICIP 30 (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 como a Chave de Hardware ICIP de licenças para Ramais e Troncos SIP e modem 3G. 1 Porta USB D para uso da Assistência Técnica.	
Interface de rede WAN	Porta UTP fast Ethernet RJ45 10/100 para conexão externa de acesso a internet.	
LEDs de Codec1 à Codec3 (um para cada módulo) Placa Codec ICIP 30	Cadência	Estado
	Permanentemente apagado	Módulo com ID inválido ou módulo não detectado
	Permanentemente aceso	Módulo com ID válido detectado, mas não inicializado
	Piscando muito rapidamente (100 ms ON / 100 ms OFF)	Módulo sendo inicializado (download de firmware)
	Piscando rapidamente (300 ms ON / 300 ms OFF)	Módulo inicializado e FW operando
LED indicativo do status da Placa Base ICIP 30	Piscando intermitente (1.400 ms ON / 100 ms OFF)	Falha de inicialização do módulo
	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)
Parafusos de fixação	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	Existem 3 posições disponíveis para a conexão, podendo assim atingir até 30 canais VoIP (depende das licenças adquiridas através da Chave de Hardware ICIP).	

7. Produto

7.1. Tecnologia

Visão geral

Com a Placa ICIP a central Impacta 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, siga o procedimento:

1. Em uma superfície aterrada conecte a pulseira antiestática;
2. Retire a Placa Base ICIP 30 e a/a Placa Codec ICIP 30 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 sobre a superfície e insira a(as) Placa 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;
8. Desligue a alimentação AC da central Impacta e retire a tampa frontal;
9. A Placa Base ICIP 30 pode ser conectada em qualquer uma das posições disponíveis do backplane, mas recomendamos que seja inserida no centro, devido aos cabos de rede e periféricos instalados nas portas USB;
10. Após o encaixe, certifique-se de que os parafusos de fixação do perfil da placa estejam devidamente apertados. Estes parafusos, além da fixação, também são responsáveis pelo aterramento dos conectores;
11. Conecte os cabos da rede LAN e WAN nos respectivos conectores RJ45, a Chave de Hardware ICIP de Licenças e o modem 3G, caso tenha, nas portas USB;
12. Organize e identifique os cabos de rede junto com os demais cabos no DG da central e no caso de utilizar um modem 3G deixe-o para fora do espaço interno do backplane onde não possa comprometer a circulação forçada de ar. Dependendo do modelo, talvez seja necessário utilizar um cabo USB extensor;
13. Antes de colocar em serviço o sistema, deve ser efetuada 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;

14. Recoloque a tampa frontal e ligue a alimentação AC da central Impacta;
15. Após a inicialização do sistema confira, através do *Programador Web / Menu Interfaces / Disposição placas*, se nenhuma placa está programada para utilizar aquele slot;
16. Programe os dados necessários através do Programador Web.

8.1. Recomendações técnicas

Este 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 uma 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. Chave de hardware ICIP

A Chave de Hardware ICIP é um dispositivo do tipo USB, inserida no painel da Placa ICIP liberando as licenças de ramais e troncos SIP adquiridos.

O sistema permite a configuração de 1 juntor IP e até 4 ramais IP para cada canal VoIP presente no sistema. Então, o número de ramais e juntores IP depende das Licenças e da programação do sistema, sendo no máximo 120 ramais e 30 juntores IP.

Obs.: ao retirar a chave de hardware da central telefônica Impacta em funcionamento, as ligações VoIP (ramais e troncos IP) deixarão de funcionar após alguns segundos.

8.3. Licenças

As licenças são adquiridas no momento da compra ou quando for necessário aumentar o número de ramais e/ou juntores IP. Para consultar as licenças disponíveis, acesse o *Programador Web / Menu Sistema / Licenças*, onde é possível visualizar o ID da chave e as licenças existentes.

Após a consulta das licenças disponíveis, caso queira aumentar a quantidade de troncos e/ou ramais, não é necessário trocar a chave de hardware da central. Consulte uma revenda autorizada Intelbras de posse do ID da chave e solicite a compra de mais licenças. A revenda irá gerar um arquivo criptografado para esta chave de hardware e enviar o arquivo.

Através do *Programador Web* o arquivo criptografado, contendo as novas licenças, pode ser inserido na chave de hardware, liberando mais ramais e/ou troncos IP.

10.1. Ouvir os endereços IP

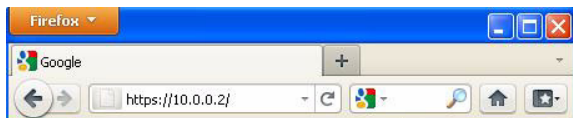
A placa ICIP pode ser configurada para obter o endereço IP automaticamente, via DHCP. Nesse caso o PABX disponibiliza uma forma de o usuário escutar o endereço IP obtido. O usuário, usando um telefone, deve digitar os seguintes comandos:

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

Abra seu navegador web (recomendado Firefox 4.0) 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, verifique se seu navegador não possui bloqueio de pop-ups ou não há algum 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

10.2. 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.

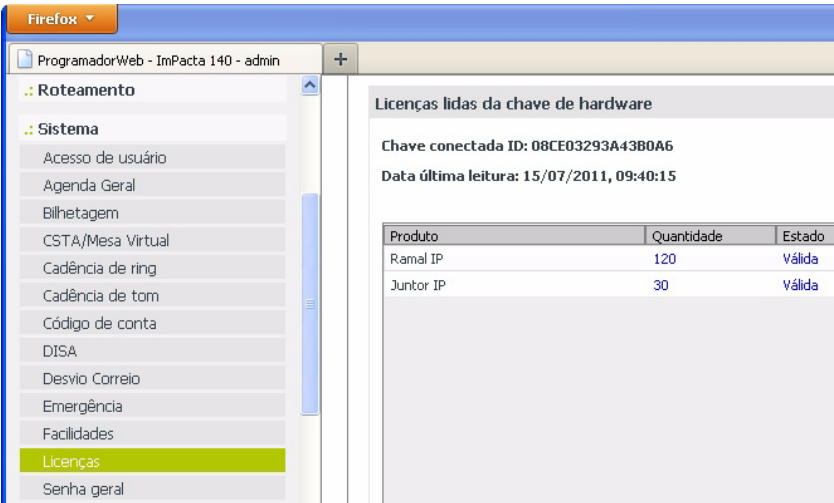
Atenção: o processo de criação e configuração de ramais e juntores IP é semelhante ao dos ramais e troncos analógicos, no mesmo menu de *Configuração>Portas*.

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:

10.3. Sistema

Licenças

Acessando este submenu é exibido o status da *Chave de Hardware ICIP* (Conectada ou Desconectada), o ID da chave e o número de licenças válidas para ramais IP e jutores IP.



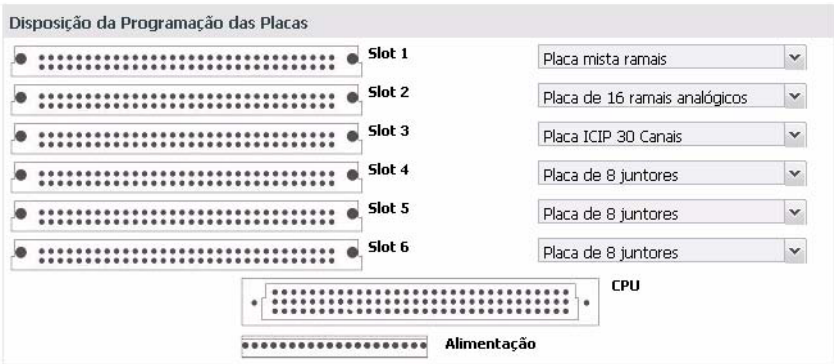
Visualização/confirmação da conexão da Chave Hardware e suas Licenças

10.4. 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";
2. Confirme esta operação;
3. Selecione a Placa Base ICIP 30 para aquele slot (neste exemplo 30 canais).

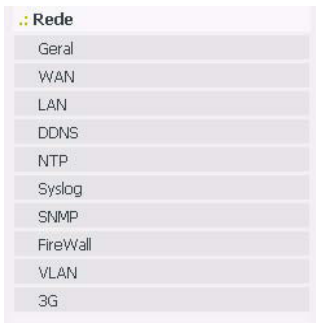


Localização/atualização para Placa Base ICIP 30

10.5. 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.

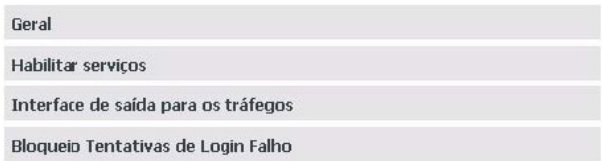
Atenção: algumas destas informações podem ser obtidas junto ao administrador de rede ou técnico de informática.



Menu Rede e seus componentes

Geral

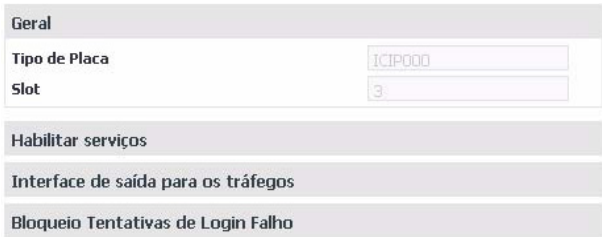
Este submenu apresenta as informações gerais sobre a rede e os parâmetros disponíveis para a configuração, distribuídos nas seguintes guias:



Menu Rede/ SubMenu Geral

Guia Geral

Apresenta as informações físicas da placa para o administrador.



Menu Rede - 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 serviços

Aqui podem ser selecionados os serviços a serem utilizados, assim como algumas facilidades da rede para o sistema. A escolha destes itens, irá ter um reflexo direto no Menu Rede, onde serão habilitados os submenus equivalentes para futuras configurações.

Geral	
Habilitar serviços	
Habilitar	
DDNS	☒
NTP	☒
Syslog	☒
SNMP	☒
Firewall	☒
VLAN	☒
Número de VLANs	2
Fuso Horário	Brasilia
Horário de verão	☐
Interface de saída para os tráfegos	
Bloqueio Tentativas de Login Falho	

Menu Rede / Submenu Geral / Habilitar serviços

- » **DDNS**: habilita o item DDNS.
- » **NTP**: habilita o item NTP.
- » **Syslog**: habilita o item Syslog.
- » **SNMP**: habilita o item SNMP.
- » **Firewall**: habilita o item Firewall.
- » **VLAN**: 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.
- » **Fuso Horário**: permite selecionar o fuso horário local.
- Padrão de fábrica**: hora oficial do Brasil - Brasília GMT -03:00. A hora pode ser alterada dependendo da localidade em que se encontre. Este item será utilizado quando habilitada a opção de utilizar *Servidor NTP*.
- » **Horário de Verão**: adianta em 1 hora o horário obtido do servidor NTP ou configurado manualmente.

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.

Geral	
Habilitar serviços	
Interface de saída para os tráfegos	
Interface de saída para os tráfegos	LAN
Bloqueio Tentativas de Login Falho	

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.

Bloqueio Tentativas de Login 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 analisados por esta regra, ficando livres de bloqueio.

Geral

Habilitar serviços

Interface de saída para os tráfegos

Bloqueio Tentativas de Login Falho

Bloqueio de tentativas de login

☒

Número de tentativas de login falho

2

Período de verificação (segundos)

3

Tempo de bloqueio (segundos)

5

End. IP (Exceção)

Adicionar

Remover

Whitelist

10.1.1.1

Menu Rede/ SubMenu Geral/Bloqueio Tentativas de Login Falho

- » **Bloqueio de tentativas de login:** habilita o serviço de verificação da autenticação dos logins dos usuários no sistema.
- » **Número de tentativas de login 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.

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:

WAN

Habilitar tráfego

QoS

Rotas

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.

WAN

Velocidade de acesso meio físico

Auto-Negociação

Obter endereço IP automaticamente (DHCP)

☐

Endereço IP

10 . 1 . 30 . 18

Máscara de sub-rede

255 . 255 . 255 . 0

Gateway padrão

10 . 1 . 30 . 1

Servidor DNS preferencial

.

Servidor DNS alternativo

.

Endereço MAC

1 : 2 : 3 : 4 : 5 : 6

Upload

100000

kbps

Download

100000

kbps

Habilitar tráfego

QoS

Rotas

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. 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.

WAN	
Habilitar tráfego	
SIP	☒
RTP	☒
Administração	☒
QoS	
Rotas	

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 (switches e roteadores) dar prioridade ao tráfego de voz.

WAN				
Habilitar tráfego				
QoS				
Habilitar QoS de camada 3 ☒				
SIP:	TOS	▼	(tipo)	0 (valor)
RTP:	TOS	▼	(tipo)	0 (valor)
Administração:	TOS	▼	(tipo)	0 (valor)
Rotas				

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 switches 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 saínte 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.

10.6. 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.

WAN			
Habilitar tráfego			
QoS			
Rotas			
Destino	Gateway	Upload	Download
1.			
2.			
3.			
4.			
5.			

- » **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, distribuídos nas seguintes guias:

LAN

Habilitar tráfego

QoS

Rotas

Menu Rede/ SubMenu LAN

LAN

Permite a configuração dos parâmetros de conexão física e endereçamento referentes à interface LAN. Portanto é importante consultar o administrador de rede para obter os dados necessários.

LAN

Velocidade de acesso meio físico

Auto-Negociação

Obter endereço IP automaticamente (DHCP)

☐

Endereço IP

10 . 1 . 30 . 12

Máscara de sub-rede

255 . 255 . 255 . 0

Gateway padrão

10 . 1 . 30 . 1

Servidor DNS preferencial

.

Servidor DNS alternativo

.

Endereço MAC

aa : da : da : da : ea : fa

Largura de banda para internet (link provedor)

Upload

:00000

Download

:00000

Habilitar tráfego

QoS

Rotas

Menu Rede/ SubMenu LAN/LAN

- » **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 recomendamos a opção de *AutoNegociação*, caso não exista nenhuma indicação do administrador de rede.
- » **Obter endereço IP automaticamente (DHCP):** disponibiliza 2 opções de acesso a rede LAN:
- » **Selecionado:** o acesso á rede LAN 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 á rede LAN será estático, isto é, será necessário preencher os campos: Endereço IP, Máscara de Rede, IP do Gateway e IP dos servidores DNS, de acordo com as especificações do administrador de rede.
- » **Endereço IP:** define o endereço IP da interface LAN da placa.
- » **Máscara de sub-rede:** define os valores da máscara de sub-rede da interface LAN.
- » **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 porte que este endereço IP seja o mesmo do endereço de gateway (roteador de saída).

- » **Endereço MAC:** informe o endereço de MAC da placa para a interface LAN.
- » **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 LAN disponível, para poder manter o equilíbrio na conexão e evitar qualquer saturação e consequente perda de qualidade.

Habilitar tráfego

Aqui são habilitados os tráfegos de administração e sinalização SIP e RTP (relativos ao tráfego de voz) na rede LAN.

LAN	
Habilitar tráfego	
SIP	☒
RTP	☒
Administração	☒
QoS	
Rotas	

Menu Rede/ SubMenu LAN/Habilitar tráfego

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

LAN					
Habilitar tráfego					
QoS					
Habilitar QoS de camada 3					☐
SIP:	TOS	▼	(tipo)	0	(valor)
RTP:	TOS	▼	(tipo)	0	(valor)
Administração:	TOS	▼	(tipo)	0	(valor)
Rotas					

Menu Rede/ SubMenu LAN/QoS

Habilitar QoS de camada 3

Nos campos indicados nesta tela existe a opção de seleccionar 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 seleccionado 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):** 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 saínte 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 LAN, criando caminhos pré-determinados, onde as informações podem ser direcionadas até um host ou uma outra rede específica.

LAN

Habilitar tráfego

QoS

Rotas

	Destino	Gateway	Download	Upload
1.				
2.				
3.				
4.				
5.				

Menu Rede/ SubMenu LAN/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.

DDNS

Com o DDNS (Dynamic Domain 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.

Atenção: a configuração do serviço de DNS dinâmico para o sistema só será possível após a habilitar deste submenu no item *Habilitar serviços*.

DDNS - DNS Dinâmico

Menu Rede/ SubMenu DDNS

DDNS - DNS Dinâmico

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.

DDNS - DNS Dinamico	
Endereço do servidor DDNS	(IP/FQDN)
Habilitar DDNS para a WAN	☐
Login	
Senha	
Tempo de atualizacao no servidor	600

Menu Rede/ SubMenu DDNS/DDNS

- » **Endereço do servidor DDNS:** informe o endereço IP ou nome cadastrado no DynDNS, ex: ictp.dyndns.org.
- » **Habilitar DDNS para a WAN:** habilita a atualização do DynDNS para a interface de saída para a internet.
- » **Login:** digite o login de usuário no DynDNS.
- » **Senha:** digite a senha de usuário no DynDNS.
- » **Tempo de atualização no servidor:** 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.

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*.

NTP

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: antes de inserir os servidores de NTP certifique-se de que as configurações de fuso horário e horário de verão estão corretas no item *Habilitar serviços*.

NTP		
Servidor NTP Primario	200.160.0.8	(IP/FQDN)
Servidor NTP Secundario		(IP/FQDN)
Servidor NTP Terciario		(IP/FQDN)

Menu Rede/ SubMenu NTP/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.

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>.

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.

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

Este serviço não funcionará corretamente se as configurações de data e hora não estiverem corretas.

Syslog

Menu Rede/ SubMenu Syslog

Syslog

Nesta guia é possível configurar o servidor de Syslog.

Syslog	
Tamanho máximo do arquivo de log	200 (kB)
Habilitar servidor syslog remoto	☐
Endereço do servidor syslog	(IP/FQDN)

Menu Rede/ SubMenu Syslog/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.

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*.

Engine ID
SNMP v1 e v2
TRAP
SNMP V3
Criptografia SNMP V3

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.

Engine ID
Utilizar padrão ☒
Ajustado pelo Administrador [80661A04]
SNMP v1 e v2
TRAP
SNMP V3
Criptografia SNMP V3

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.

Engine ID										
SNMP v1 e v2										
Habilitar SNMP V1 e V2 ☐										
<table><tr><th>Nome da comunidade</th><th>Tipo de acesso</th></tr><tr><td>1. </td><td>Somente leitura </td></tr><tr><td>2. </td><td>Somente leitura </td></tr><tr><td>3. </td><td>Somente leitura </td></tr><tr><td>4. </td><td>Somente leitura </td></tr></table>	Nome da comunidade	Tipo de acesso	1.	Somente leitura	2.	Somente leitura	3.	Somente leitura	4.	Somente leitura
Nome da comunidade	Tipo de acesso									
1.	Somente leitura									
2.	Somente leitura									
3.	Somente leitura									
4.	Somente leitura									
TRAP										
SNMP V3										
Criptografia SNMP V3										

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.

Engine ID

SNMP v1 e v2

TRAP

Habilitar o envio de TRAP ☐

	Versão	Tipo de Notificação	Comunidade	Destino
1.	v1	Trap		
2.	v1	Trap		
3.	v1	Trap		
4.	v1	Trap		

SNMP V3

Criptografia SNMP V3

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.

Engine ID

SNMP v1 e v2

TRAP

SNMP V3

Habilitar SNMP v3 ☐

Usuário	Tipo de Acesso	Modo	Tipo Senha	Senha
1.	Somente leitura	authPriv	MD5	
2.	Somente leitura	authPriv	MD5	
3.	Somente leitura	authPriv	MD5	
4.	Somente leitura	authPriv	MD5	

Criptografia SNMP V3

Menu Rede/ SubMenu SNMP/SNMP V3

- » **Habilitar SNMP v3:** habilita os serviços de autenticação e privacidade por usuário.
- » **Menu Rede**
- » **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 algoritmo 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.

Engine ID

SNMP v1 e v2

TRAP

SNMP V3

Criptografia SNMP V3

Tipo de criptografia	Senha de criptografia
1. AES	
2. AES	
3. AES	
4. AES	

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.

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.

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

Firewall

Menu Rede/ SubMenu Firewall

Firewall

Nesta guia o Firewall da ICIP verifica as informações e solicitações vindas da rede, bloqueando ou permitindo seu acesso.

Firewall		
Permitir acesso as interfaces de administracao (Web, ICTI, SNMP) ☐		
Endereço 1		
Endereço 2		
Endereço 3		
Endereço 4		
Endereço 5		
Ativar anti-DoS ☐		
Limite de SYN Flood:	☐ 100	(pac/s)
Limite de FIN Flood:	☐ 100	(pac/s)
Limite de UDP Flood:	☐ 100	(pac/s)
Limite de ICMP Flood:	☐ 100	(pac/s)
Limite de SYN Flood por origem:	☐ 100	(pac/s)
Limite de FIN Flood por origem:	☐ 100	(pac/s)
Limite de UDP Flood por origem:	☐ 100	(pac/s)
Limite de ICMP Flood por origem:	☐ 100	(pac/s)
Port Scan TCP/UDP:	☐ Baixa	(sensib)
Ativar bloqueio da origem ☐		
Tempo de bloqueio:	3600	(s)

Menu Rede/ SubMenu Firewall/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.

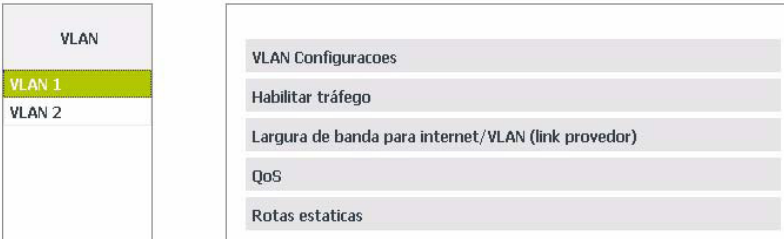
- » **Port Scan TCP/UDP:** ativa a detecção de tentativas de portscan na ICIP. Portscan é o nome dado a técnica de escanear as portas abertas em um dispositivo de rede para determinar quais serviços este dispositivo disponibiliza. Com esta opção é possível detectar um dispositivo fazendo portscan na 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.

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.

VLAN Configurações	
VLAN_NUMBER	1
VLAN ID	1
Prioridade IEEE 802.1q	Melhor esforço
Obter endereço IP automaticamente (DHCP)	☐
Endereço IP	. . .
Máscara de sub-rede	. . .
Gateway padrão	. . .
Habilitar tráfego	
Largura de banda para internet/VLAN (link provedor)	
QoS	
Rotas estáticas	

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 saindo 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.

VLAN Configuracoes	
Habilitar tráfego	
SIP	☒
RTP	☒
Administracao	☒
Largura de banda para internet/VLAN (link provedor)	
QoS	
Rotas estaticas	

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.

VLAN Configuracoes	
Habilitar tráfego	
Largura de banda para internet/VLAN (link provedor)	
Upload	100000
Download	100000
QoS	
Rotas estaticas	

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.

VLAN Configuracoes

Habilitar tráfego

Largura de banda para internet/VLAN (link provedor)

QoS

Habilitar QoS de camada 3☐

SIP:

TOS

(tipo)

0

(valor)

RTP:

TOS

(tipo)

0

(valor)

Administração:

TOS

(tipo)

0

(valor)

Rotas estaticas

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 switches 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 saiente 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.

VLAN Configuracoes			
Habilitar tráfego			
Largura de banda para internet/VLAN (link provedor)			
QoS			
Rotas estaticas			
	Destino	Gateway	Download Upload
1.			
2.			
3.			
4.			
5.			

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.

3G

Este submenu apresenta as informações necessárias para instalar um modem 3G na ICIP, disponibilizando para o sistema a tecnologia 3G para acesso a internet.

Atenção: consulte no site da Intelbras a lista de modems homologados para funcionar com a ICIP.

3G
Configurações avançadas
Largura de banda para internet (link provedor)
Habilitar Tráfego
Rotas Estáticas / Rede Destino

Menu Rede/ SubMenu 3G

3G

Permite a configurar o sistema com as informações necessárias para o acesso 3G.

3G	
Habilitar 3G	☐
Número de acesso	
Usuário	
Senha	
Configurações avançadas	
Largura de banda para internet (link provedor)	
Habilitar Tráfego	
Rotas Estáticas / Rede Destino	

Menu Rede/ SubMenu 3G/3G

- » **Habilitar 3G:** habilita a interface de acesso 3G no sistema.
- » **Número de acesso:** insira o número de acesso fornecido pela operadora 3G.
- » **Usuário:** digite o usuário de autenticação de acordo com a operadora 3G.
- » **Senha:** digite a senha de autenticação de acordo com a operadora 3G.

Configurações avançadas

Permite a configuração dos parâmetros do ponto de acesso de Internet e o tipo de autenticação junto a operadora 3G.

3G	
Configurações avançadas	
APN	
Código PIN	1234
Automática	☒
PAP	☐
CHAP	☐
Largura de banda para internet (link provedor)	
Habilitar Tráfego	
Rotas Estáticas / Rede Destino	

Menu Rede/ SubMenu 3G/ Configurações avançadas

- » **APN:** informe o endereço APN (Access Point Name) da operadora 3G, isto é, o endereço do ponto de acesso a internet (por exemplo, bandalarga.claro.com.br).
- » **Código PIN:** insira o código PIN (Personal Identification Number) de acordo com a operadora 3G (normalmente não é necessário informar).
- » **Automática, PAP e CHAP:** disponibilizam o método de autenticação do usuário e senha de acordo com a operadora 3G.
 - » **Automática:** o sistema seleciona a autenticação.
 - » **PAP (Password Authentication Protocol):** é um protocolo utilizado para autenticar usuários de uma forma simples. O envio da senha é feita em ASCII de forma não encriptada.
 - » **CHAP (Challenge-Handshake Authentication Protocol):** tem a mesma função do PAP, porém envia a senha de forma encriptada.

Largura de banda para internet (link provedor)

Nesta guia são configuradas as velocidades contratadas da banda do provedor 3G dentro da rede.

3G	
Configurações avançadas	
Largura de banda para internet (link provedor)	
Upload	100000 kbps
Download	100000 kbps
Habilitar Tráfego	
Rotas Estáticas / Rede Destino	

Menu Rede/ SubMenu 3G/Largura de banda para internet (link provedor)

- » **Upload e Download:** são definidas as taxas máximas para a conexão com o link provedor 3G em função dos equipamentos conectados. É importante saber as taxas de upload e download com a interface 3G disponível, para poder manter o equilíbrio na conexão e evitar qualquer saturação e consequente perda de qualidade.

Habilitar tráfego

Aqui são habilitados os tráfegos de administração e de pacotes de sinalização SIP e RTP (relativos ao tráfego de voz), na interface 3G.

3G	
Configurações avançadas	
Largura de banda para internet (link provedor)	
Habilitar Tráfego	
SIP	☒
RTP	☒
Administração	☒
Rotas Estáticas / Rede Destino	

Menu Rede/ SubMenu 3G/Habilitar tráfego

- » **SIP:** habilita o tráfego dos pacotes de sinalização SIP junto a interface 3G configurada.
- » **RTP:** habilita o tráfego dos pacotes de sinalização RTP junto a interface 3G, fornecendo um meio uniforme para transmitir dados sujeitos a “problemas” de tempo real (áudio, vídeos,...).
- » **Administração:** habilita a administração do tráfego de administração na interface 3G. Isto pode ser utilizado para evitar acesso às configurações de administração por pessoas não autorizadas.

Rotas estáticas/Rede Destino

Esta configuração permite definir rotas específicas para sub-redes de destino do lado da interface 3G, criando caminhos pré-determinados, onde as informações podem ser direcionadas até um host ou uma outra rede específica.

3G

Configurações avançadas

Largura de banda para internet (link provedor)

Habilitar Tráfego

Rotas Estáticas / Rede Destino

Rota 1	
Rota 2	
Rota 3	
Rota 4	
Rota 5	

Menu Rede/ SubMenu 3G/Rotas estáticas/Rede Destino

Rota 1, 2, 3, 4 e 5

No campo *Rota* são informados os endereços IPs e a máscara (endereços IP / netmask tipo CIDR) das rotas destino.

10.7. Menu 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.

VoIP - Placa ICIP 30 canais

Geral

Ponto a ponto

Proxy

Autoconfiguração Ramais IP

Menu VoIP - Placa ICIP e seus componentes

Geral

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

VOIP Geral

Codecs

Reserva Canais VoIP

Menu VoIP - Placa ICIP / SubMenu Geral

VoIP Geral

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

VOIP Geral

Enviar eventos DTMF
(apenas para ramais IP)

SIP info

Valor do payload se RFC2833

101

Jitter buffer Adaptável:

☐

40

mínimo atraso (ms)

☐

100

máximo atraso (ms)

Jitter buffer fixo

☒

40

atraso (ms)

Cancelamento de eco

☒

SIP keep alive:

☐

60

período(s)

Codecs

Reserva Canais VoIP

Menu VoIP - Placa ICIP/SubMenu Geral/ VoIP Geral

- » **Enviar eventos DTMF (apenas para ramais IP):** 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.
Obs.: para o correto funcionamento dos ramais IP utilize sempre o método SIP INFO.
- » **Valor do payload se RFC2833:** configura 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.
- » **SIP keep alive:** quando habilitado, o sistema envia periodicamente uma mensa-gem SIP ao destino da ligação, com o intuito de manter a sessão da NAT (Network Address Translation) disponível. Padrão 60s.
- » **Jitter buffer adaptável:** 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 ruim. 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. Tecnicamente é mais simples porém, apresenta desempenho inferior pois não consegue acompanhar o comportamento da rede. O padrão é 40 ms.
- » **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.

Codecs

A função dos codecs é reduzir a largura de banda necessária para a 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.

VOIP Geral	
Codecs	
Codecs	Tempo empacotamento (ms)
1. G729	20
2. GSM FR 6.10	20
3. G725-40	10
4. G725-40	10
5. G725-32	20

Reserva Canais VoIP	
---------------------	--

Menu VoIP - Placa ICIP/SubMenu Geral/ Codecs

- » **Opção de 1 a 5:** definem a ordem de preferência dos Codecs (7 opções) e o período do Pacote RTP, quando se realiza ou se recebe uma ligação.
- » **Codecs:** possuem diferentes relações de compressão, qualidade de áudio e ocupação de largura de banda. A ICIP suporta os codecs: G.729AB, GSM FR 6.10, G.726 e G.711 PCMa e u.
- » **Período do pacote RTP:** 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.

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).

VOIP Geral	
Codecs	
Reserva Canais VoIP	
Reservar canais VoIP	☒
Canais para Juntores IP	15
Canais para Ramais IP	15
Canais sem reserva	0
Habilitar economia de canal VoIP	☒
FAX	T.38

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 VoIP:** 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.

- » **FAX:** define qual codec será utilizado para envio e recebimento de fax pela rede VoIP.
- » **Bypass:** é utilizado quando se deseja que o PABX envie e receba os sinais de FAX na banda de áudio.
- » **T.38:** é utilizado quando se deseja que o PABX envie e receba os sinais de FAX via protocolo T.38.
- » **Desabilitado:** desativa o envio/recepção de fax pela ICIP.

Ponto a ponto

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

NAT
Numeração

Menu VoIP - Placa ICIP/ SubMenu Ponto a ponto

NAT

A guia NAT (Network Address Translation) possibilita a configuração dos parâmetros para que a central possa acessar dispositivos IP que estão atrás de NAT (consegue-se estabelecer corretamente os endereços IP envolvidos no fluxo RTP).

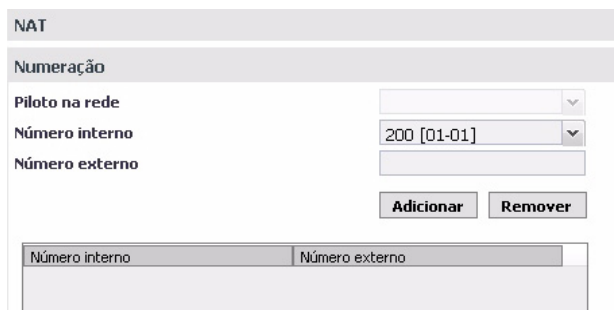
NAT	
☒ Nenhuma	
☐ Endereço público do NAT	(IP/FQDN)
☐ Endereço do STUN TURN ICE	(IP/FQDN)
Porta do STUN TURN ICE	3478
Enviar eventos DTMF:	Out of band (RFC2833) ▼
Valor do payload se RFC2833:	01
Numeração	

Menu VoIP - Placa ICIP/SubMenu Ponto a ponto/ NAT

- » **Nenhuma:** quando habilitado, o sistema não utilizará NAT para comunicação. Essa opção só pode ser escolhida se não houver necessidade de comunicação com dispositivos IP atrás de NAT.
 - » **Endereço público do NAT:** informe o endereço IP ou nome público do gateway NAT.
 - » **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.
- Obs.:** o método In-Band só pode ser escolhido caso a(s) rede(s) envolvida(s) na ligação seja(m) controlada(s) e o codec seja G.711A ou G.711u.
- » **Valor do payload se RFC2833:** configura 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.

Numeração

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



Número interno	Número externo
----------------	----------------

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

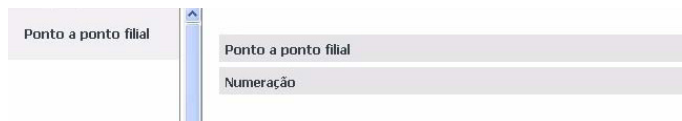
- » Piloto na rede define o número externo que será usado como assinante chamador caso o ramal originador da ligação não esteja cadastrado na tabela.
- » Número interno selecione o ramal que poderá encaminhar e receber ligação VoIP envolvendo as filiais.
- » Número externo informe o número VoIP pelo 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)
- » **IP:** informe o endereço IP da central ou dispositivo VoIP da Filial.

Numeração

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

Ponto a ponto filial

Numeração

Número interno

Número externo

Adicionar **Remover**

Número interno	Número externo

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.

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.

Ao selecionar este submenu, é apresentada uma guia onde é/está cadastrada a operadoras 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).

Servidor de registro

- VOIP proxy
- Numeração
- Codec
- VOIP proxy - Avançado

Menu VoIP - Placa ICIP/ SubMenu Proxy

VoIP proxy

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

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

VOIP proxy

Estado da Operadora:

Operadora:

Endereço do servidor (IP ou FQDN):

Porta do servidor:

Bloquear DDC ☐

Considerar DDC se assinante origem iniciar com

Numeração

Codec

VOIP proxy - Avançado

Menu VoIP - Placa ICIP/SubMenu Proxy/ VoIP proxy

- » **Estado da Operadora:** podemos visualizar se a operadora está operacional perante o sistema (Operadora contatável).
- » **Operadora:** entre com o nome da Operadora VoIP .
- » **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:** define 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 ramos que irão gerar e receber ligações VoIP.

Núm. interno	Nome externo	Identif. Chm	Senha	Estado
--------------	--------------	--------------	-------	--------

Menu VoIP - Placa ICIP/SubMenu Proxy/ Numeração

- » **Localidade:** informe um nome que faça referência a localidade onde a central esta instalada.
- » **Nome Piloto:** define o número que será usado como assinante chamador caso o ramal originador da ligação não esteja cadastrado na tabela.
- » **Originar ligação sempre usando o piloto:** selecionado, as ligações externas utilizarão o “valor” do campo Nome Piloto como assinante chamador para todas as chamadas originadas.
- » **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 12 dígitos.
- » **Utilize os botões Adicionar e Remover:** administre os números internos/nomes desejados.

10.8. Codec

A função dos codecs é reduzir a largura de banda necessária para a 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.

VOIP proxy	
Numeração	
Codec	
1. G729	20 (ms)
2. GSM FR G.10	20 (ms)
3. G726-32	30 (ms)
4. PCMA	20 (ms)
5. PCM.U	20 (ms)

VOIP proxy - Avançado

Menu VoIP Placa ICIP/SubMenu Proxy/ Codec

- » **Opção de 1 a 7:** 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 áudio e ocupação de largura de banda. A ICIP suporta os codecs: G.729AB, GSM FR 6.10, G.726 e G.711 PCMA e u.
- » **Período do pacote RTP:** 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.

VOIP proxy - Avançado

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

VOIP proxy	
Numeração	
Codec	
VOIP proxy - Avançado	
Nome de domínio:	
Porta RTP Min:	5000
Porta RTP Max:	5535
Habilitar envio de tempo entre registro:	☒
Tempo entre registro (s):	3600
Enviar eventos DTMF:	Out of band (RFC2833)
Valor do payload se RFC2833:	101
Cancelamento de eco:	☒
FAX	Eypass
Endereço do OutBound Proxy (IP ou FQDN):	
Porta do OutBound Proxy:	5060
ToS/DiffServ-pacote RTP:	E8
ToS/DiffServ-pacote sinalização:	E0
Suporte a Número Global (E.164):	☐
Flash no junitor usar c = 0.0.0.0 (RFC 2543) no DSP:	☐

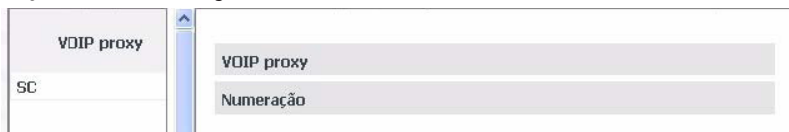
Menu VoIP - Placa ICIP/SubMenu Proxy/ Avançado

- » **Nome de domínio:** informe o nome de domínio do provedor VoIP. É uma informação enviada na requisição de registro e no envio de INVITE (ex.: Na mensagem "INVITE SIP: 6504@xpto.com.br" xpto.com.br é o nome de domínio).
- » **Porta RTP Min e Porta RTP Max:** 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.
- » **Habilitar envio de tempo entre registro:** quando habilitado, o sistema disponibiliza a opção de especificar o tempo entre registro(s).
- » **Tempo entre registro(s):** permite especificar com que frequência a central irá atualizar seu registro com a Operadora VoIP. Padrão de fábrica: 3600 segundos.
- » **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.
- 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.
- » **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.
- » **FAX:** define qual codec que será utilizado para envio e recebimento de fax pela rede VoIP.
 - » **Bypass:** utilizado se o dispositivo de fax for conectado em um adaptador ATA para a rede VoIP.
 - » **T.38:** É utilizado se o dispositivo de fax e o provedor VoIP forem compatíveis com o protocolo T.38.
 - » **Desabilitado:** desativa o envio/recepção de fax pela ICIP.

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



VOIP proxy	Numeração
SC	

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.



VOIP proxy	Numeração
Localidade	

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.

The screenshot shows a web interface titled "VOIP proxy". Under the "Numeração" section, there are two input fields: "Número interno" and "Nome externo (registro na operadora)". Below these fields are two buttons: "Adicionar" and "Remover". At the bottom, there is a table with two columns: "Número interno" and "Nome externo".

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.

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 disponíveis 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 sequência o administrador pluga o próximo ramal.

Lista de ramais pertencentes a autoconfiguração de terminais IP

Menu VoIP - Placa ICIP/ SubMenu Auto configuração ramais IP

O telefone TIP100, ao inicializar 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 TIP100 irá requisitar via DHCP um endereço de IP, nesta requisição o TIP100 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 TIP100 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 TIP100 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 TIP100 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 TIP100. Toda vez que um TIP100 adquirir um número da central, o ramal correspondente sairá da lista de disponíveis e não será mais oferecido a outro TIP100.

Caso o número de ramais disponíveis esteja esgotado, a central ICIP irá retornar uma configuração inválida e o TIP100 não registrará na ICIP.

Em servidores Linux a configuração do serviço DHCP é editável no arquivo `"/etc/dhcpd/ dhcpd.conf"`. O TIP100 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 gerenciamento.

Lista de ramais pertencentes a autoconfiguração de terminais IP

Número - ramal IP

Estado

Disponível

Adicionar

Remover

Ramal IP	Estado
234	Disponível
235	Disponível
233	Disponível

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.

Termo de garantia

Para a sua comodidade, preencha os dados abaixo, pois, somente com a apresentação deste em conjunto com a nota fiscal de compra do produto, você poderá utilizar os benefícios que lhe são assegurados.

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

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

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais defeitos 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 de entrega do produto ao Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo território nacional. Esta garantia contratual implica na troca gratuita das partes, peças e componentes que apresentarem defeito de fabricação, além da mão-de-obra utilizada nesse reparo. Caso não seja constatado defeito de fabricação, e sim defeito(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com estas despesas.
2. Constatado o defeito, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que consta na relação oferecida pelo fabricante - somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isto não for respeitado esta garantia perderá sua validade, pois o produto terá sido violado.
3. Na eventualidade do Senhor Consumidor solicitar o 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, transporte, segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
4. A garantia perderá totalmente sua validade se ocorrer qualquer das hipóteses a seguir: a) se o defeito não for de fabricação, mas sim, ter sido causado pelo Senhor Consumidor ou 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 decorrente 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 houver sido adulterado ou rasurado; e) se o aparelho houver sido violado.

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

O processo de fabricação deste produto não está coberto pelo sistema de gestão ambiental da Intelbras.

Todas as imagens deste manual são ilustrativas.



Placas Base y Codec ICIP 30 Intelbras
Modelo Impacta 94/140/220

¡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 para las centrales telefónicas de la línea Impacta, modelos Impacta 94, 140 y 220, mejorando su desempeño y garantizando una alta disponibilidad de llamadas.

La ICIP 30 es una placa 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 de la planta para pequeñas y medianas empresas.

1. Especificaciones técnicas

Patrones	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
Interfaces de red	IEEE802.3ac VLAN tagging
	1 puerta LAN UTP fast Ethernet RJ45 10/100 Mbps
Protocolo de señalización	1 puerta WAN UTP fast Ethernet RJ45 10/100 Mbps
	SIP 2.0
Interfaz USB	2 puertos USB host tipo A
	Compatibles con USB 1.1/2.0
Canales VoIP	Hasta 30 canales (10 canales por Placa Codec ICIP 30/licencias liberadas en la Llave de Hardware ICIP)
	G.711 PCM (A/u-law) hasta 64 kbps
Codificación de voz	G.729 AB CS- ACELP hasta 8 kbps
	GSM Full Rate 6.10 hasta 13,2 kbps
	G.726 (ADPCM)
LEDs	Indicativos del estatus del 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.
- » Hasta 4 extensiones/internos IP y 1 troncal IP para cada canal VoIP (adquisición de licencias con Llave de Hardware ICIP).
- » Hasta 30 canales VoIP (utilizando hasta 3 submódulos del tipo Placa Codec ICIP 30).
- » Troncales IP: Punto a Punto y Proxy (operador VoIP).
- » Soporta hasta 5 VLANs.
- » 2 puertos UTP Fast Ethernet 10/100 Mbps para LAN y WAN.
- » Detección automática de la Placa 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 los browsers Mozilla Firefox® 3.6 o posterior.
- » Protección del sistema vía Firewall.
- » Control de licencias vía Llave de Hardware ICIP.
- » Control de tráfico.
- » Permite conectar a un Billetador, 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).
- » Acceso a banda ancha vía módem 3G (módem no incluido).

- » Autoabastecimiento para 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 un técnico autorizado puede abrir la tapa del PABX, así como conectar y manipular 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.
- » Apagar 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 Placa 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 placas.
- » El transporte y el almacenaje deben ser solamente en embalajes a prueba de electricidad estática.
- » Coloque la placa 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 placa 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 se aplican a los funcionarios de Intelbras

Los funcionarios de Intelbras están sujetos a prácticas de comercio seguro y confidencialidad de datos bajo los términos de los procedimientos de trabajo de la compañía.

Es imperativo que se observen las reglas a continuación para asegurar que las provisiones estatutarias relacionadas a servicios (sean éstos servicios internos o administración y manutención remotas) sean estrictamente seguidas. Esto preserva los intereses del cliente y ofrece protección personal adicional.

5.3. Directrices que controlan el tratamiento de datos

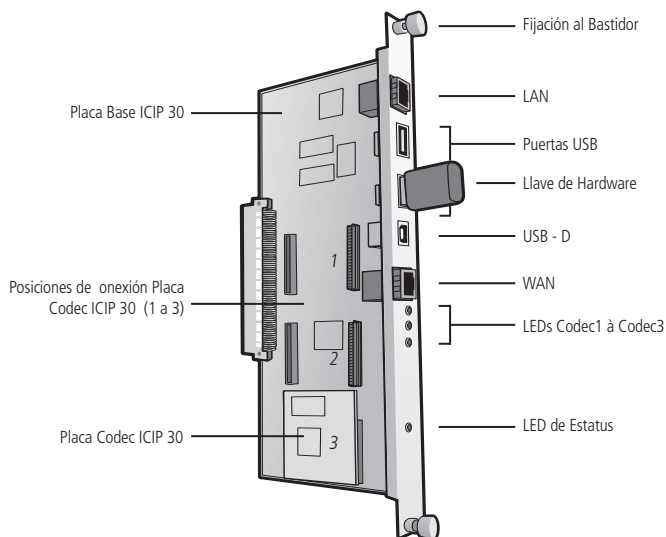
- » Asegurar que apenas personas autorizadas tengan acceso a los datos de clientes.
- » Usar las facilidades de atribución de claves, sin permitir cualquier excepción. Nunca informar claves a personas no autorizadas.
- » Asegurar que ninguna persona no autorizada tenga como procesar (almacenar, modificar, 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.

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:

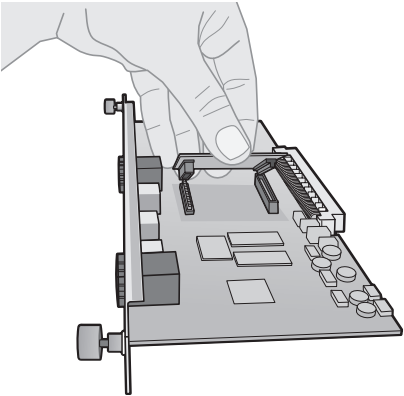
- » **Placa Base ICIP 30:** responsable por el procesamiento de las informaciones de red, protocolos de acceso y conexiones a red del cliente e Internet;
- » **Placa Codec ICIP 30:** responsable por los canales VoIP disponibles en la Placa Base ICIP 30 y por el procesamiento de las señales de "voz" y a su conversión en paquetes de datos dentro de la red. Cada placa Codec habilita 10 canales VoIP.
- » **Llave de Hardware con licencias de extensión/interno y troncales IP.**

6.1. Placa Base ICIP 30



ICIP: Interfaz de Comunicación IP

6.2. Posiciones de conexión Placa Codec ICIP 30 (1 a 3)



6.3. Protección y seguridad de datos

Interfaz de red LAN	Puerta UTP fast Ethernet RJ45 10/100 para acceso a red local.	
Puertas USB	2 puertas USB host para conexión de periféricos como la Llave de Hardware ICIP de licencias para Extensiones/internos y Troncales SIP y módem 3G. 1 puerta USB D para uso de la Asistencia Técnica.	
Interfaz de red WAN	Puerta UTP fast Ethernet RJ45 10/100 para conexión externa de acceso a Internet.	
LEDs de Codec1 a Codec3 (uno para cada módulo) Placa Codec ICIP 30	Cadencia	Estado
	Permanentemente apagado	Módulo con ID inválido o módulo no detectado
	Permanentemente encendido	Módulo con ID válido detectado, pero no inicializado
	Parpadeando muy rápidamente (100 ms ON / 100 ms OFF)	Módulo siendo inicializado (descarga de firmware)
	Parpadeando rápidamente (300 ms ON / 300 ms OFF)	Módulo inicializado y FW operando
LED indicativo del estatus de la Placa Base ICIP 30	Parpadeando intermitente (1.400 ms ON / 100 ms OFF)	Falla de inicialización del módulo
	Cadencia	Estado
	Permanentemente encendido	Placa no inicializada
	Parpadeando muy rápidamente (100 ms ON / 100 ms OFF)	Placa inicializando (Linux inactivo)
	Parpadeando rápidamente (500 ms ON / 500 ms OFF)	Placa inicializando (Linux activo, e inicializando servicios)
Tornillos de fijación	Parpadeando moderadamente (1 s ON / 1 s OFF)	Placa inicializada y operando (Programador WEB activo)
	Parpadeando intermitente (1400 ms ON / 300 ms OFF)	Falla de Inicialización de la placa
	2 tornillos responsables por la fijación de la placa en el bastidor y por la puesta a tierra.	
Conectores para Placa Codec ICIP 30	Existen 3 posiciones disponibles para la conexión, pudiendo así alcanzar hasta 30 canales VoIP (depende de las licencias adquiridas a través de la Llave de Hardware ICIP).	

7. Producto

7.1. Tecnología

Vista general

Con la Placa ICIP, la central Impacta 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 SIP.

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 apenas inicia, termina y modifica la sesión, lo que lo vuelve un protocolo que se adapta tranquilamente en diferentes arquitecturas.

El 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 Placa Base y Codec ICIP 30, siga el procedimiento:

1. En una superficie conectada a tierra conecte la pulsera antiestática;
2. Retire la Placa Base ICIP 30 y la(s) Placa(s) Codec ICIP 30 de los embalajes y póngalas sobre la superficie conectada a tierra;
3. Verifique el estado de las placas y sus conectores;
4. Apoye de manera estable la Placa Base ICIP 30 sobre la superficie e inserte la(s) Placa(s) Codec ICIP 30 en las posiciones disponibles, siguiendo el esquema a continuación;
5. Inserte el conjunto montado en un embalaje antiestático hasta la central estar 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 auxiliario a reconocer en cuál escenario la Placa 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;
8. Apague la alimentación AC de la central Impacta y retire la tapa frontal;
9. La Placa Base ICIP 30 puede ser conectada en cualquiera una de las posiciones disponibles del backplane, sin embargo, recomendamos que se la inserte en el centro, debido a los cables de red y periféricos instalados en las puertas USB;
10. Tras el encaje, verifique si los tornillos de fijación del perfil de la placa están debidamente apretados. Estos tornillos, además de la fijación, también son responsables por la puesta a tierra de los conectores;
11. Conecte los cables de la red LAN y WAN en los respectivos conectores RJ45, la Llave de Hardware ICIP de Licencias y el módem 3G, caso haya, en las puertas USB;
12. Organice e identifique los cables de red junto con los demás cables en el DG de la central y, en el caso de utilizar un módem 3G, déjelo afuera del espacio interno del backplane, donde no comprometa la circulación forzada de aire. Dependiendo del modelo, tal vez sea necesario utilizar un cable USB extensor;
13. Antes de la puesta en marcha del sistema, debe efectuarse la confirmación visual de todas las conexiones de cables, módulos, placas y alimentación AC, corrigiendo cualquier eventual falla. La confirmación visual debe efectuarse con el sistema apagado;

14. Recoloque la tapa frontal y conecte la alimentación AC de la central Impacta;
15. Tras la inicialización del sistema, verifique a través del *Programador Web / Menú Interfaces / Disposición de placas*, si ninguna placa está programada para utilizar aquel slot;
16. 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 anomalías 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 *Guía "Codec"*)
- » Para que las extensiones/internos IP funcionen adecuadamente, el modo de envío DTMF debe ser SIP INFO (ver *Guía "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. Llave de Hardware ICIP

La Llave de Hardware ICIP es un dispositivo del tipo USB que, insertada en el tablero de la Placa ICIP, libera las licencias de extensiones/internos y troncales SIP adquiridas.

El sistema permite la configuración de 1 troncal IP y hasta 4 extensiones/internos IP para cada canal VoIP presente en el sistema. Así, el número de extensiones/internos y troncales IP depende de las Licencias y de la programación del sistema, siendo como máximo 120 extensiones/internos y 30 troncales IP.

Obs.: al retirar la Llave de Hardware de la central telefónica Impacta en funcionamiento, las llamadas VoIP (extensiones/internos y troncales IP) dejarán de funcionar tras algunos segundos.

8.3. Licencias

Las licencias son adquiridas en el momento de la compra o cuando sea necesario aumentar el número de extensiones/internos y/o troncales IP. Para consultar las licencias disponibles, acceda al *Programador Web / Menú Sistema / Licencias*, donde es posible visualizar el ID de la llave y las licencias existentes.

Tras la consulta de las licencias disponibles, caso quiera aumentar la cantidad de troncales y/o extensiones/internos, no es necesario cambiar la Llave de Hardware de la central. Consulte una reventa autorizada Intelbras necesitando para esto el ID de la llave y solicite la compra de más licencias. La reventa va a generar un archivo criptografiado para esta Llave de Hardware y le enviará el archivo.

A través del *Programador Web*, el archivo criptografiado, que contiene las nuevas licencias, puede ser insertado en la llave de hardware, liberando más extensiones/internos y/o troncales IP.

- » *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 común:

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

Abra su navegador web (recomendado Firefox 4.0) 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 (caso no se abra, verifique si su navegador no posee bloqueo de pop-ups o si no hay algún producto del género activo en su computadora). Inserte el nombre de Usuario y Clave para la autenticación. El patrón de fábrica es:

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

10.2. 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 > Puertas*.

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 Placa ICIP, como siguen:

10.3. Sistema

Licencias

Al acceder a este submenú se exhibirá el estatus de la *Llave de Hardware ICIP* (Conectada o Desconectada), el ID de la llave y el número de licencias válidas para extensiones/internos IP y troncales IP.

Enrutamiento

Sistema

Acesso de usuario

Agenda/directorio general

Aplicar configuración

Registro de Llamadas

CSTA/Mesa Virtual

Cadencia de timbre

Cadencia de tono

Código de cuenta

DISA

Desvío correo/buzón

Emergencia

Facilidades

Información da la empresa

Licencia

Clave general

Licencias leídas de la llave de hardware

Clave conectada ID: 08:CE:03:28:DD:FB:F7:BE

Data última leitura: 19/06/2012, 08:36:31

Produto	Espere	Estado
Ramal IP	120	Válida
Línea IP	30	Válida

Visualización/confirmación de la conexión de la Llave Hardware y sus Licencias

10.4. Interfaces

Disposición de las placas

Al acceder a este submenú se exhibirá un esquema con la cantidad y los dispositivos conectados en los slots del back-plane. Verifique si se exhibe el tipo de la Placa ICIP instalada en el slot correcto, caso no lo exhiba, será necesario realizar la configuración.

1. Seleccione en el menú de placas la opción “Vacío”;
2. Confirme esta operación;
3. Seleccione la Placa Base ICIP 30 para aquel slot (en este ejemplo 30 canales).

Disposición de las placas/tarjetas

Slot 1

Slot 2

Slot 3

Slot 4

Slot 5

Slot 6

Slot 7

Slot 8

Slot 9

Slot 10

Slot 11

Tarjeta de accesorios

Tarjeta mixta de extensiones

Tarjeta de 16 extensiones analógi

Tarjeta de 16 extensiones analógi

Tarjeta de 16 extensiones analógi

Tarjeta de 16 extensiones analógi

Tarjeta de 16 extensiones analógi

Tarjeta de 16 extensiones analógi

Tarjeta de 16 extensiones analógi

Tarjeta ICIP 30 Canales

Tarjeta E1

CPU

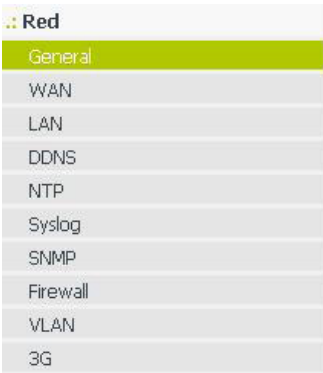
Alimentación

Localización/actualización para Placa Base ICIP 30

10.5. 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 la Internet.

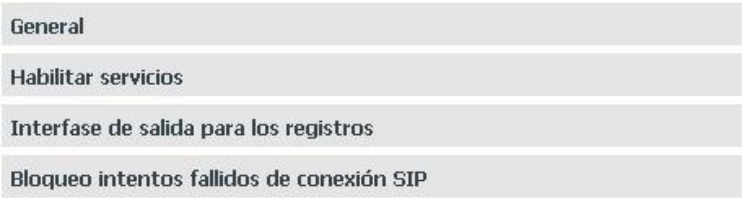
Atención: algunas de estas informaciones pueden obtenerse junto al administrador de red o técnico de informática.



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 guías:



Menú Red/ Submenú General

Guía General

Presenta las informaciones físicas de la placa para el administrador.



Menú red - General

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

Habilitar servicios

Aquí pueden ser seleccionados los servicios a utilizarse, así como algunas facilidades de la red para el sistema. La elección de estos ítems, reflejará directamente en el *Menú Red*, donde serán habilitados los submenús equivalentes para futuras configuraciones.

General

Habilitar servicios

Habilitar

DDNS

NTP

Syslog

SNMP

Firewall

VLAN

Número de VLANs

Huso Horario

Horario de verano

☒

☒

☒

☒

☒

☒

2

Brasilia

☒

Interfase de salida para los registros

Bloqueo intentos fallidos de conexión SIP

Menú red / Submenú General / Habilitar servicios

- » **DDNS**: habilita el ítem DDNS.
- » **NTP**: habilita el ítem NTP.
- » **Syslog**: habilita el ítem Syslog.
- » **SNMP**: habilita el ítem SNMP.
- » **Firewall**: habilita el ítem Firewall.
- » **VLAN**: habilita el ítem VLAN para configuración del servicio y permite seleccionar cuantas VLANs estarán disponibles en la red de la ICIP.
- » **Número de VLANs**: define el número de VLANs que estará disponible para la red del sistema. Son posibles hasta 5 VLANs.
- » **Huso Horario**: permite seleccionar el huso horario local.
- » **Estandar de fábrica**: hora oficial de Brasil - Brasilia GMT -03:00. La hora puede ser modificada dependiendo de la localidad en que se encuentre. Este ítem será utilizado cuando se habilite la opción de utilizar **Servidor NTP**.
- » **Horario de Verano**: adelanta en 1 hora el horario obtenido del servidor NTP o configurado manualmente.

Interfase 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.

General

Habilitar servicios

Interfase de salida para los registros

Interfase de salida para los registros

LAN

Bloqueo intentos fallidos de conexión SIP

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.

Bloqueo Intentos de Login Fallo

Ésta es una herramienta de seguridad de los datos para accesos no autorizados, implantada en el sistema para garantizar su confiabilidad. Si durante la autenticación del login, éste no es reconocido por el sistema, el usuario podrá intentar otras veces, antes de recibir un mensaje de bloqueo, o aun, puede configurarse una lista de IPs que no serán analizados por esta regla, estando libres de bloqueo.

General

Habilitar servicios

Interfase de salida para los registros

Bloqueo intentos fallidos de conexión SIP

Bloqueo de intentos de conexión (login SIP)

☒

Número de intentos fallidos de conexión SIP

2

Período de verificación (segundos)

3

Tiempo de bloqueo (segundos)

5

End. IP (excepcional)

.

.

.

Añadir

Remover

Whitelist

Menú Red/ Submenú General/Bloqueo Intentos de Login Fallo

Bloqueo de intentos de login: habilita el servicio de verificación de la autenticación de los logins de los usuarios en el sistema.

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

Período de verificación (segundos): define un período de tiempo en el que se analizará el número de intentos de login. En el caso que el número sobrepase el valor configurado en el campo Número de intentos fallidos, se bloqueará la dirección IP que intenta login.

Tiempo de bloqueo (segundos): define el período de duración del bloqueo del IP origen de los logins incorrectos.

Direc. IP (Excepción): permite definir una dirección IP que no será analizada por las reglas, estando libre del bloqueo. Ingrese las direcciones IPs deseadas y utilice los botones Añadir y Remover para administrarlos.

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

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:

WAN

Habilitar Tráfico

QoS

Rutas

Menú Red/ Submenú WAN

61

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.

WAN	
Velocidad de acceso del medio físico	Auto-Negociação ▾
Obtener dirección IP automáticamente (DHCP)	☐
Dirección IP	10 . 1 . 30 . 18
Máscara de sub-red	255 . 255 . 255 . 0
Gateway patrón	10 . 1 . 30 . 1
Servidor DNS preferencial	. . .
Servidor DNS alternativo	. . .
Dirección de MAC	1 : 2 : 3 : 4 : 5 : 6
Ancho de banda para Internet (link proveedor)	
Upload	100000 kbps
Download	100000 kbps
Habilitar Tráfico	
QoS	
Rutas	

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, caso 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 de la puerta WAN en la red en la que se conectará la placa.
- » **Máscara de subred:** define el valor de la máscara de subred en la que se conectará la placa.
- » **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:** ingrese la dirección de MAC para interfaz WAN. Esto es típicamente útil, 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.

WAN

Habilitar Tráfico

SIP

RTP

Administración

QoS

Rutas

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 mejora 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 extremadamente útil en condiciones de embotellamiento de tráfico en la interfaz de salida de estos datos (por ejemplo, la puerta de conexión con el ruteador para Internet).

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

WAN

Habilitar Tráfico

QoS

Habilitar QoS de capa 3

SIP:

TOS

(tipo)

0

(valor)

RTP:

TOS

(tipo)

0

(valor)

Administración:

TOS

(tipo)

0

(valor)

Rutas

Menú Red/ Submenú WAN/QoS

Habilitar QoS de camada 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 encabezamiento 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 encabezamiento, 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 encabezamiento 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.

10.6. 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 o una otra red específica.

WAN

Habilitar Tráfico

QoS

Rutas

	Destino	Gateway	Upload	Download
1.	. . . /	. . .	100000	100000
2.	. . . /	. . .	100000	100000
3.	. . . /	. . .	100000	100000
4.	. . . /	. . .	100000	100000
5.	. . . /	. . .	100000	100000

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

LAN

Habilitar Tráfico

QoS

Rutas

Menú Red/ Submenú LAN

LAN

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

LAN

Velocidad de acceso del medio físico

Auto-Negociação

Obtener dirección IP automáticamente (DHCP)

☐

Dirección IP

10 . 1 . 30 . 12

Máscara de sub-red

255 . 255 . 255 . 0

Gateway patrón

10 . 1 . 30 . 1

Servidor DNS preferido

.

Servidor DNS alternativo

.

Dirección de MAC

aa : da : da : da : ea : fa

Ancho de banda para Internet (link proveedor)

Upload

100000

kbps

Download

100000

kbps

Habilitar Tráfico

QoS

Rutas

Menú Red/ Submenú LAN/LAN

- » **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, relacionándose directamente con los dispositivos existentes en la red (cables, hubs, etc.). Así, recomendamos la opción de Auto Negociación, caso no haya ninguna indicación del administrador de red.
- » **Obtener dirección IP automáticamente (DHCP):** dispone 2 opciones de acceso a la red LAN:
- » **Seleccionado:** el acceso a la red LAN 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 conectado en la red.

- » **Sin selección:** el acceso a la red LAN será estático, es decir, será necesario llenar los campos: Dirección IP, Máscara de Red, IP del Gateway e IP de los servidores DNS, de acuerdo con las especificaciones del administrador de red.
- » **Dirección IP:** define la dirección IP de la interfaz LAN de la placa.
- » **Máscara de subred:** define los valores de la máscara de subred de la interfaz LAN.
- » **Gateway por defecto:** 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 porte que esta dirección IP sea la misma de la dirección de gateway (ruteador de salida).

- » **Dirección MAC:** ingrese la dirección de MAC de la placa para la interfaz LAN.
- » **Carga y Descarga:** son definidas 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 LAN disponible, para mantener el equilibrio en la conexión y evitar cualquier saturación y consecuente pérdida de calidad.

Habilitar tráfico

Aquí son habilitados los tráfico de administración y señalización SIP y RTP (relativos al tráfico de voz) en la red LAN.

LAN	
Habilitar Tráfico	
SIP	☒
RTP	☒
Administração	☒
QoS	
Rutas	

Menú Red/ Submenú LAN/Habilitar tráfico

- » **SIP:** habilita el tráfico de los paquetes de señalización SIP junto a la red LAN configurada.
- » **RTP:** habilita el tráfico de los paquetes de señalización RTP junto a la red LAN, suministrando un medio uniforme para transmitir datos sujetos a "problemas" de tiempo real (audio, vídeos,...).
- » **Administración:** habilita el tráfico de administración en la red LAN. 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 extremadamente útil en condiciones de embotellamiento de tráfico en la interfaz de salida de estos datos (por ejemplo, la puerta de conexión con el ruteador para la Internet).

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

LAN				
Habilitar Tráfico				
QoS				
Habilitar QoS de llamada 3				☐
SIP:	TOS	(tipo)	0	(valor)
RTP:	TOS	(tipo)	0	(valor)
Administración:	TOS	(tipo)	0	(valor)
Rutas				

Menú Red/ Submenú LAN/QoS

Habilitar QoS de camada 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 encabezamiento 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 encabezamiento, dando 64 diferentes posibilidades para códigos de prioridad.
- » **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 encabezamiento, 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 LAN, creando caminos predeterminados, donde las informaciones pueden ser direccionadas hasta un host o una otra red específica.

LAN

Habilitar Tráfico

QoS

Rutas

	Destino	Gateway	Upload	Download
1.	. . . /	. . .	100000	100000
2.	. . . /	. . .	100000	100000
3.	. . . /	. . .	100000	100000
4.	. . . /	. . .	100000	100000
5.	. . . /	. . .	100000	100000

Menú Red/ Submenú LAN/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 el equilibrio en la conexión del enlace y evitar cualquier saturación y consecuente pérdida de calidad.

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.

Atención: la configuración del servicio de DNS dinámico para el sistema sólo será posible tras la habilitación de este submenú en el ítem *Habilitar servicios*.

DDNS - DNS Dinámico

Menú Red/ Submenú DDNS

DDNS - DNS Dinámico

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.

DDNS - DNS Dinámico

Hostname (IP/FQDN)

Habilitar DDNS para la WAN

☐

Login

Clave

Tiempo de actualización en el servidor (seg)

Menú Red/ Submenú DDNS/DDNS

- » **Dirección del servidor DDNS:** ingrese la dirección IP o el nombre registrado en el DDNS, ej.: icip.dyndns.org.
- » **Habilitar DDNS para WAN:** 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.
- » **Tiempo de actualización en el servidor:** define el tiempo de actualización de las informaciones en el servidor DDNS.

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

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.

NTP

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: antes de insertar los servidores de NTP verifique si las configuraciones de huso horario y horario de verano están correctas en el ítem Habilitar servicios.

NTP

Servidor NTP Primario	200.168.0.8	(IP/FQDN)
Servidor NTP Secundario		(IP/FQDN)
Servidor NTP Terciario		(IP/FQDN)

Menú Red/ Submenú NTP/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.

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 el caso no posea servidores NTP en su red, utilícelos. Para mayores informaciones visite la dirección <http://www.ntp.br>.

Syslog

El Syslog es el protocolo de envío de mensajes de Logs. Los logs registran las informaciones del funcionamiento del sistema, como eventos y errores ocurridos, para uso posterior.

Estos registros poseen 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, siguiendo el patrón del IETF para la RFC 5424.

Atención: la configuración del servicio de Syslog sólo será posible tras habilitar este submenú en el ítem Habilitar servicios. Este servicio no funcionará correctamente si las configuraciones de fecha y hora no estuvieren correctas.

Syslog

Menú Red/ Submenú Syslog

Syslog

En esta guía es posible configurar el servidor de Syslog.

Syslog		
Tamaño máximo del archivo log	200	(kB)
Habilitar el servidor syslog remoto	☐	
Dirección del servidor syslog		(IP/FQDN)

Menú Red/ Submenú Syslog/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, para un servidor Syslog.
- » **Dirección del servidor syslog:** ingrese la dirección IP o el nombre del servidor Syslog que recibirá los mensajes de log del sistema.

SNMP

El SNMP (Simple Network Management Protocol) es un protocolo de administración de redes TCP/IP, de la camada 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*.

Engine ID
SNMP v1 e v2
TRAP
SNMP v3
Criptografía SNMP v3

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.

Engine ID
Utilizar padrão ☒
Ajustado pelo Administrador [80661A04]
SNMP v1 e v2
TRAP
SNMP v3
Criptografía SNMP v3

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 caso la opción de *Engine ID* estandar no esté. El administrador debe informar el Engine ID personalizado (solo caracteres hexadecimales).

SNMP vt1 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.

Engine ID	
SNMP v1 e v2	
Habilitar SNMP V1 e V2 ☐	
Nombre de la comunidad	Tipo de Acceso
1.	Solamente lectura
2.	Solamente lectura
3.	Solamente lectura
4.	Solamente lectura
TRAP	
SNMP V3	
Criptografía SNMP V3	

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.

Engine ID			
SNMP v1 e v2			
TRAP			
Habilitar el envío de TRAP ☐			
Versión	Tipo de Notificación	Comunidad	Destino
1. v1	Trap		
2. v1	Trap		
3. v1	Trap		
4. v1	Trap		
SNMP V3			
Criptografía SNMP V3			

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.

Engine ID					
SNMP v1 e v2					
TRAP					
SNMP V3					
Habilitar SNMP v3 					
Usuario	Tipo de Acceso	Modo	Tipo Clave	Clave	
1.	Solamente lectura ▼	authPriv ▼	MD5 ▼		
2.	Solamente lectura ▼	authPriv ▼	MD5 ▼		
3.	Solamente lectura ▼	authPriv ▼	MD5 ▼		
4.	Solamente lectura ▼	authPriv ▼	MD5 ▼		
Criptografia SNMP V3					

Menú Red/ Submenú SNMP/SNMP V3

- » **Habilitar SNMP v3:** habilita los servicios de autenticación y privacidad por usuario.
- » **Menú red**
- » **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 escrita 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.

Engine ID

SNMP v1 e v2

TRAP

SNMP V3

Criptografía SNMP V3

Tipo de encriptación	Clave de encriptación
1. AES	
2. AES	
3. AES	
4. AES	

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.

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.

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

Firewall

Menú Red/ Submenú Firewall

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 las puertas abiertas 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 dice respecto a 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 ser 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.

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.

VLAN

VLAN 1

VLAN Configuraciones

Habilitar Tráfico

Ancho de banda para Internet (link proveedor)

QoS

Rutas Estáticas

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.

VLAN Configuraciones

VLAN_NUMBER

VLAN ID

Prioridad IEEE 802.1q

Obtener dirección IP automáticamente (DHCP)

Dirección IP

Máscara de sub-red

Gateway patrón

1

1

Mejor esfuerzo

☐

.

.

.

.

.

.

.

.

.

Habilitar Tráfico

Ancho de banda para Internet (link proveedor)

QoS

Rutas Estáticas

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 (rótulos) 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.
 - » Sin selección, 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.

VLAN Configuraciones	
Habilitar Tráfico	
SIP	☒
RTP	☒
Administración	☒
Ancho de banda para Internet (link proveedor)	
QoS	
Rutas Estáticas	

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.

VLAN Configuraciones

Habilitar Tráfico

Ancho de banda para Internet (link proveedor)

Upload

100000

kbps

Download

100000

kbps

QoS

Rutas Estáticas

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 mejora 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 extremadamente útil en condiciones de embotellamiento de tráfico en la interfaz de salida de estos datos (por ejemplo, la puerta de conexión con el router para Internet).

Atención: la Placa ICIP marca los paquetes de datos, tocando a los activos de red (switchs y routers) dar prioridad al tráfico de voz.

VLAN Configuraciones

Habilitar Tráfico

Ancho de banda para Internet (link proveedor)

QoS

Habilitar QoS de llamada 3

SIP:

TOS

(tipo)

0

(valor)

RTP:

TOS

(tipo)

0

(valor)

Administración:

TOS

(tipo)

0

(valor)

Rutas Estáticas

Menú Red/ Submenú VLAN/QoS

Habilitar QoS de llamada 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 encabezamiento 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 routers 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 encabezamiento, 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 encabezamiento 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 una otra red específica.

VLAN Configuraciones				
Habilitar Tráfico				
Ancho de banda para Internet (link proveedor)				
QoS				
Rutas Estáticas				
Destino	Gateway	Upload	Download	
1. 	. . .	100000	100000	
2. 	. . .	100000	100000	
3. 	. . .	100000	100000	
4. 	. . .	100000	100000	
5. 	. . .	100000	100000	

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.

3G

Este submenú presenta las informaciones necesarias para instalar un módem 3G en la ICIP, disponiendo para el sistema la tecnología 3G para acceso a Internet.

Atención: consulte en el web sitio de Intelbras la lista de módems homologados para funcionar con la ICIP.

3G
Configuraciones avanzadas
Ancho de banda para Internet (link proveedor)
Habilitar Tráfico
Rutas Estáticas / Red Destino

Menú Red/ Submenú 3G

3G

Permite configurar el sistema con las informaciones necesarias para el acceso 3G.

3G	
Habilitar 3G	☐
Número de acceso	
Usuario	
Clave	
Configuraciones avanzadas	
Ancho de banda para Internet (link proveedor)	
Habilitar Tráfico	
Rutas Estáticas / Red Destino	

Menú Red/ Submenú 3G/3G

- » **Habilitar 3G:** habilita la interfaz de acceso 3G en el sistema.
- » **Número de acceso:** inserte el número de acceso suministrado por el operador 3G.
- » **Usuario:** inserte el usuario de autenticación de acuerdo con el operador 3G.
- » **Clave:** inserte la clave de autenticación de acuerdo con el operador 3G.

Configuraciones avanzadas

Permite la configuración de los parámetros del punto de acceso de Internet y el tipo de autenticación junto al operador 3G.

3G

Configuraciones avanzadas

APN

Código PIN

1234

Automática

☒

PAP

☐

CHAP

☐

Ancho de banda para Internet (link proveedor)

Habilitar Tráfico

Rutas Estáticas / Red Destino

Menú Red/ Submenú 3G/ Configuraciones avanzadas

- » **APN:** ingrese la dirección APN (Access Point Name) del operador 3G, es decir, la dirección del punto de acceso a Internet (por ejemplo, bandalarga.claro.com.br).
- » **Código PIN:** inserte el código PIN (Personal Identification Number) de acuerdo con el operador 3G (normalmente no es necesario informar).
- » **Automática, PAP y CHAP:** dispone el método de autenticación del usuario y clave de acuerdo con el operador 3G.
 - » **Automática:** el sistema selecciona la autenticación.
 - » **PAP (Password Authentication Protocol):** es un protocolo utilizado para autenticar usuarios de una forma sencilla. El envío de la clave es hecho en ASCII de forma no cifrada.
 - » **CHAP (Challenge-Hankshake Authentication Protocol):** tiene la misma función del PAP, pero envía la clave de forma cifrada.

Ancho de banda para Internet (enlace proveedor)

En este sub-menú se configuran las velocidades contratadas de la banda del proveedor 3G dentro de la red.

3G

Configuraciones avanzadas

Ancho de banda para Internet (link proveedor)

Upload

100000

kbps

Download

100000

kbps

Habilitar Tráfico

Rutas Estáticas / Red Destino

Menú Red/ Submenú 3G/Ancho de banda para Internet (enlace proveedor)

- » **Carga y Descarga:** se definen las tasas máximas para la conexión con el enlace proveedor 3G de acuerdo con los equipos conectados. Es importante saber las tasas de carga y descarga con la interfaz 3G disponible, para mantener el equilibrio en la conexión y evitar cualquier saturación y consecuente pérdida de calidad.

Habilitar tráfico

Aquí son habilitados los tráficos de administración y de paquetes de señalización SIP y RTP (relativos al tráfico de voz), en la interfaz 3G.

3G

Configuraciones avanzadas

Ancho de banda para Internet (link proveedor)

Habilitar Tráfico

SIP

☒

RTP

☒

Administración

☒

Rutas Estáticas / Red Destino

Menú Red/ Submenú 3G/Habilitar tráfico

- » **SIP:** habilita el tráfico de los paquetes de señalización SIP junto a la interfaz 3G configurada.
- » **RTP:** habilita el tráfico de los paquetes de señalización RTP junto a la interfaz 3G, suministrando un medio uniforme para transmitir datos sujetos a “problemas” de tiempo real (audio, videos,...).
- » **Administración:** habilita la administración del tráfico de administración en la interfaz 3G. Esto puede ser utilizado para evitar acceso a las configuraciones de administración por personas no autorizadas.

Rutas estáticas/Red Destino

Esta configuración permite definir rutas específicas para subredes de destino al lado de la interfaz 3G, creando caminos predeterminados, donde las informaciones pueden ser direccionadas hasta un host o una otra red específica.

3G

Configuraciones avanzadas

Ancho de banda para Internet (link proveedor)

Habilitar Tráfico

Rutas Estáticas / Red Destino

Ruta 1

.

.

.

/

Ruta 2

.

.

.

/

Ruta 3

.

.

.

/

Ruta 4

.

.

.

/

Ruta 5

.

.

.

/

Menú Red/ Submenú 3G/Rutas estáticas/Red Destino

Ruta 1, 2, 3, 4 y 5

En el campo *Ruta* se informan las direcciones IPs y la máscara (direcciones IP / netmask tipo CIDR) de las rutas destino.

10.7. Menú VoIP - Placa 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 - Placa ICIP y sus componentes

General

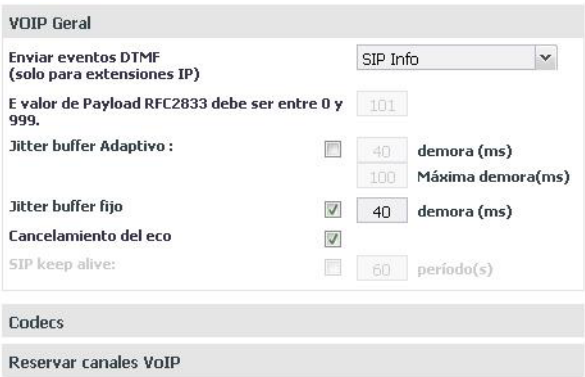
Este submenú permite configurar algunas características del VoIP, codecs y esquema de canales VoIP del sistema.



Menú VoIP - Placa 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/interos IP y conexiones punto a punto.



Menú VoIP - Placa ICIP/Submenú General/ VoIP General

- » **Enviar eventos DTMF (solo para extensiones/interos IP):** define con cual método se enviarán los dígitos DTMF en la red así que se complete 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, usando RFC 2833.
- » **In-Band:** envía los eventos DTMF en el paquete de voz.
Obs.: para el correcto funcionamiento de las extensiones/interos IP utilice siempre el método SIP INFO.
- » **Valor del payload si RFC2833:** configura el tipo de carga (payload) del DTMF cuando seleccionado el evento DTMF Out-of-band (RFC2833). El valor oscila del 96 hasta el 127, siendo por defecto 101.

- » **SIP keep alive:** cuando esta habilitado, el sistema envía periódicamente un mensaje SIP al destino de la llamada, con el intuito de mantener la sesión de la NAT (Network Address Translation) disponible. Estandar 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 “represamiento” de los paquetes que llegan desde la red, antes de “ejecutarlos”, es siempre el mismo. Técnicamente es más sencillo, aunque presente desempeño inferior, pues no consigue acompañar el comportamiento de la red. El patrón es 40 ms.
- » **Cancelación de eco:** cuando esta habilitado, el sistema evita que el eco en la híbrida (cuando se pasa de 4 para 2 hilos) vuelva para la red IP. Es decir, la cancelación 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, garantizando calidad de audio y confort al originador de la llamada.

10.8. 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.

VOIP Geral	
Codecs	
Codecs	Tiempo empaquetado (ms)
1. G729	20
2. GSM FR 6.10	20
3. G726-40	10
4. G726-32	10
5. G726-32	20

Reservar canales VoIP

Menú VoIP - Placa 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 si 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.726 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.

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/interinos, troncales y libre acceso (sin reserva).

VOIP Geral

Codecs

Reservar canales VoIP

Reservar canales VoIP

15

15

T.38

Menú VoIP - Placa 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/interinos IP y disponer los canales restantes para que se utilicen conforme demanda de la central. Si no estuviere habilitado, los canales son alocados libremente, por demanda.
- » **Canales para Troncales IP:** define el número de canales VoIP que estarán reservados para Troncales IP.
- » **Canales para Extensiones/interinos IP:** define el número de canales VoIP que estarán reservados para Extensiones/interinos IP.
- » **Canales sin reserva:** define el número de canales VoIP a ser usados libremente por troncales o extensiones/interinos IP, conforme demanda.
- » **Habilitar Ahorro de canal VoIP:** seleccionado, el sistema ahorra canales cuando los dos dispositivos IP involucrados en la llamada sean extensiones/interinos IP.
Obs.: algunas situaciones huyen a esa regla, es decir, ahorro no será posible si:
 - » Al menos una de las extensiones/interinos IP estuviere atrás de NAT.
 - » Haya conferencia involucrando las extensiones/interinos IP.
 - » El teléfono, conectado en la extensión/interino IP, no estuviere preparado para funcionar con la ICIP de forma plena.

Atención: funciona correctamente con TIP100 y ATA 2210T.

- » **FAX:** define cual codec será utilizado para envío y recibimiento de fax por la red VoIP.
 - » **Bypass:** es utilizado cuando si desea que el PABX envíe y reciba las señales de FAX en la banda de audio.
 - » **T.38:** es utilizado cuando se desea que el PABX envíe y reciba las señales de FAX vía protocolo T.38.
 - » **Deshabilitado:** desactiva el envío/recepción de fax por la ICIP.

Punto a punto

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

NAT

Numeración

Menú VoIP - Placa ICIP/ Submenú Punto a punto

NAT

La guía NAT (Network Address Translation) posibilita la configuración de los parámetros para que la central pueda acceder a dispositivos IP que están atrás de NAT (consigue establecerse correctamente las direcciones IP involucradas en el flujo RTP).

NAT

Nenhuma

Dirección pública del NAT

Dirección del STUN TURN ICE

Puerta del STUN TURN ICE

Enviar eventos DTMF:

Valor del payload si RFC2833:

(IP/FQDN)

(IP/FQDN)

3478

RFC 2833

101

Numeración

Menú VoIP - Placa ICIP/Submenú Punto a punto/ NAT

- » **Ninguna:** cuando habilitado, el sistema no utilizará NAT para comunicación. Sólo puede elegirse esa opción si no hubiere necesidad de comunicación con dispositivos IP atrás de NAT.
 - » **Dirección público del NAT:** ingrese la dirección IP o nombre público del gateway NAT.
 - » **Enviar eventos DTMF:** define con cual método se enviarán los dígitos DTMF en la red así que se complete 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, usando RFC 2833.
 - » **In-Band:** envía los eventos DTMF en el paquete de voz.
- Obs.: Sólo puede elegirse el método In-Band caso la(s) red(es) involucrada(s) en la llamada sea(n) controlada(s) y el codec sea G.711A o G.711u.*
- » **Valor del payload si RFC2833:** configura el tipo de carga (payload) del DTMF cuando seleccionado el evento DTMF Out-of-band (RFC2833). El valor oscila de 96 hasta 127, siendo el patrón 101.

Numeración

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

NAT

Numeración

Número piloto en la red

Número interno

Número externo

Añadir

Remover

Número interno

Número externo

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

- » **Piloto en la red:** define el número externo que será usado como abonado llamador en la caso 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).

Punto a punto filial	VOIP Punto a punto filial
	Numeración

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

VOIP Punto a punto filial	
Localidad	
IP	
Numeración	

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.)
- » **IP:** 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.

VOIP Punto a punto filial	
Numeración	
Número interno	
Número externo	
Añadir Remove	
Número interno	Número externo

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 *Remove* para administrar los números internos/externos deseados.

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.

Al seleccionar esta opción, 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 en el menú).

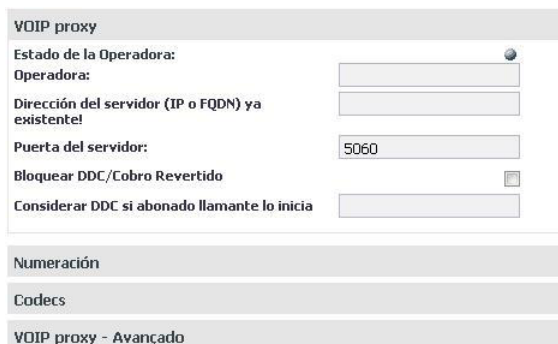
Servidor de registro	VOIP proxy
	Numeración
	Códex
	VOIP proxy - Avanzado

Menú VoIP - Placa ICIP/ Submenú Proxy

VoIP proxy

Aquí son configuradas las informaciones repasadas 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.

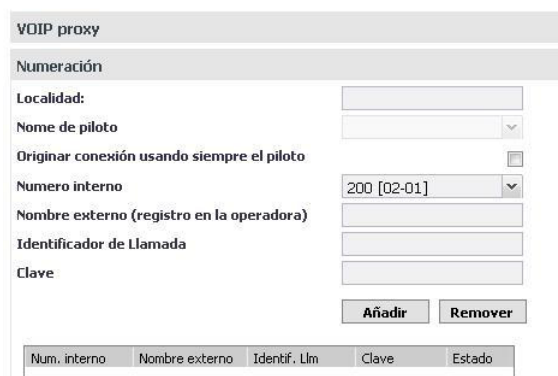


Menú VoIP - Placa ICIP/Submenú Proxy/ VoIP proxy

- » **Estado del Operador:** Es posible visualizar si el operador está operacional ante el sistema (Operador localizable).
- » **Operador:** entre con el nombre del Operador VoIP.
- » **Dirección del servidor (IP o FQDN):** informe la dirección IP o nombre de dominio del operador VoIP, de acuerdo con las informaciones repasadas por el Operador VoIP (ej.: operadora.net.br).
- » **Puerta del servidor:** define la puerta por la 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 - Placa ICIP/Submenú Proxy/ Numeración

- » **Localidad:** ingrese un nombre que referencie la localidad donde la central esta instalada.
- » **Nombre Piloto:** define el número que será usado como abonado llamador caso la extensión/interno originadora de la llamada no esté registrada en la tabla.
- » **Originar llamada siempre usando el piloto:** seleccionado, las llamadas externas utilizarán el "valor" del campo Nombre Piloto como abonado llamador para todas las llamadas originadas.

- » **Número interno:** seleccione la extensión/interno interna 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.
- » **Utilice los botones Añadir y Remove:** administre los números internos/nombres deseados.

Codec

La función de los codecs es reducir el ancho de banda necesario para la 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.

VOIP proxy	
Numeración	
Codecs	
Codecs	Tiempo empaquetamiento
1. G729	20 (ms)
2. GSM FR 6.10	20 (ms)
3. G726-32	30 (ms)
4. PCMA	20 (ms)
5. PCMU	20 (ms)

VOIP proxy - Avanzado

Menú VoIP Placa ICIP/Submenú Proxy/ Codec

- » **Opción de 1 a 7:** definen el orden de preferencia de los Codecs 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.726 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 el sistema guardará para envío de los paquetes RTP para la red.

VOIP proxy - Avanzado

En este sub-menú es posible configurar los datos VoIP proxy más específicos.

VOIP proxy	
Numeración	
Codecs	
VOIP proxy - Avanzado	
Nombre del Dominio:	
Puerta RTP Min:	6000
Puerta RTP Max:	65535
Habilitar envío de solicitud de registro:	☒
Tiempo entre registro (s):	3600
Enviar eventos DTMF:	RFC 2833
Valor del payload si RFC2833:	101
Cancelación de eco:	☒
FAX	Bypass
Dirección del OutBound Proxy (IP o FQDN):	
Puerta del OutBound Proxy:	5060
ToS/DiffServ-paquete RTP:	88
ToS/DiffServ-paquete señalización:	60
Soporte a Número Global (E.164):	☐
Flash en la troncal usar c = 0.0.0.0 (RFC 2543) en el DSP:	☐

Menú VoIP - Placa ICIP/Submenú Proxy/ Avanzado

- » **Nombre de dominio:** ingrese el nombre de dominio del proveedor VoIP. Es una información enviada en la requisición de registro y en el envío de INVITE (ej.: En el mensaje "INVITE SIP: 6504@xpto.com.br" xpto.com.br es el nombre de dominio).
- » **Puerta RTP Min y puerta RTP Max:** definen el rango de puertas que podrán ser utilizadas en la transmisión y recepción del audio. El rango de puertas RTP del proveedor VoIP debe estar contenido en este rango.
- » **Caso haya un Firewall, verificar si estas puertas están liberadas.**
- » **Habilitar envío de tiempo entre registro:** cuando esta habilitado, el sistema dispone de la opción de especificar el tiempo entre registro(s).
- » **Tiempo entre registro(s):** permite especificar con que frecuencia la central actualizará su registro con el Operador VoIP. Patrón de fábrica: 3600 segundos.
- » **Enviar eventos DTMF:** define con cual método los dígitos DTMF serán enviados en la red así que se complete 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, usando RFC 2833.
 - » **In-Band:** envía los eventos DTMF en el paquete de voz.

Obs.: utilice el método definido por el operador.

- » **Valor del payload si RFC2833:** configure el tipo de carga (payload) del DTMF cuando seleccionado el evento DTMF Out-of-band (RFC2833). El valor oscila de 96 hasta 127, siendo el patrón 101.
- » **Cancelación de eco:** cuando habilitada, el sistema evita que el eco en la híbrida (cuando se pasa de 4 para 2 hilos) retorne para la red IP. Es decir, la cancelación 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, garantizando calidad de audio y confort al originador de la llamada.

- » **FAX:** define cual codec será utilizado para envío y recibimiento de fax por la red VoIP.
- » **Bypass:** utilizado si se conecta el dispositivo de fax en un adaptador ATA para la red VoIP.
- » **T.38:** Es utilizado si el dispositivo de fax y el proveedor VoIP fueran compatibles con el protocolo T.38.
- » **Deshabilitado:** desactiva el envío/recepción de fax por la ICIP.

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 - Placa 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.

Auto configuración extensiones/internos IP

Ese submenú es extremadamente 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 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 requisita 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.

Lista de extensiones pertenecientes a la auto configuración de terminales IP

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

El teléfono TIP100, 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 TIP100 solicitará vía DHCP una dirección de IP, en esta requisición, el TIP100 embutirá 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 TIP100 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 TIP100 irá configurarse para realizar una solicitud, con el intuito 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 TIP100 seguirá 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 TIP100. Toda vez que un TIP100 adquiriera un número de la central, la extensión/interno correspondiente sale de la lista de disponibles y no será más ofrecida a otro TIP100.

En el caso el número de extensiones/internos disponibles esté agotado, la central ICIP retornará una configuración inválida y el TIP100 no registrará en la ICIP.

En servidores Linux la configuración del servicio DHCP es editable en el archivo “/etc/dhcpd/ dhcpd.conf”. El TIP100 analizará si 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 placa ICIP.

Lista de extensiones/interos pertenecientes a autoconfiguración de terminales IP

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

Lista de extensiones pertenecientes a la auto configuración de terminales IP

Número - Ramal IP

328

Estado

Disponible

Añadir

Remover

Ramal IP	Estado
333	Disponible
334	Disponible
335	Disponible

Menú VoIP - Placa ICIP/Submenú Autoconfiguración extensiones/interos IP/ Extensiones/interos

- » **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/interos IP deseadas.

Poliza de garantía

Este documento solamente tiene validez en el territorio de la Republica Mexicana.

Importado por:

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

Calle Michoacán, 20 – Nave 9 C - Parque Industrial Finsa - Col. Renovación – Deleg. Iztapalapa – México, D.F.

C.P. 09209 - Teléfono: (55) 56 87 74 84

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

INDUSTRIA DE TELECOMUNICACIÓN ELECTRÓNICA BRASILEÑA DE MÉXICO S.A. DE C.V. garantiza este producto por 12 (doce) meses, en todas sus partes y mano de obra contra cualquier defecto de fabricación a partir de la fecha de adquisición bajo las siguientes condiciones:

1. Para hacer efectiva esta garantía, no deberá exigirse mayores requisitos que la presentación del producto y esta póliza, debidamente sellada en el establecimiento donde fue adquirido.
Centro de Servicio y Distribuidor Autorizado Intelbras:
Intelbras
Calle Michoacán, 20 – Nave 9 C - Parque Industrial Finsa - Col. Renovación – Deleg. Iztapalapa – México, D.F.
C.P. 09209 - Teléfono: (55) 56 87 74 84
soporte.tec@intelbras.com.mx
Consulte en el sitio www.intelbras.com.mx la relación completa de los centros de servicio y distribuidores autorizados.
2. La empresa se compromete a reparar o cambiar el producto así como las piezas y componentes defectuosos del mismo sin ningún cargo para el consumidor. El aparato defectuoso debe ser enviado a nuestro servicio técnico para evaluación y eventual reparación.
3. El tiempo de reparación en ningún caso será mayor de 30 hábiles días contados a partir de la fecha de recepción del producto en cualquiera de los sitios en donde pueda hacerse efectiva.
4. Con cualquier Distribuidor Autorizado Intelbras podrá adquirir refacciones, accesorios y partes.
5. ESTA GARANTÍA NO ES VÁLIDA EN LOS SIGUIENTES CASOS:
 - a) Cuando el producto ha sido utilizado en condiciones distintas de las normales.
 - b) Cuando el producto no ha sido operado de acuerdo con el Manual del Usuario en idioma español proporcionado.
 - c) Cuando el producto ha sido alterado o reparado por personas no autorizadas por el fabricante nacional, importador o comercializador responsable respectivo.

Datos del consumidor/producto.

Producto:	Marca:
Modelo:	No. Serie:
Distribuidor:	
Calle y Número:	
Colonia:	Estado:
CP:	Fecha de Entrega:
Sello y Firma:	

Término de garantía

Este CERTIFICADO DE GARANTÍA es una ventaja adicional a lo que determina la ley, ofrecida al Señor Consumidor. No obstante, para que el mismo posea VALIDAD, ES IMPRESCINDIBLE que se complete el presente y se haga la presentación de la nota fiscal de compra del producto, sin los cuales todo lo que se encuentra aquí expresado deje de ser efectivo.

Nombre del cliente:

Firma:

Fecha de compra:

Nº de nota fiscal:

Modelo:

Nº de série:

Revendedor:

Señor consumidor,

Este producto ha sido proyectado y fabricado buscando atender plenamente a vuestras necesidades. Este es el objetivo primordial de nuestra actividad. Para tanta, es **IMPORTANTE** que se lea atentamente este término.

Queda expresado que esta garantía contractual se otorga ante las condiciones que siguen:

6. Todas las partes, piezas y componentes del producto, son garantizadas contra eventuales defectos de fabricación, que por ventura vengan a presentar, 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, contado a partir de la entrega del producto al Señor Consumidor, según consta en la nota fiscal de compra del producto, que es parte integrante de este TERMINO en todo territorio nacional. Esta garantía contractual implica el cambio gratuito de las partes, piezas y componente que presenten defecto de fabricación, además de mano de obra utilizada en el reparo. Caso no constatado defecto de fabricación y, si, defecto(s) resultante(s) de uso inadecuado, el Señor Consumidor correrá con dichos gastos.
7. Constatado el defecto, el Señor Consumidor deberá de inmediato comunicarse con el SERVICIO AUTORIZADO más cercano que consta en el rol ofrecido por el fabricante – apenas estos estan autorizados a examinar y corregir el defecto durante el plazo de garantia aqui previstos. Si esto no es respetado, esta garantía perdera su validez, pues el producto tendrá sido violado.

Consulte en el sitio www.intelbras.com la relación de los centros de servicios.

8. En la eventualidad del Señor Consumidor solicitar la atención domiciliar, deberá dirigirse al Servicio Autorizado más cercano para consulta de la tasa de visita técnica. Caso sea constatada la necesidad de la retirada del producto, los gastos procedentes, transporte, seguridad de traslado, ida y vuelta del producto, quedan bajo la responsabilidad del Señor Consumidor.
9. La GARANTIA perderá totalmente su validez si ocurrir cualquiera de las hipótesis expresadas a continuación: a) si el defecto no es de fabricación, aún, causado por el Señor Consumidor, terceros ajenos al fabricante; b) si los daños al producto han sido oriundos de accidentes, siniestros, agentes de la naturaleza (rayos, inundaciones, derrumbamientos, etc.), humedad, tensión en la red eléctrica (exceso de tensión provocada por accidentes o oscilaciones excesivas en la red), instalación/ uso en desacuerdo con el Manual del Usuario o resultante de 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 rasurado; e) si el aparato ha sido violado.

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

Todas las imágenes de este manual son ilustrativas.

intelbras



eco amigável



uma das melhores
empresas para se trabalhar



fale com a gente

Brasil

Suporte a clientes: (48) 2106 0006

Contato e chat: www.intelbras.com.br/suporte

Sugestões, reclamações e rede autorizada: 0800 7042767

México

soporte.tec@intelbras.com.mx

(55) 5687 7484

Otros países

soporte@intelbras.com

Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia BR 101, km 210 - Área Industrial - São José/SC - 88104-800
www.intelbras.com.br | www.intelbras.com