SIEMENS

WERNER | von | SIEMENS ACADEMY

HiPath 3000 – HiPath Gateway

HG 1500V3.0 – Networking IP

Curso TNS:UD0016PB00BR_0001

Siemens Ltda.
Werner von Siemens Academy
R. Pedro Gusso, 2635 - CEP 81310-900
Curitiba - PR
☎ 55 (41) 341-6000
✉ education@siemens.com.br
www.education.siemens.com.br

SIEMENS

Papel é reciclável!
Preserve a natureza.

Este documento consiste em 63 páginas.

Elaborado por: U37, IC CS AT (Fernando Dias)
Liberado em abril de 2004.

Publicado pela Doc-Services Ltda.

Impresso no Brasil.

Sujeito a alterações técnicas.

Siemens Ltda.

Índice

1 Introdução 5
1.1 Visão Geral do HG 1500 V 3.0 5
2 Conexão serial via CLI 9
2.1 Software Upgrade via a interface CLI 10
2.2 Mudanças na configuração 11
3 Boot via CLI 15
3.1 Parâmetros gerais 15
3.2 Processo para atualização via Boot-CLI 15
3.3 Exercícios 17
4 Acesso via WBM – Web Based Management 20
4.1 Instalação 20
4.2 Iniciando uma seção WBM 20
4.3 WBM – Ícones da janela de controle 22
4.4 Diferenças entre Wizards, Maintenence e Explorer 22
4.5 Exercício 2 24
5 Conversão de Base de dados 25
5.1 Ferramenta de conversão 25
5.2 Exercício 3 28
6 Conectividade do HG 1500 como Router 29
6.1 LAN-LAN e Teleworking 29
6.2 Exercício 4 32
7 Conexão via Cornet IP 34
7.1 Configuracão IP Networking 34
7.2 Configurando PBX Nodes 36
7.3 Exercício 5 39
8 Simple Network Management Protocol 40
8.1 SNMP configuração para HiPath 3000 SMG 40
8.2 Parceiro SNMP 42
8.3 Atualização - HiPath 3000 via SNMP 44
8.4 Configuração TFTP Server 47
9 Geração de TRAPS via SNMP 50
9.1 Lista de todos TRAPS 50
9.2 Lista de todos - Critical TRAPS 51
9.3 TRAPS Individual 52

9.4 Lista de todos SNMP Communities 53
9.5 SMTP Read Communities 53
9.6 SNMP Write Communities 56
9.7 TRAP Communities 59
9.8 Exercício 6 62
10 Anexo 63
10.1 Pinos 63

1 Introdução

Esta documentação tem por objetivo habilitar aos participantes a instalar, programar e manter um HiPath Gateway para a linha de produtos HiPath 3000, além de proporcionar conhecimentos na área de interligação e aplicativos do HG1500.

1.1 Visão Geral do HG 1500 V 3.0

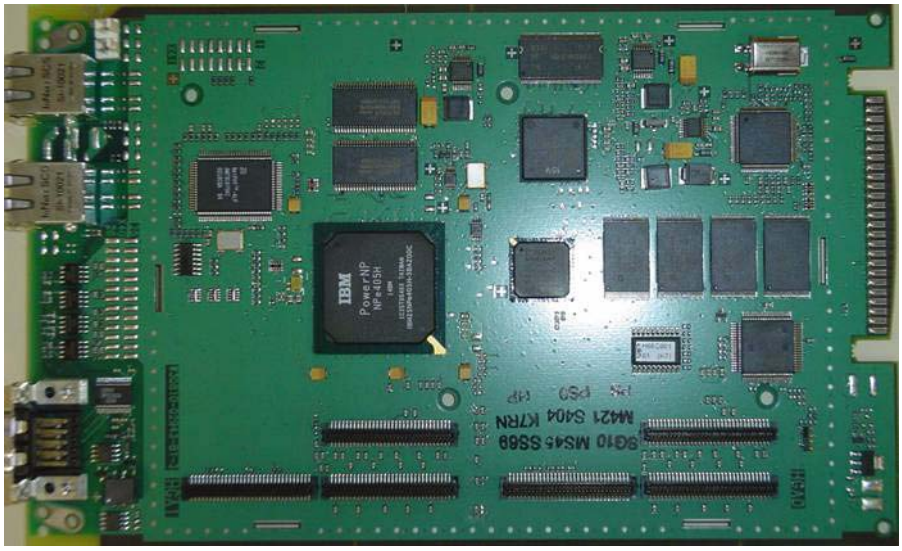
O HG 1500 V 3.0 é o novo Gateway IP para a Plataforma de comunicação HiPath 3000 e 5000.

Este produto é baseado sobre um novo conceito de HW e abrange todas as facilidades fornecidas pelo HW da HG 1500 V.2.0 e é ideal para IP trunking, IP telephony e CTI sobre a LAN.

Devido a grande demanda do mercado de tecnologia este produto é baseado na demanda sobre o IP networkin.

O HiPath Gateway é o Gateway que permite a integração direta dos sistemas HiPath 3000 com a rede do Cliente.

O novo sistema garante toda a gama de facilidades propostas pelo HG 1500 V.2.0.

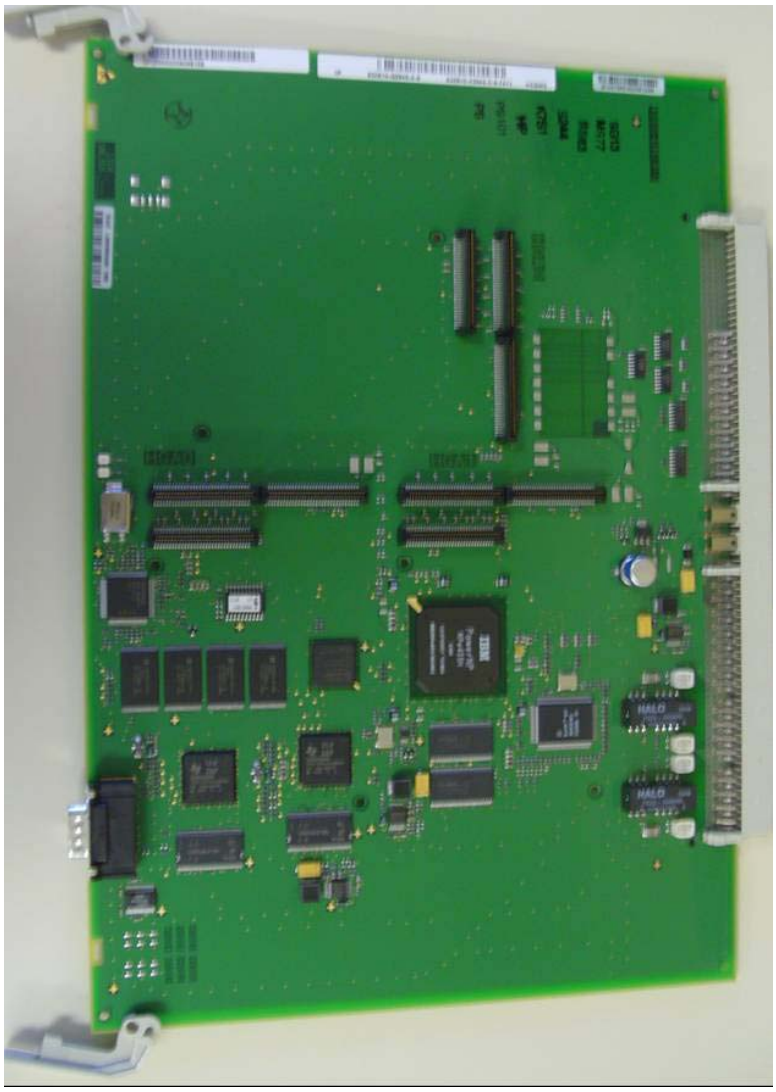


- Nova interface Serial de programação.
- Nova interface LAN 2 com 10/100 Mbps no módulo.
- Capacidade de Ampliação dos Codecs
- Entroncamento IP.
- IP Security
- Novo codec G729 AB

1.1.1 HXGSR V.3.0

- Módulo Responsável pela interconexão do sistema HiPath 3500 e 3300, com a rede LAN do cliente.
- Pode ser usado como interface de conexão ADSL, ISDN ou simplesmente LAN para a linha HiPath 3000/5000.
- Pode ser ampliado o número de Codecs através dos módulos PDM 1.
- Nova conexão serial e nova interface de programação.

1.1.2 HXGM



- Novo HW com um novo processador.
- Capacidade de Ampliação com o módulo PDM 1.
- Fornece conexão LAN-LAN e roteamento via ISDN para otimização do processo.
- Acesso Remoto a HG1500 via modem Analógico.
- Até 03 módulos de expansão (no Step 2).
- Nova interface LAN 2

1.1.3 Razões e objetivos

- Concentração de dois produtos em existentes (RG2500 e HG1500) e a criação de um Hardware comum para a Plataforma HiPath 3000/5000.
- Este produto é baseado nas últimas versões do HG1500 V2.0 e RG 2500 V.2.5 mantendo todas as facilidades existentes.
- Conexão dos sistemas somente através de terminais IP.
- Conexão dos sistemas HiPath 3000 como Gateway de voz TDM e IP.
- IP Networking com Transparência de Facilidades.
- Acesso a Internet através de ISDN ou ADSL
- Roteamento em LAN ou WAN.
- Interface Aberta de TAPI e CTI.

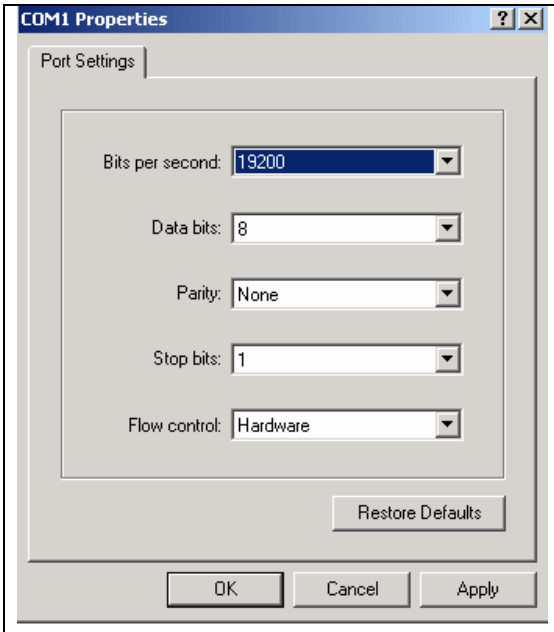
1.1.4 Novidades

- Melhora no desempenho.
- Aumento gradual dos recursos.
- Possibilidade de Ampliação
- Novo Hardware completamente revisado
- Aumento na Capacidade de Voice Clientes
- Aumento na quantidade de codecs.
- Suporte seguro e fácil através de uma nova ferramenta desenvolvida em HTML.
- Integração total com o mundo IP.
- Expansão adicional do codec G. 729 AB

1.1.5 Marketing

- HG 1500 V3.0 é um módulo de expansão para os sistemas HiPath 3000 V3.0 e V4.0
- A configuração básica do módulo continua habilitada para dois canais B.
- O processo de ampliação agora passa a ser adcionado de dois em dois canais.
- 05 pacotes para Voice Clients (optiClient 130, optiPoint 400 / 600 oferecidos de:
- 01 usuário
- 10 usuários
- 25 usuários
- 50 usuários
- 100 usuários

2 Conexão serial via CLI



Conectar a HG 1500 V3 com a interface do PC direto via cabo modem.

Inicia-se o programa terminal com composição 19200,N,8,1.

Pressione qualquer tecla para mostrar o prompt para entrar com “user name” e “password”.

O nome do usuário e senha são verificados novamente e os dados são armazenados no HiPath 3000.

vxTarget> get write acess – **Habilita o acesso escrito**

vxtarget> set ip address 192.168.100.X - **Entre com o número do endereço IP da HG 1500 V3. A placa deve ser inicializada depois dessa mudança.**

vxTarget> set ip subnet 255.255.255.0 – **Entre com o endereço IP da subnet mask. A placa deve ser inicializada depois dessa mudança.**

vxTarget> set default gateway 192.168.100.X - **Entre com a default gateway, se necessário.**

vxTarget> show ip address – **Mostra a configuração.**

Configured IP Address is 192.168.100.X
Configured IP Netmask is 255.255.255.0
Active IP Address is 192.168.10X.X
Active IP Netmask is 255.255.255.0

vxTarget> save configuration - **Salva os parâmetros estabelecidos.**

vxTarget> reset – **Inicialize a HG 1500 V3 para habilitar os parâmetros mudados. A inicialização pode ser efetuada a qualquer momento usando a combinação de teclas Ctrl + x.**

vxTarget> logout – **Sai da interface do CLI (sem efetuar um Boot)**

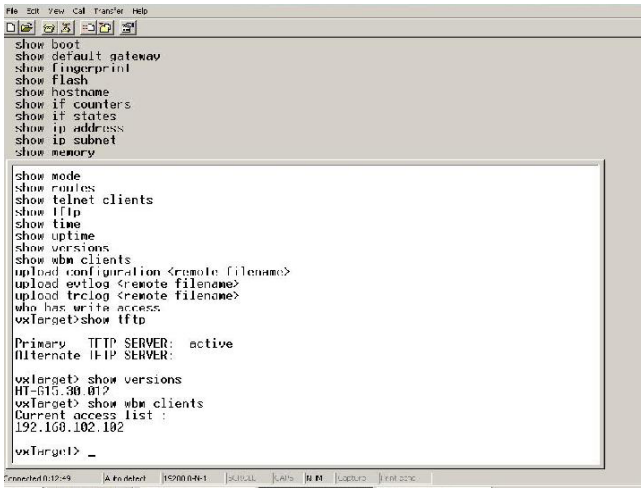
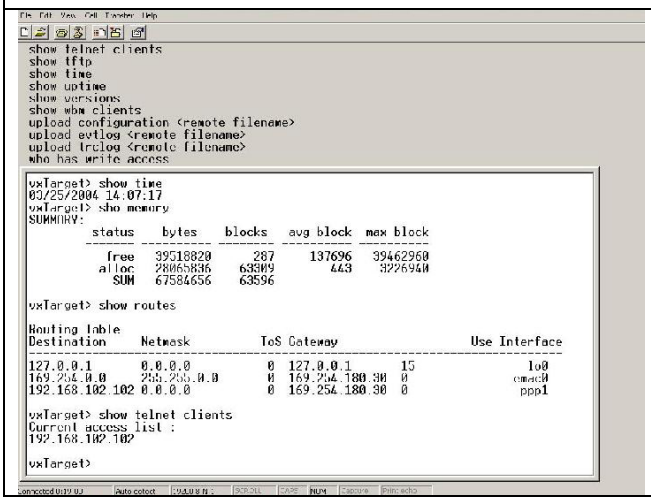
2.1 Software Upgrade via a interface CLI

A configuração e operação TFTP servidor é necessário na rede:

vxTarget> set tftp 192.168.100.X:8085 – **Entre com endereço IP e número da porta do servidor TFTP.**

vxTarget> download software vxworks.inst - **Download do software atual.**

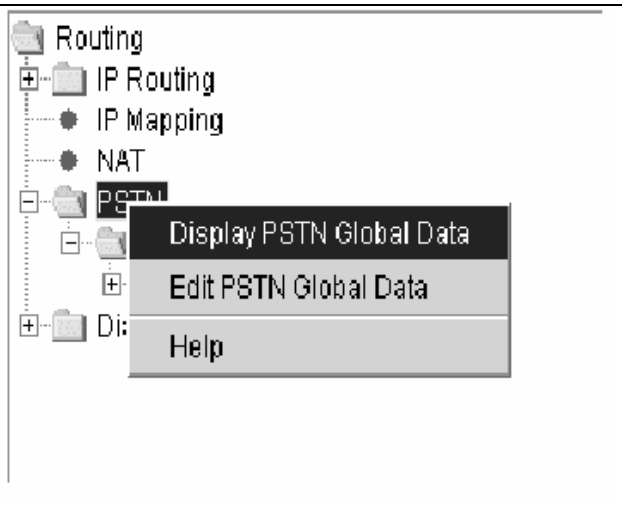
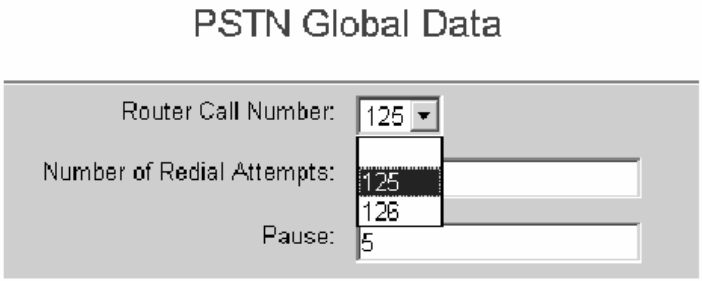
vxTarget> activate software – **Habilita o novo software de imagens. Depois disso, a HG 1500 V3 efetuará automaticamente a inicialização.**

	Conexão TFTP.
	Mostra as rotas TFTP. Procedimento: show routes

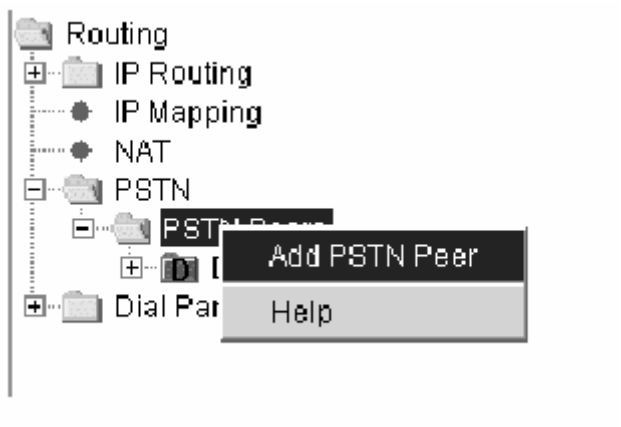
2.2 Mudanças na configuração

2.2.1 Internet CBC com 2 canais B via Arcor

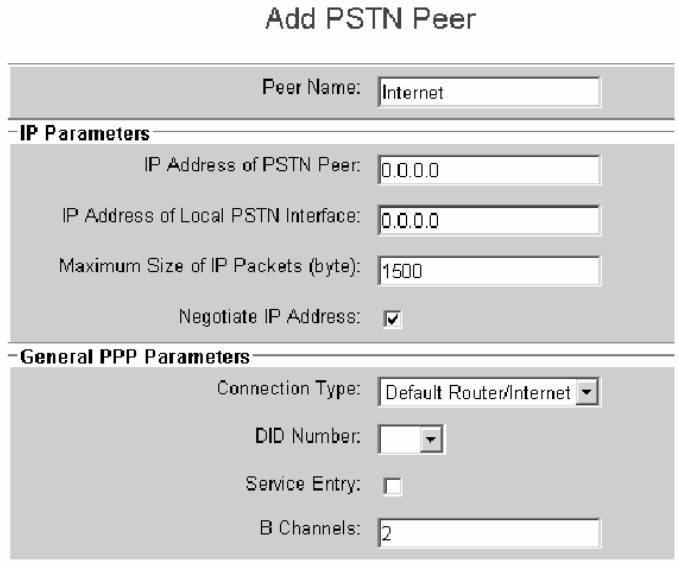
Nota:
Uma interface ISDN3 não é usada por longo tempo. Tudo é configurado sob PSTN. Por Internet routing, e entrando por ”IP Routing” não é solicitado por longo tempo.

	Para entrar ou editar parâmetros no WBM, clique com o botão direito do mouse.
	Adicionar e configurar uma PSTN Peer . Router Call Number, Number of Redial Attemps, Pause.

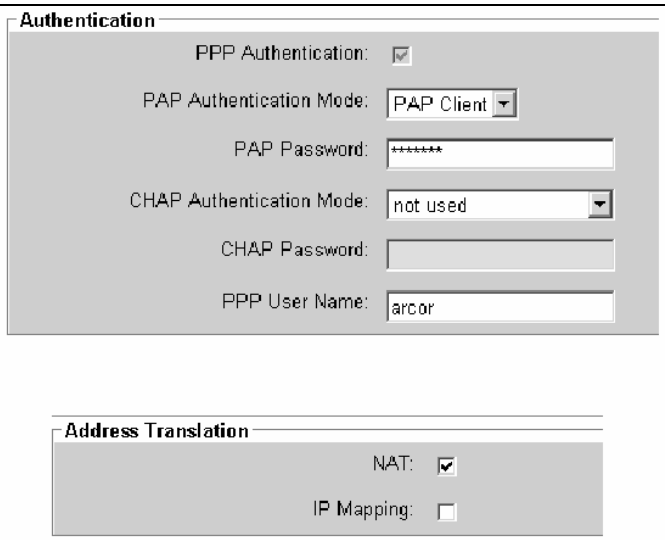
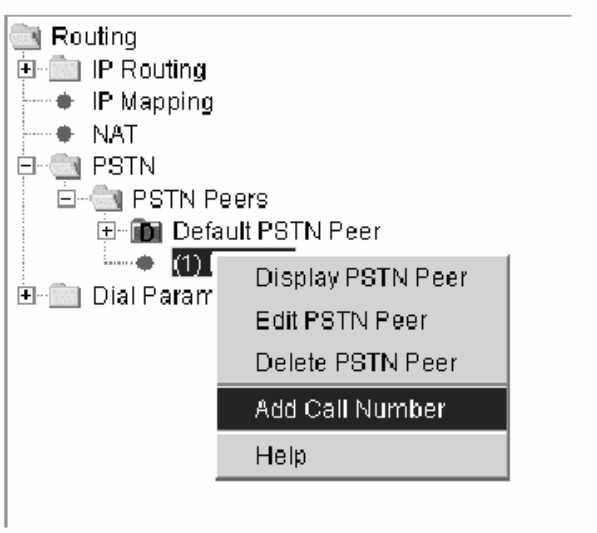
,



Outrora ISDN Peer. Caminho: Routing-> PSTN -> PSTN Peer.



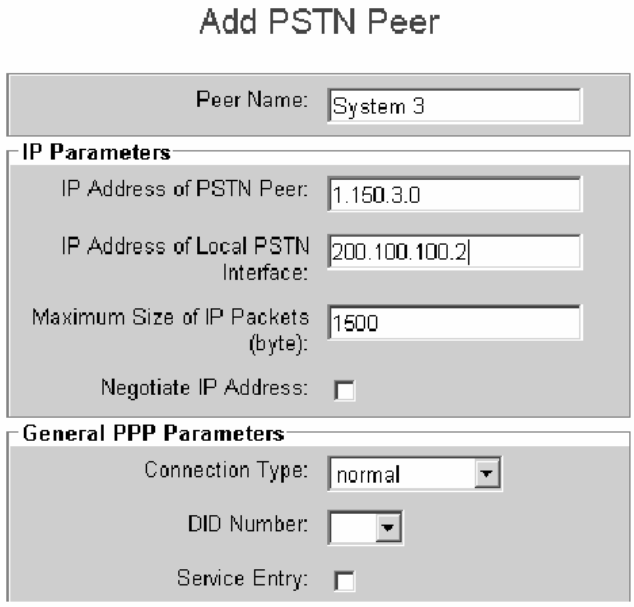
Adicionar os dados.

	Autenticar.
	Adicionar número de chamada.

2.2.2 IP Routing via ISDN

2.2.2.1 Static Routing

Nota:
Uma interface ISDN1 ou ISDN2 não são usados por longo tempo. Tudo é configurado sob PSTN.

	Adicionando um PSTN Peer.

2.2.2.2 Dynamic Routing

Todos os outros parâmetros são quase idênticos ao da HG 1500 V2.

3 Boot via CLI

3.1 Parâmetros gerais

Para entrar o Boot-CLI, você deve interromper o processo de boot pressionando qualquer tecla.
(pressione Ctrl + x no programa terminal para iniciar o processo de boot).

[HG 1500 V3 Boot CLI]: p – **Mostra os parâmetros do boot (bootline.act file)**

[HG 1500 V3 Boot CLI]: c - **Edita os parâmetros do boot**

[HG 1500 V3 Boot CLI]: z - **Salva os parâmetros editados em bootline.act.**
O arquivo padrão é salvo como bootline.bck

[HG 1500 V3 Boot CLI]: w – **Carrega o novo software image via FTP ou TFTP e**
copia os mesmos para TFFS (True Flash File System).

[HG 1500 V3 Boot CLI]: @ - **Salva o novo software image e reset da HG 1500 V3**

[HG 1500 V3 Boot CLI]: y - **Formata o TFFS.**
Aviso: Todos os dados serão perdidos!

Nota:

O departamento do desenvolvimento indica que apenas esses parâmetros podem ser usados no Boot-CLI!

3.2 Processo para atualização via Boot-CLI

[HG 1500 V3 Boot CLI]: c
'.' = clear field; '-' = go to previous field; ^D = quit

boot device : tffs/0 emac0 - **Set o parâmetro boot para a interface LAN1**

processor number : 0 – **É sempre 0**

host name : HG1500V3 – **Nome do administrador da HG 1500 V3**

file name : vxworks.inst – **Entrada do nome do software image**

inet on ethernet (e) : 192.168.100.X:ffffff00 - **Endereço IP e subnet mask (subnet mask deve ser em hex)**

inet on backplane (b): - **Não usado até o momento**

host inet (h) : 192.168.100.X - **Endereço IP do FTP ou TFTP server**

gateway inet (g) : 192.168.10X.X - **Default gateway**

user (u) : Siemens - **User code para identificação do FTP server**

ftp password (pw) (blank = use rsh): 123456 - **FTP password**

flags (f) : 0x0 - **0x0 = FTP, 0x80 = TFTP**

target name (tn) : - **Sem entrada**

startup script (s) : - **Sem entrada**

other (o) : emac – **É sempre emac**

[HG 1500 V3 Boot CLI]: z **– "Save" os parâmetros**
Copy content of /tffs/bootline.act into /tffs/bootline.bck.
write /tffs/bootline.act ok!

[HG 1500 V3 Boot CLI]: w

SW_IMAGE.002
Entrar um novo sufixo SW_IMAGE.x: 1 - "1".
Isso irá registrar SW_IMAGE.001.

Novo image name: SW_IMAGE.001 ok (y/n)? y – Confirme com "y"

8296702 bytes
Loading ok. – **O novo software image está carregado.**

Muda o bootline para a imagem carregada e write bootline para TFFS (y/n)? y - **Do you want to set the boot device from emac0 (LAN1) back to TFFS? Confirm with "y".**

Write /tffs/bootline.act ok!
[HG 1500 V3 Boot CLI]: @ - **Reset of HG 1500 V3 and saving of the new software image**

Loading SW_IMAGE.001...8319496

Instalar novo HXG3 APS HI-G15.3A.056-XXX…

Dois tipos diferentes de instalação são atendidos:

1. initial download: download de uma imagem com database vazia, a memória flash será formatada, todos dados serão perdidos!

2. upgrade download: download de uma imagem, sem formatação.

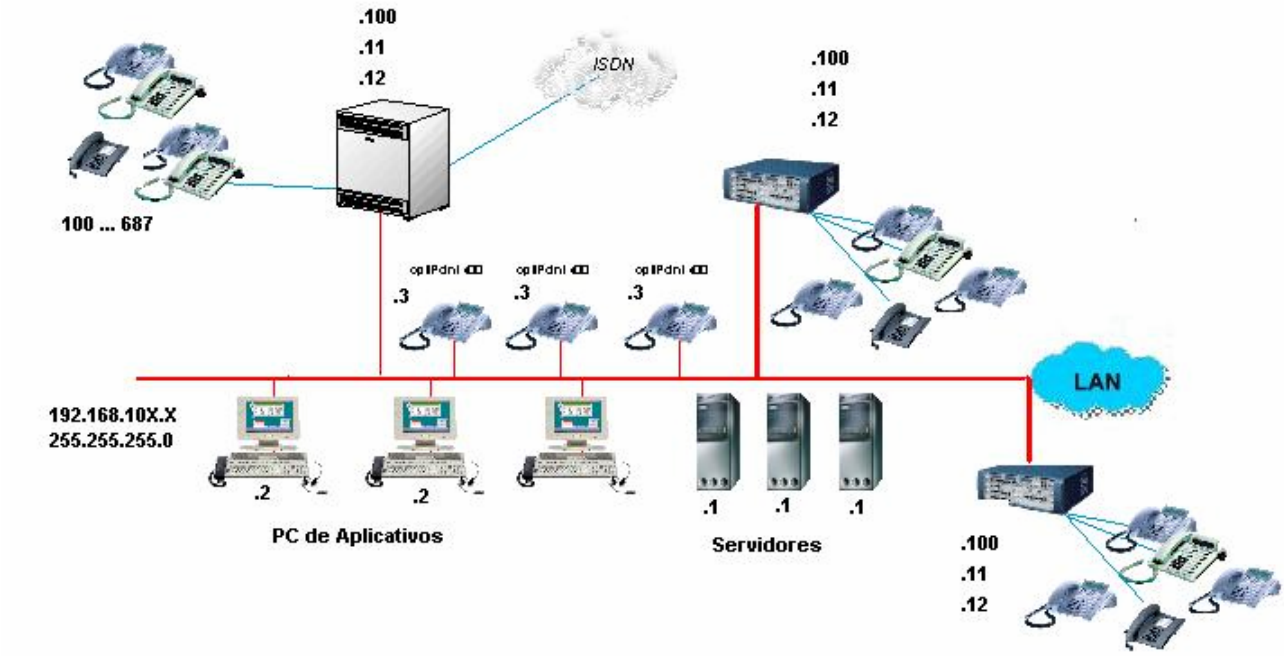
Qual instalação você quer (1 = initial download, 2 = upgrade) ? 2 -
Entrar em "1" results in a reload of the board,
"2" results in upgrading of the HG 1500 V3, including a conversion of the customer data to a new format, if required.

Depois disso, a HG 1500 V3 realizará vários resets e inicializa a operação.

3.3 Exercícios

3.3.1 Exercício 1

3.3.1.1 Configuração do Sistema



Nota : Os equipamentos estão dispostos, para todos os grupos porém o X do endereçamento de rede, será relacionado com o número de cada equipe, que será disposto de 1 a 3. Cada usuário utilizará uma central com 02 placas HG 1500, uma na versão 2 e outra na Versão 3, para fazer o roteamento entre os sistemas.

Endereçamento IP

	Grupo 1	Grupo 2	Grupo 3
Servidor	192.168.101.1	192.168.102.1	192.168.103.1
PC 2	192.168.101.2	192.168.102.2	192.168.103.2
Subnet	255.255.255.0	255.255.255.0	255.255.255.0
HiPath	HiPath 3500	HiPath 3500	HiPath 3700
HG1500 V.2.0	192.168.101.10	192.168.102.10	192.168.103.10
HG1500 V.3.0	192.168.101.11	192.168.102.11	192.168.103.11
HG p/ Man. E	192.168.101.100	192.168.102.100	192.168.103.100
optiPoint 400	192.168.101.3	192.168.102.3	192.168.103.3
AP 1120	192.168.101.4	192.168.102.4	192.168.103.4
Plano de Num	341-1XX	342-2XX	343-XXX

1. Usando a interface de SW CLI para configuração dos parâmetros iniciais (Capitulo 5 do Manual se Serviço)
2. Ativar o WBM (WEB Based Management) e ativar as configurações iniciais. (Cap.2 do Manual de Serviço)
3. Use o “Wizard” no WBM para configurar os parâmetros iniciais no produto. (Cap.2 do Manual de Serviço).
4. Navegue através dos parâmetros de “Explorer”:

   - É possível trocar o endereço IP do HG 1500 V.3.0

   - Os CodePoints AF/EF possuem o mesmo valor do HG 1500 V.2.0.

   - Os parâmetros de QoS, possuem o mesmo valor do HG 1500 V.2.0.

   - Configure o “Online Help Destination”, veja os procedimentos no capitulo 03 do Manual de serviço.

Anotações:

4 Acesso via WBM – Web Based Management

4.1 Instalação

Os seguintes componentes devem ser instalados:

- Java plug-in JRE 1.3.1
- Microsoft Internet Explorer 5.5 ou 6.0
- XML Extension DLL V3.0 SP2
- Explorer settings deve permitir o uso do ActiveX e Java.

Devem ser instaladas as últimas versões.

Para WIN NT:
- istmsi_12.exe
- msxml3.exe
- xmlinst.exe
- msxml3sp2setupGer.exe – XML\XML SP2 necessário para HXG3

Para WIN 200:
- msxml3sp2setupGer.exe – XML\XML SP2 necessário para HXG3

Para WIN 98:
- instmsia_Win9x.exe
- msxml3.exe
- xmlinst.exe
- msxml3sp2setupGer.exe – XML\XML SP2 necessário para HXG3

Após a instalação reboot do PC.

Para últimas atualizações entre em:

Additionally needed components for WBM:
- Java 2 (TM) with Java-PlugIn2 (SUN), V1.3, download from *SUN download*
- XML Parser 3.0 (SP4) from Microsoft, download from *Microsoft download*
- only neccessary, if XML Parser installation fails: Windows Installer V2.0 from *Microsoft download*

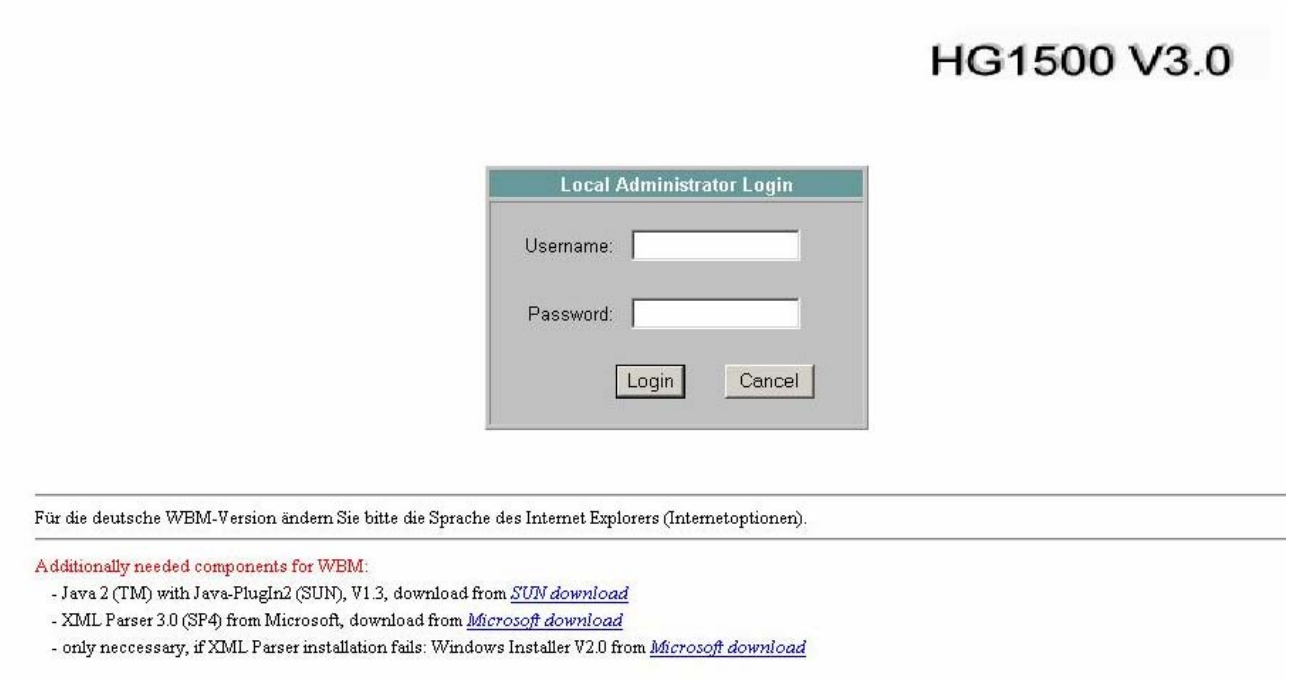
4.2 Iniciando uma seção WBM

Proceder com os seguintes parâmetros:

1. Iniciar o Web browser.
2. Entrar com o endereço gateway IP com a URL no campo de endereço.

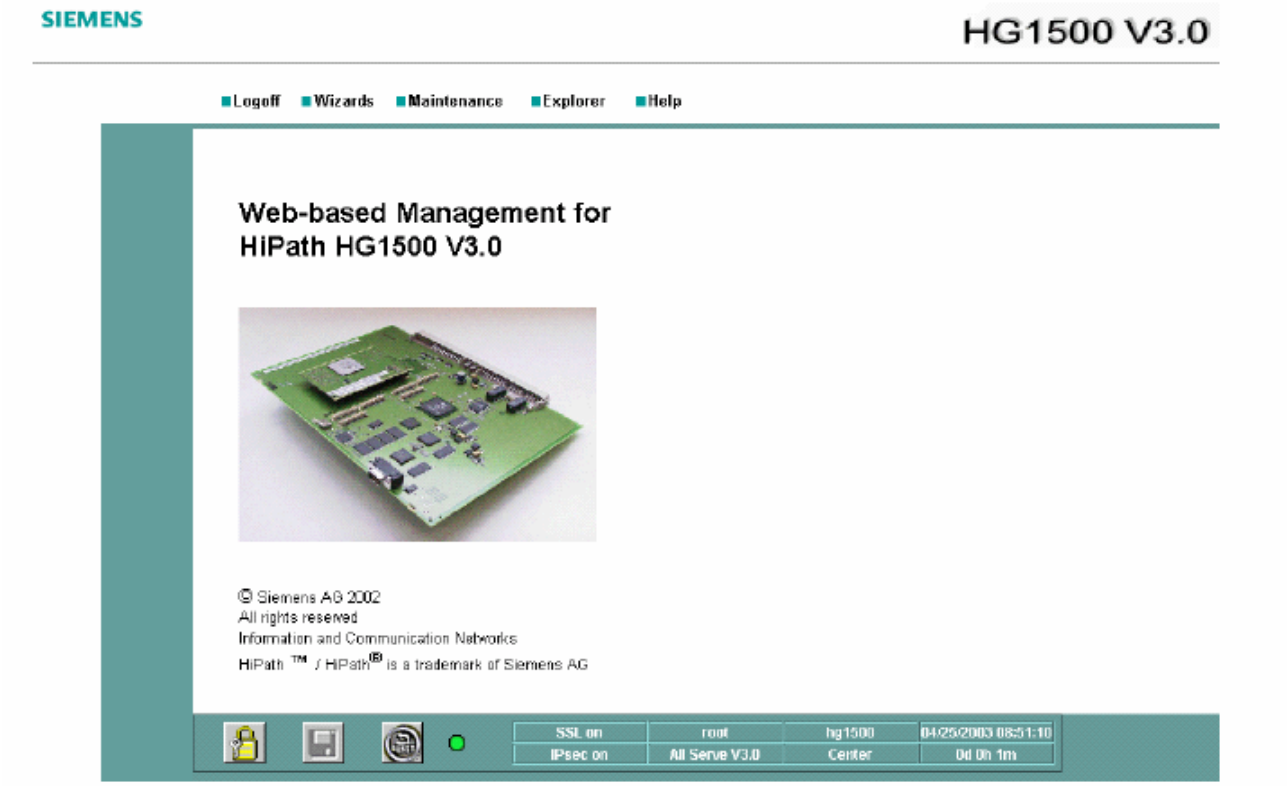
(http://num.num.num.num:8085, onde num é o número entre 0 e 255).

3. Precionar a chave de voltar.
4. Entrar com o username e password na página de login e clique o botom de login.



Você verá a abertura da homepage, na qual você pode visualizar a administração dos módulos disponíveis.

A seguinte figura mostra um exemplo do WBM homepage:



4.3 WBM – Ícones da janela de controle

A área de controle constantemente prove controle e informações de estado.
A figura abaixo mostra um exemplo:

Os seguintes ícones são acessíveis:

- Cadeado (1)
- Save (2)
- Reset (3)
- Ação (4)

O seguinte estado de informação é também mostrado:

- Estado do SSL e IPsec (5)
- Categoria de acesso do usuário e sistema da versão (6)
- Nome do sistema e localização (7)
- Data e hora do sistema, e quanto tempo desde do último restart (8)

4.3.1 Conceito do ícone de controle

Nem todos os ícones de controle estão sempre ativos. Ícones inativos estão em cinza.

Antes de o administrador modificar os dados, o cadeado deve estar desbloqueado. Essa restrição ao acesso, impede o mesmo dado ser modificado de qualquer computador. Os dados podem apenas ser modificados do computador o qual acesso foi reservado. De todos os outros computadores os dados podem apenas ser lidos. Os ícones de “save” e “reset” são apenas disponíveis se o acesso escrito foi reservado. Eles indicam se o dado deve ser salvo, o gateway deve ser resetado ou both é exigido para o fim do processo.

4.4 Diferenças entre Wizards, Maintenence e Explorer

O objetivo do Wizards, Maintenance e Explorer é o mesmo, isto é para mostrar e modificar os dados. A diferença encontra-se na operação e serviço.

. Wizards:

O módulo para iniciar o setup combina todas as operações solicitadas para iniciar a configuração do gateway. O outro Wizards habilita dados para entrar e modificar usando o editor de tabelas.

. Maintenence:

Funções Maintenance são mostradas como estruturas de tronco hierarquicamente. Esse módulo contém todas funções necessárias para o HiPath HG 1500.

. Explorer:

Funções Explorer são mostradas como estruturas de tronco hierarquicamente. Esse módulo contém todas funções necessárias para o HiPath HG 1500.

4.4.1 Wizards – Funções

Todas wizards são selecionadas via um menu. As seguintes wizards são disponíveis:

. Initial Setup
. PBX Routing
. IP Mapping
. IP Filter
. NAT
. MAC Filter

4.4.2 Maintenance – Funções

. Conguration
. Software Image
. Multigateway Admin
. Joblist
. Traces
. Events
. SNMP
. Admin Log
. Actions
. Conversion

4.4.3 Explorer – Funções

. Basic settings
. Security
. Network Interfaces
. Routing (router settings)
. Voice Gateway
. VCAPI
. Payload
. Statistics

4.5 Exercício 2

1. Inicie um SW Up Grade do HG 1500 V.3.0 para a última versão de imagem utilizada em sala via WBM. (Conforme Manual de Manutenção do Produto – Capitulo 5).
2. Efetue um reset Geral da HG V 3.0 com o “Factory Settings”. (Manutenção – Configuração – Dados e Performance, com o botão direito do mouse poderemos ativar um reset).
3. Salve a configuração default do HG V.3.0, conforme Manual de Administração e Manual de Manutenção – CAP 5).
4. Efetue um Upload e salve a configuração do HG 1500 V.3.0. (Conforme o Capitulo 5 do Manual de Administração e Manual de Serviço).

Anotações;

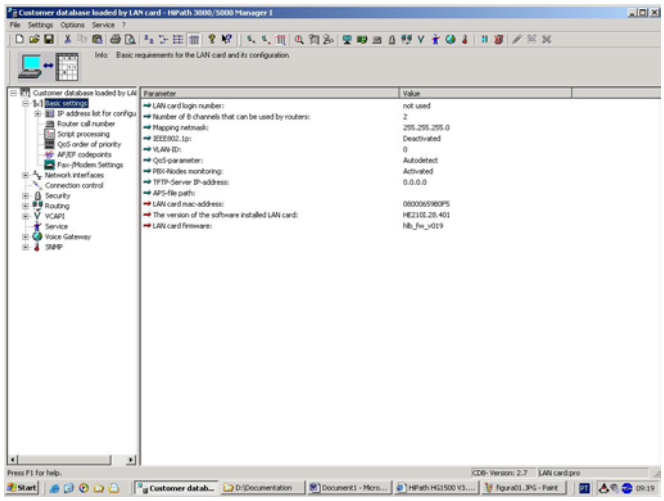
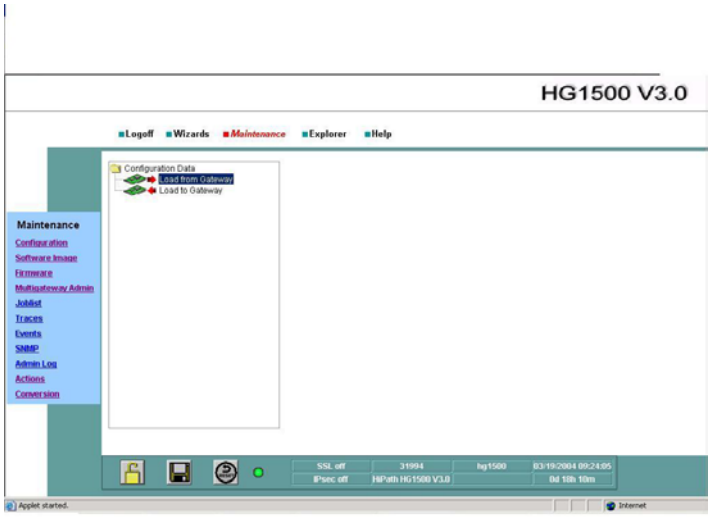
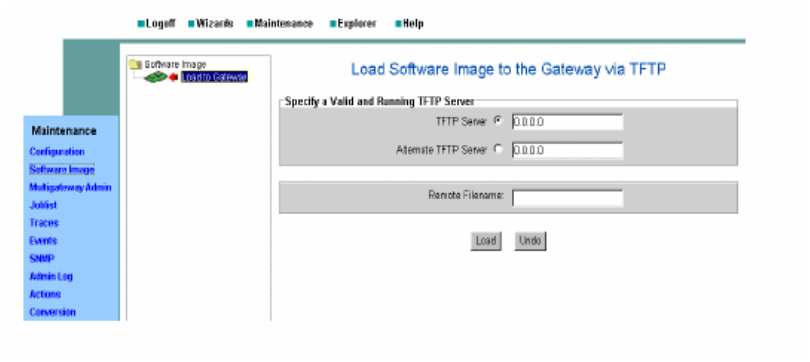
5 Conversão de Base de dados

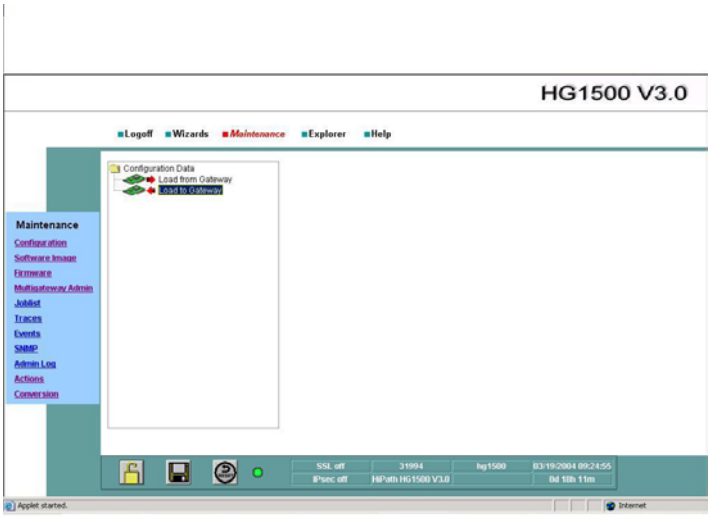
5.1 Ferramenta de conversão

Essa ferramenta ajuda a facilitar a transição de um HXGS, HXGR ou HXGM para um HXGS3, HXGR3 ou HXGM3.

Para fazer a transição:

	1. Download da ferramenta de conversão para "C:\conversion\" directory e unzip o downloaded o arquivo "conversion.zip" nesse diretório.

	2. Use o HiPath 3000 Manager I para salvar a base de dados da HXGS, HXGR ou HXGM para "C:\conversion\hg1500.hic". Salve a base de dados em "KDS-Version: 2.6" ou em "KDS-Version: 2.7" format. Escolha o nome do arquivo de base (e.g. "hg1500") como desejado e dê a extensão "hic".
	3. Use o "Maintenance/Configuration/Load from Gateway" para salvar os dados da nova configuração do HXGS3, HXGR3 ou HXGM3 para o "C:\conversion\hg1500.xml". De fato use o mesmo nome de arquivo base como no passo 2 e adicionando a extensão “xml”.
	4. Inicie a ferramenta de conversão clique no arquivo "C:\conversion\conversion.bat". O programa perguntará para selecionar o arquivo "hic" para ser convertido. O programa lê o arquivo, converte toda informação da base de dados e insere no arquivo em "xml".

	5.Use a função Maintenance/Configuration/Load to Gateway" para fazer o upload do arquivo em "xml" para o novo HXGS3, HXGR3 or HXGM3.

5.2 Exercício 3

1. habilite *o IP Address Filtering*. Somente para os computadores do seu grupo (Manual de Serviço Capitulo 4).
2. Somente o servidor terá direito de administrar o HG 1500 V.3.0, via Telnet. (Manual de Configuração – Cap.4).
3. Configure dois optiPoint 400, e um optiClient 130 (PC 2) e um H323 Client NetMeeting (PC 1) e testar o número de chamadas simultâneas através do Hipath 3000 com telefones IP utilizando os diversos tipos de codecs.
4. Configure um “Static IP Routing” através de uma interligação ISDN entre todos os grupos
5. Configurar Rotas dinâmicas através do “Dinamic IP Routing” sobre uma interligação ISDN entre os 03 PABX.
6. Conversão de Base de Dados.

Anotações:

6 Conectividade do HG 1500 como Router

6.1 LAN-LAN e Teleworking

Conexões LAN-LAN, isto é conexões WAN, podem ser estabelecidas entre HiPath HG 1500 e outro HiPath HG 1500, HiPath 3000 LAN-Bridge 1.x ou outros routers. Roteamento também habilita acesso para provedor internet. A característica do princípio IP descreve a opção de alocação de acesso a Internet custo de base da origem de acordo para quantidade de transferência de dados e vários modelos de tarifas armazenadas na aplicação.
HiPath HG 1500 oferece pacote de canal para acima de 16 canais B (HiPath 3300/3350 oferecem um máximo de oito canais B em CO-side).
IP é auxiliado como um protocolo de transporte.
Neste caso do HiPath Gateway 1500 com duas interfaces LAN, roteamento também é possível entre duas interfaces LAN.

Características
- PPP conexões (conexões LAN-LAN e teleworking)
- PPP multilink conexões (channel bundling)

Firewall mecanismos
- Verificação do MAC ou endereço IP
- TCP, UDP e ICMP port Firewall
- Controle de acesso usando ISDN call numbers
- Automatic callback
- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol).

Uma estação teleworking necessita um cartão ISDN com software de acesso remoto (e. g. Dial-Up Networking). Uma concexão em rede para HiPath HG 1500 é estabelecida com cartão ISDN.

Acessos para rede locais podem ser estabelecidos via as seguintes conexões:
- Analog V.34 (max. 33,600 bit/s)
- ISDN DSS1
- GSM V.110

6.1.1 Configuração LAN-LAN via ISDN

Os seguintes passos devem ser completados no programa de administração para usar HiPath HG 1500 Como um ISDN router:

- Identificar o endereço IP da LAN remota
- Definir o endereço IP da porção WAN (ISDN)
- Para todos os PCs, entrar com o endereço IP do HiPath HG 1500 como o gateway abaixo.
Network Interface > Network interfaces > LAN.. Entre com o endereço IP definido anteriormente como WAN aqui.

Onde solicitado, habilita a interface para configurar abaixo.”Network Interfaces”.
- Com o botão esquerdo do mouse, selecione a “IP routing” e pressione.”New” na janela de diálogo, entrar com o endereço IP da LAN para ser alcançado e confirmar sua entrada.
Reduzir a entrada de carga, você pode entrar com valores para.”Network mask” e “Gateway” abaixo. Prefixos.

Selecione a nova entrada usando o mouse.
- Network mask:

Especifique a netmask da rede de destino.
- Gateway:

Under Gateway, entrar com o endereço IP da interface remota ISDN.
- Com o botão esquerdo do mouse, selecione **ISDN partner** e pressione ”New” na janela de diálogo, entrar com nome ISDN peer e confirme sua entrada.

Selecione a nova entrada usando o mouse.
- Endereço IP:

Entrar com o endereço IP da inteface remota ISDN. O mesmo endereço é usado aqui como abaixo.
Routing - IP-routing - Gateway. (IP address of the remote ISDN interface).
- Canais B:

Entrar o número máximo de canais B para essa conexão.
- Duplo-click correspondente ISDN partner.
- Call number list

Pressine. “New” para criar a nova entrada e entrar em remote call number.
- Call direction:

Defina a chamada direta permitida para esse par.
Adaptar o outro protocolo settings na linha com a estação remota e configure essa colocação para o HiPath HG 1500.
Finalmente, check a conecção para aestação remota usando o comendo “Ping”.

Se a resposta correta não é recebida por Ping, o peer pode ter sido configurado incorretamente.

6.1.2 Configuração LAN-LAN entre interfaces LAN

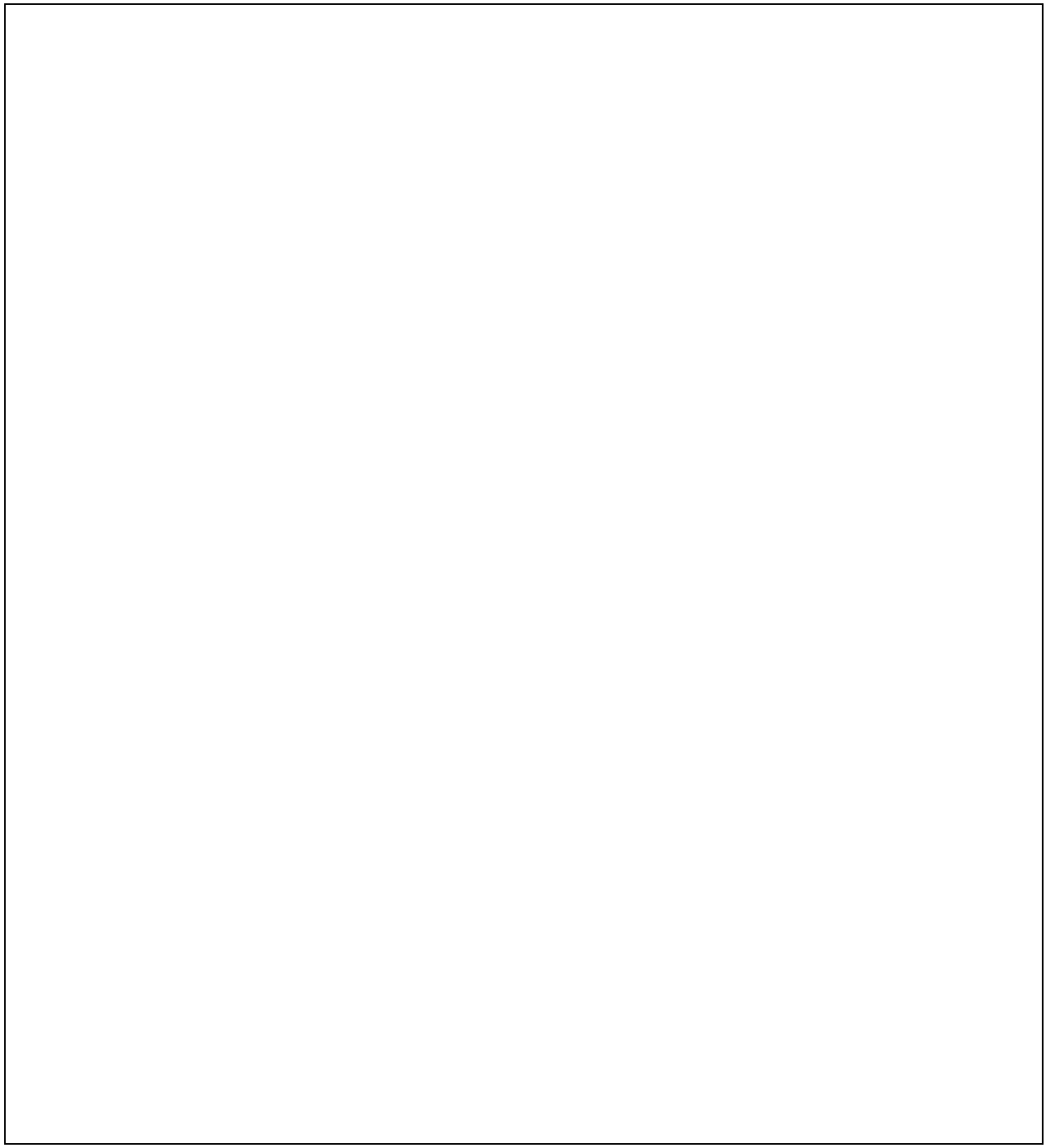
As duas interfaces LAN podem conectar duas diferentes redes. A configuração da interface LAN2 é similar a interface da primeira LAN.
Sem roteamento precisa ser feito para duas conexões de rede diretamente.

Além disso, o parâmetro “NAT” pode ser usado para selecionar interpretação de endereço vis-à-vis a outras interfaces.

6.2 Exercício 4

1. Configure uma conexão de Internet CBC (Call by Call). (Veja o exemplo na documentação do curso - capitulo 2)
2. Configure um IP Networking entre os grupos 1, 2 e 3, utilizando a numeração do grupo, testar o novo codec G.729 AB. Conforme o capitulo 11 do Manual de Configuração

Anotações:



7 Conexão via Cornet IP

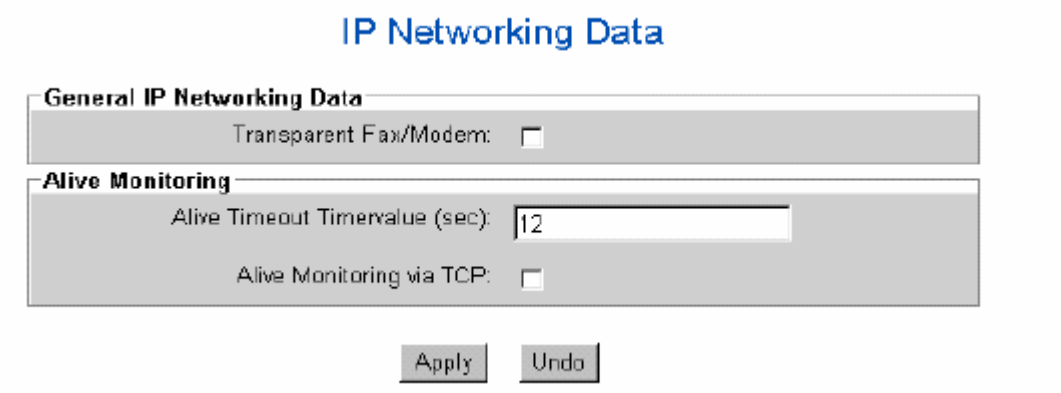
7.1 Configuracão IP Networking

Você pode fazer colocações gerais para IP networking e PBX node monitorando com essa função.

7.1.1 Edit - IP Networnking

Para IP networking:
Procedimento:
1. Abrir o WBM.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Explorer”.
4. Click em “Voice Gateway” à esquerda da janela.
5. Click com o botão direito em “IP Mapping” na estrutura de árvore e selecione “Edit” do menu pop-up.

O seguinte diálogo é mostrado no conteúdo da área:

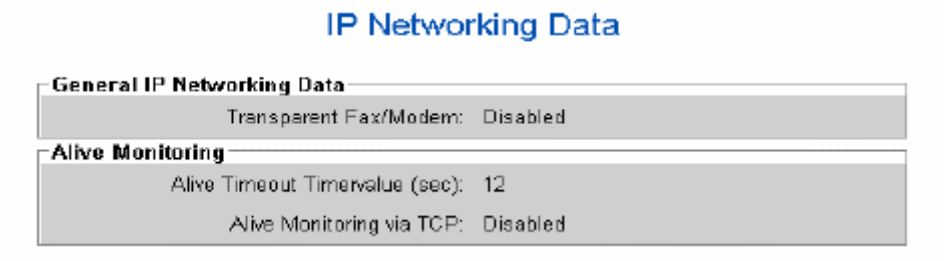


Você pode editar os seguintes parâmetros:
. **Transparent Fax/Modem:** Especificar se as transmissões transparentes do fax e modem podem ser ativadas usando IP Networking.
. **Alive Timeout Timervalue (sec):** Neste campo, entrar o intervalo de tempo para o monitoramento e nó.
. **Alive Monitoring via TCP:** Selecione esta opção se a componente é para ser monitorada.
TCP. Se esta opção não é selecionada, a componente é monitorada via UDP (via ping).
6. Click em “Apply”. A configuração é modificada.
7. Click no ícone “save” na área de controle.

7.1.2 IP Networking Settings

Para mostrar os parâmetros correntes H.323:
Procedimento:
1. Abrir o WBM.
2. Click em “Explorer”.
3. Click em ‘Voice Gateway” à esquerda da janela.
4. Click com o botão direito em “IP Networking Data” na estrutura de árvore e selecione “Display” do menu pop-up.

A seguinte informação é mostrada na área do conteúdo:



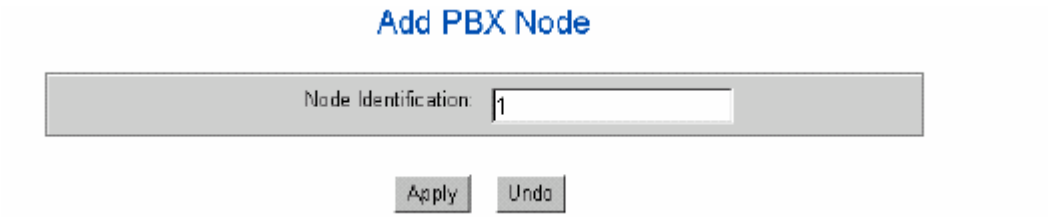
7.2 Configurando PBX Nodes

PBX nodes (HiPath systems) pode ser identificado por um número de 1 para 64. O endereço IP pode ser fixadopara a identificação do número.
As funções “Explorer” descritos abaixo podem ser usados para configurar e administrar PBX nodes, Editar e associar endereços IP e codec settings e configurar números chamados para esse nós.

7.2.1 Configurando um PBX Node

Para configurar um novo PBX node:
Procedimento:
1. Abrir o WBM.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Explorer”.
4. Click em “Voice Gateway” à esquerda da janela.
5. Duplo-click em “PBX” no menu.
6. Click com o botão direito em “Nodes” na estrutura de árvore e selecione “Add PBX Node” do menu pop-up.

O seguinte diálogo é mostrado no conteúdo de área:

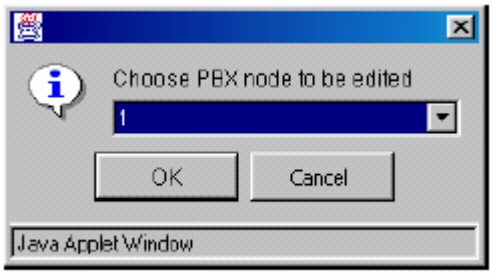


7. Entrar o número desejado de um PBX node.
8. Click em “Apply”. A configuração é modificada e o diálogo é mudado do “add.” Para ”edit”.
9. Click no ícone “save” na área de controle.

7.2.2 Editando uma configuração PBX Node

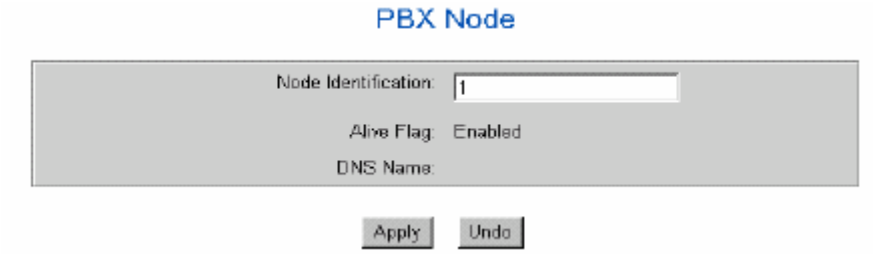
Para editar o número de nó da configuração do PBX node:
Procedimento:
1. Abrir o WBM.
2. Click no ícone do cadeado para ativar o write access (se ainda não fez).
3. Click em “Explorer”.
4. Click em “Voice Gateway” à esquerda da janela no menu.
5. Duplo-click em “PBX” no menu.
6. Click com o botão direito em “Nodes” na estrutura de árvore e selecione. “Edit PBX Node” do menu pop-up.

O seguinte diálogo é mostrado no conteúdo da área:



7. No menu pop-up , selecione ”PBX node” para editar.
8. Click “OK”.

O seguinte diálogo é mostrado no conteúdo da área:

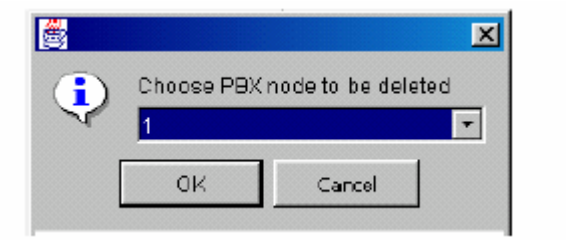


9. Entrar em identificação de “new node”. O emblema e o nome DNS name são mostrardos para sua informação.
10. Click em “Apply”. A configuração é modificada.
11. Click no ícone “save” na área de controle.

7.2.3 Deletando uma configuração PBX Node

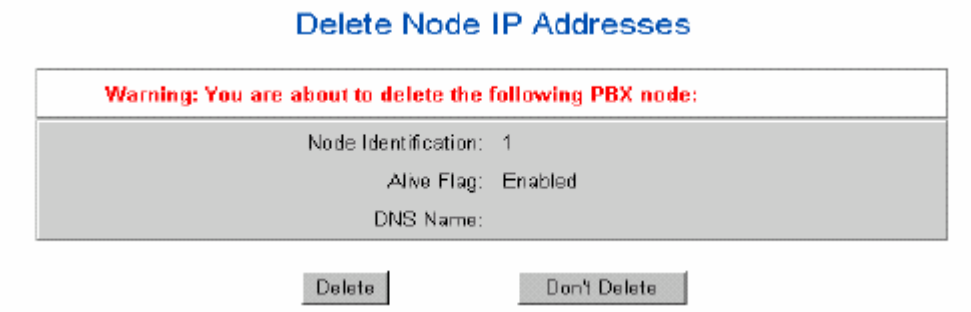
Para deletar uma configuração PBX node:
Procediemnto:
1. Abrir o WBM.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Explore”.
4. Click em “Voice Gateway” no menu à esquerda da janela.
5. Duplo-click em “PBX” no menu.
6. Click com o botão direito em “Nodes” na estrutura de árvore e selecione“Delete PBX Node” do menu pop-up.

O seguinte diálogo é mostrado no conteúdo da área:



7. No menu pop-up, selecione “PBX node” para ser deletado.
8. Click “OK”.

O seguinte aviso aparece:



9. Click em “Delete”. O nó PBX especificado é deletado.
10. Click no ícone “save” na área de controle.

7.3 Exercício 5

1. Configure a LAN 2, para fazer roteamento de pacotes para a HG 1500 V.2 0 do HiPath 3700, de modo que esta faça o acesso ao ADSL do treinamento e ative Internet em todas as maquinas de sala.
2. Salve as configurações do HG 1500 V.2.0 e converta para uma HG V.3. (Manual de Instalação Cap-4).

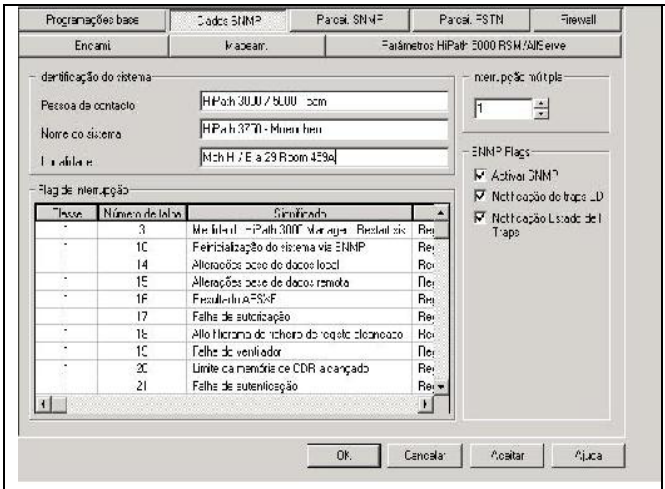
Anotações:

8 Simple Network Management Protocol

8.1 SNMP configuração para HiPath 3000 SMG

8.1.1 Dados SNMP

O SNMP é ativado com esta opção. Note que o SNMP para o HiPath 5000 RSM network deve ser ativado!

	Entrar em Programações -> Rede ->em seguida Dados SNMP.

8.1.2 Identificação do Sistema

Pessoa de contacto

Esse campo deve conter o nome da pessoa que é tecnicamente responsável para o HiPath 3000.

Nome do Sistema

Uma network-wide sem ambigüidade de nome para o HiPath 3000 deve ser dado aqui.

Localidade

Descrição da localização exata do HiPath 3000 com processo e ocasião do número.

8.1.3 SNMP Flags

Activar SNMP

Essa opção habilita o acesso ao sistema via MIB browser.

Notificação de traps CD

Sobre alcançar os valores setados dos detalhes de chamada do buffer de memória para a central deve gravar via TFTP Server, uma mensagem de informação é enviada.

Notificação Estado de Porta Traps

Se o estado mudar à porta do módulo no sistema é revelado uma mensagem de informação correspondente é enviada.

8.1.4 Flag de interrupção

A mensagem de infomação (traps) para o sistema são idênticos para as mensagens de erro que são salvas no histórico de erro, uma descrição de mensagens podem ser encontrados em eSHB na seção de serviço.

Classe

Classe do (class-B) erro.

Número de falha

Número do (classe-B) erro. A mensagem de erro e descrição pode ser encontrado no eSHB.

Significado

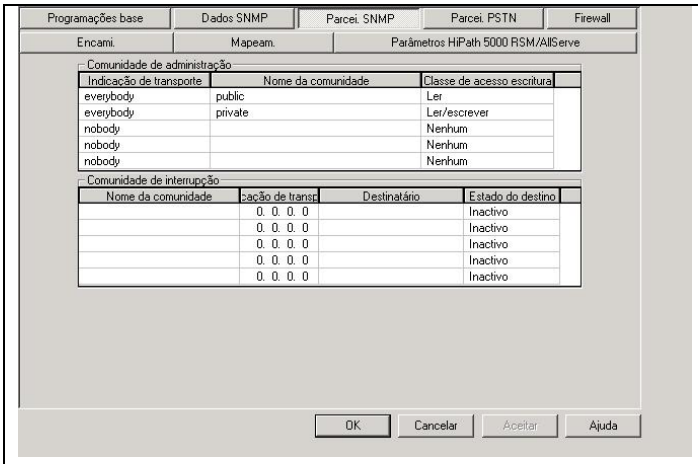
Descrição do evento de erro no texto livre.

Valor

Para cada tipo de erro que pode ser avisado pelo significado do SNMP mensagem de erro (trap), isso pode ser determinado aqui se apenas uma entrada é feita em histórico de erro, ou se um trap é também adicionado inicialmente.

- log — apenas entra em histórico de erro
- log + trap — entra em histórico e envia mensagem SNMP adicional (trap)
- log + multiple trap — entra em histórico e envia um adicional ou mais mesnsagem SNMP (traps). O número de trapas (1-5) é definido pelo valor no campo “Múltiplo Trap”

8.2 Parceiro SNMP



Entrar em Programações -> Rede -> em seguida Parcei. SNMP

Comunidade de administração

Indicação de transporte

Administração de dados nessa coluna é feito com duplo-click com o botão esquerdo do mouse. Aqui, cada endereço IP especifico, isto é 192.168.100.X um wildcard como todos = tudo (indiferentemente do endereço IP) ou ninguém = nada (sem acesso) é dado.

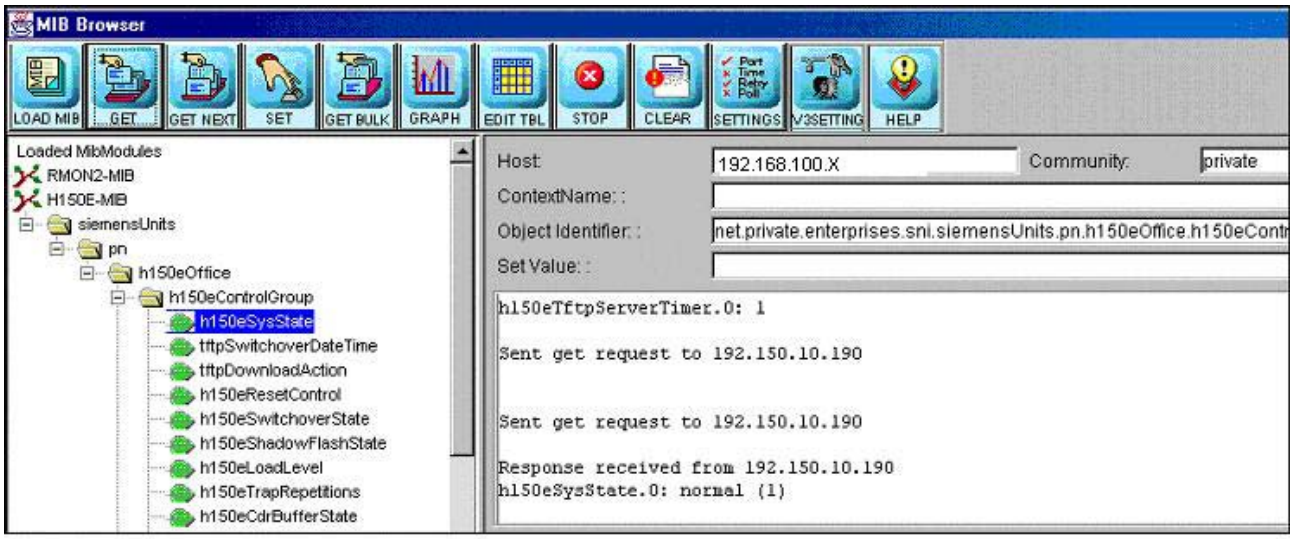
Nome da comunidade

O nome da comunidade Server na versão 1 do protocolo SNMP como uma senha de acesso. O aplicativo SNMP, isto é MIB browser apenas recebe acesso via a comunidade específico nome da comunidade.

8.2.1.1 SNMP access

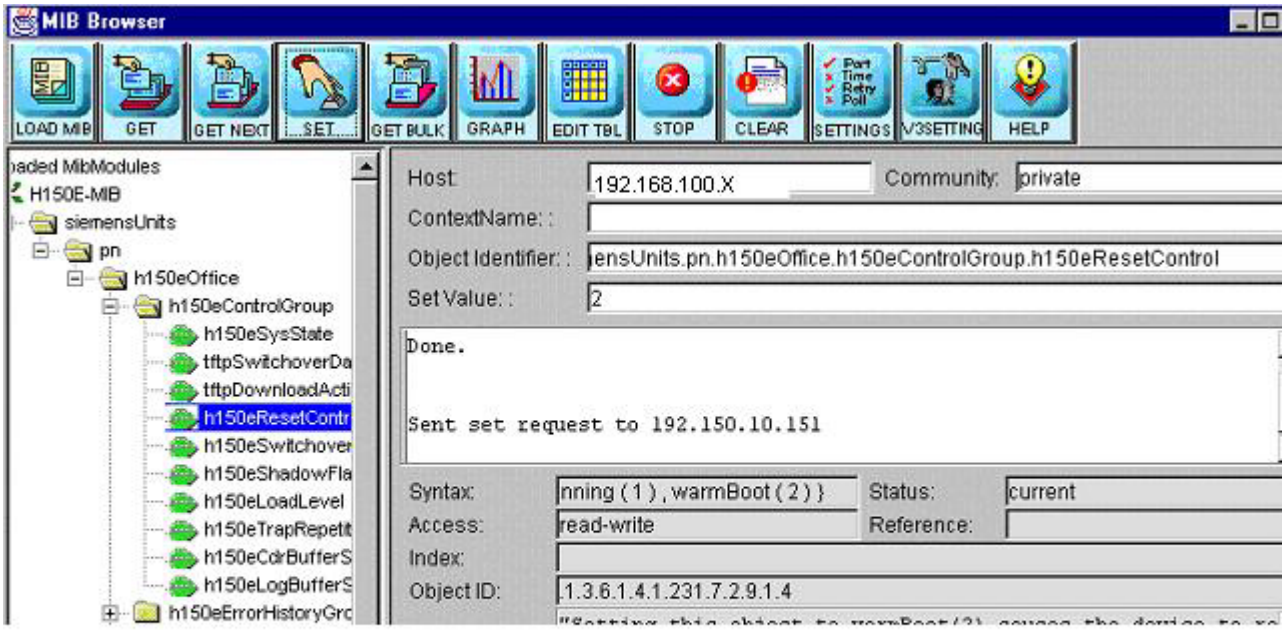
- Read

O endereço IP associado apenas possui autorização para o reading access. Via o MIB browser apenas o comando GET pode ser executado.



- Read / write

O endereço IP asociado é denominado para leitura e write access. Os comandos GET e SET podem ser executados via o MIB browser.



- None

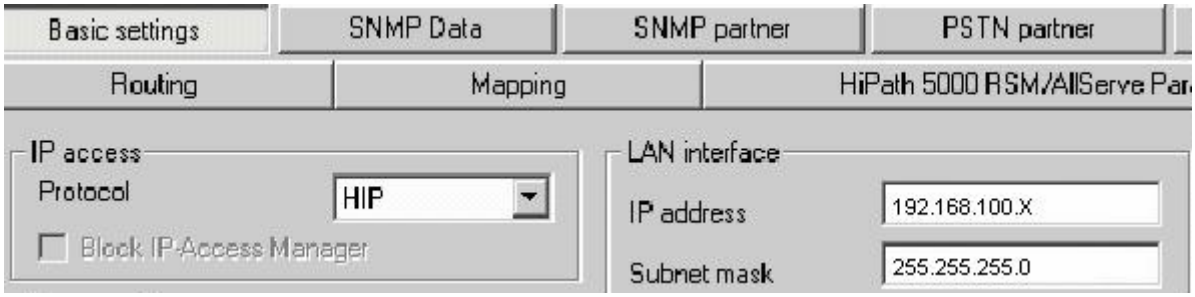
O endereço IP associado não possui access rights. Esta opção habilita entrada para ser temporariamente desativado sem ter apagado ele completamente (SNMP transport label, community name).

8.3 Atualização - HiPath 3000 via SNMP

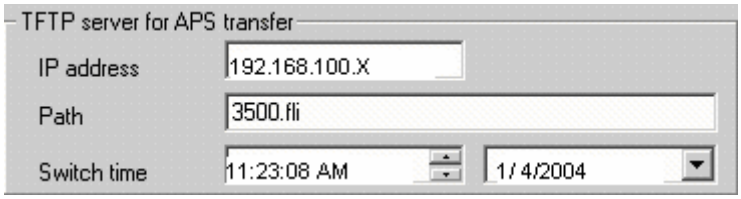
É possível atualizar um sistema HiPath 3000 via SNMP Manager isto é HP Openview ou MIB Browsers.

8.3.1 Configuração do HiPath 3000

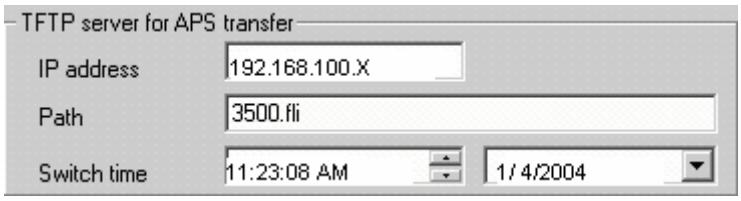
Composição básica dos parâmetros de rede



O nome do arquivo do sistema APS pode ser renomeado isto é 3700.fli para o HiPath 3700 ou para 3500.fli para o HiPath 3300/3500. No campo parâmetro "Path" deve ser inserido o arquivo de nome do sistema HiPath 3000, pois o caminho do arquivo é configurado em TFTP Server option/preseting. O mesmo arquivo APS pode ser usado para o HiPath 3300 e HiPath 3500, pois o Contol Board é o mesmo.

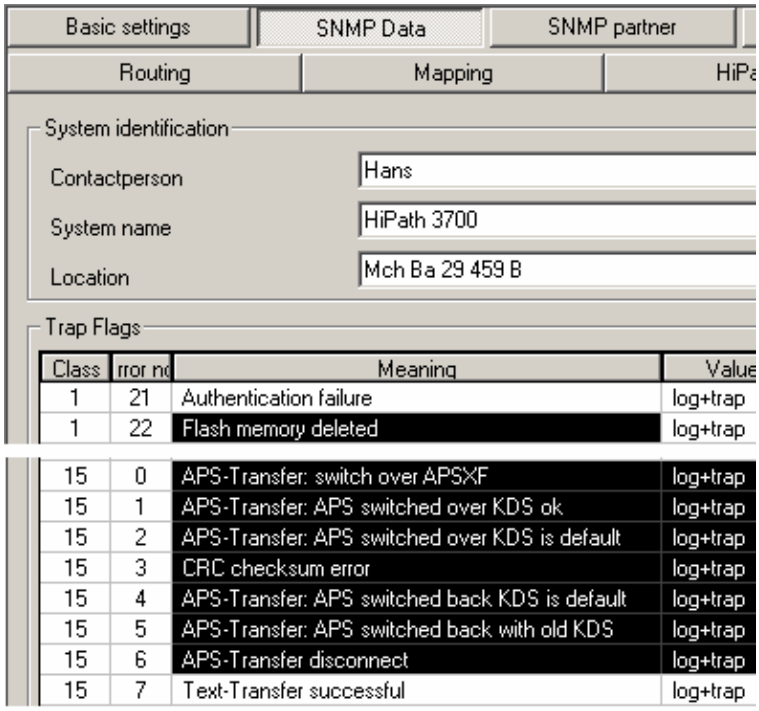


HiPath 3500

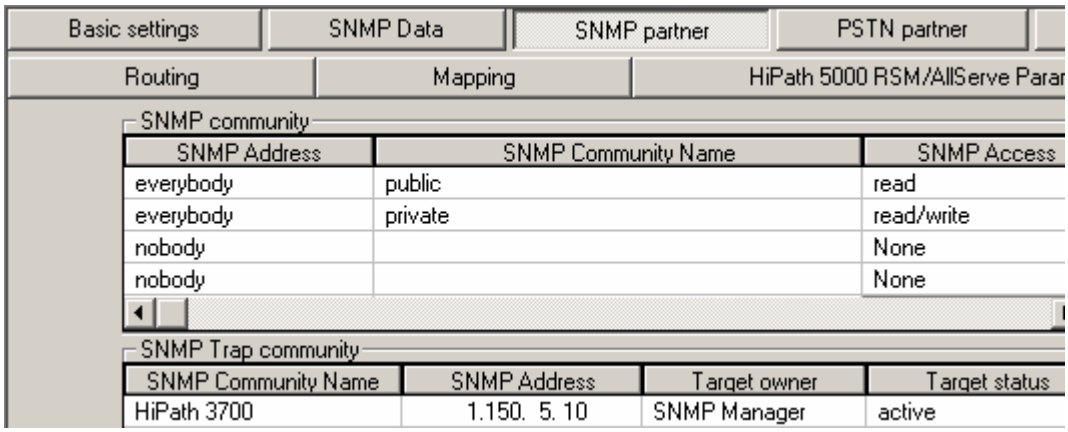


HiPath 3300

8.3.2 Configuração SNMP-Data – Trap messages para atualização

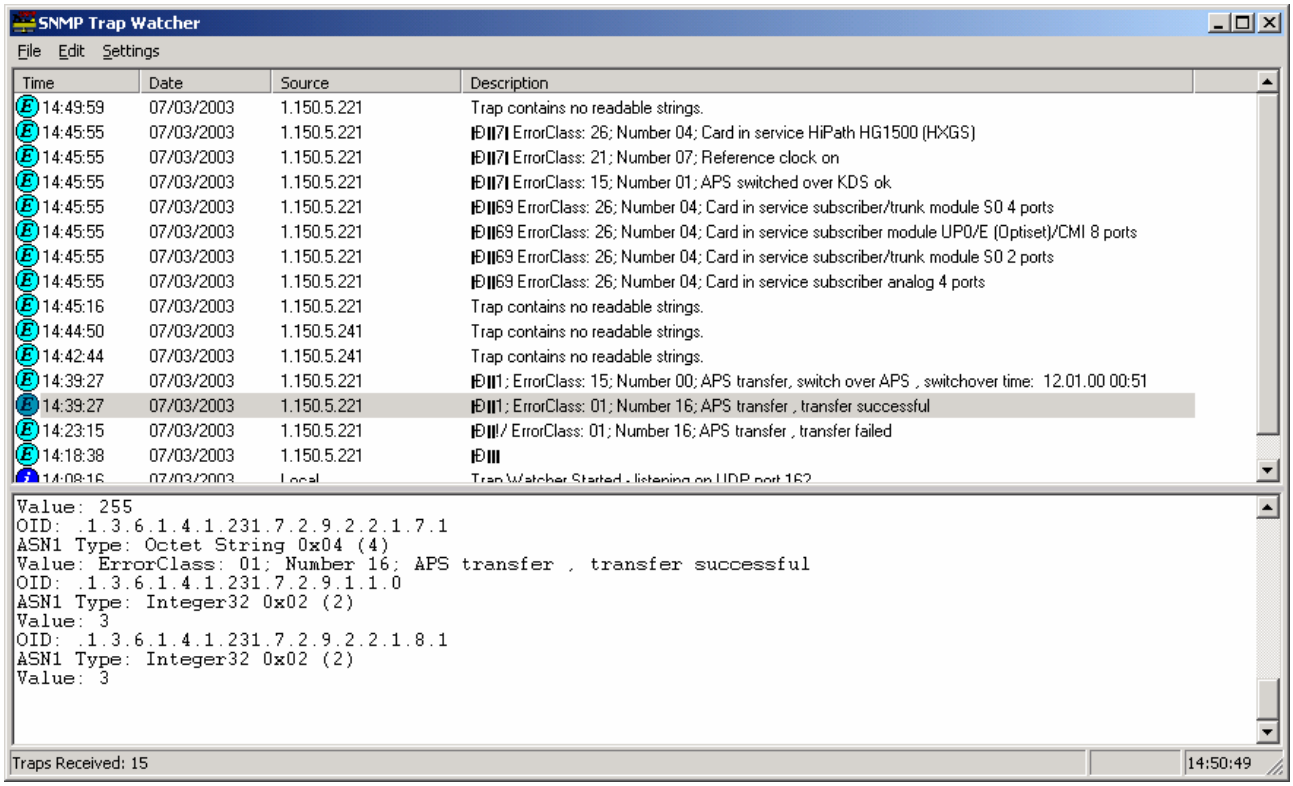


8.3.3 Configuração SNMP – partner – Trap-destination



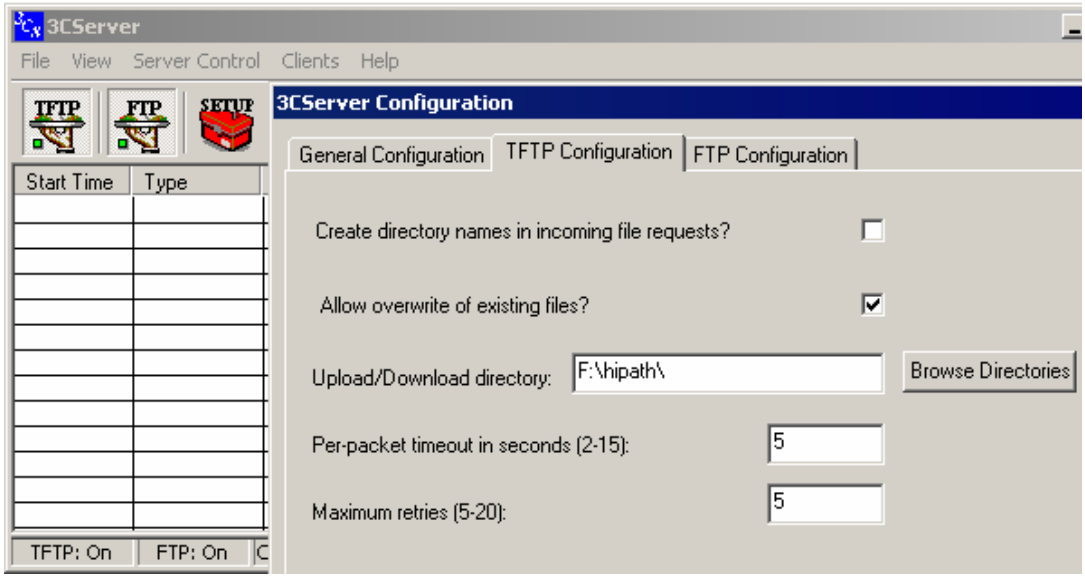
8.3.4 Trap Watcher – verificação de atualização via SNMP

Possível Trap mensagem para o sistema de atualização.

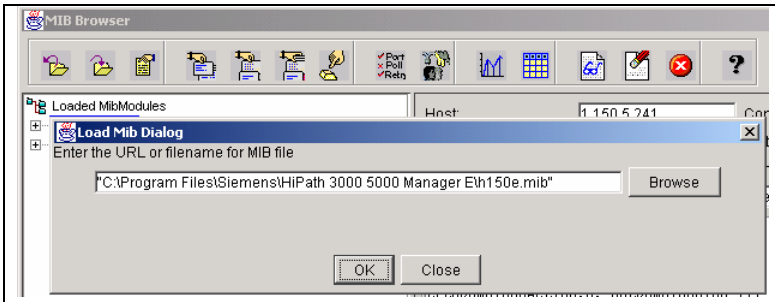


8.4 Configuração TFTP Server

Configuração do diretório de download.



Carregando o arquivo particular MIB para o HiPath 3000

	Procedimento: entrar em File -> open Selecione o diretório do HiPath 3000/5000 Manager E e abra o arquivo de nome “h150e.mib”para o sistema HiPath 3000.

Atualização via SNMP

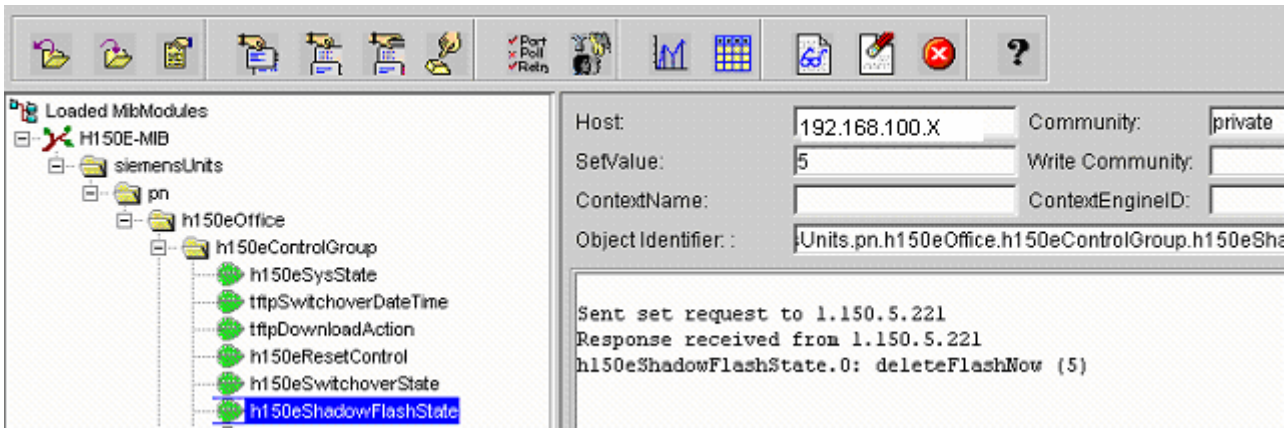
Delete o passive APS-Memory em MMC

Você pode deletar via comando SNMP

Procedimento:
h150eShadowFlashState e deleteFlashNow,
o percurso passivo para o APS com isto é armazenado em MMC, o percurso ativo não pode ser deletado. Se o Flash é deletado o sistema criará uma mensagem TRAP. Isto pode levar até 7 minutos para deletar a memória Flash.

Mensagem de status:

FlashDeleted	(1)
flashNotDeleted	(2) – Não é possivel deletar o flash
flashWriteProtected	(3)
flashTooSmall	(4)
deleteFlashNow	(5)



Ativando o APS download para MMC

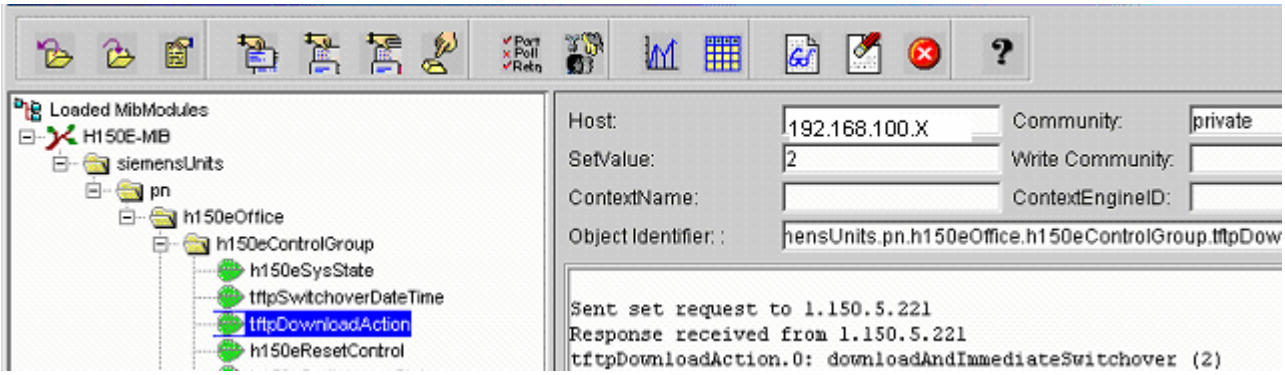
Quando o flash é deletado, a transferência APS pode ser inicializada via comando SNMP:

- tftpDownloadAction e downloadAndImmediateSwitchover,

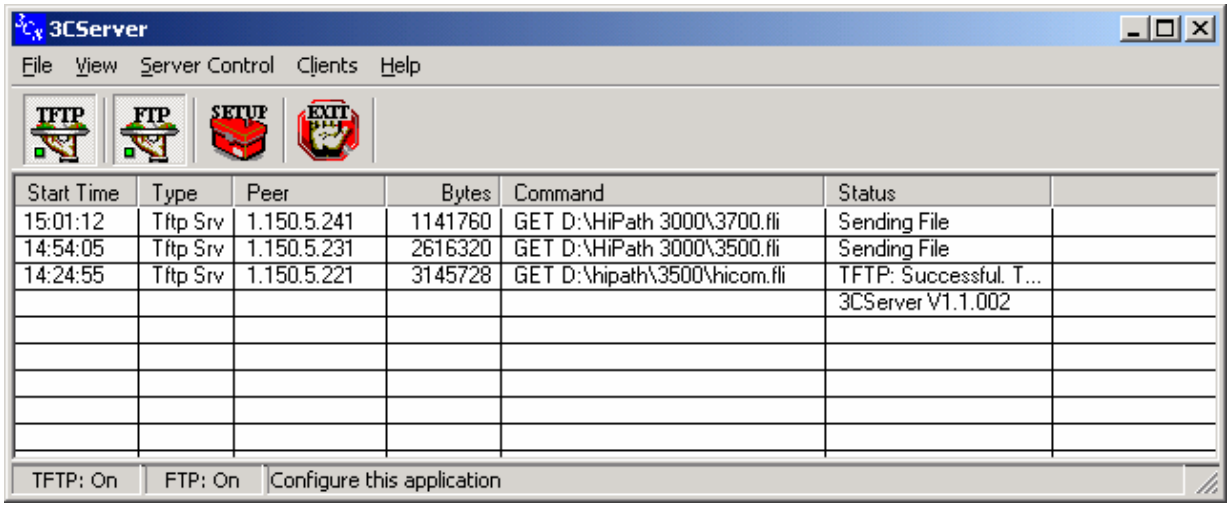
Quando o download é finalizado, desviará imediatamente para o novo APS. O download é finalizado, você consegue uma mensagem TRAP, também se a transferência APS é errada uma mensagem TRAP é criada.

Possíveis opções de commando SNMP

notDownloading	(1)
downloadAndImmediateSwitchover	(2)
downloadAndDelayedSwitchover	(3)
downloadWithoutSwitchover	(4)


Loaded MibModules
H150E-MIB
siemensUnits
pn
h150eOffice
h150eControlGroup
h150eSysState
tftpSwitchoverDateTime
tftpDownloadAction
h150eResetControl
Host:
192.168.100.X
Community:
private
SetValue:
2
Write Community:
ContextName:
ContextEngineID:
Object Identifier: :
hensUnits.pn.h150eOffice.h150eControlGroup.tftpDow
Sent set request to 1.150.5.221
Response received from 1.150.5.221
tftpDownloadAction.0: downloadAndImmediateSwitchover (2)

TFTP Server


3CServer
File View Server Control Clients Help
TFTP
FTP
SETUP
EXIT
Start Time | Type | Peer | Bytes | Command | Status
15:01:12 | Tftp Srv | 1.150.5.241 | 1141760 | GET D:\HiPath 3000\3700.fli | Sending File
14:54:05 | Tftp Srv | 1.150.5.231 | 2616320 | GET D:\HiPath 3000\3500.fli | Sending File
14:24:55 | Tftp Srv | 1.150.5.221 | 3145728 | GET D:\hipath\3500\hicom.fli | TFTP: Successful. T...
3CServer V1.1.002
TFTP: On
FTP: On
Configure this application

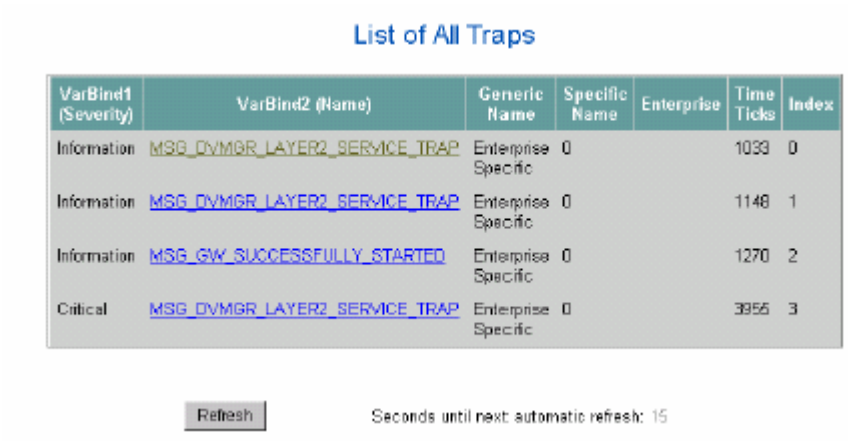
9 Geração de TRAPS via SNMP

9.1 Lista de todos TRAPS

Você pode mostrar uma lista de todos os Traps.
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Click com o botão direito em “Traps” e selecione “Display All Traps” do menu pop-up.

Os seguintes diálogos aparecem:



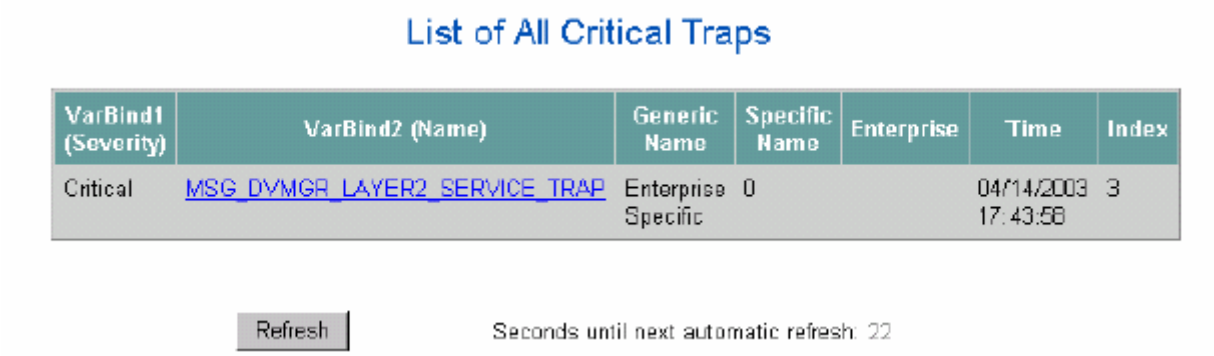
O display é automaticamente atualizado a cada 30 segundos.
O tempo até a próxima atualização é mostrado.
Click em “Refresh” se você deseja atualizar a “window sooner”.

9.2 Lista de todos - Critical TRAPS

Você pode mostrar a lista de todos critical traps.
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Click com o botão direito em “Traps” e selecione “Display All Critical Traps”. Do menu pop-up.

Os seguintes diálogos aparecem:



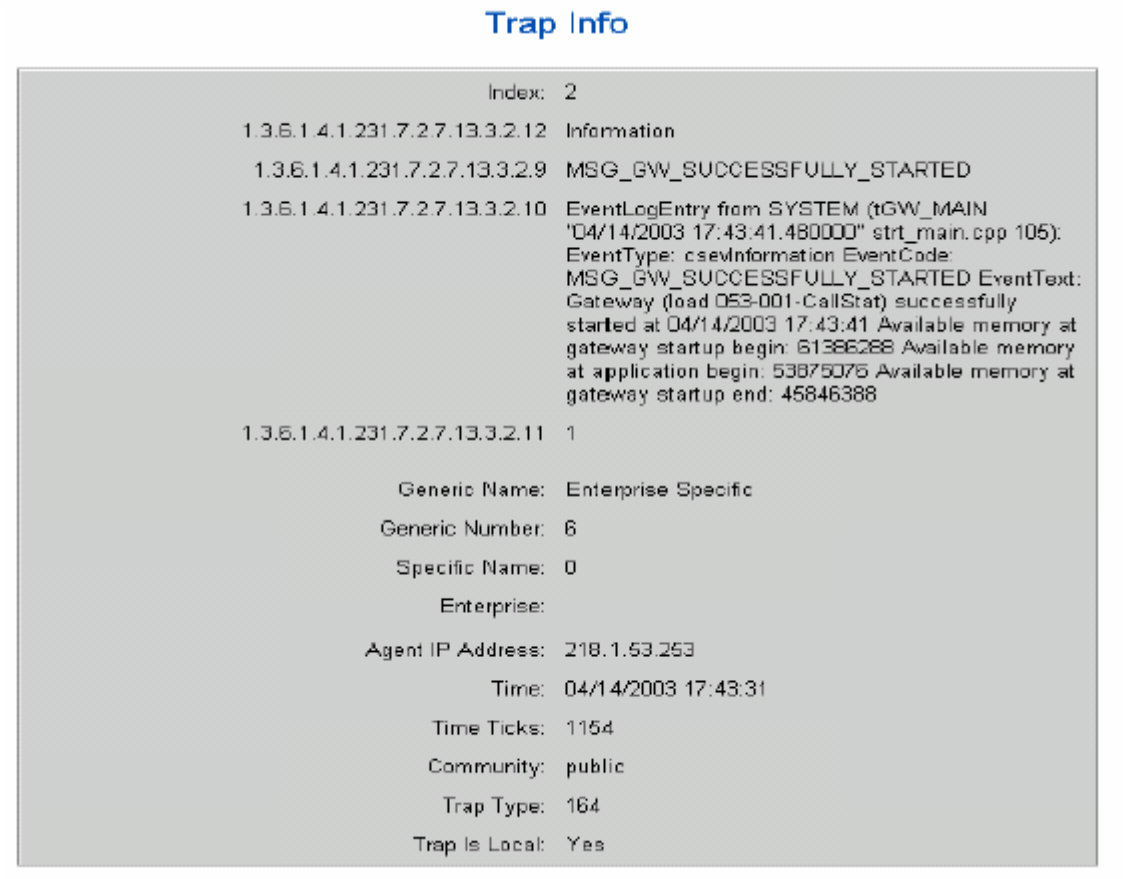
O display é automaticamente atualizado a cada 30 segundos.
O tempo até a próxima atualização é mostrado.
Click em “Refresh” se você deseja atualizar o window sooner.

9.3 TRAPS Individual

Você pode mostrar informações em individual Traps.
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Duplo-click em “Traps”.
5. Click com o botão direito em “Trap” e selecione “Display Trap” do menu pop-up.

As seguintes listas aparecem:



As primeiras quatro entradas têm os seguintes significados:
. Trap severity (por exemplo, Informação)
. Trap name
. Explanation of this trap
. Trap type (1 = software, 2 = hardware)

9.4 Lista de todos SNMP Communities

Você pode mostrar uma lista de todos os SNMP Communities.
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Click com botão direito em “Communities” e selecione “Display Communities” do menu pop-up.

As seguintes tabelas aparecem:

List of Communities

IP Address	Community	Type
0.0.0.0	public	ReadCommunity
127.0.0.1	wbm	WriteCommunity
127.0.0.1	public	TrapCommunity

Cada assinante SNMP é mostrado na tabela com o endereço IP.
O acesso SNMP rights (community) e classe SNMP também são mostrados.

9.5 SMTP Read Communities

Para mostrar uma lista de todos SNMP Read Communities:
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP”. À esquerda do menu “Maintenance”.
4. Duplo-click em “Communities”.
5. Click com o botão direito em “Read Communities” e selecione “Display Read Communities” do menu pop-up.

As seguintes tabelas aparecem:

List of Read Communities

IP Address	Community
0.0.0.0	public

Cada SNMP Read Community é mostrado na tabela com o endereço IP.

Para mostrar informação de um SNMP read community:
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Duplo-click em “Communities”.
5. Duplo-click em “Read Communities”.
6. Click com o botão direito em assinante SNMP e selecione “Display Community” do menu pop-up.

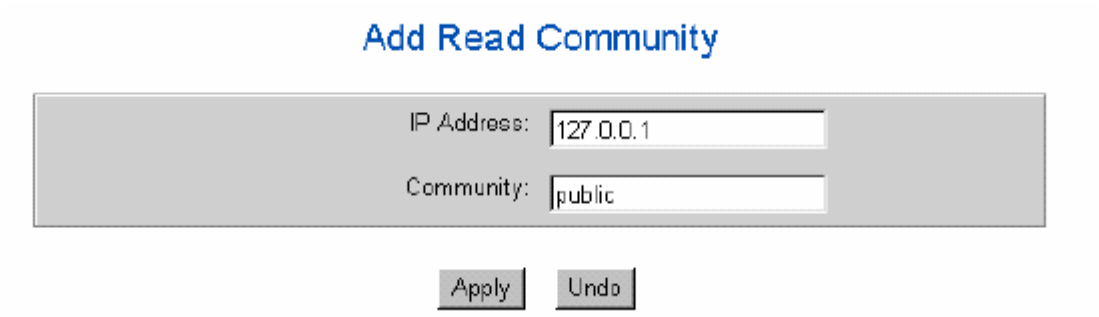
O seguinte diálogo aparece:

O endereço IP e acesso SNMP rights (community) são mostrados para selecionar SNMP community.

Para criar um SNMP read community:
Procedimento:

1. Abrir o WBM.
2. Click no ícone do cadeado para ativar o write access (se ainda não fez).
3. Click no módulo “Maintenance”.
4. Click em “SNMP” à esquerda do menu “Maintenance”.
5. Duplo-click em “Communities”.
6. Click com o botão direito em “Read Communities” e selecione “Add Read Community” do menu pop-up.

O seguinte diálogo aparece:

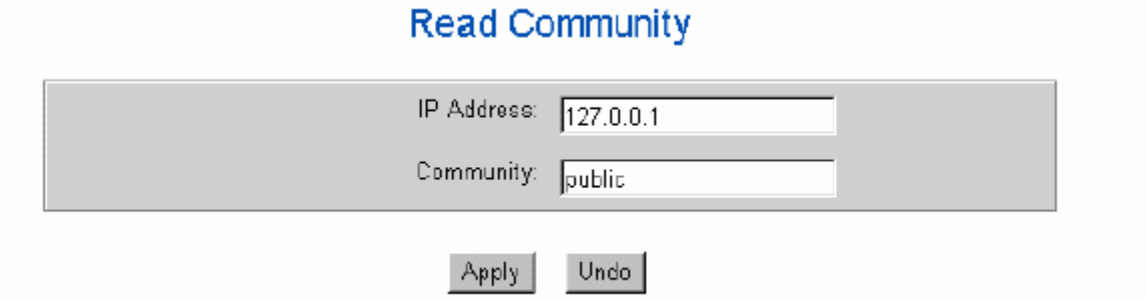


Entrar com o a informação de no campo input:
. **IP Address:** Entrar com o endereço IP do new trap recipiente deste campo.
. **Community:** Esse campo define o acesso direto SNMP. Entrar em community com uma fileira de caracteres.
7. Click em “Apply”. O read community é set up e o título de diálogo é mudado em “add” para “edit”
8. Click no ícone “save” na área de controle.

Para editar um SNMP read community:
Procedimento:

1. Abrir o WBM.
2. Click no ícone do cadeado ara ativar o write access (se ainda não fez).
3. Click em “Maintenance”.
4. Click em “SNMP” à esquerda do menu “Maintenance”.
5. Duplo-click em “Communities”.
6. Duplo-click em “Read Communities”.
7. Click com o botão direito o required community e selecione ”Edit Community” do menu pop-up.

O seguinte diálogo aparece:



Entrar com o recipiente de informação no campo input:
. **IP Address:** Entrar com o endereço IP do recipiente new trap recipient neste campo.
. **Community:** Este campo define o acesso direto SNMP. Entrar com o grupo com uma fileira de caracteres.
8. Click em “Apply”. O read community é modificado.
9. Click no ícone save na area de controle.

Para deletar um SNMP read community:
Procedimento:

1. Abrir o WBM.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Maintenance”.
4. Click em “SNMP” à esquerda do menu “Maintenance”.
5. Duplo-click em “Communities”.
6. Duplo-click em “Read Communities”.
7. Click com o botão direito para solicitar community e selecionar “Delete Community” do menu pop-up.

O seguinte diálogo aparece:

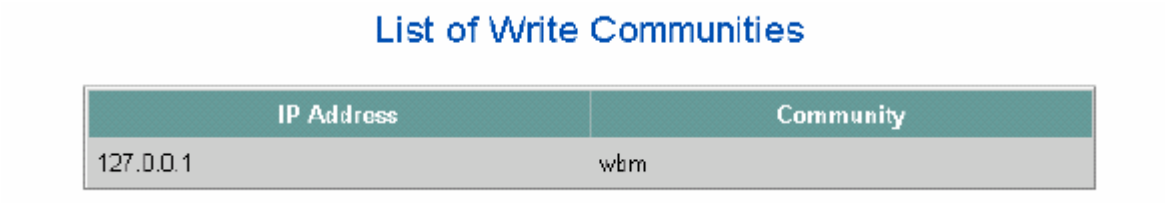
8. Click em “Delete”. O read community é deletado.
9. Click no ícone “save” na área de controle.

9.6 SNMP Write Communities

Para mostrar uma lista de todos SNMP write communities:
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Duplo-click em ”Communities”.
5. Click com o botão direito em “Write Communities” e selecione “Display Write Communities” do menu pop-up

A seguinte tabela aparece:

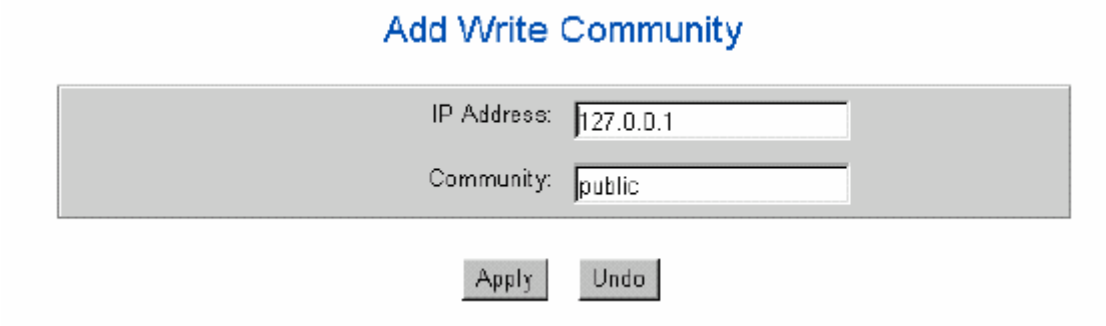


Cada SNMP write community é mostrado na tabela com endereço IP.

Para criar SNMP write community:
Procedimento:

1. Abrir o WBM.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Maintenance”.
4. Click em “SNMP” à esquerda do menu “Maintenance”.
5. Duplo-click em “Communities”
6. Click com o botão direito em “Write Communities” e selecione “Add Write Community” do menu pop-up.

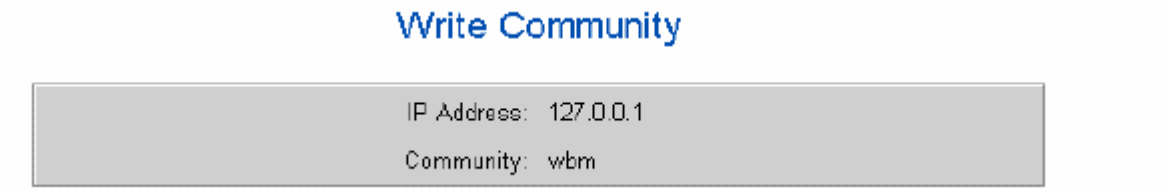
O seguinte diálogo aparece:



Entrar com o recipiente de informação no campo input:
. **IP Address:** Entrar com o endereço IP do recipiente new trap neste campo.
. **Community:** este campo defineo acesso direto SNMP. Entrar em community com uma fileira de caracteres.
7. Click em “Apply”. O community é set up e o título de dialogo é mudado em “add” para ”edit”.
8. Click no ícone “save” na área de controle.

Para mostra a informação em SNMP write community:
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Duplo-click em “Communities”.
5. Duplo-click em “Write Communities”.
6. Click com o botão direito no assinante SNMP e selecione “Display Community” do menu pop-up.
O seguinte diálogo aparece:

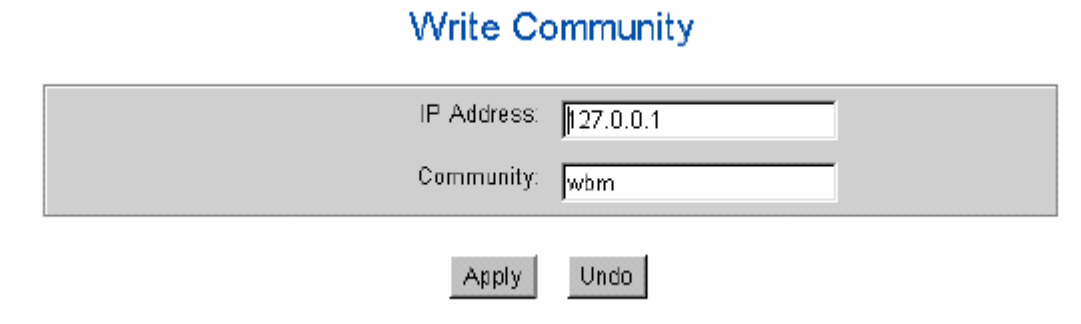


O endereço IP e acesso direto SNMP (community) são mostrados para selecionar SNMP community.

Para editar um SNMP write community:
Procedimento:

1. Abrir o WBM.
2. Click no ícone do cadeado para ativar o write access (se ainda não fez).
3. Click em “Maintenance”.
4. Click em SNMP à esquerda do menu “Maintenance”.
5. Duplo-click em “Communities”.
6. Duplo-click em “Write Communities”.
7. Click com o botão direito em “community” e selecione ”Edit Community” do menu pop-up.

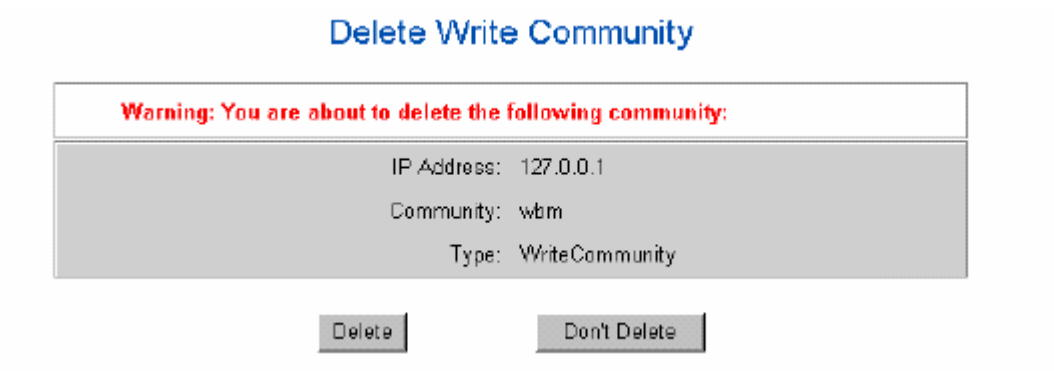
O seguinte diálogo aparece:



Entrar o recipiente de informação no campo input:
. **IP Address:** Entrar com o endereço IP do recipiente new trap neste campo.
. **Community:** Este campo define o acesso direto SNMP. Entrar em “community” com uma fileira de caracteres.
8. Click em “Apply”. O write community é modificado.
9. Click no ícone “save” na área de controle.

Para deletar um SNMP write community:
Procedimento:

1. Abrir o WBM window.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Maintenance”.
4. Click em “SNMP” à esqueda do menu ”Maintenance”.
5. Duplo-click em “Communities”.
6. Duplo-click em “Write Communities”.
7. Click com o botão direito em community e selecione “Delete Community” do menu pop-up.
O seguinte diálogo aparece:



8. Click em “Delete”. O write community é deletado.
9. Click no ícone “save” na área de controle

9.7 TRAP Communities

Para mostrar uma lista de todos os trap communities:
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Duplo-click em “Communities”.
5. Click com o botão direito em “Trap Communities” e selecione “Display Trap Communities” do menu pop-up.

A seguinte tabela aparece:

O endereço IP e o acesso direto SNMP (community) são mostrados para todos trap recipients.

Para adicionar um novo trap community:
Procedimento:

1. Abrir o WBM.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Maintenance”.
4. Click em “SNMP” à esquerda do menu “Maintenance”.
5. Duplo-click em “Communities”.
6. Click com o botão direito em “Trap Communities” e selecione ”Add Trap Community” do menu pop-up.

O seguinte diálogo aparece:

Entrar o recipiente de informação no campo input:
. **IP Address:** Entrar com o endereço IP do new trap recipient neste campo.
. **Community:** Esse campo define o acesso direto SNMP. Entrar em community com uma fileira de caracteres.
7. Click em “Apply”. O new trap community é set up e o título dialog muda de “add” para “edit”.
8. Click no ícone “save” na área de controle.

Para mostrar a informação on a selected trap community:
Procedimento:

1. Abrir o WBM.
2. Click em “Maintenance”.
3. Click em “SNMP” à esquerda do menu “Maintenance”.
4. Duplo-click em “Communities”.
5. Duplo-click em “Trap Communities”.
6. Click com o botão direito a solicitar o recipiente e selecione “Display Trap Community” do menu pop-up.

O seguinte diálogo aparece:

O endereço IP e o acesso direto SNMP (community) são motrados para esse trap recipient.

Para editar os atributos do selected trap community:
Procedimento:

1. Abrir o WBM.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Maintenance”.
4. Click em “SNMP” à esquerda do menu “Maintenance”.
5. Duplo-click em “Communities”.
6. Duplo-click em “Trap Communities”.
7. Click com o botão direito a solicitar o trap recipient e selecione “Edit Trap Community” do menu pop-up.

O seguinte diálogo aparece:

Entrar a informação recipiente no campo input:
. **IP Address:** Entrar o endereço IP do recipiente new trap recipient neste campo.
. **Community:** Este campo define o acesso direto SNMP. Entrar em community com uma fileira de caracteres.
8. Click em “Apply”. O trap community é modificado.

Para deletar um trap community:
Procedimento:

1. Abrir o WBM.
2. Click no ícone cadeado para ativar o write access (se ainda não fez).
3. Click em “Maintenance”.
4. Click em “SNMP” à esquerda do menu “Maintenance”.
5. Duplo-click em “Communities”.
6. Duplo-click em “Trap Communities”.
7. Click com o botão direito a solicitar o trap recipient e selecione “Delete Trap Community” do menu pop-up.

O seguinte aviso aparece:

8. Click em “Delete”. O “trap community” é deletado.
9. Click no ícone “save” na área de controle.

9.8 Exercício 6

1. Salve a configuração do HG 1500 V.3.
2. Ative um reset e interrompa o boot, entrar no CLI.
3. Formate os arquivos Flash (Nível Baixo) e instale uma nova imagem via FTP, conforme o manual de Manutenção.
4. Atualize a configuração do HG V.3.0 e teste as funções da placa.

Anotações:

10 Anexo

10.1 Pinos

DB-9	DB-25		DB-25	DB-9	Signale
3	2	<--->	3	2	Xmit-Recv data
2	3	<--->	2	3	Recv-Xmit data
7	4	<--->	5	8	RTS-CTS
8	5	<--->	4	7	CTS-RTS
1&6	6	<--->	20	4	DSR-DTR
5	7	<--->	7	5	Gnd-Gnd
4	20	<--->	6	1&6	DTR-DSR

Deve ser um conector DB9 fêmea nos dois lados