intelbras

Manual da Interface de Linha de Comandos (CLI)

SG 2404 PoE L2+

intelbras

SG 2404 PoE L2+

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

O SG 2404 PoE L2+ é um switch de 24 portas PoE Gigabit Ethernet com 4 portas Mini-GBIC independentes. Atende aos padrões IEEE802.3af e IEEE802.3at, podendo fornecer potência máxima de até 192 W, distribuídos conforme o padrão utilizado e a quantidade de portas disponíveis. Com a tecnologia PoE é possível transmitir energia elétrica e dados através do mesmo cabo de rede (cat5 ou superior) para dispositivos compatíveis com os padrões 802.3af ou 802.3at, eliminando a necessidade de tomadas para os produtos alimentados, minimizando os custos de instalação.

Este manual destina-se a administradores de rede fornecendo informações referenciadas sobre a Interface de Linha de Comandos (CLI - Command Line Interface).

ATENÇÃO: esse produto vem com uma senha-padrão de fábrica. Para sua segurança, é IMPRESCINDÍVEL que você a troque assim que instalar o produto e questione o seu técnico quanto as senhas configuradas, quais os usuários que possuem acesso e os métodos de recuperação.

Índice

1. Usando o CLI

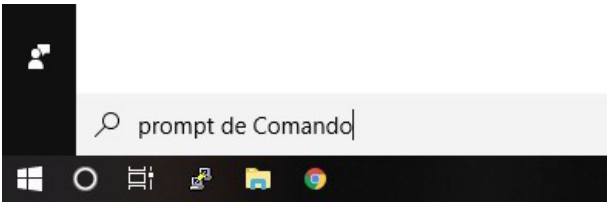
1.1. Acessando o CLI

Acessar o switch remotamente através de uma porta Ethernet utilizando uma conexão Telnet ou SSH.

1.1.1. Login via Telnet

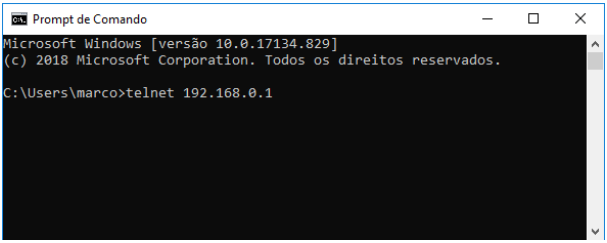
Para efetuar o login no switch via Telnet, favor acompanhar os seguintes passos:

1. Clique em **Iniciar**, digite **Prompt de Comando** ou **cmd** e pressione a tecla **Enter**;



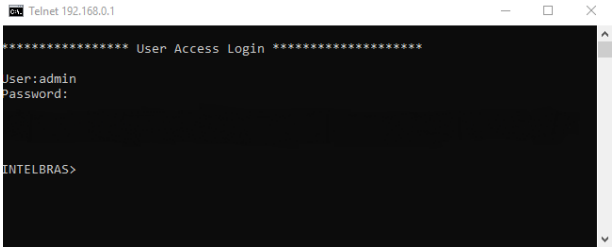
Janela Iniciar

2. Digite *telnet 192.168.0.1* no Prompt de Comandos e pressione **Enter**;



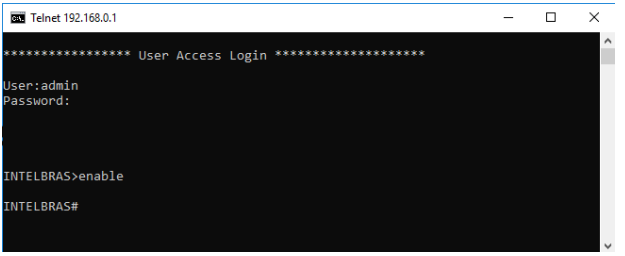
Prompt de comando

3. Para efetuar o login, digite o usuário e pressione **Enter**, depois digite a senha e pressione **Enter**;



Login no switch

4. Digite o comando *enable* para entrar no modo *Privileged EXEC* de administrador, por padrão não é exigida senha após o comando, porém, poderá ser configurada posteriormente.



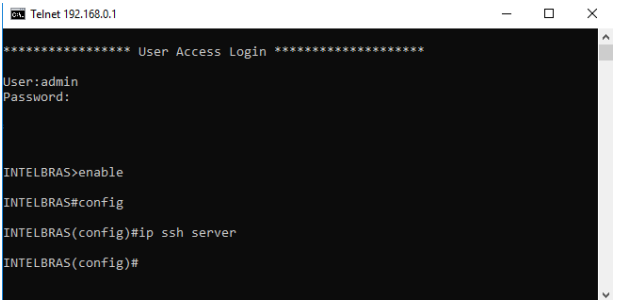
Modo administrador de execução

1.1.2. Login via SSH

Para o acesso via SSH, é recomendado o uso do software *Putty client*. Existem dois modos de autenticação para uma conexão SSH:

- **Modo de autenticação por senha:** requer um nome de usuário e senha, por padrão, ambos são *admin*.
- **Modo de autenticação por chave:** requer uma chave pública para o switch e uma chave privada para o software cliente SSH. Tanto a chave pública quanto a privada, podem ser geradas através do software *Putty Key Generator.*

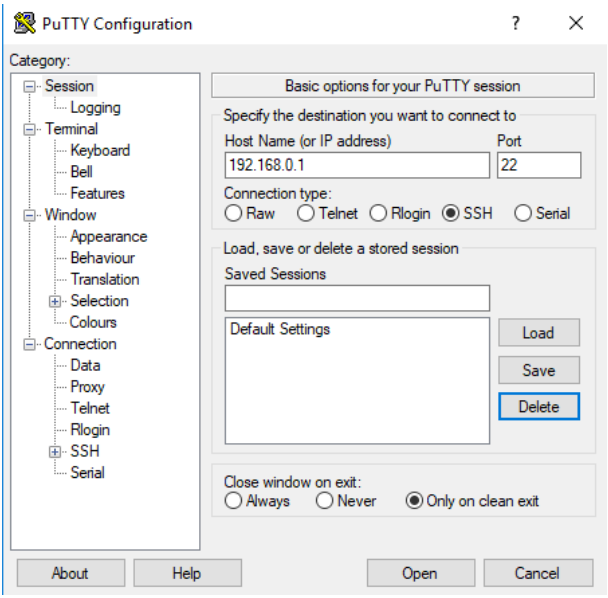
Obs.: *antes de efetuar o login via SSH, favor seguir as etapas demonstradas na Ativar a função SSH, para ativar a função* SSH *através de uma conexão via Telnet.*



Ativar a função SSH

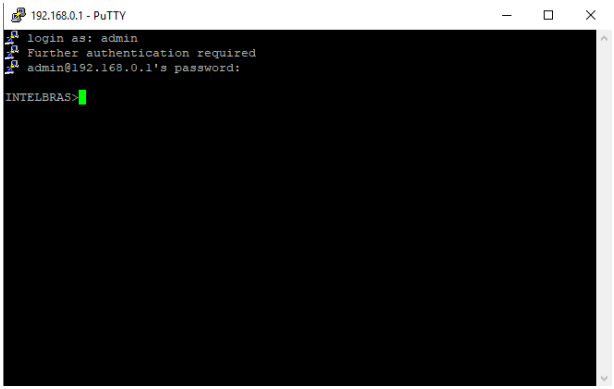
» **Modo de autenticação por senha**

1. Abra o software para efetuar login através da interface PuTTY. No campo **Host Name**, entre com o endereço IP do switch; no campo **Port**, adicione o número *22*; selecione *SSH* em **Connection type**;



Configurando uma conexão SSH

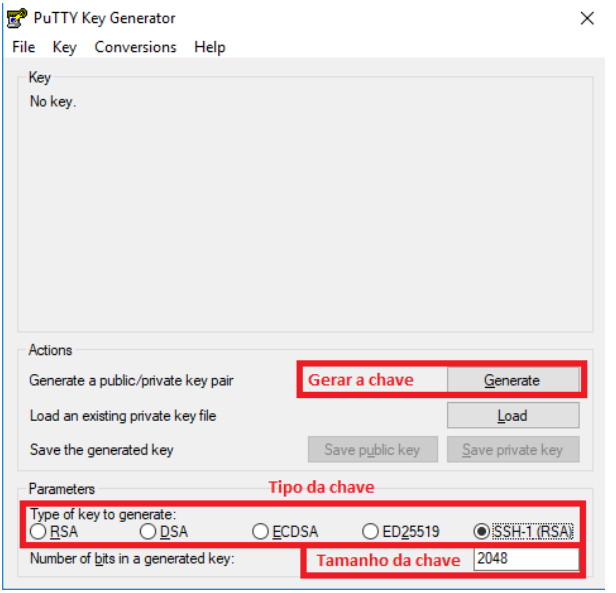
2. Clique no botão **Open** para iniciar a conexão. Entre com o usuário e senha para login no switch, em seguida, para que o switch possa ser configurado, digite o comando *enable* para entrar no *Privileged EXEC Mode* de administrador.



Login via PuTTY

» **Modo de autenticação por chave**

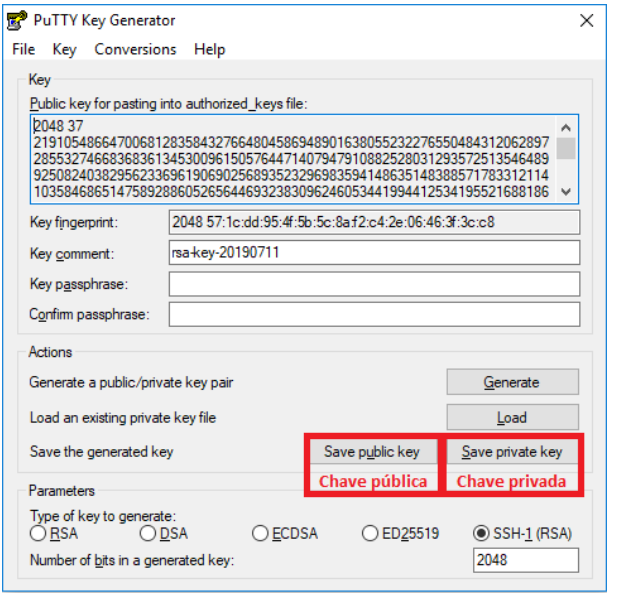
1. Selecione o tipo e o tamanho da chave, depois clique em **Generate**;



Gerando uma chave SSH

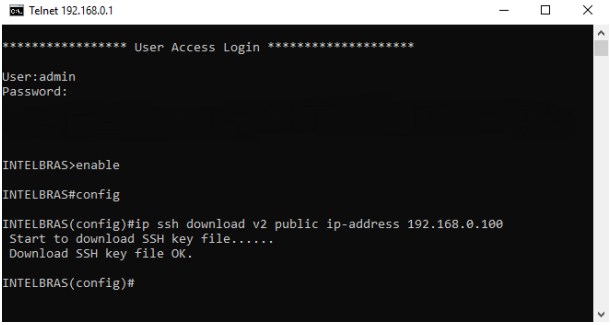
Obs.: *o tamanho da chave deve ser entre 512 e 3072 bits. Durante o processo para gerar a chave, mova rapidamente o mouse sobre a interface para acelerar o processo.*

2. Após gerar a chave com sucesso, salve a chave pública e a chave privada em um servidor TFTP;



Salvando as chaves geradas

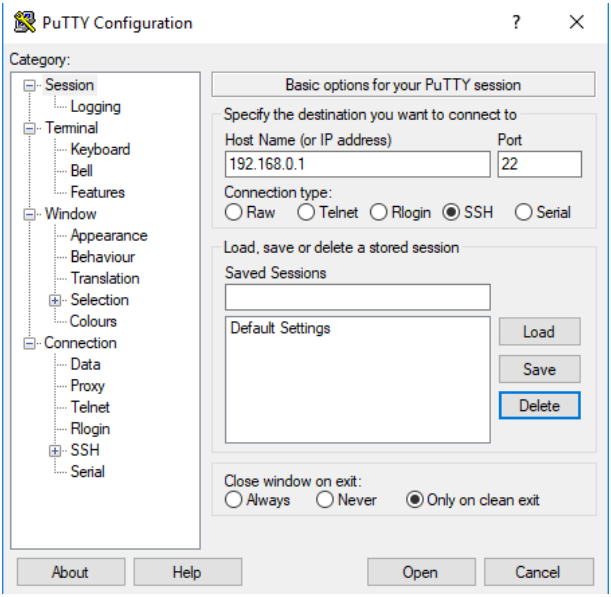
3. Efetue login no switch via Telnet e efetue o download da chave pública salva no servidor TFTP, siga os passos da *Download da chave pública*;



Download da chave pública

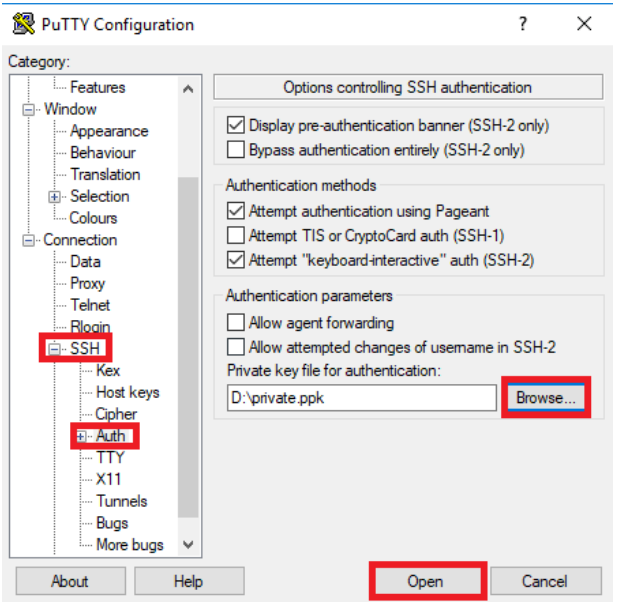
Obs.: *o tipo da chave deve estar de acordo com o tipo de arquivo de chave. O download da chave não deve ser interrompido.*

4. Após efetuar o download da chave pública, abra o software para efetuar login através da interface PuTTY. No campo **Host Name**, entre com o endereço IP do switch; no campo **Port**, adicione o número *22*; selecione *SSH* em **Connection type**;



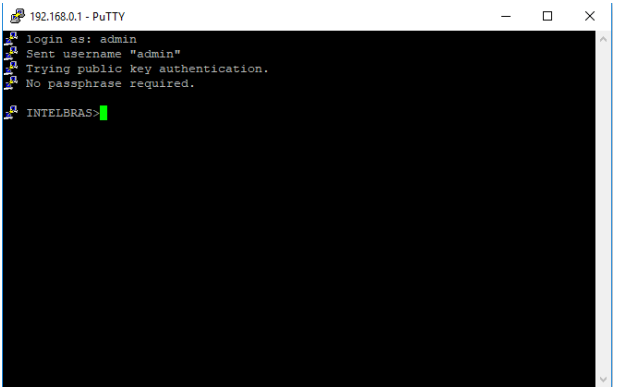
Configurando uma conexão SSH

5. Na guia *SSH>Auth*, clique em *Browse* e selecione o diretório onde foi salva a chave privada, para finalizar clique em *Open*;



Download da chave privada

6. Após o sucesso de autenticação, entre com o nome de usuário. O switch não solicitará que a senha seja digitada, indicando que a autenticação por chave pública foi efetuada com sucesso.



Login com chave pública

1.2. Modos de comando CLI

O CLI é dividido em diferentes modos de comandos *User EXEC Mode*, *Privileged EXEC Mode*, *Global Configuration Mode*, *Interface Configuration Mode* e *VLAN Configuration Mode*.

O modo *Interface Configuration* está dividido em *interface Ethernet*, *interface link-aggregation* e alguns outros modos. A tabela a seguir fornece informações detalhadas sobre o caminho de acesso, o prompt de cada modo e como sair do modo atual e acessar o próximo modo.

Modo	Caminho de acesso	Prompt	Logout ou acessar o próximo modo
User EXEC Mode	Primeiro modo quando conectado ao switch.	**INTELBRAS>**	Use o comando ***exit*** para se desconectar do switch. Use o comando ***enable*** para acessar o Privileged EXEC Mode.
Privileged EXEC Mode	Use o comando ***enable*** para entrar no Privileged EXEC Mode.	**INTELBRAS#**	Entre com o comando ***disable*** ou ***exit*** para retornar ao User EXEC Mode. Entre com o comando ***configure*** para acessar o Global Configuration.
Global Configuration Mode	Use o comando ***configure*** para entrar no modo Privileged EXEC.	**INTELBRAS(config)#**	Use os comandos ***exit*** e ***end*** ou pressione ***Ctrl+Z*** para retornar ao Privileged EXEC Mode. Use a Interface gigabitEthernet ***port*** ou gigabitEthernet ***port-list*** para acessar o interface Configuration Mode. Use o comando ***vlan-list*** para acessar o VLAN Configuration mode.
Interface Configuration Mode	Interface de camada 2: use a interface gigabitEthernet ***port***, interface canais-portas ***port-channel-id*** ou uma quantidade de interfaces ***port-list*** para entrar no Global Configuration Mode.	**INTELBRAS(config-if)#** ou **INTELBRAS(config-if-range)#**	Use o comando ***end*** ou pressione ***Ctrl+Z*** para retornar ao Privileged EXEC Mode. Entre com o comando ***exit*** ou ***#*** para retornar ao Global Configuration. O número da porta deve ser especificado na interface de comando.
	Interface de camada 3: use o comando ***switchport*** para entrar no Interface Configuration Mode de roteamento de portas. Use o comando ***vlan-id*** para acessar o VLAN interface no Global Configuration. Para acessar a interface de loopback use o comando ***interface loopback*** *id* no Global Configuration.		Use o comando ***switchport*** para acessar modo de configuração de camada 2. Use o comando ***end*** ou pressione ***Ctrl+Z*** para retornar ao Privileged EXEC Mode. Digite o comando ***exit*** ou ***#*** para retornar Global Configuration.
VLAN Configuration Mode	Use o comando ***vlan-list*** para entrar no Global Configuration.	**INTELBRAS(config-vlan)#**	Use o comando ***end*** ou pressione ***Ctrl+Z***, para retornar ao Privileged EXEC Mode. Digite o comando ***exit*** ou ***#*** para retornar ao Global Configuration.

Obs.: » *Após estabelecida a conexão entre o switch e um PC através do Telnet ou SSH, o usuário automaticamente estará no User EXEC.*

» *Cada modo de comando possui seu próprio conjunto de comandos específicos. Para configurar alguns comandos, você deve acessar o modo de comando correspondente em primeiro lugar.*

» **Global Configuration Mode:** neste modo, são fornecidos comandos globais, como a Spanning Tree, Schedule Mode e assim por diante.

» **Interface Configuration Mode:** neste modo, os usuários podem configurar uma ou várias portas, diferentes portas correspondem a diferentes comandos.

» **Interface gigabitEthernet:** configure os parâmetros para uma porta Ethernet, como o modo *Duplex* e controle de fluxo.

» **Faixa de interface gigabitEthernet:** configure os parâmetros para várias portas Ethernet.

» **Interface link-aggregation:** configure os parâmetros do link-aggregation e transmissão broadcast.

» **Faixa de interface link-aggregation:** configure os parâmetros de multi-trunks.

» **Interface vlan:** configure os parâmetros para uma porta VLAN.

» **VLAN Configuration Mode:** neste modo, os usuários podem criar uma VLAN e adicionar uma porta especifica à VLAN.

Alguns comandos são globais, isso significa que eles podem ser executados em todos os modos:

» **show:** exibe todas as informações do switch, por exemplo - informações estatísticas, informações de porta, informações de VLAN.

» **history:** exibe o histórico de comandos.

1.3. Restrições de privilégio

A segurança desse switch é dividida em quatro níveis de privilégio*: Nível de usuário, Nível de usuário avançado, Nível de operador* e *Nível de administrador*. Você pode definir pares de nome de usuário e senha e atribuir um nível de privilégio específico a cada par. Diferentes níveis de privilégio têm acesso a comandos especificados, o que é ilustrado no *Requisito de privilégio* em cada comando. Para obter detalhes sobre como configurar os nomes de usuário e senha, consulte o item *3. Comandos de gerenciamento de usuários*.

Os usuários podem entrar no modo de execução *Privilegiado* quando no modo de execução do usuário usando o comando *enable*. No caso padrão, nenhuma senha é necessária. No *Global Configuration Mode*, você pode configurar a senha para o nível de administrador ativando o comando de senha. Uma vez que a senha esteja configurada, você deverá inseri-la para acessar o modo de execução *Privilegiado*.

1.4. Convenções

1.4.1. Formato das convenções

As seguintes convenções são usadas neste manual:

» Itens entre colchetes [] são opcionais.

» Itens entre chaves {} são obrigatórios.

» Itens alternativos são agrupados em chaves e separados por barras verticais. Por exemplo: velocidade {10|100|1000}.

» Negrito indica uma palavra-chave inalterável. Por exemplo: **show logging**.

» Fonte normal indica uma constante (várias opções são enumeradas e apenas uma pode ser selecionada). Por exemplo: **mode** {dynamic|static|permanent}.

» Fonte itálico indica uma variável (um valor real deve ser atribuído). Por exemplo: **bridge aging-time** *aging-time*.

1.4.2. Caracteres especiais

Você deve prestar atenção à descrição a seguir onde está diferenciado se é uma variável ou um texto:

» Esses seis caracteres "<>, \ & não podem ser inseridos.

» Se um espaço em branco estiver contido em uma cadeia de caracteres, aspas simples ou duplas devem ser usadas, por exemplo, 'hello world', "hello world", e as palavras entre aspas serão identificadas como texto. Caso contrário, as palavras serão identificadas como variáveis.

1.4.3. Formato dos parâmetros

Alguns parâmetros devem ser inseridos em formatos especiais que são mostrados da seguinte maneira:

» O endereço MAC deve ser inserido no formato *xx:xx:xx:xx:xx:xx*.

» Um ou vários valores podem ser digitados para uma *port-list* ou uma *vlan-list* usando vírgula para separar. Use um hífen para designar um intervalo de valores, por exemplo, 1/0/1, 1/0/3-5, 1/0/7 para a escolha das portas 1/0/1, 1/0/3, 1/0/4, 1/0/5, 1/0/7.

2.1. enable

Descrição: o comando **enable** é usado para acessar o Privileged EXEC Mode quando estiver no User EXEC.

Sintaxe: **enable**

Modo de comando: User EXEC.

Privilégio requerido: nenhum.

Exemplo: acesso ao modo Privileged EXEC configurado com senha:

```
INTELBRAS>enable
Enter password:
INTELBRAS#
```

2.2. service password-encryption

Descrição: o comando **service password-encryption** é usado quando a senha é definida ou quando a configuração é ativada, usando o algoritmo de criptografia simétrica. A criptografia impede que a senha seja legível no arquivo de configuração. Para desativar a função de criptografia global use o comando **no service password-encryption.**

Sintaxe: **service password-encryption**
no service password-encryption

Modo de Comando: Global Configuration.

Privilégio requerido: apenas usuários do nível de administrador têm acesso a esses comandos.

Exemplo: ative a opção de criptografia global:

```
INTELBRAS(config)# service password-encryption
```

2.3. enable password

Descrição: o comando **enable password** é usado para definir ou alterar a senha para os usuários acessarem o modo de execução privilegiado no modo de execução do usuário. Para remover a senha, use o comando **no enable password**. Este comando usa a criptografia simétrica.

Sintaxe: **enable password** {[0] *password* | 7 *encrypted-password*}
no enable password

Parâmetros:

- **0:** especifique o tipo de criptografia. 0 indica que uma senha não criptografada será exibida. Por padrão, o tipo de criptografia é *0*.
- **password:** senha, uma cadeia de 1 a 31 caracteres alfanuméricos ou símbolos. A senha é sensível a maiúsculas e minúsculas, permite dígitos, letras (sensíveis a maiúsculas e minúsculas), sublinhados e dezesseis caracteres especiais (! $% '() *, -. / [] {|}). Por padrão é *vazio*.
- **7:** indica uma senha criptografada simétrica de tamanho fixo.
- **encrypted-password**: uma senha criptografada simétrica com tamanho fixo, que você pode copiar do arquivo de configuração de outro switch. Depois que a senha criptografada estiver configurada, você deverá usar a senha não criptografada correspondente se entrar novamente nesse modo.

Modo de Comando: Global Configuration.

Privilégio requerido: apenas usuários do nível de administrador têm acesso a esses comandos.

Diretrizes do usuário: se a senha que você configurou aqui não estiver criptografada e a função de criptografia global estiver ativada no **service password-encryption**, a senha no arquivo de configuração será exibida no formulário criptografado simétrico.

Exemplo: defina a senha como "admin" sem criptografia para acessar o modo de execução privilegiado no modo de execução do usuário:

INTELBRAS(config)# enable password 0 admin

2.4. enable secret

Descrição: o comando **enable secret** é usado para definir uma senha secreta, usando um algoritmo de criptografia MD5, para que os usuários acessem o Modo de execução Privilegiado do Modo de execução do Usuário. Para retornar à configuração padrão, use o comando **no enable secret**. Este comando usa a criptografia MD5.

Sintaxe: **enable secret** {[0] *password* | 5 *encrypted-password*}
no enable secret

Parâmetros:

- **0:** especifica o tipo de criptografia. 0 indica que uma senha não criptografada será exibida. Por padrão, o tipo de criptografia é *0*.
- **password:** senha, uma cadeia de 1 a 31 caracteres alfanuméricos ou símbolos. A senha é sensível a maiúsculas e minúsculas, permite dígitos, letras inglesas (sensíveis a maiúsculas e minúsculas), sublinhados e dezesseis caracteres especiais (! $% '() *, -. / [] {|}). Por padrão é *vazio*. A senha no arquivo de configuração será exibida no formulário criptografado MD5.
- **5:** indica uma senha criptografada MD5 de tamanho fixo.
- **encrypted-password:** uma senha criptografada MD5 com tamanho fixo, que você pode copiar do arquivo de configuração de outro switch. Depois que a senha criptografada estiver configurada, você deverá usar a senha não criptografada correspondente se entrar novamente nesse modo.

Modo de comando: Global Configuration.

Privilégio requerido: apenas usuários do nível de administrador têm acesso a esses comandos.

Diretrizes do usuário: se a senha de ativação e o segredo de ativação estiverem definidos, você deverá inserir a senha configurada em habilitar segredo.

Exemplo: defina a senha como "admin" sem criptografia para acessar o modo de execução privilegiado no modo de execução do usuário. A senha será exibida no formulário criptografado.

INTELBRAS(config)# enable secret 0 admin

2.5. configure

Descrição: o comando **configure** é usado para acessar o Global Configuration Mode no Privileged EXEC Mode.

Sintaxe: **configure**

Modo de comando: Privileged EXEC Mode.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: acesse o Global Configuration Mode no Privileged EXEC Mode:

INTELBRAS# configure
INTELBRAS(config)#

2.6. exit

Descrição: o comando **exit** é usado para retornar ao modo anterior.

Sintaxe: **exit**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: retorne ao Global Configuration Mode no modo de configuração da interface, retornando ao Privileged EXEC Mode:

```
INTELBRAS(config-if)# exit
INTELBRAS(config)# exit
INTELBRAS#
```

2.7. end

Descrição: o comando **end** é usado para retornar ao modo de execução privilegiado.

Sintaxe: **end**

Modo de Comando: Configuration e Privileged EXEC.

Privilégio requerido: nível de administrador para ter acesso aos comandos.

Exemplo: retorne ao Privileged EXEC Mode no modo de configuração de interface:

```
INTELBRAS(config-if)# end
INTELBRAS#
```

2.8. clipaging

Descrição: o comando **clipaging** é usado para habilitar função de pausa para a exibição na tela. Se você quiser exibir todas as informações relacionadas ao switch ao usar o comando **show**, favor usar o comando de **no clipaging**.

Sintaxe: **clipaging**
no clipaging

Modo de Comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: desabilite a função de pausa no display:

```
INTELBRAS(config)# no clipaging
```

2.9. history

Descrição: o comando **history** é usado para exibir os últimos vinte comandos inseridos no modo atual.

Sintaxe: **history**

Modo de Comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: exiba os comandos inseridos no modo atual:

```
INTELBRAS(config)# history
1 history
```

2.10. history clear

Descrição: o comando **history clear** é usado para apagar os comandos inseridos no modo atual. Portanto, esses comandos não serão mostrados caso seja inserido o comando **history**.

Sintaxe: **history clear**

Modo de Comando: Configuration e Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: apague os comandos inseridos no modo atual:

```
INTELBRAS(config)# history clear
```

3. Comandos de gerenciamento de usuários

Os comandos de gerenciamento de usuários são usados para gerenciar as informações de registro do usuário pela web, Telnet ou SSH, para proteger as configurações do switch de serem alteradas aleatoriamente.

3.1. user name(senha)

Descrição: o comando **user name** é usado para adicionar um novo usuário ou modificar as informações dos usuários existentes. Para excluir os usuários existentes, use o comando **no user name**. Este comando usa a criptografia simétrica.

Sintaxe: **user name** *name* [**privilege** admin | operator | power_user | user] **password** {[0] *password* | 7 *encrypted-password*}
no user name *name*

Parâmetros:

- **name**: digite um nome para o login dos usuários, que contenha no máximo 16 caracteres, composto de dígitos, letras e apenas traços.
  - **admin | *operador* | power_user | *usuário*:** nível de acesso. *Admin* significa que você pode editar, modificar e visualizar todas as configurações de diferentes funções. *Operador* significa que você pode editar, modificar e visualizar a maioria das configurações de diferentes funções. *Usuário avançado* significa que você pode editar, modificar e visualizar algumas das configurações de diferentes funções. *Usuário* significa que você só pode visualizar algumas das configurações de diferentes funções sem o direito de editar ou modificar. É *admin* por padrão. Para mais detalhes sobre **restrições de privilégios**, por favor consulte a parte de privilégios requeridos em cada comando.
- **0:** especifique o tipo de criptografia. 0 indica que uma senha não criptografada será exibida. Por padrão, o tipo de criptografia é *0*.
- **password:** a senha de login dos usuários, uma cadeia de 1 a 31 caracteres alfanuméricos ou símbolos. A senha é sensível a maiúsculas e minúsculas, permite dígitos, letras (sensíveis a maiúsculas e minúsculas), sublinhados e dezesseis caracteres especiais (! $% '() *, -. / [] {|}).
- **7:** indica uma senha criptografada simétrica com tamanho fixo.
- **encrypted-password:** uma senha criptografada simétrica com tamanho fixo, que você pode copiar do arquivo de configuração de outro switch. Depois de configurada, você deverá usar a senha não criptografada correspondente se entrar novamente nesse modo.

Modo de Comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Diretrizes do usuário: se a senha que você configurou aqui não estiver criptografada e a função de criptografia global estiver ativada no **service password-encryption**, a senha no arquivo de configuração será exibida no formulário criptografado simétrico.

Exemplo: adicione e ative um novo usuário administrador chamado "intelbras", cuja senha é "admin" e não criptografada:

```
INTELBRAS(config)#user name intelbras privilege admin password 0 admin
```

3.2. user name(secreto)

Descrição: o comando **user name** é usado para adicionar um novo usuário ou modificar as informações dos usuários existentes. Para excluir os usuários existentes, use o comando **no user name**. Este comando usa a criptografia simétrica.

Sintaxe: ***user name*** *name* [**privilege** admin | operator | power_user | user] **secret** {[0] *password* | 5 *encrypted-password*}
no user name *name*

Parâmetros:

» **name:** digite um nome para o login dos usuários, que contém no máximo 16 caracteres, composto de dígitos, letras e apenas traços.

admin | *operador* | power_user | *usuário*: nível de acesso. *Admin* significa que você pode editar, modificar e visualizar todas as configurações de diferentes funções. *Operador* significa que você pode editar, modificar e visualizar a maioria das configurações de diferentes funções. *Usuário avançado* significa que você pode editar, modificar e visualizar algumas das configurações de diferentes funções. *Usuário* significa que você só pode visualizar algumas das configurações de diferentes funções sem o direito de editar ou modificar. É *admin* por padrão. Para mais detalhes sobre restrições de privilégios, por favor consulte a parte de privilégios requeridos em cada comando.

» **0:** especifique o tipo de criptografia. 0 indica que uma senha não criptografada será exibida. Por padrão, o tipo de criptografia é *0*.

» **password:** a senha de login dos usuários, uma cadeia de 1 a 31 caracteres alfanuméricos ou símbolos. A senha é sensível a maiúsculas e minúsculas, permite dígitos, letras (sensíveis a maiúsculas e minúsculas), sublinhados e dezesseis caracteres especiais (! $% '() *, -. / [] {|}).

» **5:** indica uma senha criptografada MD5 com tamanho fixo.

» **encrypted-password:** uma senha criptografada simétrica com tamanho fixo, que você pode copiar do arquivo de configuração de outro switch. Depois de configurada, você deverá usar a senha não criptografada correspondente se entrar novamente nesse modo.

Modo de Comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Diretrizes do usuário: se o **user name**(senha) e o **user name**(secreto) forem definidos, apenas a última senha configurada entrará em vigor.

Exemplo: adicione e ative um novo usuário administrador chamado "intelbras", cuja senha é "admin". A senha será exibida na forma criptografada:

INTELBRAS(config)#user name intelbras **privilege** admin **secret** 0 admin

3.3. show user account-list

Descrição: o comando **show user account-list** é usado para exibir no display a informação dos usuários atuais.

Sintaxe: **show user account-list**

Modo de Comando: Configuration e Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: visualize as informações dos usuários atuais:

INTELBRAS(config)#show user account-list

3.4. show user configuration

Descrição: o comando **show user configuration** é usado para exibir as informações de configuração e de segurança dos usuários, incluindo o controle de acesso, o número máximo o tempo limite ocioso etc.

Sintaxe: **show user configuration**

Modo de Comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: visualize as informações de configuração dos usuários atuais:

INTELBRAS(config)#show user configuration

4. Comandos de configuração de sistema

Os comandos de sistema são usados para configurar as informações de sistema e IP do sistema, reboot e reset do switch, atualização do switch e outras operações.

4.1. system-time manual

Descrição: o comando **system-time manual** é usado para configurar manualmente a data e horário do sistema.

Sintaxe: **system-time manual** *time*

Parâmetro:

» **time:** data e hora manual, *MM/DD/YYYY-HH:MM:SS*. São aceitos valores para o ano entre 2000 e 2037.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure de forma manual a data e horário do sistema em 7/20/2019 09:32:00.

INTELBRAS(config)# system-time manual 7/20/2019-09:32:00

4.2. system-time ntp

Descrição: o comando **system-time ntp** é usado para configurar a zona de fuso horário e o endereço IP do servidor NTP. O switch receberá o UTC automaticamente se estiver conectado a um servidor NTP.

Sintaxe: **system-time ntp** {*timezone*} {*ntp-server*} {*backup-ntp-server*} {*fetching-rate*}

Parâmetros:

» **timezone:** local do fuso horário, variando entre UTC-12:00 e UTC+13:00. As informações detalhadas que cada fuso horário significa são exibidas a seguir:
  » **UTC-12:00:** TimeZone for International Date Line West.
  » **UTC-11:00:** TimeZone for Coordinated Universal Time-11.
  » **UTC-10:00:** TimeZone for Hawaii.
  » **UTC-09:00:** TimeZone for Alaska.
  » **UTC-08:00:** TimeZone for Pacific Time (US Canada).
  » **UTC-07:00:** TimeZone for Mountain Time (US Canada).
  » **UTC-06:00:** TimeZone for Central Time (US Canada).
  » **UTC-05:00:** TimeZone for Eastern Time (US Canada).
  » **UTC-04:30:** TimeZone for Caracas.
  » **UTC-04:00:** TimeZone for Atlantic Time (Canada).
  » **UTC-03:30:** TimeZone for Newfoundland.
  » **UTC-03:00:** TimeZone for Buenos Aires, Salvador, Brasilia.
  » **UTC-02:00:** TimeZone for Mid-Atlantic.
  » **UTC-01:00:** TimeZone for Azores, Cape Verde Is.
  » **UTC:** TimeZone for Dublin, Edinburgh, Lisbon, London.
  » **UTC+01:00:** TimeZone for Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna.
  » **UTC+02:00:** TimeZone for Cairo, Athens, Bucharest, Amman, Beirut, Jerusalem.
  » **UTC+03:00**: TimeZone for Kuwait, Riyadh, Baghdad.
  » **UTC+03:30:** TimeZone for Tehran.
  » **UTC+04:00**: TimeZone for Moscow, St.Petersburg, Volgograd, Tbilisi, Port Louis.
  » **UTC+04:30**: TimeZone for Kabul.
  » **UTC+05:00**: TimeZone for Islamabad, Karachi, Tashkent.
  » **UTC+05:30**: TimeZone for Chennai, Kolkata, Mumbai, New Delhi.
  » **UTC+05:45:** TimeZone for Kathmandu.
  » **UTC+06:00:** TimeZone for Dhaka, Astana, Ekaterinburg.
  » **UTC+06:30:** TimeZone for Yangon (Rangoon).

- » **UTC+07:00:** TimeZone for Novosibrisk, Bangkok, Hanoi, Jakarta.
- » **UTC+08:00:** TimeZone for Beijing, Chongqing, Hong Kong, Urumqi, Singapore.
- » **UTC+09:00:** TimeZone for Seoul, Irkutsk, Osaka, Sapporo, Tokyo.
- » **UTC+09:30:** TimeZone for Darwin, Adelaide.
- » **UTC+10:00:** TimeZone for Canberra, Melbourne, Sydney, Brisbane.
- » **UTC+11:00:** TimeZone for Solomon Is., New Caledonia, Vladivostok.
- » **UTC+12:00:** TimeZone for Fiji, Magadan, Auckland, Welington.
- » **UTC+13:00:** TimeZone for Nuku'alofa, Samoa.

» **ntp-server:** endereço IP do servidor primário NTP.

» **backup-ntp-server:** endereço IP do servidor secundário NTP.

» **fetching-rate:** especifique taxa de busca do servidor NTP.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o fuso horário do sistema através de um servidor NTP, usando o fuso horário UTC-12:00, com o servidor primário NTP 133.100.9.2 e o secundário 139.79.100.163, com a taxa de busca de 11 horas:

INTELBRAS(config)# system-time ntp UTC-12:00 133.100.9.2 139.79.100.163 11

4.3. system-time dst predefined

Descrição: o comando **system-time dst predefined** é usado para selecionar uma configuração de horário de verão a partir do modo predefinido. A configuração pode ser usada recorrentemente. Para desabilitar a função *DST*, use o comando **no system-time dst.**

Sintaxe: **system-time dst predefined** [USA / Australia | Europe | New-Zealand]
no system-time dst

Parâmetros:

» **USA / Australia | Europe | New-Zeland:** existem 4 opções para o modo de horário de verão, que são: USA, Australia, Europe e New-Zeland, respectivamente. O valor padrão é a *Europa*. A seguir estão os intervalos de tempo de cada opção:
- » **USA:** segundo domingo de março, 02:00 até primeiro domingo de novembro, 02:00.
- » **Australia:** primeiro domingo de outubro, 02:00 até primeiro domingo de abril, 03:00.
- » **Europe:** último domingo de março, 01:00 - último domingo de outubro, 01:00.
- » **New-Zeland:** último domingo de setembro, 02:00 até primeiro domingo de abril, 03:00.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure horário de verão com padrão EUA:

INTELBRAS(config)# system-time dst predefined USA

4.4. system-time dst date

Descrição: o comando **system-time dst date** é usado para configurar o horário de verão único. A data de início está no ano atual por padrão. O intervalo de tempo do horário de verão deve ser menor que um ano, mas você pode configurá-lo ao longo dos anos. Para desabilitar a função DST, use o comando **no system-time dst.**

Sintaxe: **system-time dst date** {*smonth*} {*sday*} {*stime*} {*syear*} {*emonth*} {*eday*} {*etime*} {*eyear*}[*offset*]
no system-time dst

Parâmetros:

» **smonth:** o mês inicial do horário de verão. Existem 12 valores possíveis: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

» **sday:** o dia de início do horário de verão, variando de 1 a 31. Aqui você deve mostrar atenção especial para fevereiro e as diferenças entre um mês solar e um mês lunar.

» **stime:** o momento de início do horário de verão, *HH:MM*.

» **syear:** o ano inicial do horário de verão.

» **emonth:** o mês final do horário de verão. Existem 12 valores possíveis: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.
» **eday:** o dia final do horário de verão, variando de 1 a 31. Aqui você deve mostrar atenção especial a fevereiro e as diferenças entre um mês solar e um mês lunar.
» **etime:** o momento final do horário de verão, *HH:MM*.
» **eyear:** o ano final do horário de verão.
» **offset:** o número de minutos para adicionar durante o horário de verão. São *60 minutos* por padrão.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure horário de verão para começar as 00:00 horas, em primeiro de abril, até as 00:00 horas de primeiro de outubro, com offset de 30 minutos em 2018:

INTELBRAS(config)# system-time dst date Apr 1 00:00 2015 Oct 1 00:00 2018 30

4.5. system-time dst recurring

Descrição: o comando **system-time dst recurring** é usado para configurar o horário de verão recorrente. Pode ser configurado abrangendo anos. Para desabilitar a função *DST*, use o comando **no system-time dst.**

Sintaxe: **system-time dst recurring** {*sweek*} {*sday}* {*smonth*} {*stime*} {*eweek*} {*eday*} {*emonth*} {*etime*} [*offset*]
no system-time dst

Parâmetros:

» **sweek:** a semana inicial do horário de verão. Existem 5 valores possíveis: first, second, third, fourth, last.
» **sday:** o dia de início do horário de verão. Existem 7 valores possíveis: Sun, Mon, Tue, Wed, Thu, Fri, Sat.
» **smonth:** o mês de início do horário de verão. Existem 12 valores possíveis: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.
» **stime:** o momento de início do horário de verão, *HH:MM*.
» **eweek:** a semana final do horário de verão. Existem 5 valores possíveis: first, second, third, fourth, last.
» **eday:** o dia final do horário de verão. Existem 7 valores possíveis: Sun, Mon, Tue, Wed, Thu, Fri, Sat.
» **emonth:** o mês final do horário de verão. Existem 12 valores possíveis: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.
» **etime:** o momento final do horário de verão, *HH:MM*.
» **offset:** o número de minutos para adicionar durante o horário de verão. São *60 minutos* por padrão.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o horário de verão das 2:00 da manhã, do primeiro domingo de maio às 2:00 da manhã, do último domingo de outubro com offset de 45 minutos em 2018:

INTELBRAS(config)# system-time dst recurring first Sun May 02:00 last Sun Oct 02:00 45

4.6. hostname

Descrição: o comando **hostname** é usado para configurar o nome do sistema. Para limpar o nome do sistema, use o comando **no hostname.**

Sintaxe: **hostname** [*hostname*]
no hostname

Parâmetro:

» **hostname:** nome do sistema. O nome deve ter entre 1 a 32 caracteres. Por padrão, o nome do dispositivo é *INTELBRAS*.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o nome do dispositivo como INTELBRAS:

INTELBRAS(config)# hostname INTELBRAS

4.7. location

Descrição: o comando **location** é usado para configurar o local do dispositivo. Para limpar a informação de local do dispositivo, use o comando **no location.**

Sintaxe: **location** [*location*]
no location

Parâmetro:

» **location:** local do dispositivo. O local deve ter entre 1 a 32 caracteres.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o local do dispositivo como "SANTA CATARINA":

INTELBRAS(config)# location "SANTA CATARINA"

4.8. contact-info

Descrição: o comando **contact-info** é usado para configurar as informações de contato do sistema. Para limpar as informações de contato, use o comando **no contact-info.**

Sintaxe: **contact-info** [*contact-info*]
no contact-info

Parâmetro:

» **contact-info:** informação de contato. A informação deve ter entre 1 a 32 caracteres.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configurar as informações de contato do sistema como "www.intelbras.com.br":

INTELBRAS(config)# contact-info www.intelbras.com.br.

4.9. ip address

Descrição: o comando **ip address** é usado para configurar o endereço IP e a máscara de sub-rede IP para a interface especificada manualmente. O tipo de interface inclui: routed port, interface port-channel, interface loopback e interface VLAN.

Sintaxe: **ip address** {*ip-addr*} {*mask*} [**secondary**]
no ip address [*ip-addr*] [*mask*]

Parâmetros:

» **Ip-addr:** endereço IP da interface de camada 3.
» **mask:** máscara de sub-rede da interface de camada 3.
» **secondary:** especifique o endereço IP secundário da interface. Se este parâmetro for omitido aqui, o endereço IP configurado será o endereço principal da interface.

Modo de comando: Interface Configuration

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie a interface VLAN 2 com endereço IP primário igual a 192.168.1.1/24 e IP secundário igual a 192.168.2.1/24:

INTELBRAS(config)# interface vlan 2
INTELBRAS(config-if)# ip address 192.168.1.1 255.255.255.0
INTELBRAS(config-if)# ip address 192.168.2.1 255.255.255.0 **secondary**

4.10. ip address-alloc

Descrição: o comando **ip address-alloc** é usado para habilitar a função *Cliente DHCP* ou o *Protocolo BOOTP*. Quando esta função está ativada, a interface especificada obtém o IP do servidor DHCP ou do servidor BOOTP. Para desativar a função de obtenção de IP na interface especificada, use o comando **no ip address**. Este comando se aplica a routed port, interface port-channel e interface VLAN.

Sintaxe: **ip address-alloc** {dhcp|bootp}
no ip address

Parâmetros:

- **dhcp:** especifique a interface da camada 3 para obter o endereço IP do servidor DHCP.
- **bootp:** especifique a interface da camada 3 para obter o endereço IP do servidor BOOTP.

Modo de comando: Interface Configuration.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Habilite a função de cliente DHCP na porta 1/0/1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# no switchport
INTELBRAS(config-if)# ip address-alloc dhcp
```

Desabilite a função de obtenção do endereço IP na interface VLAN 2:

```
INTELBRAS(config)# interface vlan 2
INTELBRAS(config-if)# no ip address
```

4.11. reset

Descrição: o comando **reset** é usado redefinir o software do switch. Após a redefinição, toda a configuração do switch será restaurada para os padrões de fábrica e suas configurações atuais serão perdidas.

Sintaxe: **reset**

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: redefina o software do switch:

```
INTELBRAS# reset
```

4.12. reboot

Descrição: o comando **reboot** é usado para reiniciar o switch. Para evitar danos, não desligue o dispositivo durante a reinicialização.

Sintaxe: **reboot**

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: reinicie o switch:

```
INTELBRAS# reboot
```

4.13. reboot-schedule

Descrição: o comando **reboot-schedule** é usado para configurar o switch para reiniciar em um determinado momento. Para excluir as configurações da programação de reinicialização, use o comando **reboot-schedule cancel**.

Sintaxe: **reboot-schedule at** *time* [*date*] [**save_before_reboot**]
reboot-schedule in *interval* [**save_before_reboot**]
reboot-schedule cancel

Parâmetros:

- **time:** especifique o ponto de tempo para o switch ser reinicializado, no formato de *HH:MM*.
- **date:** especifique a data para o switch ser reinicializado, no formato *DD:MM:YYYY*. A data deve estar dentro de 30 dias.
- **save_before_reboot:** salve o arquivo de configuração antes que o switch seja reinicializado.
- **interval:** especifique um período após o qual o switch é reinicializado. Variando de 1 a 43200 minutos.
- **cancel:** exclua as configurações de agendamento de reinicialização.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Diretrizes do usuário: no comando **reboot-schedule** *time* [*date*] [**save_before_reboot**], se nenhuma data for especificada e a hora que você definir aqui for posterior à hora em que este comando for executado, o switch será reinicializado mais tarde naquele dia; caso contrário, o switch será reinicializado no próximo dia.

Exemplo: especifique para que o switch salve as configurações e reinicie em 200 minutos:

```
INTELBRAS(config)# reboot-schedule in 200 save_before_reboot
```

4.14. copy running-config startup-config

Descrição: o comando **copy running-config startup-config** é usado para salvar as configurações atuais.

Sintaxe: **copy running-config startup-config**

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: salve as configurações atuais:

```
INTELBRAS# copy running-config startup-config
```

4.15. copy startup-config tftp

Descrição: o comando **copy startup-config tftp** é usado para fazer backup do arquivo de configuração no servidor TFTP.

Sintaxe: **copy startup-config tftp ip-address** *ip-addr* **filename** *name*

Parâmetros:

- **ip-addr:** endereço IP do servidor TFTP. Ambos os endereços IPv4 e IPv6 são suportados, por exemplo, 192.168.0.1 ou fe80::1234.
- **name:** especifique o nome do arquivo de configuração que seria o backup.

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Faça o backup do arquivo de configuração para o servidor TFTP com IP 192.168.0.148, o nome do arquivo é config:

```
INTELBRAS# copy startup-config tftp ip-address 192.168.0.148 filename config
```

Faça o backup do arquivo de configuração para o servidor TFTP com IP fe80::1234, o nome do arquivo é config:

```
INTELBRAS# copy startup-config tftp ip-address fe80::1234 filename config
```

4.16. copy tftp startup-config

Descrição: o comando **copy tftp startup-config** é usado para fazer download do arquivo de configuração do switch no servidor TFTP.

Sintaxe: **copy tftp startup-config ip-address** *ip-addr* **filename** *name*

Parâmetros:

- **ip-addr:** endereço IP do servidor TFTP. Ambos os endereços IPv4 e IPv6 são suportados, por exemplo, 192.168.0.1 ou fe80::1234.
- **name:** especifique o nome do arquivo de configuração que deseja fazer o download.

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplos:

Faça o download para o switch do arquivo de configuração config.cfg do servidor TFTP com IP 192.168.0.148:

```
INTELBRAS# copy tftp startup-config ip-address 192.168.0.148 filename config
```

Faça o download para o switch do arquivo de configuração config.cfg do servidor TFTP com IP fe80::1234:

```
INTELBRAS# copy tftp startup-config ip-address fe80::1234 filename config
```

4.17. copy backup-config tftp

Descrição: o comando **copy backup-config tftp** é usado para exportar o arquivo de configuração de backup do switch para o servidor TFTP.

Sintaxe: **copy backup-config tftp ip-address** *ip-addr* **filename** *name*

Parâmetros:

- **ip-addr:** endereço IP do servidor TFTP. Ambos os endereços IPv4 e IPv6 são suportados, por exemplo, 192.168.0.1 ou fe80::1234.
- **name:** especifique o nome do arquivo de configuração que deseja exportar.

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: exporte o arquivo de configuração de backup do switch para o servidor TFTP com o IP 192.168.0.148 e nomeie o arquivo config:

```
INTELBRAS# copy backup-config tftp ip-address 192.168.0.148 filename config
```

4.18. copy backup-config startup-config

Descrição: o comando **copy backup-config startup-config** é usado para substituir o arquivo de configuração de inicialização usando o arquivo de configuração de backup.

Sintaxe: **copy backup-config startup-config**

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: substitua o arquivo de configuração de inicialização usando o arquivo backup de configuração:

```
INTELBRAS# copy backup-config startup-config
```

4.19. copy running-config backup-config

Descrição: o comando **copy running-config backup-config** é usado para salvar a configuração atual em execução como o arquivo de configuração de backup.

Sintaxe: **copy running-config backup-config**

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: salve a configuração atual em um arquivo de backup de configuração:

```
INTELBRAS# copy running-config backup-config
```

4.20. copy tftp backup-config

Descrição: o comando **copy tftp backup-config** é usado para fazer o download do arquivo de configuração de um servidor TFTP.

Sintaxe: **copy tftp backup-config ip-address** *ip-addr* **filename** *name*

Parâmetros:

- **ip-addr:** endereço IP do servidor TFTP. Ambos os endereços IPv4 e IPv6 são suportados, por exemplo, 192.168.0.1 ou fe80::1234.
- **name:** especifique o nome do arquivo de configuração que deseja exportar.

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: download do arquivo de configuração chamado config.cfg de um servidor TFTP com IP 192.168.0.148:

```
INTELBRAS# Copy tftp backup-config ip-address 192.168.0.148 filename config
```

4.21. boot application

Descrição: o comando **boot application** é usado para configurar o arquivo de imagem como imagem de inicialização ou imagem de backup.

Sintaxe: **boot application filename** {image1 | image2} {startup | backup}
no boot application

Parâmetros:

- **Image1|image2:** especifique o arquivo de imagem a ser configurado. Por padrão, o image1.bin é a imagem de inicialização e o image2.bin é a imagem de backup.
- **startup|backup:** especifique a propriedade da imagem, imagem de inicialização ou imagem de backup.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configurar a image2.bin como imagem de inicialização:

```
INTELBRAS# boot application filename image2 startup
```

4.22. boot config

Descrição: o comando **boot config** é usado para configurar o arquivo de configuração como configuração de inicialização ou configuração de backup.

Sintaxe: **boot config filename** {config1 | config2} {startup | backup}
no boot application

Parâmetros:

- **config1|config2:** especifique o arquivo a ser configurado. Por padrão, o config1.cfg é a imagem de inicialização e o config2.cfg é a imagem de backup.
- **startup|backup:** especifique a propriedade da configuração.

Modo de comando: Global Configuration.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configurar a image2.bin como imagem de inicialização:

INTELBRAS# boot config filename config2 startup

4.23. remove backup-image

Descrição: o comando **remove backup-image** é usado para apagar a imagem de backup.

Sintaxe: **remove backup-image**

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: apague o arquivo imagem de backup:

INTELBRAS# remove backup-image

4.24. firmware upgrade

Descrição: o comando **firmware upgrade** é usado para atualizar o arquivo de imagem de backup do switch através do servidor TFTP. O arquivo de firmware carregado terá lugar da imagem de backup, e o usuário pode escolher se deseja reiniciar o switch com o arquivo de backup.

Sintaxe: **firmware upgrade ip-address** *ip-addr* **filename** *name*

Parâmetros:

- **ip-addr:** endereço IP do servidor TFTP. Ambos os endereços IPv4 e IPv6 são suportados, por exemplo, 192.168.0.1 ou fe80::1234.
- **name:** especifique o nome do arquivo de firmware.

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplos:

Atualize o arquivo de imagem de backup do switch com o arquivo firmware.bin no servidor TFTP com o endereço IP 192.168.0.148 e reinicialize o switch com este firmware:

INTELBRAS# firmware upgrade ip-address 192.168.0.148 **filename** firmware.bin
It will only upgrade the backup image. Continue? (Y/N):y
Operation OK!
Reboot with the backup image? (Y/N): y

Atualize o arquivo de imagem de backup do switch com o arquivo firmware.bin no servidor TFTP com o endereço IP fe80::1234, mas não reinicialize o switch:

INTELBRAS# firmware upgrade ip-address fe80::1234 **filename** firmware.bin
It will only upgrade the backup image. Continue? (Y/N):y
Operation OK!
Reboot with the backup image? (Y/N): n

4.25. ping

Descrição: o comando **ping** é usado para teste de conectividade entre o switch e um nó da rede.

Sintaxe: **ping** [ip | ipv6] {*ip_addr*} [**-n** *count*] [**-l** *size*] [**-i** *interval*]

Parâmetros:

- **ip:** o tipo do endereço IP para o teste de ping deve ser IPv4.
- **ipv6:** o tipo do endereço IP para o teste de ping deve ser IPv6.
- **ip_addr:** o endereço IP do nó de destino para o teste de ping. Se o parâmetro ip/ipv6 não estiver selecionado, os endereços IPv4 e IPv6 são suportados, por exemplo, 192.168.0.100 ou fe80::1234.
- **-n count:** a quantidade de vezes para enviar dados de teste durante o teste de ping. Ele varia de 1 a 10. Por padrão, esse valor é *4*.
- **-l size:** o tamanho dos dados de envio durante o teste de ping. Varia de 1 a 1500 bytes. Por padrão, esse valor é *64*.
- **-i interval:** o intervalo para enviar pacotes de requisição ICMP. Varia de 100 a 1000 milissegundos. Por padrão, esse valor é *1000*.

Modo de comando: Privileged EXEC

Privilégio requerido: nenhum.

Exemplos:

Para testar a conectividade entre o switch e o dispositivo de rede com o IP 192.168.0.131, especifique o *count* (**-l**) como 512 bytes e o *interval* (**-i**) como 1000 milissegundos. Se não houver resposta após o teste de Ping de 8 vezes, a conexão entre o switch e o dispositivo de rede não foi estabelecida:

INTELBRAS# ping 192.168.0.131 **–n** 8 **–l** 512

Para testar a conectividade entre o switch e o dispositivo de rede com o IP fe80::1234, especifique o *count* (**-l**) como 512 bytes e *interval* **(-i**) como 1000 milissegundos. Se não houver resposta após o teste de Ping de 8 vezes, a conexão entre o switch e o dispositivo de rede não foi estabelecida:

INTELBRAS# ping fe80::1234 **– n** 8 **–l** 512

4.26. tracert

Descrição: o comando **tracert** é usado para teste de conectividade entre os gateways durante a jornada de origem e destino dos dados de teste.

Sintaxe: **tracert** [ip | ipv6] *ip_addr* [*maxHops*]

Parâmetros:

- **ip:** o tipo do endereço IP para o teste de tracert deve ser IPv4.
- **ipv6:** o tipo do endereço IP para o teste de *tracert* deve ser IPv6.
- **ip_addr:** o endereço IP do dispositivo de destino. Se o parâmetro ip/ipv6 não estiver selecionado, os endereços IPv4 e IPv6 são suportados, por exemplo, 192.168.0.100 ou fe80::1234.
- **maxHops:** o número máximo de rotas que os dados de teste podem passar. Ele varia de 1 a 30. Por padrão, esse valor é *4*.

Modo de comando: Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador e usuários avançados têm acesso a esses comandos.

Exemplos:

Teste a conectividade entre o switch e o dispositivo de rede com o IP 192.168.0.131. Se o dispositivo de destino não foi encontrado após 20 saltos, a conexão entre o switch e o dispositivo de destino não foi estabelecida:

INTELBRAS# tracert 192.168.0.131 20

Teste a conectividade entre o switch e o dispositivo de rede com o IP fe80::1234. Se o dispositivo de destino não foi encontrado após 20 saltos, a conexão entre o switch e o dispositivo de destino não foi estabelecida:

```
INTELBRAS# tracert fe80::1234 20
```

4.27. show system-info

Descrição: o comando **show system-info** é usado para exibir a descrição do sistema, nome do dispositivo, localização do dispositivo, contato do sistema, versão do hardware, versão do firmware, hora do sistema, tempo de execução e assim por diante.

Sintaxe: **show system-info**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: exiba as informações do sistema:

```
INTELBRAS# show system-info
```

4.28. show image-info

Descrição: o comando **show image-info** é usado para exibir as informações dos arquivos de imagem do sistema.

Sintaxe: **show image-info**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: exiba as informações dos arquivos de imagem do sistema:

```
INTELBRAS# show image-info
```

4.29. show boot

Descrição: o comando **show boot** é usado para exibir as configurações de inicialização do sistema.

Sintaxe: **show boot**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: exiba as informações de configuração de inicialização:

```
INTELBRAS# show boot
```

4.30. show running-config

Descrição: o comando **show running-config** é usado para exibir a configuração operacional atual do sistema ou de uma porta especificada.

Sintaxe: **show running-config**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: exiba a configuração operacional atual do sistema:

```
INTELBRAS# show running-config
```

4.31. show startup-config

Descrição: o comando **show startup-config** é usado para exibir a configuração atual salva no switch. Essas configurações não serão perdidas na próxima vez que o switch for reinicializado.

Sintaxe: **show startup-config**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: exiba as configurações salvas:

```
INTELBRAS# show startup-config
```

4.32. show system-time

Descrição: o comando **show system-time** é usado para exibir as informações de data e hora do switch.

Sintaxe: **show system-time**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: exiba as informações de data e hora do switch:

```
INTELBRAS# show system-time
```

4.33. show system-time dst

Descrição: o comando **show system-time dst** é usado para exibir as informações DST do switch.

Sintaxe: **show system-time dst**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: exiba as informações DST do switch:

```
INTELBRAS# show system-time dst
```

4.34. show system-time ntp

Descrição: o comando **show system-time ntp** é usado para exibir as informações de configuração do modo NTP.

Sintaxe: **show system-time ntp**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: exiba as informações de configuração do modo NTP do switch:

```
INTELBRAS# show system-time ntp
```

4.35. show cable-diagnostics interface

Descrição: o comando **show cable-diagnostics interface** é usado para exibir os diagnósticos de cabo da porta Ethernet conectada, o que facilita a verificação do status da conexão do cabo conectado ao switch, a localização e o diagnóstico do ponto de problema da rede.

Sintaxe: **show cable-diagnostics interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*}

Parâmetro:

» **port:** o número da porta selecionada para efetuar o teste do cabo.

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: exiba os diagnósticos do cabo na porta 3:

```
INTELBRAS# show cable-diagnostics interface gigabitEthernet 1/0/3
```

4.36. show cpu-utilization

Descrição: o comando **show cpu-utilization** é usado para exibir as informações de utilização da CPU nos últimos 5 segundos / 1 minuto / 5 minutos.

Sintaxe: **show cpu-utilization**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: exiba as informações de utilização de CPU do switch:

```
INTELBRAS# show cpu-utilization
```

4.37. show memory-utilization

Descrição: o comando **show memory-utilization** é usado para exibir as informações de utilização de memória nos últimos 5 segundos / 1 minuto / 5 minutos.

Sintaxe: **show memory-utilization**

Modo de comando: Configuration e Privileged EXEC.

Privilégio requerido: nenhum.

Exemplo: exiba as informações de utilização de memória do switch:

```
INTELBRAS# show memory-utilization
```

5. Comando configuração EEE

EEE (*Energy Efficient Ehternet*) é usado para economizar o consumo de energia do switch durante períodos de baixo tráfego. Você pode simplesmente ativar esse recurso nas portas para permitir a redução de consumo.

5.1. eee

Descrição: o comando **eee** é usado para ativar o EEE na porta. Para desativar o EEE na porta, utilize o comando **no eee**.

Sintaxe: **eee**
no eee

Modo de Comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative EEE na porta 1/0/1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# eee
```

5.2. show interface eee

Descrição: o comando **show interface eee** é usado para mostrar a configuração do EEE em cada porta.

Sintaxe: **show interface eee** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*]

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração EEE em cada porta:

```
INTELBRAS# show interface eee
```

6. Comandos modelo SDM

Este capítulo descreve como configurar os modelos do SDM (*Switch Database Management*) para alocar recursos de hardware no switch para diferentes usos.

6.1. sdm prefer

Descrição: O comando **sdm prefer** é usado para configurar o modelo SDM. O modelo SDM é usado para alocar recursos do sistema para melhor suportar os recursos que estão sendo usados em sua aplicação. Para voltar a usar ao modelo padrão, use o comando **sdm prefer default**. A alteração do modelo entrará em vigor após reinicialização.

Sintaxe: **sdm prefer** {default | enterpriseV4 | enterpriseV6}

Parâmetros:

- **default:** especifica o template SDM usado no switch como *padrão*.
- **enterpriseV4:** especifica o template SDM usado no switch como *enterpriseV4*.
- **enterpriseV6:** especifica o template SDM usado no switch como *enterpriseV6*.

Modo de Comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: especifique o template SDM como enterpriseV4:

```
INTELBRAS(config)# sdm prefer enterpriseV4
```

6.2. show sdm prefer

Descrição: o comando **show sdm prefer** é usado para exibir a alocação de recursos do modelo atual do SDM em uso ou os modelos do SDM que podem ser usados.

Sintaxe: **show sdm prefer** {used | default | enterpriseV4 | enterpriseV6}

Parâmetros:

- **used:** exibe a alocação de recursos do modelo atualmente em uso e o modelo que ficará ativo após a reinicialização.
- **default:** exibe a alocação de recursos do template *padrão*.
- **enterpriseV4:** exibe a alocação de recursos do template *enterpriseV4*.
- **enterpriseV6:** exibe a alocação de recursos do template *enterpriseV6*.

Modo de Comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: exiba a alocação de recursos do template atualmente em uso e o modelo que ficará ativo após a reinicialização:

```
INTELBRAS# show sdm prefer used
```

7. Comandos Time Range

Com esse recurso, você pode configurar um intervalo de tempo e vinculá-lo a uma porta PoE ou a uma regra ACL.

7.1. time-range

Descrição: o comando **time-range** é usado para criar a entrada de intervalo de tempo para o switch e entrar no modo de configuração de intervalo de tempo. Depois que uma entrada de time range é criada, você precisa especificar a data e a hora. Um time range pode implementar vários intervalos de tempo simultaneamente, desde que eles não entrem em conflito entre si. Para excluir a configuração do intervalo de tempo correspondente utilize o comando **no time-range**.

Sintaxe: **time-range** *name*
no time-range *name*

Parâmetro:

- **name:** digite o nome do time-range, máximo 16 caracteres.

Modo de Comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie um time-range chamado "tRange1" para o switch:

```
INTELBRAS(config)# time-range tRange1
```

7.2. absolute

Descrição: o comando **absolute** é usado para criar um intervalo de tempo absoluto para o time-range do switch. Para excluir a configuração de intervalo de tempo absoluto correspondente utilize o comando **no absolute**.

Sintaxe: **absolute from** *start-date* **to** *end-date*
no absolute [*index*]

Parâmetros:

- **start-date:** data de início do absolute, no formato *MM/DD/YYYY*.
- **end-date:** data de fim do absolute, no formato *MM/DD/YYYY*.

Modo de comando: Power Time-range Create Configuration Mode.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: criar um time-range absoluto para o switch especificando o período entre 5 de maio de 2019 até 5 de outubro de 2019:

```
INTELBRAS(config)# time-range tRange1
INTELBRAS(config-time-range)# absolute from 05/05/2019 to 10/05/2019
```

7.3. periodic

Descrição: o comando **periodic** é usado para criar um time-range periódico para um intervalo de tempo do switch. Para excluir a configuração de time-range periódico correspondente utilize o comando **no periodic**.

Sintaxe: **periodic** {[start *start-time*] [end *end-time*] [day-of-the-week *week-day*]}
no periodic [*index*]

Parâmetros:

- **start-time:** especifica o horário de início, no formato *HH:MM*.
- **end-time:** especifica o horário de fim, no formato *HH:MM*.
- **week-day:** especifica os dias da semana, no formato *1-3* ou *7*. Os números 1-7 representam respectivamente segunda-feira, terça-feira, quarta-feira, quinta-feira, sexta-feira, sábado e domingo.

Modo de comando: Power Time-range Create Configuration Mode.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configuração de um time-range periódico de nome "tRange2" especificando o período entre 8:30 e 12:00 durante os finais de semana:

```
INTELBRAS(config)# time-range tRange2
INTELBRAS(config-time-range)# periodic start 08:30 end 12:00 day-of-the-week 6-7
```

7.4. holiday (time-range mode)

Descrição: o comando **holiday** é usado para criar um time-range do tipo feriado para um intervalo de tempo do switch. Quando ocorre a exclusão de um feriado no time-range, o switch não fornecerá energia para o intervalo de tempo excluído.

Sintaxe: **holiday** {exclude | include}

Parâmetros:

- **exclude:** o time-range não terá efeito no feriado.
- **Include:** o time-range terá efeito no feriado.

Modo de comando: Power Time-range Create Configuration Mode.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configuração de um time-range "tRange3" excluindo o feriado para este intervalo de tempo:

```
INTELBRAS(config)# time-range tRange3
INTELBRAS(config-time-range)# holiday exclude
```

7.5. holiday

Descrição: o comando **holiday** é usado para criar feriado para o switch. Para excluir a configuração de feriados correspondente utilize o comando **no holiday**.

Sintaxe: **holiday** *name* **start-date** *start-date* **end-date** *end-date*
no holiday name

Parâmetros:

- **name:** nome do holiday com no máximo 16 caracteres.
- **start-date:** data de início do holiday, no formato *MM/DD*.
- **end-date:** data de fim do holiday, no formato *MM/DD*.

Modo de Comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: criação de um feriado "holiday1" para o switch especificando o período entre 1 de outubro até 3 de outubro:

```
INTELBRAS(config)# holiday holiday1 start-date 10/01 end-date 10/03
```

7.6. show holiday

Descrição: O comando **show holiday** é usado para exibir o *feriado* definido.

Sintaxe: **show holiday**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba os "feriados" definidos:

```
INTELBRAS# show holiday
```

7.7. show time-range

Descrição: o comando **show time-range** é usado para exibir o time-range definido.

Sintaxe: **show time-range**

Modo de Comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba o time-range definido:

```
INTELBRAS# show time-range
```

8. Comandos de configuração de portas

Os comandos de configuração Ethernet podem ser usados para configurar o *Controle de banda*, o *Modo de negociação* e o *Storm Control* para as portas Ethernet.

8.1. interface gigabitEthernet

Descrição: o comando **interface gigabitEthernet** é usado para entrar no modo de configuração Interface gigabitEthernet e configurar a porta Gigabit Ethernet correspondente.

Sintaxe: **interface gigabitEthernet** *port*

Parâmetro:

» **port:** número da porta Ethernet correspondente.

Modo de Comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: entre no modo de configuração Interface gigabitEthernet e configurar a porta 2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2

8.2. interface range gigabitEthernet

Descrição: o comando **interface range gigabitEthernet** é usado para entrar em um determinado range de interfaces Gigabit e configurar várias portas Gigabit Ethernet ao mesmo tempo.

Sintaxe: **interface range gigabitEthernet** *port-list*

Parâmetros:

» **port-list:** lista das portas Ethernet a serem configuradas.

Modo de Comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: entre no modo de configuração Interface gigabitEthernet e configurar as portas 1, 2, 3, 6, 7 e 9 ao mesmo tempo adicionando-as a uma port-list:

INTELBRAS(config)# interface range gigabitEthernet 1/0/1-3,1/0/6-7,1/0/9

8.3. description

Descrição: o comando **description** é usado para adicionar uma descrição para a porta Ethernet, para limpar a descrição de uma porta utilize o comando **no description**.

Sintaxe: **description** *string*
no description

Parâmetro:

» **string:** descrição da porta com no máximo 16 caracteres.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: descreva a porta 1/0/5 como Port_5.

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# description Port_5

8.4. shutdown

Descrição: o comando **shutdown** é usado para desabilitar uma porta Ethernet. Para habilitar uma porta novamente utilize o comando **no shutdown**.

Sintaxe: **shutdown**
no shutdown

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: desabilite a porta 1/0/3 como Port_5:

INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# shutdown

8.5. flow-control

Descrição: o comando **flow-control** é usado para ativar a função de controle de fluxo para uma porta. Para desabilitar a função de controle de fluxo para a porta correspondente utilize o comando **no flow-control**. Com a função de controle de fluxo ativada, a taxa de entrada e a taxa de saída podem ser sincronizadas para evitar a perda de pacotes na rede.

Sintaxe: **flow-control**
no flow-control

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o controle de fluxo para a porta 1/0/5:

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# flow-control

8.6. duplex

Descrição: o comando **duplex** é usado para configurar o modo duplex para uma porta Ethernet. Para retornar para a configuração padrão utilize o comando **no duplex**.

Sintaxe: **duplex** {auto | full | half}
no duplex

Parâmetro:

» **auto | full | half:** o modo *Duplex* para a porta Ethernet possui três opções: *Negociação automática, Full-duplex* e *Half-duplex*. Por padrão a porta Gigabit está configurada no modo de negociação automática.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo *Duplex* da porta 1/0/3 como full-duplex:

INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# duplex full

8.7. jumbo-size

Descrição: o comando **jumbo-size** é utilizado para especificar o tamanho dos quadros jumbo, jumbo frames.

Sintaxe: **jumbo-size** *size*

Parâmetro:

» **size:** valor para o pacote jumbo. O seu tamanho pode ser entre 1518 e 9216 bytes, por padrão vem configurado como *1518*.

Modo de Comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o tamanho global do pacote jumbo como 9216:

```
INTELBRAS(config)# jumbo-size 9216
```

8.8. speed

Descrição: o comando **speed** é usado para configurar a velocidade da porta Ethernet. Para retornar para a configuração padrão utilize o comando **no speed**.

Sintaxe: **speed** {10 | 100 | 1000 | auto}
no speed

Parâmetro:

» **10 | 100 | 1000 | auto:** a velocidade da porta Ethernet possui quatro opções: *10 Mbps, 100 Mpbs, 1000 Mbps* e *Negociação automática* (padrão).

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a velocidade da porta 1/0/3 como 100 Mbps:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# speed 100
```

8.9. clear counters

Descrição: o comando **clear counters** é usado para limpar as informações estatísticas de todas as portas Ethernet port channels.

Sintaxe: **clear counters**
clear counters interface [gigabitEthernet *port*] [port-channel *port-channel-id*]

Parâmetros:

» **port:** número da porta Ethernet.
» **port-channel-id:** identificação do port channel.

Modo de Comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: limpe as estatísticas de todas as portas e port channels:

```
INTELBRAS# clear counters
```

8.10. show interface status

Descrição: o comando **show interface status** é utilizado para exibir o status de conexão da porta Ethernet e port channel.

Sintaxe: **show interface status** [gigabitEthernet *port*] [port-channel *port-channel-id*]

Parâmetros:

» **port:** número da porta Ethernet.
» **port-channel-id:** identificação do port channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Exiba o status de conexão de todas as portas e port channels:

```
INTELBRAS# show interface status
```

Exibir o status de conexão da porta 1/0/1:

```
INTELBRAS# show interface status gigabitEthernet 1/0/1
```

8.11. show interface counters

Descrição: o comando **show interface counters** é utilizado para exibir as informações de estatísticas de todas as portas Ethernet e port channel.

Sintaxe: **show interface counters** [**gigabitEthernet** *port*] [**port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta Ethernet.
- **port-channel-id**: identificação do port channel.

Modo de Comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Exiba a informação de estatísticas de todas as portas e port channels:

```
INTELBRAS# show interface counters
```

Exiba as estatísticas da porta 1/0/2:

```
INTELBRAS# show interface counters gigabitEthernet 1/0/2
```

8.12. show interface configuration

Descrição: o comando **show interface configuration** é utilizado para exibir as configurações de todas as portas Ethernet e port channel, incluindo seu status, controle de fluxo, modo de negociação e descrição da porta.

Sintaxe: **show interface configuration** [gigabitEthernet *port*] [port-channel *port-channel-id*]

Parâmetros:

- **port:** número da porta Ethernet.
- **port-channel-id:** identificação do port channel.

Modo de Comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as configurações de todas as portas e port channels:

```
INTELBRAS# show interface configuration
```

Exibir as configurações da porta 1/0/2.

```
INTELBRAS# show interface configuration gigabitEthernet 1/0/2
```

9. Comandos para isolamento de portas

O isolamento de porta fornece um método de restringir o fluxo de tráfego para melhorar a segurança da rede, proibindo a porta de encaminhar pacotes para as portas que não estão na lista de portas de encaminhamento.

9.1. port isolation

Descrição: o comando **port isolation** é utilizado para realizar a configuração de uma porta, garantindo que ela somente possa se comunicar com as portas pertencentes sua lista de portas. Para remover a configuração, use o comando **no port isolation**.

Sintaxe: **port isolation** {[**fa-forward-list** *fa-forward-list*] [**gi-forward-list** *gi-forward-list*] [**po-forward-list** *po-forwar-list*] [**te-forwar-list** *te-forward-list*]}
no port isolation

Parâmetros:

- **fa-forward-list gi-forward-list te-forward-list:** lista de portas Ethernets.
- **po-forward-list:** lista de port channels.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Adicione as portas 1, 2, 4 e a port channel 2 na forward list da porta 1/0/5:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# port isolation gi-forward-list 1/0/1-2,1/0/4,po-forward-list 2
```

Adicione todas as port channels na forward list da porta 1/0/2:

```
INTELBRAS(config)#interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# no port isolation
```

9.2. show port isolation interface

Descrição: o comando **show port isolation** interface é utilizado para exibir a forward list da porta ou port channel.

Sintaxe: **show port isolation interface** {[**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]}

Parâmetros:

- **port:** número da porta Ethernet a qual você quer exibir as informações de forward list no formato *1/0/2*.
- **port-channel-id:** identificação do port channel que você quer mostrar as informações da forward list, ranging from 1 to 6.

Modo de Comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Exiba a forward-list da porta 1/0/2.

```
INTELBRAS# show port isolation interface gigabitEthernet 1/0/2
```

Exiba a forward-list de todas as portas e port channels.

```
INTELBRAS# show port isolation interface
```

10. Comandos para detecção de loopback

Com o recurso de detecção de loopback ativado, o switch pode detectar loops usando pacotes de detecção de loopback. Quando um loop é detectado, o switch exibirá um alerta ou bloqueará a porta correspondente de acordo com a configuração.

10.1. loopback-detection (global)

Descrição: o comando de **loopback-detection** é usado para habilitar a função de detecção de loopback globalmente. Para desativá-lo utilize o comando **no loopback-detection**.

Sintaxe: **loopback-detection**
no loopback-detection

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função global de detecção de loopback:

```
INTELBRAS(config)# loopback-detection
```

10.2. loopback-detection interval

Descrição: o comando **loopback-detection interval** é usado para definir o intervalo de envio de pacotes de detecção de loopback das portas do switch para a rede, com o objetivo de detectar periodicamente os loops da rede.

Sintaxe: **loopback-detection interval** *interval-time*

Parâmetro:

» **interval-time:** o intervalo de envio de pacotes de detecção de loopback. Varia de 1 a 1000 segundos. Por padrão, esse valor é *30*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o intervalo de detecção de loopback como 50 segundos:

```
INTELBRAS(config)# loopback-detection interval 50
```

10.3. loopback-detection recovery-time

Descrição: o comando **loopback-detection recovery-time** é usado para configurar o tempo após o qual a porta bloqueada se recuperaria automaticamente para o status normal.

Sintaxe: **loopback-detection recovery-time** *recovery-time*

Parâmetro:

» **recovery-time:** o tempo após o qual a porta bloqueada se recuperaria automaticamente para o status normal e a detecção de loopback seria reiniciada. Ele varia de 2 a 1000000 segundos. Por padrão, esse valor é *90*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o tempo de recuperação para o retorno da verificação de loopback como 70 segundos:

```
INTELBRAS(config)# loopback-detection recovery-time 70
```

10.4. loopback-detection (interface)

Descrição: o comando de **loopback-detection** é usado para habilitar a função de detecção de loopback de uma porta específica. Para desativá-lo utilize o comando **no loopback-detection**.

Sintaxe: **loopback-detection**
no loopback-detection

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a detecção de loopback nas portas 1-3:

INTELBRAS(config)# interface range gigabitEthernet 1/0/1-3
INTELBRAS(config-if-range)# loopback-detection

10.5. loopback-detection config process-mode

Descrição: o comando **loopback-detection config process-mode** é usado para configurar o modo de processo para as portas pelas quais o switch lida com os loops detectados. Você também precisa configurar o modo de recuperação para remover o status do bloco da porta ou da VLAN quando o modo de processo for Baseado em porta ou Baseado em VLAN.

Sintaxe: **loopback-detection config process-mode** {alert | port-based | valan-based}
recovery-mode {auto | manual}

Parâmetros:

- **alert:** quando um loop é detectado, o switch enviará uma mensagem de interceptação e gerará uma entrada no log. Esta é a configuração padrão.
- **port-based:** quando um loop é detectado, o switch enviará uma mensagem de interceptação e gerará uma entrada no log, além disso, o switch bloqueará a porta.
- **vlan-based:** quando um loop é detectado, o switch enviará uma mensagem de interceptação e gerará uma entrada no log, além disso, o switch bloqueará a VLAN na qual o loop é detectado e somente os pacotes da VLAN bloqueada não poderão passar pela porta.
- **auto:** o bloqueio pode ser removido automaticamente após o tempo de recuperação previamente estabelecido.
- **manual:** o bloqueio só poderá ser removido manualmente.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e usuário avançado têm acesso a esses comandos.

Exemplo: configure o modo do processo de detecção de loopback como port-based e configure o modo de recuperação como manual para a porta 2.

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# loopback-detection config process-mode port-based
recovery-mode manual

10.6. loopback-detection recover

Descrição: o comando **loopback-detection recover** é usado para remover o status de bloqueio das portas selecionadas, recuperando as portas bloqueadas para o status normal.

Sintaxe: **loopback-detection recover**

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: recupere a porta bloqueada 1/0/2 para o status normal:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if-range)# loopback-detection recover

10.7. show loopback-detection global

Descrição: o comando **show loopback-detection global** é usado para exibir a configuração global da função de detecção de loopback, como status global de detecção de loopback, intervalo de detecção de loopback e tempo de recuperação de detecção de loopback.

Sintaxe: **show loopback-detection global**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração da detecção de loopback global:

```
INTELBRAS# show loopback-detection global
```

10.8. show loopback-detection interface

Descrição: o comando **show loopback-detection interface** é usado para exibir a configuração da função de detecção de loopback e o status de uma determinada porta.

Sintaxe: **show loopback-detection interface** [**gigabitEthernet** *port* | **port-channel** *lagid*] [**detail**]

Parâmetros:

- **port:** número da porta Ethernet.
- **lagid:** número do LAG, varia de 1 até 14.
- **detail:** exibe o status do loop e o status do bloqueio da VLAN à qual a porta especificada pertence.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Exiba a configuração da detecção de loopback e o status de todas as portas:

```
INTELBRAS#show loopback-detection interface
```

Exiba a configuração da detecção de loopback e o status da porta 5:

```
INTELBRAS#show loopback-detection interface gigabitEthernet 1/0/5
```

11. Comandos Etherchannel

Os comandos Etherchannel são usados para configurar a função LAG e LACP.

LAG (*Link Aggregation Group*) serve para combinar um número de portas para criar um único caminho de dados de alta capacidade de banda. A capacidade de banda do LAG é a soma da largura de banda das suas portas que a compõem.

O LACP (*Link Aggregation Control Protocol*) é definido no IEEE802.3ad e permite o dinamismo do Link Aggregation trocando pacotes LACP com seus componentes. O switch pode agrupar dinamicamente portas configuradas em um único link lógico, o que aumentará a largura de banda e equilibrará de maneira flexível a carga.

11.1. channel-group

Descrição: o comando **channel-group** é usado para adicionar uma porta ao Grupo EtherChannel e configurar seu modo. Para excluir a porta do Grupo EtherChannel utilize o comando **no channel-group**.

Sintaxe: **channel-group** *num* **mode** {on | active | passive}
no channel-group

Parâmetros:

- **num:** número do grupo EtherChannel correspondente, varia de 1 até 14.
- **on:** ativa o LAG estático.
- **active:** ativa o modo *LACP ativo*.

» **passive:** ativa o modo *LACP passivo*.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: adicione as portas 2-4 ao grupo 1 do EtherChannel e ative o LAG estático:

```
INTELBRAS(config)#interface range gigabitEthernet 1/0/2-4
INTELBRAS(config-if-range)#channel-group 1 mode on
```

11.2. port-channel load-balance

Descrição: o comando **port-channel load-balance** é usado para configurar o balanceamento de carga para o LAG. Para retornar às configurações padrão utilize o comando **no port-channel load-balance**.

Sintaxe: **port-channel load-balance** {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip}
no port-channel load-balance

Parâmetros:

» **src-mac:** endereço MAC de origem. Quando esta opção é selecionada, o balanceamento de carga será baseado no endereço MAC de origem dos pacotes.

» **dst-mac:** endereço MAC de destino. Quando esta opção é selecionada, o balanceamento de carga será baseado no endereço MAC de destino dos pacotes.

» **src-dst-mac:** endereço MAC de origem e destino. Quando esta opção é selecionada, o balanceamento de carga será baseado no endereço MAC de origem e destino dos pacotes.

» **src-ip:** endereço IP de origem. Quando esta opção é selecionada, o balanceamento de carga será baseado no endereço IP de origem dos pacotes.

» **dst-ip:** endereço IP de destino. Quando esta opção é selecionada, o balanceamento de carga será baseado no endereço IP de destino dos pacotes.

» **src-dst-ip:** endereço IP de origem e destino. Quando esta opção é selecionada, o balanceamento de carga será baseado nos endereços IP de origem e destino dos pacotes.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o balanceamento de carga para o LAG como "src-dst-ip":

```
INTELBRAS(config)# port-channel load-balance src-dst-ip
```

11.3. lacp system-priority

Descrição: o comando **lacp system-priority** é usado para configurar globalmente a prioridade do sistema LACP. Para retornar às configurações padrão, **no lacp system-priority.**

Sintaxe: **lacp system-priority** *pri*
no lacp system-priority

Parâmetro:

» **pri:** prioridade do sistema, varia de 0 até 65535. *32768* é a configuração padrão.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o a prioridade do sistema LACP como 1024 de forma global:

```
INTELBRAS(config)# lacp system-priority 1024
```

11.4. lacp port-priority

Descrição: o comando **lacp port-priority** é usado para configurar a prioridade para as portas especificadas do LACP. Para retornar às configurações padrão, **no lacp port-priority.**

Sintaxe: **lacp port-priority** *pri*
no lacp port-priority

Parâmetro:

» **pri:** prioridade do sistema, varia de 0 até 65535. *32768* é a configuração padrão.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Configure o a prioridade do systema LACP como 1024 para as portas 1-3:

INTELBRAS(config)# interface range gigabtiEthernet 1/0/1-3
INTELBRAS(config-if-range)# lacp port-priority 1024

Configure o a prioridade do systema LACP como 2048 para a porta 4:

INTELBRAS(config)# interface range gigabtiEthernet 1/0/4
INTELBRAS(config-if)# lacp port-priority 2048

11.5. show etherchannel

Descrição: o comando **show etherchannel** é usado para mostrar as informações de EtherChannel.

Sintaxe: **show etherchannel** [*channel-group-num*] {detail | summary}

Parâmetros:

» **channel-group-num:** número do grupo do EtherChannel, varia entre 1 e 14, definida como *vazio* por padrão e irá mostrar a informação de todas as portas.
» **detail:** informação detalhada do EtherChannel.
» **summary:** informação em sumário do EtherChannel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostrar as informações detalahadas do grupo 1 do EtherChannel:

INTELBRAS(config)# show etherchannel 1 detail

11.6. show etherchannel load-balance

Descrição: o comando **show etherchannel load-balance** é usado para mostrar as informações de Aggregate Arithmeetic do LAG.

Sintaxe: **show etherchannel load-balance**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o balanceamento de carga do LAG:

INTELBRAS(config)# show etherchannel load-balance

11.7. show lacp

Descrição: o comando **show lacp** é usado para mostrar as informações de LACP para um grupo específico de EtherChannel.

Sintaxe: **show lacp** [*channel-group-num*] {internal | neighbor}

Parâmetros:

- **channel-group-num:** número do grupo do EtherChannel, varia entre 1 e 14, definida como *vazio* por padrão e irá mostrar a informação de todas as portas.
- **internal:** informação interna do LACP.
- **neighbor:** informação da vizinhança do LACP.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as informações internas do LACP do grupo 1 do EtherChannel.

INTELBRAS(config)# show lacp 1 internal

11.8. show lacp sys-id

Descrição: o comando **show lacp sys-id** é usado para mostrar a prioridade do sistema LACP de forma global.

Sintaxe: **show lacp sys-id**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre prioridade do systema LACP:

INTELBRAS(config)# show lacp sys-id

12. Comandos MAC address

A configuração do endereço MAC pode melhorar a segurança da rede, configurando a segurança da porta e mantendo as informações de endereço, gerenciando a tabela de endereços.

12.1. mac address-table static

Descrição: o comando **mac address-table static** é usado para adicionar a entrada de endereço MAC estático. Para remover a entrada correspondente, utilize o comando **no mac address-table static**. O endereço estático pode ser adicionado ou removido manualmente, independentemente do aging-time. Nas redes estáveis, as entradas de endereços MAC estáticos podem facilitar a troca para reduzir os pacotes de transmissão e aumentar a eficiência do encaminhamento de pacotes notavelmente.

Sintaxe: **mac address-table static** *mac-addr* **vid** *vid* **interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **tem-gigabitEthernet** *port*}
no mac address-table static *mac-addr* **vid** *vid* **interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **tem-gigabitEthernet** *port*}

Parâmetros:

- **mac-addr:** endereço MAC desejável para adição à tabela.
- **vid:** ID da VLAN desejada, varia de 1 à 4094.
- **por:** número da porta a qual deseja realizar a entrada.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: adicione um endereço MAC estático e acorrente o MAC 00:02:58:4f:6c:23 à VLAN1 e a porta 1:

INTELBRAS(config)#mac address-table static 00:02:58:4f:6c:23 **vid 1 interface gigabitEthernet** 1/0/1

12.2. mac address-table aging-time

Descrição: o comando **mac address-table aging-time** é utilizado para determinar o tempo de validade do endereço dinâmico. Para retornar para a configuração padrão utilize o comando **no mac address-table aging-time**.

Sintaxe: **mac address-table aging** *aging-time*
no address-table aging aging-time

Parâmetro:

» **aging-time:** o aging-time para o endereço dinâmico. O valor pode ser 0 ou varia de 10 a 630 segundos. Quando 0 é inserido, a função *Envelhecimento automático* é desativada. É *300* por padrão.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o aging-time como 500 segundos:

INTELBRAS(config)# mac addresss-table aging-time 500

12.3. mac address-table filtering

Descrição: o comando **mac address-table filtering** é usado para evitar que o endereço seja salvo na tabela MAC. Para excluir a entrada correspondente, utilize o comando **no mac address-table filtering**. A função da filtragem é proibir o encaminhamento de pacotes indesejados. A filtragem pode ser adicionada ou removida manualmente, independente do aging-time.

Sintaxe: **mac address-table filtering** *mac-addr* **vid** *vid*
no address-table filtering {[*mac-addrl*] [**vid** *vid*]}

Parâmetros:

» **mac-addr:** endereço MAC desejável para adição à tabela.
» **vid:** ID da VLAN desejada, varia de 1 à 4094.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: adicione ao filtro de endereço a entrada a qual a VLAN ID é 1 e o endereço 00:1e:4b:04:01:5d:

INTELBRAS(config)# mac addresss-table filtering 00:1e:4b:04:01:5d **vid** 1

12.4. mac address-table max-mac-count

Descrição: o comando **mac address-table max-mac-count** é usado para configurar a segurança da porta. Para retornar às configurações padrões utilize o comando **no mac address-table max-mac-count**. A função do Port Security é proteger o switch do ataque de endereço MAC malicioso, limitando o número máximo de endereços MAC que podem ser aprendidos na porta. A porta com o recurso Port Security ativado aprenderá o endereço MAC dinamicamente. Quando o número do endereço MAC aprendido atingir o máximo, a porta parará de aprender. Portanto, os outros dispositivos com o endereço MAC desaprendido não podem acessar a rede através desta porta.

Sintaxe: **mac address-table max-mac-count** {[max-number *num*] [**mode** {dynamic | static | permanent}] [**status** {forward | drop | disable}]
no mac address-table max-mac-count [max-number | mode | status]

Parâmetro:

» **num:** número máximo de endereços MAC que podem ser aprendidos pela porta, varia de 0 até 64, definida como *64* por padrão.
» **Dynamic | static | permanent:** tipo de aprendizagem dos endereços MAC. Existem três modos. Quando o modo *Dinâmico* é selecionado, o endereço MAC aprendido será excluído automaticamente após aging-time. Quando o modo *Estático* estiver selecionado, o endereço MAC aprendido ficará fora da influência do aging-time e só poderá ser excluído manualmente. As entradas aprendidas serão apagadas depois que o switch for reinicializado. Quando o modo *Permanente* é selecionado, o endereço MAC aprendido ficará fora da influência do aging-time e só poderá ser excluído manualmente também. No entanto, as entradas aprendidas serão salvas até que o switch seja reinicializado.

» **status:** seleciona a ação que deve ser tomada quando o número de endereços MAC máximo é alcançado, por padrão está função vem desabilitada.
  » **forward:** o pacote será encaminhado mas o endereço MAC não será aprendido quando o número exceder o máximo definido para esta porta.
  » **drop:** o pacote será recusado quando o número exceder o máximo definido para esta porta.
  » **disable:** o limite de endereços MAC que podem ser aprendidos não está habilitado para esta porta.
» **New-mac-learned *enable* | *disable*:** habilita / desabilita a notificação de new-mac-learn para esta porta. Com esse recurso ativado, uma notificação SNMP é gerada e enviada ao sistema de gerenciamento de rede quando a porta aprende um novo endereço MAC.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de Port Security para a porta 1/0/1, configure-a como modo estático para modo de aprendizado, especifique o número máximo de endereços MAC que esta porta pode aprender como 30. E quando o número máximo é alcançado a nova entrada deve ser rejeitada:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# mac address-table max-mac-count max-number 30 mode static status drop
```

12.5. show mac address-table

Descrição: o comando **show mac address-table** é usado para mostrar as informações de todas as entradas da tabela.

Sintaxe: **show mac address-table** {dynamic | static | filtering}

Parâmetros:

» **dynamic | static | filtering:** tipo de entrada que você deseja consultar. Por padrão todas as entradas são exibidas.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as informações de todas as entradas de endereço:

```
INTELBRAS# show mac address-table
```

12.6. clear mac address-table

Descrição: o comando **clear mac address-table** é usado para mostrar as informações de todas as entradas da tabela.

Sintaxe: **clear mac address-table** {dynamic | static | filtering}

Parâmetros:

» **dynamic | static | filtering:** tipo de entrada que você deseja consultar.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: limpe todas as entradas estáticas da tabela:

```
INTELBRAS# clear mac address-table static
```

12.7. show mac address-table aging-time

Descrição: o comando **show mac address-table aging-time** é usado para mostrar as informações de aging time dos endereços MAC.

Sintaxe: **show mac address-table aging-time**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o aging-time dos endereços MAC:

```
INTELBRAS# show mac address-table aging-time
```

12.8. show mac address-table max-mac-count

Descrição: o comando **show mac address-table max-mac-count interface gigabitEthernet** é usado para mostrar as informações da configuração de segurança de todas as portas ou uma em específico.

Sintaxe: **show mac address-table max-mac-count** {all | **interface gigabitEthernet** *port*}

Parâmetros:

- **all:** mostra informações de segurança de todas as portas.
- **port:** número da porta Ethernet específica.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Mostre configuração de segurança de todas as portas.

```
INTELBRAS# show mac address-table max-mac-count all
```

Mostre configuração de segurança da porta 1/0/1.

```
INTELBRAS# show mac address-table max-mac-count interface gigabitEthernet 1/0/1
```

12.9. show mac address-table interface

Descrição: o comando **show mac address-table interface** é usado para mostrar as informações de entrada de tabela para uma porta ou port channel específicos.

Sintaxe: **show mac address-table interface** {**gigabitEthernet** *port* | **port-channel** *port-channel-id*}

Parâmetros:

- **port:** número da porta Ethernet desejada.
- **port-channel-id:** identificação da port channel desejada.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações de endereçamento da porta 1/0/1:

```
INTELBRAS# show mac address-table interface gigabitEthernet 1/0/1
```

12.10. show mac address-table count

Descrição: o comando **show mac address-table count** é usado para mostrar o total de endereços MAC aprendidos.

Sintaxe: **show mac address-table count** {**vlan** *vlan-id*}

Parâmetro:

- **vlan-id:** especifica a VLAN à qual a entrada MAC pertence.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o total de entradas MAC de diferentes VLANs:

```
INTELBRAS# show mac address-table count
```

12.11. show mac address-table address

Descrição: o comando **show mac address-table address** é usado para mostrar as informações de um endereço MAC específico.

Sintaxe: **show mac address-table address** *mac-addr* [**interface** {**gigabitEthernet** *port* | **port-channel** *port-channel-id*}| **vid** *vlan-id*]

Parâmetros:

- **mac-addr:** endereço do MAC a ser consultado.
- **port:** número da porta Ethernet.
- **port-channel-id:** ID da port channel desejada.
- **vlan-id:** especifica a VLAN a qual a entrada pertence.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações do endereço MAC 00:00:00:00:23:00 na VLAN 1:

```
INTELBRAS# show mac address-table address 00:00:00:00:23:00 vid 1
```

12.12. show mac address-table vlan

Descrição: o comando **show mac address-table vlan** é usado para mostrar as informações de tabela MAC de uma VLAN específica.

Sintaxe: **show mac address-table** vid

Parâmetro:

- **vid:** especifica a VLAN a qual a entrada pertence.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações de endereço MAC da VLAN 1:

```
INTELBRAS# show mac address-table vid 1
```

13. Comandos IEEE802.1Q VLAN

A tecnologia VLAN (*Virtual Local Area Network*) foi desenvolvida para que o switch possa dividir a rede local em múltiplas redes locais lógicas flexíveis. Hosts nos na mesma VLAN podem se comunicar entre si, independentemente de seus locais físicos. A VLAN pode melhorar o desempenho economizando largura de banda e melhorando a segurança, limitando o tráfego a domínios específicos.

13.1. vlan

Descrição: o comando **vlan** é utilizado para criar uma VLAN no padrão *IEEE 802.1q* e entrar no modo *VLAN* de configuração. Para deletar uma VLAN utilize o comando **no vlan**.

Sintaxe: **vlan** *vlan-list*
no vlan *vlan-list*

Parâmetro:

- **vlan-list:** especifica a identificação da VLAN no padrão *IEEE 802.1q,* valores variam entre 2 e 4094, no formato *2-3, 5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Crie a VLAN 2-10 e a VLAN 100:

```
INTELBRAS(config)# vlan 2-10,100
```

Exclua a VLAN 2:

```
INTELBRAS(config)# no vlan 2
```

13.2. name

Descrição: o comando **name** é utilizado para adicionar uma descrição para a VLAN. Para limpar a descrição utilize o comando **no name.**

Sintaxe: **name** *description*
no name

Parâmetro:

» **description:** campo para descrição da VLAN com até 16 caracteres.

Modo de comando: VLAN Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o nome da VLAN 2 como "grupo1":

INTELBRAS(config)# vlan 2
INTELBRAS(config-vlan)# name grupo1

13.3. switchport general allowed vlan

Descrição: o comando **switchport general allowed vlan** é utilizado para adicionar uma porta à VLAN correspondente. Para remover uma porta da referida VLAN utilize o comando **no switchport general allowed vlan**.

Sintaxe: **switchport general allowed vlan** *vlan-list* {tagged | untagged}
no switchport general allowed vlan *vlan-list*

Parâmetros:

» **vlan-list:** identificação da VLAN ou lista de VLANs, varia entre 2 e 4094, no formato *1-3, 5*.

» **tagged | untagged:** regra de ingresso. Tagged significa que a porta enviará um pacote com um cabeçalho que possui uma tag com um número que corresponde ao número do cabeçalho da VLAN. Untagged não possui tal especificação no cabeçalho.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure e adicione a porta 1/0/4 com o tipo de link "general" na VLAN 2 com a regra de ingresso tagged:

INTELBRAS(config)# interface gigabitEthernet 1/0/4
INTELBRAS(config-if)# switchport mode general
INTELBRAS(config-if)# switchport general allowed vlan 2 tagged

13.4. switchport pvid

Descrição: o comando **switchport pvid** é utilizado para configurar o PVID (VLAN nativa) para as portas do switch.

Sintaxe: **switchport pvid** *vlan-id*

Parâmetro:

» **vlan-id:** identificação da VLAN, varia entre 1 e 4094.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o PVID para a porta 1/0/2 como 2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# swtichport pvid 2

13.5. switchport check ingress

Descrição: o comando **switchport check ingress** é utilizado para habilitar a função de Ingress Checking (verificação de ingresso) para as portas do switch. Com essa função ativa, as portas somente aceitarão pacotes das VLANs as quais estão em sua lista de VLANs e descartará os outros pacotes. Com essa função desabilitada a porta irá encaminhar os pacotes diretamente. Para desativar esta função utilize o comando **no switchport check ingress.**

Sintaxe: **switchport check ingress**
no switchport check ingress

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de Ingress Checking para 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# switchport check ingress

13.6. switchport acceptable frame

Descrição: o comando **switchport acceptable frame** é utilizado para especificar o tipo de quadro que será aceito para as portas do switch e as portas executarão essa operação antes do Ingress Checking. Para retornar essa configuração para o valor padrão utilize o comando **no switchport acceptable frame**.

Sintaxe: **switchport acceptable frame** {all | tagged}
no switchport acceptable frame

Parâmetro:

» **all | tagged:** tipo de quadro aceitável.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o tipo de quadros aceitos para a porta 1/0/4 como "tagged":

INTELBRAS(config)# interface gigabitEthernet 1/0/4
INTELBRAS(config-if)# switchport acceptable frame tagged

13.7. show vlan summary

Descrição: o comando **show vlan summary** é utilizado para mostrar a informação resumida das VLANs do tipo IEEE 802.1Q.

Sintaxe: **show vlan summary**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba o resumo das informações das VLAN do tipo IEEE 802.1Q:

INTELBRAS# show vlan summary

13.8. show vlan brief

Descrição: o comando **show vlan brief** é utilizado para mostrar a informações simplificadas das VLANs do tipo IEEE 802.1Q.

Sintaxe: **show vlan brief**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: exiba o resumo das informações das VLAN do tipo IEEE 802.1Q:

INTELBRAS# show vlan brief

13.9. show vlan

Descrição: o comando **show vlan** é utilizado para mostrar a informação detalhada de uma VLAN específica ou todas.
Sintaxe: **show vlan** [**id** *vland-id*]

Parâmetro:

» **vlan-id:** especifica a VLAN a ser exibida, valores variam entre 1 e 4094. É um comando multiopção. Utilizando o comando sem parâmetro mostrará as informações detalhadas de todas as VLANs.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações da VLAN 5:

```
INTELBRAS# show vlan 5
```

13.10. show interface switchport

Descrição: o comando **show interface switchport** é utilizado para mostrar a informação de configuração de VLAN para uma porta/port channel específico.

Sintaxe: **show interface switchport** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

» **port:** número da porta.
» **port-channel-id:** número do port channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba a informação de configuração de todas as portas e port channels da VLAN:

```
INTELBRAS# show interface switchport
```

14. Comandos VLAN baseados em MAC

MAC VLAN é a maneira de classificar as VLANs de acordo com o endereço MAC dos dispositivos, vinculando o endereço MAC com o VLAN ID desejado. Os pacotes originados destes endereços MAC serão marcados com o VLAN ID correspondente.

14.1. mac-vlan mac-address

Descrição: o comando **mac-vlan mac-address** é utilizado para criar uma VLAN baseada em um endereço MAC. Para deletar utilize o comando **no mac-vlan mac-address**.

Sintaxe: **mac-vlan mac-address** *mac-addr* **vlan** *vlan-id* [**description** *descript*]
no mac-vlan mac-address *mac-addr*

Parâmetros:

» **mac-addr:** endereço MAC no formato *XX:XX:XX:XX:XX:XX*.
» **vlan-id:** especifica a identificação da VLAN, valores variam entre 1 e 4094.
» **descript:** descrição para identificação do endereço MAC com no máximo 8 caracteres.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie a VLAN 2 com o endereço MAC 00:11:11:01:01:12 com o nome "grupo1":

```
INTELBRAS(config)# mac-vlan mac-address 00:11:11:01:01:12 vlan 2 description grupo1
```

14.2. mac-vlan

Descrição: o comando **mac-vlan** é utilizado para habilitar o MAC-VLAN na porta. Somente as portas com a função mac-vlan ativas podem ser configuradas com as função de MAC-VLAN. Para desabilitar essa função utilize o comando **no mac-vlan**. Por padrão todas as portas vêm com essa função desabilitada.

Sintaxe: **mac-vlan**
no mac-vlan

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de MAC-VLAN para a porta gigabit 1/0/3:

INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# mac-vlan

14.3. show mac-vlan

Descrição: o comando **show mac-vlan** é utilizado para mostrar a informação detalhada de MAC-VLAN específica ou todas. O endereço MAC e a VLAN ID podem ser utilizadas como filtro na hora que mostrar as informações.

Sintaxe: **show mac-vlan** {**all** | **mac-address** *mac-addr* | **vlan** *vlan-id*}

Parâmetros:

- **mac-addr:** endereço MAC no formato *XX:XX:XX:XX:XX:XX*.
- **vlan-id:** especifica a VLAN a ser exibida, valores variam entre 1 e 4094.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações de todas as MAC-VLAN:

INTELBRAS# show mac-vlan all

14.4. show mac-vlan interface

Descrição: o comando **show mac-vlan interface** é utilizado para mostrar os status das portas com MAC-VLAN.

Sintaxe: **show mac-vlan interface**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba o status de todas as portas com MAC-VLAN:

INTELBRAS# show mac-vlan interface

15. Comandos VLAN baseados em protocolos

Protocolo de VLAN (*Virtual Local Area Network*) é o modo de classificar as VLANs baseadas em protocolos. Cada VLAN permite somente um tipo de protocolo.

15.1. protocol-vlan template

Descrição: o comando **protocol-vlan** é utilizado para adicionar ou remover um modelo de VLAN baseada em protocolo. Para deletar este modelo utilize o comando **no protocol-vlan template mac-address**.

Sintaxe: **protocol-vlan template name** *protocol-name* **frame** {**ether_2 ether-type** *type* | **snap ether-type** *type* | **llc dsap** *dsap-type* **ssap** *ssap-type*}
no protocol-vlan template *template-idx*

Parâmetros:

- **Protocol-name:** nome para o template ao qual a VLAN será baseada com até 8 caracteres.
- **ether_2 ether-type type:** especifica o tipo do pacote Ethernet.
- **snap ether-type type:** especifica o tipo do pacote Ethernet.
- **llc dsap dsap-type ssap ssap-type:** especifica o tipo do DSAP e o tipo do SSAP.
- **template-idx:** número do modelo da VLAN baseada em protocolo. Você pode descobrir o número correspondente do modelo utilizando o comando s**how protocol-vlan template**.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie um modelo para a VLAN baseada em protocolo com o nome "grupo1", com o protocolo Ethernet do tipo 0x2024:

```
INTELBRAS(config)# protocol-vlan template name grupo1 frame ether_2 ether-type 2024
```

15.2. protocol-vlan vlan

Descrição: o comando **protocol-vlan vlan** é utilizado para criar um entrada para uma VLAN baseada em protocolo. Para excluir uma entrada utilize o comando **no protocol-vlan vlan**.

Sintaxe: **protocol-vlan vlan** *vlan-id* **priority** *priority* **template** *template-idx*
no protocol-vlan vlan *group-idx*

Parâmetros:

- **vlan-id:** identificação da VLAN, varia entre 1 e 4094, no formato *1-3, 5*.
- **priority:** especifique a prioridade 802.1p para os pacotes que pertencem ao protocolo VLAN, variando de 0 a 7. O switch determinará a sequência de encaminhamento de acordo com esse valor. Pacotes com maior valor possuem maior prioridade.
- **template-idx:** número do modelo da VLAN baseada em protocolo. Você pode descobrir o número correspondente do modelo utilizando o comando **show protocol-vlan template**.
- **group-idx:** número da entrada da VLAN baseada em protocolo. Você pode descobrir o número correspondente do modelo utilizando o comando **show protocol-vlan vlan**.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie a VLAN 2 baseada em protocolo e vincule ao modelo 3:

```
INTELBRAS(config)# protocol-vlan vlan 2 template 3
```

15.3. protocol-vlan group

Descrição: o comando **protocol-vlan group** é utilizado para adicionar uma porta a um grupo de protocolo específico. Para remover a porta desse grupo utilize o comando **no protocol-vlan group**.

Sintaxe: **protocol-vlan group** *index*
no protocol-vlan group *index*

Parâmetro:

» **index:** especifica a ID do grupo de protocolo.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: adicione a porta 20 ao grupo de protocolo grupo 1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/20
INTELBRAS(config-if)# protocol-vlan group 1
```

15.4. show protocol-vlan template

Descrição: o comando **show protocol-vlan template** é usado para exibir as informações dos templates VLAN baseados em protocolo.

Sintaxe: **show protocol-vlan template**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações dos templates VLAN baseadas em protocolo:

```
INTELBRAS# show protocol-vlan template
```

15.5. show protocol-vlan vlan

Descrição: o comando **show protocol-vlan vlan** é usado para exibir as informações da VLAN baseados em protocolo.
Sintaxe: **show protocol-vlan vlan**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações das entradas da VLAN baseada em protocolo:

```
INTELBRAS# show protocol-vlan vlan
```

16. Comandos GVRP

GVRP (*GARP VLAN registration protocol*) é uma implementação do GARP (*Generic Atribute Registration Protocol*). GVRP permite que o switch adicione ou remova automaticamente as VLANs por meio das informações de registro de VLAN dinâmica e propagar as informações de registro de VLAN locais para outros switches, sem ter que configurar individualmente cada VLAN.

16.1. gvrp

Descrição: o comando **gvrp** é utilizado para habilitar a função de GVRP de forma global. Para desabilitar o GVRP utilize o comando **no gvrp**.

Sintaxe: **gvrp**
no gvrp

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o GVRP de forma global:

```
INTELBRAS(config)# gvrp
```

16.2. gvrp (interface)

Descrição: o comando **gvrp** é utilizado para habilitar a função de GVRP para uma porta. Para desabilitar utilize o comando **no gvrp**. O GVRP só pode ser habilitado para portas do tipo trunk-type.

Sintaxe: **gvrp**
no gvrp

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o GVRP para as portas 1/0/2-6:

INTELBRAS(config)# interface range gigabitEthernet 1/0/2-6
INTELBRAS(config-if-rangef)# gvrp

16.3. gvrp registration

Descrição: o comando **gvrp registration** é utilizado para configurar o tipo de registro do GVRP para a porta especificada. Para retornar a configuração para o padrão utilize o comando **no gvrp registration**.

Sintaxe: **gvrp registration** {normal | fixed | forbidden}
no gvrp registration

Parâmetros:

» **normal | fixed | forbidden:** modo de registro. Por padrão o modo de registro é *normal*. Neste modo, a porta pode adicionar, remover e propagar VLANs dinâmicas e estáticas.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de registro do GVRP como "fixo" para as portas 1/0/2-6:

INTELBRAS(config)# interface range gigabitEthernet 1/0/2-6
INTELBRAS(config-if-rangef)# gvrp registration fixed

16.4. gvrp timer

Descrição: o comando **gvrp timer** é usado para determinar o temporizador GVRP para a porta. Para voltar a configuração para o valor padrão utilize o comando **no gvrp timer**.

Sintaxe: **gvrp timer** {leaveall | join | leave} *value*
no gvrp timer [leaveall | join | leave]

Parâmetros:

» **leaveall | join | leave:** existem 3 temporizadores: *all*, *join* e *leave*. Uma vez que o timer LeaveAll é definido, a porta com GVRP habilitada pode enviar uma mensagem LeaveAll após o tempo limite do temporizador, para que outras portas GARP possam registrar novamente todas as informações de atributo. Depois disso, o timer LeaveAll começará a iniciar um novo ciclo. Para garantir a transmissão das mensagens de associação, uma porta GARP envia cada mensagem de associação duas vezes. O Join Timer é usado para definir o intervalo entre as duas operações de envio de cada mensagem de associação. Uma vez que o temporizador Leave estiver definido, a porta GARP receberá uma mensagem leave e iniciará seu Leave timer e cancelará o registro das informações de atributo se ele não receber uma mensagem de associação novamente antes que o tempo limite esgote.

» **value:** é o valor do timer. LeaveAll varia entre 1000 e 30000 centésimos de segundo, por padrão vem definido como *1000 centésimos de segundo*. O temporizador do Join varia entre 20 e 1000 centésimos de segundos e por padrão vem defino como *20 centésimos de segundo*. O temporizador do Leave varia entre 60 e 3000 centésimos de segundo e por padrão vem configurado como *60 centésimos de segundo*.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo; configure o temporizador leaveall do GARP para a porta 1/0/6 como 2000 centésimos de segundo e defina o temporizador do join com o valor padrão:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/6
INTELBRAS(config-if)# gvrp timer leaveall 2000
INTELBRAS(config-if)# no gvrp timer join
```

16.5. show gvrp interface

Descrição: o comando **show gvrp interface** é usado para exibir as configurações GVRP para uma porta específica ou para todas as portas.

Sintaxe: **show gvrp interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta.
- **port-channel-id:** número do port channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo:

Exiba as informações de GVRP da porta gigabit Ethernet 1:

```
INTELBRAS# show gvrp interface gigabitEthernet 1/0/1
```

Exiba as informações de GVRP de todas as portas Ethernet:

```
INTELBRAS# show gvrp interface
```

16.6. show gvrp global

Descrição: o comando **show gvrp global** é usado para exibir as o status global do GVRP.

Sintaxe: **show gvrp global**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba o status global do GVRP.

```
INTELBRAS# show gvrp global
```

17. Comandos IGMP Snooping

O Snooping IGMP (*Internet Group Management Protocol Snooping*) é um mecanismo de controle de multicast executado em switches da camada 2. Ele pode efetivamente impedir que grupos de multicast sejam transmitidos na rede.

17.1. ip igmp snooping (global)

Descrição: o comando **ip igmp snooping** é usado para configurar o IGMP Snooping. Para desabilitar a função IGMP Snooping, por favor, use o comando **no ip igmp snooping**.

Sintaxe: **ip igmp snooping**
no ip igmp snooping

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o IGMP Snooping:

```
INTELBRAS(config)# ip igmp snooping
```

17.2. ip igmp snooping version

Descrição: o comando **ip igmp snooping version** é usado para configurar a versão do IGMP. Para retornar à configuração padrão, por favor use o **no comando ip igmp snooping version**.

Sintaxe: **ip igmp snooping version** {v1 | v2 | v3}
no ip igmp snooping version

Parâmetros:

- **v1 | v2 | v3:** especifique a versão do IGMP. Por padrão, é o *IGMP v3*.
  - **v1:** o switch funciona como um comutador IGMPv1 Snooping. Só pode processar mensagens IGMPv1 do host. Mensagens de relatório de outras versões são ignoradas.
  - **v2:** o switch funciona como um comutador IGMPv2 Snooping. Pode processar mensagens IGMPv1 e IGMPv2 do host. Mensagens IGMPv3 são ignoradas.
  - **v3:** o switch funciona como um comutador IGMPv3 Snooping. Pode processar mensagens IGMPv1, IGMPv2 e IGMPv3 do host.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a versão 2 do IGMP Snooping:

```
INTELBRAS (config)# ip igmp snooping version v2
```

17.3. ip igmp snooping drop-unknown

Descrição: o comando **ip igmp snooping drop-unknown** é usado para descartar multicast desconhecidos que não estejam configurados na Tabela. Por padrão, é o *Forward* ou seja, o switch encaminhará o fluxo multicast como broadcast. Para retornar à configuração padrão, use o comando **no ip igmp snooping drop-unknown**.

Sintaxe: **ip igmp snooping drop-unknown**
no ip igmp snooping drop-unknown

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure para que pacotes multicast desconhecidos sejam descartados:

```
INTELBRAS(config)# ip igmp snooping drop-unknown
```

17.4. ip igmp snooping header-validation

Descrição: o comando **ip-igmp snooping header-validation** é usado para habilitar a validação de cabeçalho IGMP globalmente. Para desabilitar a função de *Validação de cabeçalhos IGMP*, por favor, use o comando **no ip igmp snooping header-validation**. Geralmente, para pacotes IGMP, o valor TTL deve ser 1, o campo *ToS* deve ser 0xC0 e a opção *Alerta do roteador* deve ser 0x94040000. Os campos a serem validados dependem da versão do IGMP que está sendo usada. O IGMPv1 apenas verifica o campo *TTL*. O IGMPv2 verifica o campo *TTL* e a opção *Alerta do roteador*. O IGMPv3 verifica o campo *TTL*, o campo *ToS* e a opção Alerta do roteador. Pacotes que falharem no processo de validação serão descartados.

Sintaxe: **ip igmp snooping header-validation**
no ip igmp snooping header-validation

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o IGMP header validation:

```
INTELBRAS(config)# ip igmp snooping header-validation
```

17.5. ip igmp snooping vlan-config

Descrição: o comando **ip igmp snooping vlan-config** é usado para habilitar a função *VLAN IGMP Snooping* ou para modificar os parâmetros de IGMP Snooping. Para desabilitar a função do IGMP Snooping VLAN, por favor, use o comando **no ip igmp snooping vlan-config**. Para restaurar os valores padrões, por favor, use o comando **no ip igmp snooping vlan-config** com os parâmetros especificados.

Sintaxe: **ip igmp snooping vlan-config** *vlan-id-list* [**rtime** router-time | **mtime** *member-time* | **ltime** *leave-time*]
no ip igmp snooping vlan-config *vlan-id-list* [**rtime** | **mtime** | **ltime**]

Parâmetros:

- **vlan-id-list:** a lista de IDs da VLAN que deseja modificar, variando de 1 a 4094, no formato de *1-3, 5*.
- **router-time:** o aging time da porta do roteador. Nesse tempo, se o switch não receber a mensagem de consulta IGMP da porta do roteador, ele considerará que essa porta não é mais uma porta do roteador. Os valores válidos são de 60 a 600 segundos e o valor padrão é de *300 segundos*.
- **member-time:** o aging time da Porta Membro. Nesse tempo, se o comutador não receber a mensagem IGMP report da porta membro, ele não considerará essa porta como uma porta membro. Os valores válidos são de 60 a 600 segundos e o valor padrão é de *260 segundos*.
- **leave time:** o tempo de saída. Os valores válidos são de 1 a 30 segundos e o valor padrão é *1 segundo*. Quando o switch recebe uma mensagem leave de uma porta para deixar um grupo multicast, ele espera o leave-time expirar antes de remover a porta do grupo multicast. Durante o período, se o switch receber qualquer mensagem de relatório da porta, a porta não será removida do grupo multicast. As exceções são as seguintes:
  - Se o aging da porta membro expirar antes que o leave-time termine e nenhuma mensagem de relatório seja recebida, a porta será removida do grupo multicast e quando o tempo de aging-time da Porta Membro terminar.
  - A função *Leave-time* não entrará em vigor quando o Fast Leave estiver habilitado.

Modo de comando: Global Configuration.

Requisito de Privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função IGMP Snooping e modifique o aging time da porta do roteador em 300 segundos, o aging time da porta membro em 200 segundos para a VLAN 1-3:

INTELBRAS(config)# ip igmp snooping vlan-config 1-3 rtime 300
INTELBRAS(config)# ip igmp snooping vlan-config 1-3 mtime 200

17.6. ip igmp snooping vlan-config (immediate-leave)

Descrição: esse comando é usado para ativar o recurso Fast Leave para VLANs específicas. Para desabilitar o Fast Leave nas VLANs, por favor, use o **no ip igmp snooping vlan-config** *vlan-id-list* **immediate-leave**. Esta função está desativada por padrão.

Sintaxe: **ip igmp snooping vlan-config** *vlan-id-list* **immediate-leave**
no ip igmp snooping vlan-config *vlan-id-list* **immediate-leave**

Parâmetro:

- **vlan-id-list:** a lista de IDs da VLAN desejava modificar a configuração, variando de 1 a 4094, no formato de *1-3, 5*.

Modo de comando: Global Configuration.

Requisito de Privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o fast leave na VLAN 1-3:

INTELBRAS(config)# ip igmp snooping vlan-config 1-3 **immediate-leave**

17.7. ip igmp snooping vlan-config (report-suppression)

Descrição: esse comando é usado para ativar a função IGMP Report Suppression para VLANs específicas. Quando ativado, o switch só encaminhará a primeira mensagem de IGMP report para cada grupo multicast e para o IGMP querier e suprimir mensagens IGMP report subsequentes para o mesmo grupo multicast durante um intervalo de consulta (query). Esse recurso evita que as mensagens de report duplicadas sejam enviadas para o IGMP querier. Para desabilitar a função IGMP Report Suppression e encaminhar todos os IGMP Reports para o dispositivo da Camada 3 em VLANs específicas, por favor, use o comando **no ip igmp snooping vlan-config** vlan-id-list **report-suppression**. Esta função está desativada por padrão.

Sintaxe: **ip igmp snooping vlan-config** *vlan-id-list* **report-suppression**
no ip igmp snooping vlan-config *vlan-id-list* **report-suppression**

Parâmetro:

» **vlan-id-list:** a lista de IDs das VLANs podem variar de 1 a 4094, no formato de *1-3, 5*.

Modo do comando: Global Configuration.

Requisitos de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o IGMP Report Suppression na VLAN 1-3:

INTELBRAS(config)# ip igmp snooping vlan-config 1-3 **report-suppression**

17.8. ip igmp snooping vlan-config (router-ports-forbidden)

Descrição: esse comando é usado para impedir que as portas especificadas sejam portas roteador na (s) VLAN (s) especificada (s). Para excluir as portas do roteador que foram proibidas, por favor, use o comando **no ip-bin-snooping vlan-config** *vlan-id-list* **router-ports-forbidd**.

Sintaxe: **ip igmp snooping vlan-config** *vlan-id-list* **router-ports-forbidd interface** {**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}
no ip igmp snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** [**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*]

Parâmetros:

» **vlan-id-list:** a lista de IDs das VLANs pode variar de 1 a 4094, no formato de *1-3, 5*.

» **port-list:** proíbe as portas especificadas como portas do roteador. Pacotes enviados de roteadores multicast para essas portas serão descartados.

» **port-channel-list:** proíbe os canais de porta especificados como portas do roteador. Pacotes enviados de roteadores multicast para esses canais de portas (link agreggation) serão descartados.

Modo de comando: Global Configuration.

Requisitos de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: impeça que as portas Ethernet 1/0 / 1-3 sejam portas do roteador na VLAN 1:

INTELBRAS(config)# ip igmp snooping vlan-config 1 **router-ports-forbidd interface gigabitEthernet** 1/0/1-3

17.9. ip igmp snooping vlan-config (rport interface)

Descrição: esse comando é usado para especificar de forma estática quais serão as portas do roteador em cada VLAN. Para excluir as portas do roteador configuradas como estáticas, por favor, use o comando **no ip igmp snooping vlan-config** vlan-id-list **interface rport**.

Sintaxe: **ip igmp snooping vlan-config** *vlan-id-list* **rport interface** {**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}
no ip igmp snooping vlan-config *vlan-id-list* **rport interface** {**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}

Parâmetros:

» **vlan-id-list:** a lista de IDs das VLANs podem variar de 1 a 4094, no formato de *1-3, 5*.

» **port-list:** a lista de portas Ethernet.

» **port-channel-list:** o ID dos canais da porta.

Modo de comando: Global Configuration.

Requisitos de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure de forma estática as portas 1/0/1 como portas roteador na VLAN 1-2:

INTELBRAS(config)# ip igmp snooping vlan-config 1-2 **interface rport gigabitEthernet** 1/0/1

17.10. ip igmp snooping vlan-config (static)

Descrição: este comando é usado para configurar interfaces para se associar estaticamente a um grupo multicast. Para remover interfaces de um grupo multicast estático, por favor, use o comando **no ip igmp snooping vlan-config** *vlan-id-list* **static.**

Sintaxe: **ip igmp snooping vlan-config** *vlan-id-list* **static** *ip* **interface** {**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}
no ip igmp snooping vlan-config *vlan-id-list* **static** *ip* **interface** {**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}

Parâmetros:

» **vlan-id-list:** a lista de IDs das VLANs podem variar de 1 a 4094, no formato de *1-3, 5*.

» **Ip:** especifique o endereço IP do grupo multicast que os hosts desejam ingressar.

» **port-list:** a lista de portas Ethernet.

» **port-channel-list:** o ID dos canais da porta.

Modo de comando: Global Configuration.

Requisitos de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure as portas 1/0 / 1-3 na VLAN 2 para associar estaticamente o grupo multicast 225.0.0.1:

INTELBRAS(config)# ip igmp snooping vlan-config 2 **static** 225.0.0.1 **interface gigabitEthernet** 1/0/1-3

17.11. ip igmp snooping vlan-config (querier)

Descrição: esse comando é usado para ativar o recurso IGMP Snooping querier para VLANs específicas. Para desativar/restaurar o recurso IGMP Snooping Querier nas VLANs, por favor, use o comando **vlan-config** *vlan-id-list* **querier ip igmp** sem quaisquer parâmetros.

Sintaxe: **ip igmp snooping vlan-config** vlan-id-list **querier [max-response-time** response-time |
query-interval interval | **general-query source-ip** ip-addr | **last-member-query-count** count |
last-member-query-interval interval]
no ip igmp snooping vlan-config vlan-id-list **querier [max-response-time | query-interval | general-query source-ip | last-member-query-count]**

Parâmetros:

» **vlan-id-list:** a lista de IDs das VLANs podem variar de 1 a 4094, no formato de *1-3, 5*.

» **response-time:** o tempo máximo de resposta do host para mensagens de consulta geral (query). Os valores válidos são de 1 a 25 segundos e o valor padrão é *10 segundos*.

» **query-interval interval:** o intervalo entre as mensagens general query enviadas pelo switch. Os valores válidos são de 10 a 300 segundos e o valor padrão é *60 segundos*.

» **ip-addr:** o endereço IP de origem das mensagens general query enviadas pelo switch. Deve ser um endereço unicast. Por padrão, é *0.0.0.0*.

» **count:** o número de consultas (queries) específicas do grupo a serem enviadas. Com o IGMP Snooping Querier ativado, quando o comutador recebe uma mensagem IGMP leave, obtém o endereço do grupo multicast que o host deseja deixar. Em seguida, o switch envia consultas específicas do grupo para esse grupo multicast por meio da porta que recebe a mensagem IGM leave. Se a contagem de consultas específicas do grupo for enviada e nenhuma mensagem de relatório for recebida, o switch excluirá o endereço de multicast da tabela de encaminhamento de multicast. Os valores válidos são de 1 a 5 e o valor padrão é *2*.

» **last-member-query-interval interval:** o intervalo entre as consultas específicas do grupo. Os valores válidos são de 1 a 5 segundos e o valor padrão é *1 segundo*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o IGMP Snooping querier para VLAN 3 e configure o intervalo de consulta em 100 segundos:

INTELBRAS(config)# ip igmp snooping vlan-config 3 **querier**
INTELBRAS(config)# ip igmp snooping vlan-config 3 **querier query interval** 100

17.12. ip igmp snooping (interface)

Descrição: o comando **ip igmp snooping** é usado para ativar a função IGMP Snooping na porta desejada. Para desabilitar a função IGMP Snooping, por favor, use o comando **no ip igmp snooping**.

Sintaxe: **ip igmp snooping**
no ip igmp snooping

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função IGMP Snooping na porta 1/0/3:

INTELBRAS(config)# interface gigabitEthernet *1/0/3*
INTELBRAS(config-if)# ip igmp snooping

17.13. ip igmp snooping max-groups

Descrição: o comando **ip igmp snooping max-groups** é usado para configurar o número máximo de grupos que uma porta pode juntar-se. O **ip igmp snooping max-groups action** é usada para configurar a ação que a porta executa quando recebe uma mensagem IGMP report após ter atingido o número máximo de entradas na tabela de encaminhamento. Para remover a limitação máxima do grupo e retornar ao padrão sem limitação na porta especificada, use o comando **no ip igmp snooping max-groups**. Para retornar à ação padrão de descartar mensagens report, use o comando de ação **no ip igmp snooping max-groups action**. Esses comandos aplicam-se apenas aos grupos multicast dinâmicos.

Sintaxe: **ip igmp snooping max-groups** *maxgroup*
ip igmp snooping max-groups action {*drop* | *replace*}
no ip igmp snooping max-groups
no ip igmp snooping max-groups action

Parâmetros:

» **maxgroup:** especifique o número máximo de grupos que a porta pode participar. Varia de 0 a 1000 e o valor padrão é *1000*.

» **drop:** quando o número de grupos multicast dinâmicos que uma porta une exceder o grupo max, a porta não se juntará a nenhum novo grupo multicast e descartará os pacotes de novos grupos multicast.

» **replace:** quando o número de grupos multicast dinâmicos que uma porta participa exceder o grupo máximo, o grupo multicast recém aprendido substituirá um grupo multcast existente pelo menor endereço de grupo multcast.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique em 10 os números máximos de grupos que as portas 1/0 / 2-5 podem participar e configure a ação de limitação como replace:

INTELBRAS(config)#interface range gigabitEthernet 1/0/2-5
INTELBRAS(config-if-range)#ip igmp snooping max-groups 10
INTELBRAS(config-if-range)#ip igmp snooping max-groups action replace

17.14. ip igmp snooping immediate-leave

Descrição: o comando **ip igmp snooping immediate-leave** é usado para configurar a função Fast Leave na porta. Para desabilitar a função Fast Leave, por favor use o comando **no ip igmp snooping immediate-leave**.

Sintaxe: **ip igmp snooping immediate-leave**
no ip igmp snooping immediate-leave

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função Fast Leave na porta 1/0/3:

INTELBRAS(config)# interface gigabitEthernet *1/0/3*
INTELBRAS(config-if)# ip igmp snooping immediate-leave

17.15. ip igmp profile

Descrição: o comando **ip igmp profile** é usado para criar o perfil de configuração. Para deletar o perfil correspondente, por favor use o comando **no ip igmp profile**.

Sintaxe: **ip igmp profile** *id*
no ip igmp profile *id*

Parâmetro:

» **id:** especifique o id do perfil de configuração, variando de 1 a 999.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie o perfil 1:

INTELBRAS(config)# ip igmp profile 1

17.16. deny

Descrição: o comando **deny** é usado para negar o perfil do IGMP.

Sintaxe: **deny**

Modo de comando: Profile Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de filtragem do perfil 1 como negar:

INTELBRAS(config)# ip igmp profile 1
INTELBRAS(config-igmp-profile)#deny

17.17. permit

Descrição: o comando de **permit** é usado para permitir o perfil do IGMP.

Sintaxe: **permit**

Modo de comando: Profile Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de filtragem do perfil 1 como permit:

INTELBRAS(config)# ip igmp profile 1
INTELBRAS(config-igmp-profile)#permit

17.18. range

Descrição: o comando **range** é usado para configurar o intervalo de filtragem de perfil dos endereços multicast. Para excluir o intervalo de filtragem de perfil correspondente, use o comando **no range**. Um perfil contém no máximo 16 entradas de filtragem de IP.

Sintaxe: **range** start-ip end-ip
no range start-ip end-ip

Parâmetros:

» **start-ip:** o início da filtragem do endereço IP multicast.
» **end-ip:** o endereço IP multicast de filtragem final.

Modo de comando: Profile Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure um filtro do endereço multicast com o intervalo 225.1.1.1 a 226.3.2.1 no perfil 1:

```
INTELBRAS(config)# ip igmp profile 1
INTELBRAS(config-igmp-profile)# range 225.1.1.1 226.3.2.1
```

17.19. ip igmp filter

Descrição: o comando **ip igmp filter** é usado para vincular o perfil especificado à interface. Para deletar a ligação, por favor use o comando **no ip igmp filter.**

Sintaxe: **ip igmp filter** *profile-id*
no ip igmp filter

Parâmetros:

» **profile-id:** especifique o ID do perfil, variando de 1 a 999.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: vincule o perfil 1 à interface gigabitEthernet 1/0/2:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip igmp filter 1
```

17.20. clear ip igmp snooping statistics

Descrição: o comando **clear ip igmp snooping statistics** é usado para limpar as estatísticas de pacotes IGMP.

Sintaxe: **clear ip igmp snooping statistics**

Modo de comando: Configuration and Privileged EXEC.

Requisito de Privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: limpe as estatística do IGMP:

```
INTELBRAS(config)# clear ip igmp snooping statistics
```

17.21. show ip igmp snooping

Descrição: o comando **show ip igmp snooping** é usado para exibir a configuração global do IGMP Snooping.

Sintaxe: **show ip igmp snooping**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba a configuração global do IGMP:

```
INTELBRAS# show ip igmp snooping
```

17.22. show ip igmp snooping interface

Descrição: o comando **show ip igmp interface snooping** é usado para exibir a configuração de porta de snooping IGMP. Se nenhuma interface for especificada, ela exibirá todas as configurações de IGMP das interfaces.

Sintaxe: **show ip igmp snooping interface** [**gigabitEthernet** *[port-list]* | **port-channel** [*port-channel-list*]] {basic-config | max-groups | packet-stat}

Parâmetros:

- **port-list:** a lista de portas Ethernet.
- **port-channel-list:** a lista de canais de porta.
- **basic-config | max-groups | packet-stat:** as informações de configuração selecionadas para exibir.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Exiba a configuração básica do IGMP de todas as portas e canais de porta:

```
INTELBRAS# show ip igmp snooping interface basic-config
```

Exiba a configuração básica do IGMP da porta 1/0/2:

```
INTELBRAS# show ip igmp snooping interface gigabitEthernet 1/0/2 basic-config
```

Exiba as estatísticas de pacotes IGMP das portas 1/0 / 1-4:

```
INTELBRAS# show ip igmp snooping interface gigabitEthernet 1/0/1-4 packet-stat
```

17.23. show ip igmp snooping vlan

Descrição: o comando **show ip igmp snooping vlan** é usado para exibir a configuração de VLAN do IGMP snooping.

Sintaxe: **show ip igmp snooping vlan** [*vlan-id*]

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações de configuração do rastreamento IGMP da VLAN 2:

```
INTELBRAS# show ip igmp snooping vlan 2
```

17.24. show ip igmp snooping groups

Descrição: o comando **show ip igmp snooping groups** é usado para exibir as informações de todos os grupos do IGMP Snooping. Ele pode ser estendido para alguns outros comandos para exibir as informações dinâmicas e estáticas de multicast de uma VLAN selecionada.

Sintaxe: **show ip igmp snooping groups** [**vlan** {*vlan-id*}] [*multicast_addr* | count | dynamic | dynamic count | static | static count]

Parâmetros:

- **vlan-id:** o ID da VLAN selecionada para exibir as informações de todos os itens multicast.
- **multicast_addr:** endereço IP do grupo multicast.
- **count:** os números de todos os grupos multicast.
- **dynamic:** exibe grupos multicast dinâmicos.
- **dynamic count:** os números de todos os grupos multicast dinâmicos.
- **static:** exibe grupos multicast estáticos.
- **static count:** os números de todos os grupos multicast estáticos.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Exiba as informações de todos os grupos de rastreamento do IGMP:

INTELBRAS#show ip igmp snooping groups

Exiba todas as entradas multicast na VLAN 5:

INTELBRAS(config)#show ip igmp snooping groups vlan 5

Exiba a contagem de entradas multicast na VLAN 5:

INTELBRAS(config)#show ip igmp snooping groups vlan 5 count

Exiba os grupos de multidifusão dinâmicos da VLAN 5:

INTELBRAS(config)#show ip igmp snooping groups vlan 5 dynamic

Exiba os grupos multicast estáticos da VLAN 5:

INTELBRAS(config)#show ip igmp snooping groups vlan 5 static

Exiba a contagem de entradas multicast dinâmicas da VLAN 5:

INTELBRAS(config)#show ip igmp snooping groups vlan 5 dynamic count

Exiba a contagem de entradas multicast estáticas da VLAN 5:

INTELBRAS(config)#show ip igmp snooping groups vlan 5 static count

17.25. show ip igmp profile

Descrição: o comando **show ip igmp profile** é usado para exibir as informações de configuração de todos os perfis ou de um perfil específico.

Sintaxe: **show ip igmp profile** [*id*]

Parâmetro:

» **id:** especifique o ID do perfil, variando de 1 a 999.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum

Exemplo: exibA as informações de configuração de todos os perfis:

INTELBRAS(config)# show ip igmp profile

18. Comandos MLD Snooping

MLD Snooping (*Multicast Listener Discovery Snooping*) é um mecanismo de controle de multicast operando nos switchs layer 2. Esse mecanismo evita que grupos multicast sejam transmitidos em forma de broadcast nas redes IPv6.

18.1. ipv6 mld snooping (global)

Descrição: o comando **ipv6 mld snooping** é usado para ativar a função MLD Snooping de forma global. Se esta função for desabilitada, todas as funções relativas do MLD Snooping irão parar de funcionar. Para desativar o MLD Snooping utilize o comando **no mld snooping**.

Sintaxe: **ipv6 mld snooping**
no ipv6 mld snooping

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o MLD Snooping:

```
INTELBRAS(config)# ipv6 mld snooping
```

18.2. ipv6 mld snooping drop-unknown

Descrição: o comando **ipv6 mld snooping drop-unknown** é usado para ativar a função para filtragem de pacotes multicast desconhecidos, ou seja, pacotes multicast desconhecidos serão dropados. Para desativar esta função utilize o comando **no ipv6 mld snooping drop-unknown**. Por padrão esta função vem desabilitada.

Sintaxe: **ipv6 mld snooping drop-unknown**
no ipv6 mld snooping drop-unknown

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o filtro para pacotes multicast desconhecidos:

```
INTELBRAS(config)# ipv6 mld snooping drop-unknown
```

18.3. ipv6 mld snooping vlan-config

Descrição: o comando **ipv6 mld snooping vlan-config** é usado para habilitar a função MLD Snooping VLAN ou modificar seus parâmetros. Para desabilitar MLD Snoop ing VLAN utilize o comando **no ipv6 mld snooping vlan-config**.

Sintaxe: **ipv6 mld snooping vlan-config** *vlan-id-list* [**rtime** *router-time* | **mtime** *member-time* | **ltime** leave-time]
no ipv6 mld snooping vlan-config *vlan-id-list* [**rtime** | **mtime** | **ltime**]

Parâmetros:

- **vlan-id-list:** identificação da VLAN a qual se deseja alterar a configuração, varia entre 1 e 4094, no formato *1-3, 5*.
- **router-time:** aging time da router port. Durante esse período se nenhuma mensagem de consulta MLD desta porta for recebida pelo switch ele desconsiderará essa porta como uma router port. Os valores variam entre 60 e 600 segundos e o valor padrão é *300 segundos*.
- **member-time:** aging time das portas membro. Durante esse período se Nenhuma mensagem de consulta MLD desta porta for recebida pelo switch ele desconsiderará essa porta como uma porta membro. Os valores variam entre 60 e 600 segundos e o valor padrão é *260 segundos*.
- **leave-time:** Leave Time. Valores válidos variam entre 1 e 30 segundos, por padrão o valor é *1 segundo*. Quando o switch recebe uma mensagem *done message* de uma porta solicitando para sair do grupo de multicast ele irá aguardar o Leave Time antes de remover a porta do grupo multicast. Durante este período, se o switch receber qualquer mensagem da porta a mesma não será removida do grupo. Exceções:
  - Se a porta sair antes que o Leave Time termine e não houverem mensagens recebidas, a porta será removida do grupo de multicast uma vez que o *Member Port Aging Time* termine.
  - O Leave Time não atuará quando o Fast Leave estiver ativo.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o MLD Snooping e modifique o tempo da Router Port para 300 segundos e o tempo da Member Port como 200 segundos para a VLAN 1-3:

```
INTELBRAS(config)# ipv6 mld snooping vlan-config 1-3 rtime 300
INTELBRAS(config)# ipv6 mld snooping vlan-config 1-3 mtime 200
```

18.4. ipv6 mld snooping vlan-config (immediate-leave)

Descrição: o comando **ipv6 mld snooping vlan-config immediate-leave** é utilizado para habilitar a função de Fast Leave para uma VLAN específica. Para desabilitar o Fast Leave para a VLAN utilize o comando **no ipv6 mld snooping vlan-config immediate-leave**. Esta função vem desabilitada por padrão.

Sintaxe: **ipv6 mld snooping vlan-config** *vlan-id-list* **immediate-leave**
no ipv6 mld snooping vlan-config *vlan-id-list* **immediate-leave**

Parâmetro:

» **vlan-id-list:** identificação da VLAN a qual se deseja alterar a configuração, varia entre 1 e 4094, no formato *1-3, 5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o Fast Leave para a VLAN 1-3:

```
INTELBRAS(config)# ipv6 mld snooping vlan-config 1-3 immediate-leave
```

18.5. ipv6 mld snooping vlan-config (report-suppression)

Descrição: o comando **ipv6 mld snooping vlan-config** é usado para habilitar a função MLD Report Suppression para determinadas VLANs. Quando ativado o switch só encaminhará a primeira mensagem de relatório MLD (MLD report) de cada grupo multicast para o MLD Querier e suprimirá as mensagens de relatório subsequentes para o mesmo grupo multicast. Esse recurso evita que mensagens duplicadas sejam enviadas para o MLD Querier. Para desabilitar esta função e encaminhar os relatórios para os dispositivos Layer 3 nas VLANs específicas utilize o comando **no ipv6 mld snooping vlan-config report-suppression**. Esta função vem desabilitada por padrão.

Sintaxe: **ipv6 mld snooping vlan-config** *vlan-id-list* **report-suppression**
no ipv6 mld snooping vlan-config *vlan-id-list* **report-suppression**

Parâmetros:

» **vlan-id-list:** identificação da VLAN a qual se deseja alterar a configuração, varia entre 1 e 4094, no formato *1-3, 5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o MLD Report Suppression para as VLANs 1-3:

```
INTELBRAS(config)# ipv6 mld snooping vlan-config 1-3 report-suppression
```

18.6. ipv6 mld snooping vlan-config (router-ports-forbidden)

Descrição: o comando **ipv6 mld snooping vlan-config** é usado para impedir portas de serem Router Ports em especificas VLANs. Para excluir as portas sem permissão utilize o comando **no ipv6 mld snooping vlan-config router-ports-forbidd**.

Sintaxe: **ipv6 mld snooping vlan-config** *vlan-id-list* **router-ports-forbidd interface** {[**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*]}
no ipv6 mld snooping vlan-config *vlan-id-list* **router-ports-forbidd interface** {[**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*]}

Parâmetros:

» **vlan-id-list:** identificação da VLAN a qual se deseja alterar a configuração, varia entre 1 e 4094, no formato *1-3, 5*.

» **port-list:** identificação da porta que será impedida de ser uma Router Port. Pacotes enviados do multicast para essa porta serão descartados.

» **port-channel-list:** identificação das port-channels impedidos de serem uma Router Port. Pacotes enviados do multicast para esses port-channels serão descartados.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: proíba as portas Ethernet 1/0/1-3 de serem Router Ports na VLAN 1:

INTELBRAS(config)# ipv6 mld snooping vlan-config 1 **router-ports-forbidd interface gigabitEthernet** 1/0/1-3

18.7. ipv6 mld snooping vlan-config (rport interface)

Descrição: o comando **ipv6 mld snooping vlan-config rport** interface é utilizado para especificar uma Router Port estática para uma VLAN. Para excluir a entrada estática utilize o comando **no ipv6 mld snooping vlan-config rport interface**. Esta função vem desabilitada por padrão.

Sintaxe: **ipv6 mld snooping vlan-config** *vlan-id-list* **rport interface {gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}
no ipv6 mld snooping vlan-config *vlan-id-list* **rport interface** {**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}

Parâmetros:

» **vlan-id-list:** identificação da VLAN a qual se deseja alterar a configuração, varia entre 1 e 4094, no formato *1-3, 5.*
» **port-list:** lista de portas Ethernet.
» **port-channel-list:** identificação das port-channels.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: indique a porta 1/0/1 como Router Port para a VLAN 1-2:

INTELBRAS(config)# ipv6 mld snooping vlan-config 1-2 **rport interface gigabitEthernet** 1/0/1

18.8. ipv6 mld snooping vlan-config static

Descrição: o comando **ipv6 mld snooping vlan-config static** é utilizado para acrescentar de forma estática uma interface à um grupo multicast. Para remover a interface do grupo utilize o comando **no ipv6 mld snooping vlan-config static.**

Sintaxe: **ipv6 mld snooping vlan-config** *vlan-id-list* **static** *ip-addr* **interface** {**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}
no ipv6 mld snooping vlan-config *vlan-id-list* **static** *ip-addr* **interface** {**gigabitEthernet** *port-list* | **port-channel** *port-channel-list*}

Parâmetros:

» **vlan-id-list:** identificação da VLAN a qual se deseja alterar a configuração, varia entre 1 e 4094, no formato *1-3, 5.*
» **ip-addr:** especifica o endereço IP do grupo multicast que o host irá participar.
» **port-list:** lista de portas Ethernet.
» **port-channel-list:** identificação das port-channels.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure as portas 1/0/1-3 na VLAN 2 para participarem estaticamente do grupo multicast 225.0.0.1.

INTELBRAS(config)# ipv6 mld snooping vlan-config 2 static 255.0.0.1 **interface gigabitEthernet** 1/0/1-3

18.9. ipv6 mld snooping vlan-config querier

Descrição: o comando **ipv6 mld snooping vlan-config querier** é utilizado para habilitar o MLD Snooping Querier para uma VLAN especifica. Para desabilitar o MLD Snooping Querier utilize o comando **no ipv6 mld snooping vlan-config querier** sem Nenhum parâmetro. Para retornar as configurações para os valores padrões utilize o comando **no no ipv6 mld snooping vlan-config querier**.

Sintaxe: **ipv6 mld snooping vlan-config** *vlan-id-list* **querier** [**max-response-time** *response-time* | **query-interval** *interval* | **general-query source-ip** ip-addr | **last-listener-query-count** *count* | **last-listener-query-interval** *interval*]
ipv6 mld snooping vlan-config *vlan-id-list* **querier** [**max-response-time** *response-time* | **query-interval** *interval* | **general-query source-ip** ip-addr | **last-listener-query-count** *count* | **last-listener-query-interval** *interval*]

Parâmetros:

- **vlan-id-list:** identificação da VLAN a qual se deseja alterar a configuração, varia entre 1 e 4094, no formato *1-3, 5*.
- **response-time:** o tempo máximo de resposta do host para mensagens de general query. Os valores válidos são de 1 a 25 segundos e o valor padrão é *10 segundos*.
- **query-interval interval:** o intervalo entre as mensagens de general query enviadas pelo switch. Os valores válidos são de 10 a 300 segundos e o valor padrão é *60 segundos*.
- **ip-addr:** especifica o endereço IP da origem das mensagens de General Query enviadas pelo switch. Pode ser um endereço unicast. Por padrão ela é *fe80::2ff:ffff:fe00:1*.
- **count:** o número de consultas específicas a serem enviadas para o grupo. Com o MLD Snooping Querier habilitado, quando o switch recebe uma mensagem *Done message* MLD ele obtém o endereço do grupo multicast que o host deseja deixar de participar (leave message), O switch envia uma quantidade de consultas específicas para o grupo através da porta a qual ele recebeu a mensagem *Done Message*. Se a contagem especificada de consultas específicas do grupo for enviada e Nenhum.a mensagem de relatório (MLD report) for recebida, o switch irá deletar o endereço de multicast da tabela de encaminhamento. Os valores válidos variam entre 1 e 5, por padrão é defino como *2*.
- **last-member-query-interval interval:** intervalo entre as consultas específicas de grupo. Os valores válidos variam entre 1 e 5, por padrão é defino como *1*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o MLD Snooping Querier para a VLAN 3 e configure o query interval em 100 segundos:

```
INTELBRAS(config)# ipv6 mld snooping vlan-config 3 querier
INTELBRAS(config)# ipv6 mld snooping vlan-config 3 querier query interval 100
```

18.10. ipv6 mld snooping (interface)

Descrição: o comando **ipv6 mld snooping** é usado para ativar a função MLD Snooping para uma determinada interface. Para desativar o MLD Snooping utilize o comando **no mld snooping.**

Sintaxe: **ipv6 mld snooping**
no ipv6 mld snooping

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o MLD Snooping para a porta 1/0/3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# ipv6 mld snooping
```

18.11. ipv6 mld snooping max-groups

Descrição: o comando **ipv6 mld snooping max-groups** é usado para determinar o número máximo de grupos a qual uma porta pode participar. O comando **ipv6 mld snooping max-groups action** é utilizado para configurar a ação que a porta tomará quando a porta receber a mensagem que o número máximo de grupos foi alcançado nas entradas da tabela de encaminhamento. Para remover a limitação de número máximo de grupos e retornar a configuração para o valor padrão, utilize o comando **no ipv6 mld snooping max-groups**. Para retornar para a ação padrão de dropar reports utilize o comando **no ipv6 mld snooping max-groups action**. Estes comandos só se aplicam a grupos multicast dinâmicos.

Sintaxe: **ipv6 mld snooping max-groups** *maxgroup*
ipv6 mld snooping max-groups action {drop | replace}
no ipv6 mld snooping max-groups
no ipv6 mld snooping max-groups action

Parâmetros:

» **maxgroup:** especifica o número máximo de grupos que uma porta pode participar. Valor varia entre 0 e 1000 e o valor padrão é *1000*.

» **drop:** quando o número máximo de grupos multicast dinâmicos que a porta pode participar é excedido ela não irá participar de nenhum novo grupo.

» **replace:** quando o número máximo de grupos multicast dinâmicos que a porta pode participar é excedido o novo grupo ao qual a porta se tornou membro irá sobrescrever o endereço de grupo multicast mais antigo.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o número máximo de grupos para as portas 1/0/2-5 como 10 e configure a ação de limitação como replace.

```
INTELBRAS(config)# interface range gigabitEthernet 1/0/2-5
INTELBRAS(config-if-range)# ipv6 mld snooping max-groups 10
INTELBRAS(config-if-range)# ipv6 mld snooping max-groups action replace
```

18.12. ipv6 mld snooping immediate-leave

Descrição: o comando **ipv6 mld snooping immediate-leave** é utilizado para habilitar a função de Fast Leave na porta. Para desabilitar o Fast Leave utilize o comando **no ipv6 mld snooping immediate-leave**.

Sintaxe: **ipv6 mld snooping immediate-leave**
no ipv6 mld snooping immediate-leave

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o Fast Leave para a porta 1/0/3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# ipv6 mld snooping immediate-leave
```

18.13. ipv6 mld profile

Descrição: o comando **ipv6 mld profile** é utilizado para criar uma configuração de perfil. Para deletar o perfil correspondente utilize **no ipv6 mld profile.**

Sintaxe: **ipv6 mld profile** *id*
no ipv6 mld profile *id*

Parâmetros:

» **id:** especifica a identificação do perfil, varia de 1 até 999.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie o perfil 1:

```
INTELBRAS(config)# ipv6 mld profile 1
```

18.14. deny

Descrição: o comando **deny** é usado para configurar o modo de filtragem do perfil como negar.

Sintaxe: **deny**

Modo de comando: Profile Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de filtragem do perfil 1 como negar:

```
INTELBRAS(config)# ipv6 mld profile 1
INTELBRAS(config-MLD-profile)# deny
```

18.15. permit

Descrição: o comando **permit** é usado para configurar o modo de filtragem do perfil como permitir.

Sintaxe: **permit**

Modo de comando: Profile Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de filtragem do perfil 1 como permitir:

```
INTELBRAS(config)# ipv6 mld profile 1
INTELBRAS(config-MLD-profile)# permit
```

18.16. range

Descrição: o comando **range** é usado para configurar o intervalo do endereço multicast do perfil de filtragem. Para deletar o corresponde filtro utilize o comando **no range**. Um perfil contem no máximo 16 filtragens de entradas de um intervalo IP.

Sintaxe: **range** *start-ip end-ip*
no range *start-ip end-ip*

Parâmetros:

- **start-ip:** IPv6 multicast de início para entrada de filtro.
- **end-ip:** IPv6 multicast para final da entrada de filtro.

Modo de comando: Profile Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure um filtro para entrada de endereço multicast com intervalo ff80::1234 to ff80::1235 para o perfil 1:

```
INTELBRAS(config)# ipv6 mld profile 1
INTELBRAS(config-MLD-profile)# range ff80::1234 ff80::1235
```

18.17. ipv6 mld filter

Descrição: o comando **ipv6 mld filter** é usado para vincular um perfil específico à uma interface. Para deletar o correspondente vínculo utilize o comando **no ipv6 mld filter**.

Sintaxe: **ipv6 mld filter** *profile-id*
no ipv6 mld filter

Parâmetros:

- **profile-id:** especifica a identificação do perfil, varia de 1 até 999.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: vincule o perfil à interface gigabitEthernet 1/0/2:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ipv6 mld filter 1
```

18.18. clear ipv6 mld snooping statistics

Descrição: o comando **clear ipv6 mld snooping statistics** é usado para limpar as estatísticas dos pacotes MLD.

Sintaxe: **clear ipv6 mld snooping statistics**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: limpe as estatísticas dos pacotes MLD:

```
INTELBRAS# clear ipv6 mld snooping statistics
```

18.19. show ipv6 mld snooping

Descrição: o comando **show ipv6 mld snooping** é usado para mostrar a configuração global do MLD Snooping.

Sintaxe: **show ipv6 mld snooping**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração MLD Snooping:

```
INTELBRAS# show ipv6 mld snooping
```

18.20. show ipv6 mld snooping interface

Descrição: o comando **show ipv6 mld snooping interface** é usado para mostrar a configuração da porta do MLD Snooping.

Sintaxe: **ipv6 mld snooping interface** [**gigabitEthernet** [*port* | *port-list*]] {basic-config | max-groups | packet-stats}
ipv6 mld snooping interface [**port-channel** [*port-channel-list*]] {basic-config | max-groups | packet-stats}

Parâmetros:

- **port:** número da porta Ethernet.
- **port-list:** lista de portas Ethernet.
- **port-channel-list:** lista de portchannels.
- **basic-config | max-groups | packet-stats:** informação que se deseja exibir.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Mostre a configuração básica do MLD de todas as portas e port-channels:

```
INTELBRAS# show ipv6 mld snooping interface basic-config
```

Mostre a configuração básica do MLD para a porta 1/0/2:

```
INTELBRAS# show ipv6 mld snooping interface gigabitEthernet 1/0/2 basic-config
```

Mostre a estatística de pacotes do MLD para as portas 1/0/1-4.

```
INTELBRAS# show ipv6 mld snooping interface gigabitEthernet 1/0/1-4 packet-stat
```

18.21. show ipv6 mld snooping vlan

Descrição: o comando **show ipv6 mld snooping vlan** é usado para mostrar a informação do MLD Snooping VLAN.

Sintaxe: **show ipv6 mld snooping vlan** [*vlan-id*]

Parâmetro:

» **vlan-id:** identificação da VLAN, varia de 1 até 4094.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a informação de todas as VLANs:

```
INTELBRAS# show ipv6 mld snooping vlan
```

18.22. show ipv6 mld snooping groups

Descrição: o comando **show ipv6 mld snooping groups** é usado para mostrar os grupos multicast.

Sintaxe: **show ipv6 mld snooping groups** [**vlan** {vlan-id}] [*ipv6-multicast-addr* | count | dynamic | dynamic count | static | static count]

Parâmetros:

» **vlan-id:** identificação da VLAN, varia de 1 até 4094.
» **ipv6-multicast-addr:** endereço IPv6 do grupo multicast.
» **count:** número de todos os grupos multicast.
» **dynamic:** mostra os grupos multicast dinâmicos.
» **dynamic count:** número de todos os grupos multicast dinâmicos.
» **static:** mostra os grupos multicast estáticos.
» **static count:** número de todo os grupos multicast estáticos.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre todos os grupos multicast:

```
INTELBRAS# show ipv6 mld snooping groups
```

18.23. show ipv6 mld snooping profile

Descrição: o comando **show ipv6 mld snooping profile** é usado para mostrar a configuração de todos os perfis, ou um perfil específico.

Sintaxe: **show ipv6 mld profile** [*id*]

Parâmetro:

» **id:** Identificação do perfil, varia de 1 até 999.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a informação de todos os perfis:

```
INTELBRAS# show ipv6 mld profile
```

19. Comandos MVR

MVR (*Multicast VLAN Registrarion*) permite que um único multicast seja compartilhado entre as portas multicast mesmo em diferentes VLANs na rede IPv4. Enquanto no IGMP Snooping, se as portas pertencentes ao IGMP Snooping estiverem em VLANs diferentes uma cópia dos flux os multicast será enviada para cada VLAN. Já o MVR fornece uma VLAN multicast dedicada para encaminhar o tráfego multicast pela rede Layer 2, para evitar a duplicação de fluxos multicast para clientes em VLANs diferentes. Os clientes podem ingressar ou sair dinamicamente da VLAN de multicast sem interferir em seus relacionamentos em outras VLANs.

19.1. mvr (global)

Descrição: o comando **mvr** é usado para ativar o MVR de forma global. Para desativar o MVR utilize o comando **no mvr**.

Sintaxe: **mvr**
no mvr

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o MVR de forma global:

```
INTELBRAS(config)# mvr
```

19.2. mvr group

Descrição: o comando **mvr group** é usado para adicionar grupos de multicast ao MVR. Para excluir um grupo de multicast do MVR use o comando **no mvr group.**

Sintaxe: **mvr group** *ip*-addr[*count*]
no mvr group *ip*-addr[*count*]

Parâmetros:

- **ip-addr:** o endereço IP de inicial da série contínua do grupo de multicast.
- **count:** número de grupos multicast a ser adicionado ou excluído do MVR. Varia entre 1 e 256, o valor padrão é *1*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: adicione os grupos multicast 255.1.2.3-255.1.2.5 ao MVR:

```
INTELBRAS(config)# mvr group 255.1.2.3 3
```

19.3. mvr mode

Descrição: o comando **mvr mode** é usado para configurar o MVR como modo compatível ou dinâmico. Por padrão ele é configurado como modo compatível. Para voltar a configuração para o padrão utilize o comando **no mvr mode**.

Sintaxe: **mvr mode** {compatible | dynamic}
no mvr mode

Parâmetros:

- **compatible:** neste modo o switch não encaminha mensagens de report e leave dos hosts para o IGMP querier. Portanto este não pode aprender as informações dos grupos de multicast do switch, logo você terá que configurar o IGMP querier manualmente para que ele transmita todos os fluxos multicast através do switch via MVR.
- **dyamic:** neste modo, após receber uma mensagem de report e leave dos hosts o switch irá encaminhá-los para IGMP querier através do multicast VLAN (com a tradução apropriada da VLAN ID). O IGMP querier pode aprender os integrantes dos grupos multicast através das mensagens de report e leave e transmitir os fluxos multicast ao switch através da VLAN multicast de acordo com a tabela de encaminhamento multicast.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo do MVR como dinâmico:

INTELBRAS# mvr mode dynamic

19.4. mvr querytime

Descrição: o comando **mvr querytime** é usado para configurar o tempo de espera máxima para o recebimento do IGMP report de uma porta receptora antes de removê-la do grupo multicast. Para voltar a configuração ao valor padrão utilize o comando **no mvr querytime**.

Sintaxe: **mvr querytime** *time*
no mvr querytime

Parâmetro:

» **time:** tempo de espera. Valores variam entre 1 e 100 décimos de segundo o valor padrão é *5 décimos de segundo*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o tempo de resposta da consulta do MVR como 1 segundo, ou seja, 10 décimos de segundo:

INTELBRAS(config)# mvr querytime 10

19.5. mvr vlan

Descrição: o comando **mvr vlan** é usado para especificar a VLAN multicast. Por padrão é a *VLAN 1*. Para retornar para a configuração padrão utilize o comando **no mvr vlan**.

Sintaxe: **mvr vlan** *vid*
no mvr vlan

Parâmetros:

» **vid:** identificação da VLAN multicast, valores variam entre 1 e 4094.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure a VLAN 10 como VLAN multicast:

INTELBRAS(config)# mvr vlan 10

19.6. mvr (interface)

Descrição: o comando **mvr** é usado para habilitar o MVR para uma interface específica. Para desabilitar o MVR para a interface utilize o comando **no mvr.**

Sintaxe: **mvr**
no mvr

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o MVR para a porta 1/0/1:

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# mvr

19.7. mvr type

Descrição: o comando **mvr type** é usado para configurar a porta MVR como receptora ou fonte. Por padrão a porta não tem o MVR ativado. Se você tentar configurar uma porta *não MVR* com características MVR a operação falhará. Para retornar as configurações para o padrão utilize o comando **no mvr type**.

Sintaxe: **mvr type** { source | receiver }
no mvr type

Parâmetros:

- **source:** configura a porta de uplink que receberá e enviará os dados multicast na VLAN multicast como porta fonte. Essa porta deve pertencer à VLAN multicast.
- **receiver:** configura a porta que está conectada ao host como porta de recepção. A porta de recepção só pode pertencer à uma VLAN, e não pode pertencer à VLAN multicast.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a porta 1/0/3 como porta de recepção:

INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# mvr type receiver

19.8. mvr immediate

Descrição: o comando **mvr immediate** é usado para habilitar a função de Fast Leave do MVR para uma porta específica. Para desabilitar essa característica utilize o comando **no mvr immediate**.

Sintaxe: **mvr immediate**
no mvr immediate

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de Fast Leave para a porta 1/0/3:

INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# mvr immediate

19.9. mvr vlan (group)

Descrição: este comando é utilizado para adicionar portas ao grupo MVR manualmente. Assim as portas poderão receber tráfego multicast e enviar o endereço IP multicast através da VLAN multicast. Este comando se aplica somente as portas receptoras. O switch adiciona ou remove as portas receptoras aos grupos multicast correspondentes espionando as mensagens de report e leave. Você pode também adicionar manualmente a porta receptora para o grupo MVR.

Sintaxe: **mvr vlan** *vid* **group** *ip-addr*

Parâmetros:

- **vid:** identificação da VLAN multicast. Valores podem variar entre 1 e 4094.
- **Ip-addr:** endereço de IP do grupo multicast.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: adicione a porta 1/0/3 ao grupo MVR 255.1.2.3. A VLAN multicast é a VLAN10:

INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# mvr vlan 10 group 225.1.2.3

19.10. show mvr

Descrição: o comando **show mvr** é usado para exibir as configurações globais do MVR.

Sintaxe: **show mvr**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as configurações globais do MVR.

```
INTELBRAS# show mvr
```

19.11. show mvr interface

Descrição: o comando **show mvr interface** é usado para exibir as configurações do MVR de uma interface específica.

Sintaxe: **show mvr interface gigabitEthernet** [*port* | *port-list*]

Parâmetros:

- **port:** número da porta Ethernet.
- **port-list:** lista de portas Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exibir as configurações do MVR da porta 1/0/3.

```
INTELBRAS# show mvr interface gigabitEthernet 1/0/3
```

19.12. show mvr members

Descrição: o comando **show mvr members** é usado para exibir a informação dos integrantes de todos os grupos MVR ou de um determinado grupo MVR.

Sintaxe: **show mvr members** [*ip-addr*]

Parâmetro:

- **ip-addr:** endereço multicast IP do grupo MVR.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações dos integrantes de todos os grupos MVR.

```
INTELBRAS# show mvr members
```

19.13. show mvr traffic

Descrição: o comando **show mvr traffic** é usado para exibir as estatísticas de todos os grupos MVR.

Sintaxe: **show mvr traffic**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as estatísticas de todos os grupos MVR.

```
INTELBRAS# show mvr traffic
```

20. Comandos MSTP

MSTP (*Multiple Spanning Tree Protocol*) compatível com ambos STP e RSTP sujeito a IEEE 802.1s, pode associar uma rede em anel. O STP é para bloquear links redundantes e links de backup, bem como otimizar caminhos.

20.1. debug spanning-tree

Descrição: o comando **debug spanning-tree** é utilizado ativar a depuração das atividades do Spanning Tree. Para desativar esta depuração utilize o comando **no debug spanning-tree**.

Sintaxe: **debug spanning-tree** {all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc}
no debug spanning-tree {all | bpdu receive | bpdu transmit | cmpmsg | errors | flush | init | migration | proposals | roles | state | tc}

Parâmetros:

- **all:** exibe todas as mensagens de depuração do Spanning Tree.
- **bpdu receive:** mostra as mensagens de depuração recebidas do BPDU (bridge protocol data unit) do Spanning Tree.
- **bpdeu transmit:** mostra as mensagens de depuração enviadas para o BPDU (bridge protocol data unit) do Spanning Tree.
- **cmpmsg:** exibe a prioridade das mensagens de depuração.
- **erros:** exibe as mensagens de erro de depuração do MSTP.
- **flush:** exibe a tabela de endereços liberando mensagens de depuração.
- **init:** exibe a estrutura de inicialização nas mensagens de depuração.
- **migration:** exibe a versão de migração nas mensagens de depuração.
- **proposals:** exibe o MSTP handshake nas mensagens de depuração.
- **roles:** exibe as mudanças de função das interfaces do MSTP nas mensagens de depuração.
- **state:** exibe a alteração de estado da interface do MSTP nas mensagens de depuração.
- **tc:** exibe os eventos de topologia do MSTP nas mensagens de depuração.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: exiba todas as mensagens de depuração do Spanning Tree:

```
INTELBRAS(config)# debug spanning-tree all
```

20.2. spanning-tree (global)

Descrição: o comando **spanning-tree** é utilizado para ativar a função STP de forma global. Para desativar essas função utilize o comando **no spanning-tree**.

Sintaxe: **spanning-tree**
no spanning-tree

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função STP.

```
INTELBRAS(config)# spanning-tree
```

20.3. spanning-tree (interface)

Descrição: o comando **spanning-tree** utilizado para ativar a função de STP para uma porta. Para desabilitar esta função utilize o comando **no spanning-tree**.

Sintaxe: **spanning-tree**
no spanning-tree

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de STP para a porta 1/0/4:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/4
INTELBRAS(config-if)# spanning-tree
```

20.4. spanning-tree common-config

Descrição: o comando **spanning-tree common-config** é utilizado para configurar os parâmetros das portas para comparação no CIST e os parâmetros comuns de todas as instâncias. Para retornar a configuração para os valores padrões utilize o comando **no spanning-tree common-config**. CIST (*Common and Internal Spanning Tree*) é o Spanning Tree de uma rede de switches, conectando todos os dispositivos da rede.

Sintaxe: **spanning-tree common-config** [**port-priority** *pri*] [**ext-cost** *ext-cost*] [**int-cost** *int-cost*] [**portfast** {enable | disabel}] [**point-to-point** {auto | open | close}]
No spanning-tree common-config

Parâmetros:

- **pri:** prioridade da porta, o qual é um número múltiplo de 16 variando entre 0 e 240. Por padrão a prioridade da porta é *128*. A prioridade da porta é um critério importante para determina se a porta conectada a ela será escolhida como porta root. Nesta condição a porta com a maior prioridade será escolhida como root. A porta com valor menor terá maior prioridade.
- **ext-cost:** External Path Cost (custo do caminho externo), o qual é utilizado para calcular o custo e escolher o caminho para as portas em diferentes regiões MST. Esse é um critério importante para determinar a porta root. Valor menor representa uma prioridade maior, os valores variam entre 0 e 2000000. Por padrão vem definido como *0* que significa automático.
- **int-cost:** Internal Path Cost (custo de caminho interno), é utilizado para calcular o custo e escolher o caminho para as portas na mesma região MST. Esse é um critério importante para determinar a porta root. Valor menor representa uma prioridade maior, os valores variam entre 0 e 2000000. Por padrão vem definido como *0* que significa automático.
- **portfast:** habilita e desabilita o Edge Port. Por padrão vem desativada. O Edge Port pode transitar seu estado de bloqueado (blocked) para encaminhando (fowarding) rapidamente sem esperar o atraso do encaminhamento.
- **point-to-point:** representa o status do link ponto a ponto com as opções auto, open e close. Por padrão esta opção vem configurada como automática. Se as duas portas no link ponto a ponto são portas root ou portas designadas, elas podem alterar seus estados para forwarding rapidamente para reduzir os atrasos de encaminhamento desnecessários.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função STP para a porta 1 e configure a prioridade da porta como 64, configure o custo externo como 100 e o custo interno como 100, por final, ative o Edge Port:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# spanning-tree common-config port-priority 64 ext-cost 100
int-cost 100 portfast enable point-to-point open
```

20.5. spanning-tree mode

Descrição: o comando **spanning-tree mode** é utilizado para configurar o modo do STP do switch. Para retornar para o modo padrão utilize o comando **no spanning-tree mode**.

Sintaxe: **spanning-tree mode** {stp | rstp | mstp}
no spanning-tree mode

Parâmetros:

- **stp:** Spanning Trees Protocol, valor padrão.
- **rstp:** Rapid Spanning Tree Protocol.
- **mstp:** Multiple Spanning Tree Protocol.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo Spanning-tree como MSTP:

```
INTELBRAS(config)# spanning-tree mode mstp
```

20.6. spanning-tree mst configuration

Descrição: o comando **spanning-tree mst configuration** é utilizado para acessar o modo de configuração do MST através do Global Configuration, para configurar o mapeamento da instância, nome da região e nível de revisão da VLAN. Para retornar as configurações padrões utilize o comando **no spanning-tree mst configuration**.

Sintaxe: **spanning-tree mst configuration**
no spanning-tree mst configuration

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: acesse o modo de configuração do MST:

```
INTELBRAS(config)# spanning-tree mst configuration
INTELBRAS(config-mst)#
```

20.7. instance

Descrição: o comando **instance** é utilizado para configurar o mapeamento de instâncias da VLAN. Para remover o mapeamento ou desativar o correspondente mapeamento utilize o comando **no instance**. Quando uma instância é desabilitada, o mapeamento relativo da VLAN será removido.

Sintaxe: **instance** *instance-id* **vlan** *vlan-id*
no instance *instance-id* [**vlan** *vlan-id*]

Parâmetros:

- **instance-id:** identificação da instância da VLAN varia entre 1 e 8.
- **vlan-id:** número da VLAN que será mapeada, varia entre 1 e 4094.

Modo de comando: MST Configuration Mode.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Mapeie as VLANs 1 à 100 na instância 1:

```
INTELBRAS# spanning-tree mst configuration
INTELBRAS(config-mst)# instance 1 vlan 1-100
```

Remova o mapeamento das VLANs 1 à 50 do mapeamento anterior.

```
INTELBRAS# spanning-tree mst Configuration
INTELBRAS(config-mst)# no instance 1 vlan 1-50
```

Remova a instância 1 do mapeamento das VLANs.

```
INTELBRAS# spanning-tree mst configuration
INTELBRAS(config-mst)# no instance 1
```

20.8. name

Descrição: o comando **name** é usado para nomear uma região de instância MST.

Sintaxe: **name** *name*

Parâmetro:

- **name:** nome da instância com até 32 caracteres.

Modo de comando: MST Configuration Mode.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o nome da instância como "Intelbras1":

INTELBRAS# spanning-tree mst Configuration
INTELBRAS(config-mst)# name Intelbras1

20.9. revision

Descrição: o comando **revision** é usado para configurar o nível de revisão da instância MST.

Sintaxe: **revision** *revision*

Parâmetro:

» **revision:** nível de revisão para o MST. Varia entre 0 e 65535.

Modo de comando: MST Configuration Mode.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o nível da revisão do MST como 100:

INTELBRAS# spanning-tree mst Configuration
INTELBRAS(config-mst)# revision 100

20.10. spanning-tree mst instance

Descrição: o comando **spanning-tree mst instance** é utilizado para configurar a prioridade da instância MST. Para retornar a prioridade para o valor padrão utilize o comando **no spanning-tree mst instance**. Quando uma instância é desabilitada, o mapeamento relativo da VLAN será removido.

Sintaxe: **spanning-tree mst instance** *instance-id* **priority** *priority*
no spanning-tree mst instance *instance-id* **priority**

Parâmetros:

» **instance-id:** identificação da instância da VLAN varia entre 1 e 8.

» **priority:** prioridade MST a qual deve ser múltiplo de 4096, varia entre 0 e 61440. Por padrão vem configurada como *32768*. É um critério importante na determinação do Root Bridge na instância especificada.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a instância MST 1 e configure a sua prioridade como 4096:

INTELBRAS# spanning-tree mst instance 1 priority 4096

20.11. spanning-tree mst

Descrição: o comando **spanning-tree mst** é utilizado para configurar as instâncias da porta. Para retornar para a configuração padrão utilize o comando **no spanning-tree mst**. Uma porta pode ter diferentes papeis na instância do Spanning Tree. Você pode utilizar este comando para configurar os parâmetros da porta em diferentes ID de instâncias tão como ver o status da porta nas referidas instâncias.

Sintaxe: **spanning-tree mst instance** *instance-id* [**port-priority** *pri*] [**cost** *cost*]
no spanning-tree mst instance *instance-id*

Parâmetros:

» **instance-id:** identificação da instância da VLAN varia entre 1 e 8.

» **pri:** prioridade da porta, deve ser um múltiplo de 16 e varia entre 0 e 240. Por padrão vem configurada como *128*. Critério importante para determinar se a porta será utilizada como root pelo dispositivo conectado à ela.

» **cost:** custo do caminho, varia entre 0 e 200000. Quanto menor o valor maior a prioridade. Valor padrão é *0* que significa prioridade automática.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a prioridade da porta 1 na instância MST 1 como 64 e seu custo como 2000:

INTELBRAS# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# spanning-tree mst instance 1 **port-priority** 64 **cost** 2000

20.12. spanning-tree priority

Descrição: o comando **spanning-tree priority** é utilizado para configurar a prioridade da Bridge. Para voltar a prioridade da Bridge para o valor padrão utilize o comando **no spanning-tree prioirity**.

Sintaxe: **spanning-tree priority** *pri*
no spanning-tree priority

Parâmetros:

» **pri:** prioridade da Bridge, a qual é varia entre 0 e 61440. Por padrão vem configurada como *32768*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a prioridade da Bridge como 4096.

INTELBRAS(config)# spanning-tree priority 4096

20.13. spanning-tree timer

Descrição: o comando **spanning-tree timer** é utilizado para configurar os parâmetros de forward-time, hello-time e max-age do Spanning Tree. Para retornar os parâmetros para o valor padrão utilize o comando **no spanning-tree timer**.

Sintaxe: **spanning-tree timer** {[**forward-time** *forward-time*] [**hello-time** *hello-time*] [**max-age** *max-age*] }
no spanning-tree timer

Parâmetros:

» **foward-time:** atraso de encaminhamento, o qual é o tempo para a porta alterar seu estado quando há alteração na topologia da rede. Este tempo varia entre 4 e 30 segundos e por padrão vem configurado como 15 segundos. Caso contrário, 2*(forward delay -1) >= Max Age.

» **hello-time:** é o intervalo para enviar os pacotes BPDU, é utilizado para testar os links. Este tempo varia entre 1 e 10 segundos e por padrão vem configurado como 2 segundos. Caso contrário, 2*(hello time + 1) <= Max Age.

» **max-age:** é o tempo máximo que o switch pode esperar sem receber BDPU antes de tentar se reconfigurar. Varia entre 6 e 40 segundos, por padrão é *20 segundos*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure forwar-time, hello-time and max-age para o Spanning Tree em 16, 3 e 22 segundos respectivamente:

INTELBRAS(config)# spanning-tree timer forwar-time 16 **hello-time** 3 **max-age** 22

20.14. spanning-tree hold-count

Descrição: o comando **spanning-tree hold-count** é utilizado para configurar o número máximo de pacotes BPDU transmitidos a cada intervalo de Hello Time. Para voltar ao valor padrão utilize o comando **no spanning-tree hold-count**.

Sintaxe: **spanning-tree hold-count** *value*
no spanning-tree hold-count

Parâmetro:

» **value:** número máximo de pacotes, varia entre 1 e 20 pps, por padrão vem configurado como *5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o hold-count para o STP como 8pps:

INTELBRAS(config)# spanning-tree hold-count 8

20.15. spanning-tree max-hops

Descrição: o comando **spanning-tree max-hops** é utilizado para configurar número máximo de saltos que podem ocorrer em uma região específica do antes que o BPDU seja descartado. Para voltar para o valor padrão utilize o comando **no spanning-tree max-hops**.

Sintaxe: **spanning-tree max-hops** *value*
no spanning-tree max-hops

Parâmetros:

» **value:** número que define o máximo de saltos, varia entre 1 e 40 saltos e por padrão vem configurado como *20*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure em 30 o número máximo de saltos para o STP:

INTELBRAS(config)# spanning-tree max-hops 30

20.16. spanning-tree bpdufilter

Descrição: o comando **spanning-tree bpdufilter** é utilizado para habilitar a função de filtro BPDU para a porta. Com essa função ativa a porta pode ser impedida de enviar ou receber qualquer pacote BPDU. Para desabilitar o filtro utilize o comando **no spanning-tree bpdufilter**.

Sintaxe: **spanning-tree bpdufilter**
no spanning-tree bpdufilter

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o filtro BPDU para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# spanning-tree bpdufilter

20.17. spanning-tree bpduflood

Descrição: o comando **spanning-tree bpduflood** é utilizado para habilitar a função de encaminhamento de BPDU para a porta. Com essa função ativa a porta continua enviando pacotes BPDU mesmo com a função *Spanning Tree* desabilitada para ela. Para desabilitar essa função utilize o comando **no spanning-tree bpduflood**.

Sintaxe: **spanning-tree bpduflood**
no spanning-tree bpduflood

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de encaminhamento de BPDU para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# spanning-tree bpduflood

20.18. spanning-tree bpduguard

Descrição: o comando **spanning-tree bpduguard** é utilizado para habilitar a função de proteção de BPDU para a porta. Com essa proteção ativa a porta irá se identificar como ERROR-PORT automaticamente quando receber pacotes BPDU. E a porta irá desativar a função de encaminhamento por um tempo. Para desabilitar essa função utilize o comando **no spanning-tree bpduguard**.

Sintaxe: **spanning-tree bpduguard**
no spanning-tree bpduguard

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de proteção de BPDU para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# spanning-tree bpduguard

20.19. spanning-tree bpduguard loop

Descrição: o comando **spanning-tree bpduguard loop** é utilizado para habilitar a função de proteção de loop na porta. A proteção de loop serve para impedir que os loops na rede sejam recebidos e um recálculo do STP seja feito devido à falhas de link e congestionamentos de rede. Para desabilitar essa função utilize o comando **no spanning-tree bpduguard loop**.

Sintaxe: **spanning-tree bpduguard loop**
no spanning-tree bpduguard loop

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de proteção de loop para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# spanning-tree bpduguard loop

20.20. spanning-tree guard root

Descrição: o comando **spanning-tree guard root** é utilizado para habilitar a função de proteção de BPDU na porta. Com essa proteção ativa a porta irá se identificar como ERROR-PORT automaticamente quando receber pacotes BPDU. E a porta irá desativar a função de encaminhamento por um tempo. Para desabilitar essa função utilize o comando **no spanning-tree guard root**.

Sintaxe: **spanning-tree guard root**
no spanning-tree guard root

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de encaminhamento de BPDU para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# spanning-tree guard root

20.21. spanning-tree guard tc

Descrição: o comando **spanning-tree guard tc** é utilizado para habilitar a função de proteção TC dentro do Spanning Tree na porta. Para desabilitar essa função utilize o comando **no spanning-tree guard tc**. Um switch remove uma entrada de endereço MAC ao receber TC-BPDUs. Se um usuário malicioso enviar continuamente TC-BPDUs para um switch, o switch ficará ocupado removendo entradas de endereço MAC. Com a proteção do Spanning Tree guard tc habilitada você pode configurar o número de TC-BPDUs em um determinado tempo para evitar a remoção de endereços MAC frequentemente.

Sintaxe: **spanning-tree guard tc**
no spanning-tree guard tc

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função TC Protect of Spanning Tree para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# spanning-tree guard tc

20.22. spanning-tree mcheck

Descrição: o comando **spanning-tree mcheck** é utilizado para habilitar o mcheck.

Sintaxe: **spanning-tree mcheck**

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de mcheck para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# spanning-tree mcheck

20.23. show spanning-tree active

Descrição: o comando **show spanning-tree active** é utilizado mostrar as informações ativas do Spanning Tree.

Sintaxe: **show spanning-tree active**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações ativas do Spanning Tree:

INTELBRAS# show spanning-tree active

20.24. show spanning-tree bridge

Descrição: o comando **show spanning-tree bridge** é utilizado para mostrar os parâmetros de bridge.

Sintaxe: **show spanning-tree bridge** [forward-time | hello-time | hold-count | max-age | max-hops | mode | priority | state]

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba os parâmetro de bridge:

INTELBRAS# show spanning-tree bridge

20.25. show spanning-tree interface

Descrição: o comando **show spanning-tree interface** é utilizado para mostrar as informações de Spanning Tree de todas as portas ou de uma porta específica.

Sintaxe: **show spanning-tree interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*] [edge | ext-cost | int-cost | mode | p2p | priority | role | state | status]

Parâmetros:

- **port:** número da porta Ethernet.
- **port-channel-id:** ID do porthchannel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplos:

Exiba a informação de Spanning Tree de todas as portas:

```
INTELBRAS# show spanning-tree interface
```

Exiba a informação de Spanning Tree da porta 1/0/2:

```
INTELBRAS# show spanning-tree interface gigabitEthernet 1/0/2
```

Exiba o modo de Spanning Tree de porta 1/0/2:

```
INTELBRAS# show spanning-tree interface gigabitEthernet 1/0/2 mode
```

20.26. show spanning-tree interface-security

Descrição: o comando **show spanning-tree interface-security** é utilizado mostrar as informações proteção de todas as portas ou de uma porta específica.

Sintaxe: **show spanning-tree interface-security** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*] [bpdufilter | bpduguard | loop | root | tc]

Parâmetros:

- **port:** número da porta Ethernet.
- **port-channel-id:** ID do porthchannel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplos:

Exiba a informação de Spanning Tree de todas as portas:

```
INTELBRAS# show spanning-tree interface-security
```

Exiba a informação de Spanning Tree da porta 1/0/2:

```
INTELBRAS# show spanning-tree interface-security gigabitEthernet 1/0/2
```

Exiba a informação de segurança bpdufilter da interface:

```
INTELBRAS# show spanning-tree interface-security bpdufilter
```

20.27. show spanning-tree mst

Descrição: o comando **show spanning-tree mst** é utilizado mostrar as informações de uma instância MST.

Sintaxe: **show spanning-tree mst** {**configuration** [**digest**] | **instance** *instance-id* [**interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]]}

Parâmetros:

- **instance-id:** ID da instância desejada, varia entre 1 e 8.
- **port:** Número da porta Ethernet.
- **port-channel-id:** ID do porthchannel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplos:

Exiba as informações de região e mapeamento de VLAN e instância MST:

```
INTELBRAS# show spanning-tree mst configuration
```

Exiba as informações relativas à instância 1:

```
INTELBRAS# show spanning-tree mst instance 1
```

Exiba todas as informações das portas da instância 1:

```
INTELBRAS# show spanning-tree mst instance 1 interface
```

21. Comandos LLDP

A função LLDP permite que os dispositivos de rede façam a divulgação de algumas informações do dispositivo periodicamente para os vizinhos na mesma LAN. As informações dos dispositivos LLDP na LAN podem ser armazenados pelo seu vizinho em uma MIB padrão, então é possível que a informação a ser acessada por um Sistema de Gerenciamento de Rede (NMS) usando SNMP.

21.1. lldp

Descrição: o comando **lldp** é usado para habilitar a função LLDP. Para desativar a função LLDP, utilize o comando **no lldp**.

Sintaxe: **lldp**
no lldp

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a função LLDP globalmente:

```
INTELBRAS(config)# lldp
```

21.2. lldp forward_message

Descrição: o comando **lldp forward_message** é usado para habilitar a função de transmissão de mensagens LLDP quando a função LLDP estiver desabilitada. Para desativar encaminhamento de mensagens LLDP, utilize o comando **no lldp forward_message**.

Sintaxe: **lldp forward_message**
no lldp forward_message

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite o switch para encaminhar mensagens LLDP quando a função LLDP está desativada globalmente:

```
INTELBRAS(config)# lldp forward_message
```

21.3. LLDP hold-multiplier

Descrição: o comando **lldp hold-multiplier** é usado para configurar o parâmetro Hold Multiplier. O tempo de envelhecimento (aging-time) da informação local no dispositivo vizinho é determinado pelo valor do TTL real usado no envio do LLDPDU. TTL = Hold Multiplier * Intervalo de transmissão. Para retornar à configuração padrão, utilize o comando **no lldp hold-multiplier**.

Sintaxe: **lldp hold-multiplier** *multiplier*
no lldp hold-multiplier

Parâmetro:

» **multiplier:** configure o parâmetro Hold Multiplier. Ele varia de 2 a 10. Por padrão, ele é *4*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: especifique o Hold Multiplier como 5:

```
INTELBRAS(config)#lldp hold-multiplier 5
```

21.4. lldp timer

Descrição: o comando **lldp timer** é usado para configurar os parâmetros sobre a transmissão. Para retornar à configuração padrão, utilize o comando **no lldp timer**.

Sintaxe: **lldp timer** {**tx-interval** *tx-interval* | **tx-delay** *tx-delay* | **reinit-delay** *reinit-delay* | **notify-interval** *notify-interval* | **fast-count** *fast-count*}
no lldp timer {tx-interval | tx-delay | reinit-delay | notify-interval | fast-count}

Parâmetros:

» **tx-interval:** configure o intervalo para o dispositivo local para transmitir LLDPDU para seus vizinhos. O valor varia de 5 a 32768, e o valor padrão é de *30 segundos*.

» **tx-delay:** configurar um valor de 1 a 8192 segundos para especificar o tempo para o dispositivo local transmitir LLDPDU a seus vizinhos depois de ocorrerem alterações e evitar que os LLDPDU sejam enviados com frequência. O valor padrão é de *2 segundos*.

» **reinit-delay:** este parâmetro indica a quantidade de atraso a partir de quando o estado LLDP passa para *disable* até que reinicialização seja feita. O valor varia de 1 a 10 e o valor padrão é *2*.

» **notify-interval:** especifique o intervalo da mensagem TRAP que será enviada do dispositivo local ao sistema de gerenciamento de rede. O valor varia de 5 a 3600 e o valor padrão é de *5 segundos*.

» **fast-count:** quando as portas LLDP passam de *Disable* (ou Rx_Only) para Tx & Rx (ou Tx_Only), o mecanismo de início rápido será ativado, ou seja, o intervalo de transmissão será encurtado a um segundo, e vários LLDPDUs serão enviado (o número de LLDPDUs é igual a este parâmetro). O valor varia de 1 a 10, e o valor padrão é *3*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: especifique o intervalo de transmissão de LLDPDU como 45 segundos e a mensagem Trap para NMS como 120 segundos:

INTELBRAS(config)#lldp timer tx-interval 45
INTELBRAS(config)#lldp timer notify-interval 120

21.5. lldp receive

Descrição: o comando **lldp receive** é utilizado para permitir que a porta designada receba LLDPDU. Para desativar a função, utilize o comando **no lldp receive**.

Sintaxe: **lldp receive**
no lldp receive

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: ativar porta 1/0/1 para receber LLDPDU:

INTELBRAS(config)#interface gigabitEthernet 1/0/1
INTELBRAS(config)#lldp receive

21.6. lldp transmit

Descrição: o comando **lldp transmit** é utilizado para habilitar que uma porta designada transmita LLDPDU. Para desativar a função, utilize nenhum comando **no lldp transmit**.

Sintaxe: **lldp transmit**
no lldp transmit

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet)

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilitar a porta Gigabit Ethernet 1/0/1 para transmitir LLDPDU:

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config)#lldp transmit

21.7. Lldp snmp-Trap

Descrição: o comando **lldp snmp-trap** é usado para ativar a notificação SNMP da porta. Se ativado, a porta vai notificar o evento Trap no sistema de gerenciamento de rede. Para desativar a notificação SNMP das portas, por favor use comando **no lldp snmp-trap**.

Sintaxe: **lldp snmp-trap**
no lldp snmp-trap

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: ativar a notificação de SNMP para porta Gigabit Ethernet 1/0/1:

INTELBRAS(config)#interface gigabitEthernet 1/0/1
INTELBRAS(config)#lldp snmp-trap

21.8. lldp tlv-select

Descrição: o comando **lldp tlv-select** é usado para configurar TLVs para serem incluídos no LLDPDU de saída. Para excluir TLVs, utilize o comando **no lldp tlv-select**. Por padrão, todos os TLVs estão inclusos no LLDPDU saída.

Sintaxe: **lldp tlv-select** {[port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan] [protocol-vlan] [vlan-name] [link-aggregation] [mac-phy-cfg] [max-frame-size] [power] [all]}
no lldp tlv-select {[port-description] [system-capability] [system-description] [system-name] [management-address] [port-vlan] [protocol-vlan] [vlan-name] [link-aggregation] [mac-phy-cfg] [max-frame-size] [power] [all]}

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: exclua "Gestão de endereçamento" e "porta-vlan-id" TLVs no LLDPDU de saída na porta gigabit ethernet 1/0/1:

INTELBRAS(config)#interface gigabitEthernet 1/0/1
INTELBRAS(config)#no lldp tlv-select management-address port-vlan

21.9. lldp management-address

Descrição: o comando **lldp management-address** é usado para configurar o endereços de gerenciamento da porta para serem incluídos no campo de endereço de gerenciamento do TLV. A NMS usa endereços de gestão para identificar os dispositivos. Para excluir o endereço administração da porta, utilize o comando **no lldp management address**.

Sintaxe: **lldp management-address** {*ip-address*}
no lldp management-address

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure o endereço de gerenciamento da porta como 192.168.1.100 para a porta 1/0/1:

INTELBRAS(config)#interface gigabitEthernet 1/0/1
INTELBRAS(config)#lldp management-address 192.168.0.100

21.10. show lldp

Descrição: o comando **show lldp** é usado para exibir a configuração global do LLDP.

Sintaxe: **show lldp**

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: mostre a configuração global de LLDP:

INTELBRAS(config)# show lldp

21.11. show lldp interface

Descrição: o comando **show lldp interface** é usado para exibir a configuração de LLDP da porta correspondente. Por padrão, a configuração LLDP de todas as portas são exibidas.

Sintaxe: **show lldp interface** [**gigabitEthernet** *port*]

Parâmetro:

» **port:** número da porta Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: mostre a configuração LLDP de Gigabit Ethernet de porta 1/0/1:

INTELBRAS(config)# show lldp interface gigabitEthernet 1/0/1

21.12. show lldp local-information interface

Descrição: o comando **show lldp local-information interface** é utilizado para exibir as informações de LLDP da porta correspondente. Por padrão, as informações LLDP de todas as portas serão exibidas.

Sintaxe: **show lldp local-information interface** [**gigabitEthernet** *port*]

Parâmetro:

» **port:** o número da porta Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: exiba a informação LLDP da 1/0/1:

INTELBRAS(config)# show lldp local-information interface gigabitEthernet 1/0/1

21.13. show lldp neighbor-information interface

Descrição: o comando **show lldp neighbor-information interface** é utilizado para exibir as informações dos vizinhos da porta correspondente. Por padrão, as informações dos vizinhos de todas as portas são exibidas.

Sintaxe: **show lldp neighbor-information interface** [**gigabitEthernet** *port*]

Parâmetro:

» **port:** o número da porta Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: exiba as informações do vizinho da porta Ethernet gigabit 1/0/1:

```
INTELBRAS(config)# show lldp neighbor-information interface gigabitEthernet 1/0/1
```

21.14. show lldp traffic interface

Descrição: o comando **show lldp traffic interface** é utilizado para exibir a informação estatística de LLDP entre o dispositivo local e dispositivo vizinho da porta correspondente. Por padrão, o LLDP informação estatística de todas as portas serão exibidos.

Sintaxe: **show lldp traffic interface** [**gigabitEthernet** *port*]

Parâmetro:

» **port:** o número da porta Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: não há.

Exemplo: exiba a informação estatística LLDP de Gigabit Ethernet de porta 1/0/1:

```
INTELBRAS(config)# show lldp traffic interface gigabitEthernet 1/0/1
```

22. Comandos de rotas estáticas

22.1. ip routing

Descrição: o comando **ip routing** é usado para ativar o roteamento IPv4 globalmente. Para desativar o roteamento IPv4, utilize o comando **no ip routing**.

Sintaxe: **ip routing**
no ip routing

Modo de comando: Global Configuration.

Requisitos de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: ative o recurso de roteamento IPv4 para o switch:

```
INTELBRAS(config)# ip routing
```

22.2. interface vlan

Descrição: o comando **interface vlan** é usado para criar a interface VLAN. Para apagar a interface VLAN especificada, utilize o comando **no interface vlan**.

Sintaxe: **interface vlan** {*vid*}
no interface vlan {*vid*}

Parâmetro:

» **vid:** o ID da VLAN.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie a interface VLAN 2:

```
INTELBRAS(config)# interface vlan 2
```

22.3. Interface loopback

Descrição: o comando **interface loopback** é usado para criar a interface de **loopback**. Para apagar a interface de **loopback** especificada, utilize o comando **no interface loopback**.

Sintaxe: **interface loopback** {*id*}
no interface loopback {*id*}

Parâmetro:

» **id:** o nome da interface de loopback, variando de 1 a 64.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie a interface de loopback 1:

```
INTELBRAS(config)# Interface 1
```

22.4. switchport

Descrição: o comando **switchport** é usado para mudar a interface da camada 3 para a camada 2 da porta. Para mudar a porta da camada 2 para a camada 3, utilize o comando **no switchport**.

Sintaxe: **switchport**
no switchport

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: mude portas 1/0/9 para porta roteada:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/9
INTELBRAS(config)# no switchport
```

22.5. interface range port-channel canal

Descrição: o comando **interface range port-channel** é usado para criar múltiplas interfaces port-channel.

Sintaxe: **interface range port-channel** *port-channel-list*

Parâmetro:

» **port-channel-list:** a lista da interface port-channel, que varia de 1 a 14, no formato de *1-3, 5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie as interfaces port-channel 1, 3, 4 e 5:

```
INTELBRAS(config)# interface port-channel 1,3-5
```

22.6. description

Descrição: o comando **description** é utilizado para adicionar uma descrição para a interface da camada 3, incluindo routed port, port-channel interface, loopback interface e VLAN interface. Para limpar a descrição da interface correspondente, utilize o comando **no description**.

Sintaxe: **description** *string*
no description

Parâmetro:

» **string:** conteúdo de uma descrição de interface, variando de 1 a 32 caracteres.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: adicione uma descrição do system-if para a porta roteada1/0/9:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/9
INTELBRAS(config)# no switchport
INTELBRAS(config)# description system-if
```

22.7. shutdown

Descrição: o comando **shutdown** é usado para desligar a interface especificada. O tipo de interface inclui: port, port-channel interface, loopback interface and VLAN interface VLAN. Para ativar a interface especificada, utilize o comando **no shutdown.**

Sintaxe: **shutdown**
no shutdown

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: desative a porta roteada 1/0/9:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/9
INTELBRAS(config)# no switchport
INTELBRAS(config)# shutdown
```

22.8. interface port-channel

Descrição: o comando **interface port-channel** é usada para criar a interface de port-channel. Para excluir a interface port-channel especificada, utilize o comando **no interface port-channel.**

Sintaxe: **interface port-channel** { *port-channel-id* }
no interface port-channel { *port-channel-id* }

Parâmetro:

» **port-channel-id:** o nome da interface de port-channel, que varia de 1 a 14.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie a interface port-channel 1:

```
INTELBRAS(config)# interface port-channel 1
```

22.9. ip route

Descrição: o comando **ip route** é usado para configurar a rota estática. Para limpar a entrada correspondente, utilize o comando **no ip route**.

Sintaxe: **ip route** {*dest-address*} {*mask*} {*next-hop-address*} [*distance*]
no ip route {*dest-address*} {*mask*} {*next-hop-address*}

Parâmetros:

» **dest-address:** o endereço IP de destino.
» **mask:** a máscara de sub-rede.
» **next-hop-address:** o endereço da próximo salto.
» **distance:** a métrica de distância desta rota, que vai de 1 a 255. Quanto menor a distância, maior será a prioridade.

Modo de comando: Global Configuration.

Requisitos de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie uma rota estática com o endereço IP da rede remota como 192.168.2.0, a máscara de sub-rede 255.255.255.0 e o endereço do próximo salto como 192.168.0.2:

```
INTELBRAS(config)# ip route 192.168.2.0 255.255.255.0 192.168.0.2
```

22.10. Roteamento IPv6

Descrição: o comando de roteamento IPv6 é usado para ativar o recurso de roteamento IPv6. Para desativar o roteamento IPv6, utilize o comando **no ipv6 routing**.

Sintaxe: **ipv6 routing**
no ipv6 routing

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: ative o roteamento IPv6:

```
INTELBRAS(config)# ipv6 routing
```

22.11. ipv6 route

Descrição: o comando **ipv6 route** é usado para configurar uma rota estática IPv6. Para limpar a entrada correspondente, utilize o comando **no ipv6 route**.

Sintaxe: **ipv6 route** {*ipv6-dest-address*} {*next-hop-address*} [*distance*]
no ipv6 route {*ipv6-dest-address*} {*next-hop-address*}

Parâmetros:

- **ipv6-dest-address:** o endereço IPv6 da rede de destino.
- **next-hop-address:** o endereço IPv6 da próxima salto.
- **distance:** a métrica de distância desta rota, que vai de 1 a 255. Quanto menor a distância, maior será a prioridade.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie uma rota estática com o endereço IP da rede remota como 3200::/ 64 e o endereço do próximo salto como 3100::1234:

```
INTELBRAS(config)# ipv6 3200::/ 64 3100::1234
```

22.12. show interface vlan

Descrição: o comando **show interface vlan** é usado para exibir as informações da VLAN interface especificada.

Sintaxe: **show interface vlan** *vid*

Parâmetro:

- **vid:** o ID VLAN.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: mostre a informação de VLAN 2:

```
INTELBRAS(config)# show interface vlan 2
```

22.13. show ip interface

Descrição: o comando **show ip interface** é usado para exibir as informações detalhadas da interface especificada na camada 3.

Sintaxe: **show ip interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id* | **loopback** *id* | **vlan** *vlan-id*]

Parâmetros:

- **port:** o número de porta.
- **port-channel-id:** o ID port-channel. Membros desse port-channel devem ter todas suas portas roteadas.
- **id:** o nome da interface de loopback.
- **vlan-id:** o nome da interface VLAN.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: exiba as informações detalhadas da interface VLAN 2:

```
INTELBRAS(config)# show ip interface vlan 2
```

22.14. show ip interface brief

Descrição: o comando **show ip interface brief** é usado para exibir um resumo das informações de interface de camada 3.

Sintaxe: **show ip interface brief**

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: exiba as informações de sumário das interfaces de camada 3:

```
INTELBRAS(config)# show ip interface brief
```

22.15. show ip route

Descrição: o comando **show ip route** é usado para exibir as rotas da tabela de roteamento.

Sintaxe: **show ip route** [static | connected]

Parâmetros:

- **static | connected:** especifique o tipo de rota. Se não for especificado, todos os tipos de entradas da rota serão exibidos.
  - **static:** as rotas estáticas.
  - **connected:** as rotas conectadas.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: exiba as rotas estáticas:

```
INTELBRAS(config)# show ip route static
```

22.16. show ip route specify

Descrição: o comando **show ip route specify** é usado para exibir as informações de roteamento válido para o endereço de rede ou segmentos de IP especificados.

Sintaxe: **show ip route specify** {*ip*} [*mask*] [**longer-prefixes**]

Parâmetros:

- **ip:** especifique o endereço IP de destino.
- **mask:** especifique o endereço IP de destino, juntamente com o IP parâmetro.
- **longer-prefixes:** especifica as sub-redes de destino que correspondem ao segmento de rede determinada pelos parâmetros IP e a máscara.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplos:

Exiba a rota mais curta para 192.168.0.100:

```
INTELBRAS(config)# show ip route specify 192.168.0.100
```

Procure a entrada de rota com o destino como 192.168.0.0/24:

```
INTELBRAS(config)# show ip route specify 192.168.0.0 255.255.255.0
```

Exiba as rotas para todas as sub-redes que pertence a 192.168.0.0/16:

```
INTELBRAS(config)# show ip route specify 192.168.0.0 255.255.0.0 longer-prefixes
```

22.17. show ip route summary

Descrição: o comando **show ip route summary** é usado para exibir as informações resumidas das entradas de rotas.

Sintaxe: **show ip route summary**

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: exiba as informações de resumo das rotas:

```
INTELBRAS(config)# show ip route summary
```

22.18. show ipv6 interface

Descrição: o comando **show ipv6 interface** é usado para exibir as informações IPv6 da interface de gerenciamento, incluindo o endereço link-local e endereço global, grupos multicast IPv6 etc.

Sintaxe: **show ipv6 interface**

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: não há.

Exemplo: mostre as informações do IPv6 da interface de gerenciamento:

```
INTELBRAS(config)# show ipv6 interface
```

22.19. show ipv6 route

Descrição: o comando **show ipv6 route** é usado para exibir as rotas IPv6 configuradas.

Sintaxe: **show ipv6 route** [static | connected]

Parâmetros:

- **static | connected:** especifique o tipo de rota. Se não for especificado, todos os tipos de entradas da rota serão exibidos.
  - **static:** as rotas estáticas.
  - **connected:** as rotas conectadas.

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: exiba as rotas estáticas IPv6:

```
INTELBRAS(config)# show ipv6 route static
```

22.20. show ipv6 route summary

Descrição: o comando **show ipv6 route summary** é usado para exibir as informações resumidas das entradas de rotas IPv6 classificados por suas fontes.

Sintaxe: **show ipv6 route summary**

Modo de comando: Configuration and Privileged EXEC.

Requisitos de privilégio: nenhum.

Exemplo: exiba as informações resumidas das rotas IPv6:

```
INTELBRAS(config)# show ipv6 route summary
```

23. Comandos de configuração de endereços IPv6

Os comandos de configuração do endereço IPv6 são fornecidos no modo Interface Configuration Mode, que inclui a porta roteada, link-agreggation e a interface VLAN. Entre no modo de configuração dessas interfaces na Camada 3 para configurar os parâmetros IPv6.

23.1. ipv6 enable

Descrição: esse comando é usado para ativar a função IPv6 na Camada 3 na interface especificada A função IPv6 deve ser ativada antes do endereço IPv6 de gerenciamento de configurações. Por padrão, ele é ativado na interface VLAN 1. A função IPv6 só pode ser ativada em uma interface da Camada 3 de cada vez.

Se a função IPv6 estiver desativada, os módulos correspondentes baseados em IPv6 serão inválidos, por exemplo, SSHv6, SSLv6, TFTPv6 e mais. Para desabilitar a função IPv6, por favor, use o comando **no ipv6 enable.**

Sintaxe: **ipv6 enable**
no ipv enable

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o IPv6 na interface VLAN 1:

```
INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ipv6 enable
```

23.2. ipv6 addres autoconfig

Descrição: este comando é usado para habilitar a configuração automática do endereço link-local ipv6. O switch tem apenas um endereço ipv6 link-local, que pode ser configurado automaticamente ou manualmente. O endereço ipv6 link-local geral tem o prefixo como fe80::/10. Roteadores IPv6 não podem encaminhar pacotes com endereços link-local de origem ou destino para outros links. O endereço ipv6 link-local está no formato *EUI-64*. Para verificar a singularidade do link-local, o endereço IPV6 link-local configurado manualmente será excluído quando o endereço IPV6 link-local for ativado automaticamente.

Sintaxe: **ipv6 address autoconfig**

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a configuração automática do endereço ipv6 link-local na interface VLAN 1:

```
INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ipv6 address autoconfig
```

23.3. ipv6 addres link-local

Descrição: o comando **ipv6 address link-local** é usado para configurar manualmente o endereço IPv6 de link-local em uma interface especificada. Para excluir o endereço local configurado, use o comando **no comando ipv6 address link-local**.

Sintaxe: **ipv6 address** *ipv6-addr* **link-local**
no ipv6 address *ipv6-addr* **link-local**

Parâmetro:

» **Ipv6-addr:** o endereço link-local da interface deve ser um endereço IPv6 com o prefixo fe80::/10, caso contrário, este comando será inválido.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o endereço link-local como fe80::1234 na interface VLAN 1:

```
INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ipv6 address fe80::1234 link-local
```

23.4. ipv6 address dhcp

Descrição: o comando **ipv6 address dhcp** é usado para ativar a função cliente DHCPv6. Quando esta função está ativada, a interface tentará obter o IP do servidor DHCPv6. Para excluir o IP alocado do servidor DHCPv6 e desativar a função DHCPv6 Client, por favor, use o comando **no ipv6 address dhcp**.

Sintaxe: **ipv6 address dhcp**
no ipv6 address dhcp

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função Cliente DHCP na interface VLAN 1:

INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ipv6 address dhcp

23.5. ipv6 address ra

Descrição: esse comando é usado para configurar o endereço IPv6 global da interface de acordo com o prefixo de endereço e outros parâmetros de configuração da mensagem RA (anúncio de roteador) recebida. Para desabilitar esta função, por favor, use o comando **no ipv6 address ra.**

Sintaxe: **ipv6 address ra**
no ipv6 address ra

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de configuração automática do endereço IPv6 para obter o endereço IPv6 através da mensagem RA na interface VLAN 1:

INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ipv6 address ra

23.6. ipv6 address eui-64

Descrição: esse comando é usado para configurar manualmente um endereço IPv6 global com um identificador exclusivo estendido (EUI) nos 64 bits de baixa ordem na interface. Especifique apenas o prefixo da rede. Os últimos 64 bits são calculados automaticamente a partir do endereço MAC do switch. Para remover um endereço IPv6 EUI-64 da interface, use o comando **no ipv6 address eui-64**.

Sintaxe: **ipv6 address ipv6-addr eui-64**
no ipv6 address *ipv6-addr* **eui-64**

Parâmetros:

» **ipv6-addr:** endereço IPv6 global com prefixo de rede de 64 bits, por exemplo, 3ffe::/64.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure um endereço global EUI-64 na interface com o prefixo de rede 3ffe::/64:

INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ipv6 address 3ffe::/64 **eui-64**

23.7. ipv6 address

Descrição: esse comando é usado para configurar manualmente um endereço IPv6 global na interface. Para remover um endereço IPv6 global da interface, use o comando **no ipv6 address**.

Sintaxe: **ipv6 address** *ipv6-addr*
no ipv6 address *ipv6-addr*

Parâmetros:

» **ipv6-addr:** endereço IPv6 global com prefixo de rede, por exemplo 3ffe::1/64.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure um endereço global 3001::1/64 na interface VLAN 1:

```
INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ipv6 address 3001::1/64
```

23.8. show ipv6 interface

Descrição: este comando é usado para exibir as informações configuradas do IPv6 na interface de gerenciamento, incluindo o status da função IPv6, o endereço local vinculado e o endereço global, grupos multcast IPv6 entre outros.

Sintaxe: **show ipv6 interface**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações de IPv6 na interface de gerenciamento:

```
INTELBRAS(config)# show ipv6 interface
```

24. Comandos ARP

O *Address Resolution Protocol* (ARP) é usado para resolver um endereço IP para um endereço MAC Ethernet. O switch mantém uma tabela de mapeamento ARP para gravar as relações de mapeamento IP para MAC que é usado para o encaminhamento de pacotes. Uma tabela de mapeamento ARP contém dois tipos de entradas; ARP dinâmicas e ARP estáticas. Uma entrada ARP dinâmica é automaticamente criada e mantida pela ARP. Uma entrada ARP estática é configurada e mantida manualmente.

24.1. arp

Descrição: o comando **arp** é usado para adicionar uma entrada ARP estática. Para excluir a entrada ARP especificada, utilize o comando **no arp**.

Sintaxe: **arp** *ip mac type*
no arp *ip type*

Parâmetros:

» **ip:** endereço IP da entrada ARP estática.
» **mac:** endereço MAC da entrada ARP estática.
» **type:** tipo do ARP. Configurá-lo como arp.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie uma entrada ARP estática com o IP 192.168.0.1, e o MAC 00:11:22:33:44:55:

```
INTELBRAS(config)# arp 192.168.0.1 00:11:22:33:44:55 arp
```

24.2. clear arp-cache

Descrição: o comando **clear arp-cache** é usado para limpar todas as entradas ARP dinâmicas.

Sintaxe: **clear arp-cache**

Modo de comando: Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: limpe todas as entradas ARP dinâmicas:

```
INTELBRAS(config)# clear arp-cache
```

24.3. arp dynamicrenew

Descrição: o comando **arp dynamicrenew** é usado para renovar automaticamente as entradas ARP dinâmicas. Para desativar renovação automática das entradas ARP dinâmicas, utilize o comando **no arp dynamicremew**. Por padrão, esta função vem habilitada.

Sintaxe: **arp dynamicremew**
no arp dynamicremew

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite o switch para renovar automaticamente as entradas ARP dinâmicas:

```
INTELBRAS(config)# arp dynamicrenew
```

24.4. arp timeout

Descrição: o comando **arp timeout** é usado para configurar o aging time ARP (tempo de envelhecimento) da interface.

Sintaxe: **arp timeout** *timeout*
no arp timeout

Parâmetro:

» **timeout:** especifica o tempo do aging time, que vai de 10 a 3000 segundos. O valor padrão é *1200 segundos*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure o ARP aging time em 60 segundos:

```
INTELBRAS(config)# arp timeout 60
```

24.5. gratuitous-arp intf-status-up enable

Descrição: o comando **gratuitous-arp intf-status-up enable** é usado para ativar a interface de camada 3 para enviar um pacote gratuitous ARP quando o status da interface passar a ser UP.

Sintaxe: **gratuitous-arp intf-status-up enable**
no gratuitous-arp intf-status-up enable

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: ative a interface camada 3 do switch para enviar pacotes ARP gratuito quando seu estado estiver UP:

```
INTELBRAS(config)# gratuitous-arp intf-status-up enable
```

24.6. gratuitous-arp dup-ip-detected enable

Descrição: o comando **gratuitous-arp dup-ip-detected enable** é usado para ativar a interface de camada 3 para enviar um pacote de gratuitous ARP ao receber uma gratuitous packets com o mesmo endereço IP.

Sintaxe: **gratuitous-arp dup-ip-detected enable**
no gratuitous-arp dup-ip-detected enable

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: ative a interface de camada 3 do switch para enviar pacotes gratuitous ARP ao receber uma gratuitous packets com o mesmo endereço IP:

```
INTELBRAS(config)# gratuitous-arp dup-ip-detected enable
```

24.7. gratuitous-arp learning enable

Descrição: o comando **gratuitous-arp learning enable** é usado para ativar a interface de camada 3 para aprender os endereços MAC dos pacotes gratuitous ARP.

Sintaxe: **gratuitous-arp learning enable**
no gratuitous-arp learning enable

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: habilite a interface de camada 3 para aprender endereços MAC dos pacotes gratuitous ARP:

```
INTELBRAS(config)# gratuitous-arp learning enable
```

24.8. gratuitous-arp send-interval

Descrição: o comando **gratuitous-arp send-interval** é usado para configurar o intervalo no qual a interface irá enviar periodicamente os pacotes gratuitous ARP.

Sintaxe: **gratuitous-arp send-interval** *interval*

Parâmetro:

» **Interval:** especifica o intervalo no qual a interface irá enviar periodicamente os pacotes gratuitous ARP. O valor 0 significa que a interface não irá enviar pacotes ARP.

Modo de comando: Interface Configuration (interface vlan / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: nenhum.

Exemplo: configure a interface VLAN 1 para enviar pacotes gratuitous ARP a cada 1 segundo:

```
INTELBRAS(config)# interface vlan 1
INTELBRAS(config)# gratuitous-arp send-interval 1
```

24.9. ip proxy-arp

Descrição: o comando **ip proxy-arp** é usado para ativar a função de Proxy ARP na interface VLAN especificada ou porta roteada. Para desativar o Proxy ARP nesta interface, utilize o comando **no ip proxy-arp**.

Sintaxe: **ip proxy-arp**
no ip proxy-arp

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: nenhum.

Exemplos:

Habilite a função ARP Proxy na interface VLAN 2:

```
INTELBRAS(config)# Interface vlan 2
INTELBRAS(config)# ip proxy-arp
```

Habilite a função ARP Proxy na porta roteada 1/0/2:

```
INTELBRAS(config)# interface gigabitEthernet 2
INTELBRAS(config)# no switchport
INTELBRAS(config)# ip proxy-arp
```

24.10. ip local-proxy-arp

Descrição: o comando **ip local-proxy-arp local** é usado para habilitar a função Proxy ARP localmente na interface VLAN especificada, ou uma porta roteada. Para desabilitar a função Local Proxy ARP nesta interface, utilize o comando **no ip local-proxy-arp**.

Sintaxe: **ip local-proxy-arp**
no ip local-proxy-arp

Modo de comando: Interface Configuration (Interface vlan / interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: nenhum.

Exemplos:

Habilite a função ARP Proxy na interface VLAN 2:

```
INTELBRAS(config)# interface vlan 2
INTELBRAS(config)# ip local-proxy-arp
```

Habilite a função ARP Proxy na porta roteada 1/0/2:

```
INTELBRAS(config)# interface gigabitEthernet 2
INTELBRAS(config)# no switchport
INTELBRAS(config)# ip local-proxy-arp
```

24.11. show arp

Descrição: o comando **show arp** é usado para exibir as entradas ARP ativas. Se nenhum parâmetro for especificado, todas as entradas ARP ativas serão exibidas.

Sintaxe: **show arp** [*ip*] [*mac*]

Parâmetros:

- **ip:** especifica o endereço IP da sua entrada ARP desejado.
- **mac:** especifica o endereço MAC da sua entrada ARP desejada.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba a entrada ARP com o IP 192.168.0.2:

```
INTELBRAS(config)# show arp 192.168.0.2
```

24.12. show ip arp (interface)

Descrição: o comando **show ip arp (interface)** é utilizado para exibir as entradas ARP ativas associadas com uma interface especificada da Camada 3.

Sintaxe: **show ip arp** {**gigabitEthernet** *port* | **port-channel** *port-channel-id* | **vlan** *id*}

Parâmetros:

- **port:** especifica o número da porta roteada.
- **port-channel-id:** especifica o ID do canal da porta.
- **id:** especifica o ID da interface VLAN.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba a entrada ARP associada à interface VLAN 2:

```
INTELBRAS(config)# show ip arp vlan 2
```

24.13. show ip arp summary

Descrição: o comando **show ip arp summary** é usado para exibir o número de entradas ARP ativas.

Sintaxe: **show ip arp summary**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba o número de entradas ARP:

```
INTELBRAS(config)# show ip arp summary
```

24.14. show gratuitous-arp

Descrição: o comando **show gratuitous arp** é usado para exibir a configuração do gratuitous ARP.

Sintaxe: **show gratuitous-arp**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba a configuração de gratuitous ARP:

```
INTELBRAS(config)# show gratuitous-arp
```

24.15. show ip proxy-arp

Descrição: o comando **show ip proxy-arp** é usado para exibir o status do Proxy ARP.

Sintaxe: **show ip proxy-arp**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba o estado ARP Proxy:

```
INTELBRAS(config)# show ip proxy-arp
```

25. Comandos servidor DHCP

DHCP (*Dynamic Host Configuration Protocol*) é um protocolo de configuração de rede para hosts em redes TCP / IP e fornece uma estrutura para distribuição de informações de configuração para hosts. O servidor DHCP atribui endereços IP de pools de endereços especificados em um switch ou roteador a clientes DHCP e os gerencia.

25.1. service dhcp server

Descrição: o comando **service dhcp server** é utilizado para ativar o serviço de DHCP de forma global. Para desabilitar o serviço de DHCP utilize o comando **no service dhcp server**.

Sintaxe: **service dhcp server**
no service dhcp server

Modo de comando: Global Configuration.

Requisito de privilégio: Somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o serviço de servidor DHCP de forma global:

```
INTELBRAS(config)# service dhcp server
```

25.2. ip dhcp server extend-option capwap-ac-ip

Descrição: o comando **ip dhcp server extend-option capwap-ac-ip** é usado para configurar o endereço IP do servidor DHCP remoto. Para excluir este endereço IP remoto utilize o comando **no ip dhcp server extend-option capwap-ac-ip**.

Sintaxe: **ip dhcp server extend-option capwap-ac-ip** *ip-address*
no ip dhcp server extend-option capwap-ac-ip

Parâmetro:

» **ip-address:** endereço IP do servidor remoto.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique um servidor DHCP remoto no endereço 192.168.3.1:

INTELBRAS(config)# ip dhcp server extend-option capwap-ac-ip 192.168.3.1

25.3. ip dhcp server extend-option vendor-class-id

Descrição: o comando **ip dhcp server extend-option vendor-class-id** é usado para configurar o ID de classe dos pacotes do servidor DHCP em um segmento de rede diferente. Para excluir as configurações de ID de classe, utilize o comando **no ip dhcp server extend-option vendor-class-id**.

Sintaxe: **ip dhcp server extend-option vendor-class-id** *class-id*
no ip dhcp server extend-option vendor-class-id

Parâmetro:

» **class-id:** especifica a classe do ID dos pacotes DHCP de outro segmento de rede.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o ID dos pacotes DHCP de outro segmento de rede como 34:

INTELBRAS(config)# ip dhcp server extend-option vendor-class-id 34

25.4. ip dhcp server exclude-address

Descrição: o comando **ip dhcp server exclude-address** é utilizado para especificar um endereço IP reservado o qual será proibido de ser alocado, por exemplo o endereço de gateway, segmento de rede, endereço de broadcast e o endereço do servidor. Para excluir a reserva de ip, favor, utilizar o comando **no ip dhcp server exclude-address**.

Sintaxe: **ip dhcp server exclude-address** *start-ip-address end-ip-address*
no ip dhcp server exclude-address *start-ip-address end-ip-address*

Parâmetros:

» **start-ip-address:** endereço IP de início do pool reservado.
» **end-ip-address:** endereço IP final do pool reservado. Somente um IP será reservado se o endereço IP final do pool for igual o endereço de início do pool.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: reserve os endereços IP entre 192.168.1.1 à 192.168.1.9:

INTELBRAS(config)# ip dhcp server exclude-address 192.168.1.1 192.168.1.9

25.5. ip dhcp server pool

Descrição: o comando **ip dhcp server pool** é usado para criar um pool de endereços para o servidor DHCP e entrar no modo de configuração DHCP. Para deletar o pool de endereços utilize o comando **no ip dhcp server pool**.

Sintaxe: **ip dhcp server pool** *pool-name*
no ip dhcp server pool *pool-name*

Parâmetros:

» **pool-name:** especifica o nome do pool de endereços com até 8 caracteres.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie o pool de endereços com o nome POOL1:

INTELBRAS(config)# ip dhcp server pool *POOL1*

25.6. ip dhcp server ping timeout

Descrição: o comando **ip dhcp server ping timeout** é usado para determinar o tempo para timeout da solicitação PING. Para retornar o timeout para o valor padrão utilize o comando **no ip dhcp server ping timeout**.

Sintaxe: **ip dhcp server ping timeout** *value*
no ip dhcp server ping timeout

Parâmetros:

» **value:** especifica o valor de timeout, varia entre 100 e 10000ms. O valor padrão é *100ms.*

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o timeout do PING em 200ms.

INTELBRAS(config)# ip dhcp server ping timeout 200

25.7. ip dhcp server ping packets

Descrição: o comando **ip dhcp server ping packets** é usado para especificar número de pacotes de PING que serão enviados, se o valor for 0 a função PING será desabilitada. Para retornar o valor padrão use o comando **no ip dhcp server ping packets**.

Sintaxe: **ip dhcp server ping packets** *num*
no ip dhcp server ping packets

Parâmetros:

» **num:** especifica o número de pacotes PING, varia entre 0 e 10.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o número de pacotes para o PING como 2:

INTELBRAS(config)# ip dhcp server ping packets 2

25.8. network

Descrição: o comando **network** é usado para determinar o endereço e a sub-rede do pool da rede.

Sintaxe: **network** *network-address subnet-mask*

Parâmetros:

» **network-address:** especifica o endereço do pool da rede, com o formado *A.B.C.D*. Todos os endereços na mesma sub-rede serão alocados com exceção dos endereços reservados e endereços específicos.

» **subnet-mask:** especifica a máscara de sub-rede do pool no formato *A.B.C.D.*

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o endereço do pool "produto" como 192.168.1.0 255.255.255.0:

INTELBRAS(config)# ip dhcp server pool *produto*
INTELBRAS(config-dhcp)# network *192.168.1.0 255.255.255.0*

25.9. lease

Descrição: o comando **lease** é usado para determinar o tempo de concessão para o pool de endereços.

Sintaxe: **lease** *lease-time*

Parâmetros:

» **lease-time:** especifica o tempo de concessão para o pool, varia entre 1 e 2880 minutos. O valor padrão é *120 minutos*.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o tempo de concessão para o pool de endereços "produto" como 10 minutos.

INTELBRAS(config)# ip dhcp server pool produto
INTELBRAS(config-dhcp)# lease 10

25.10. address hardware-address

Descrição: o comando **address hardware-address** é usado para reservar o endereço estático vinculado ao endereço de hardware no pool de endereços. Para excluir a ligação utilize o comando **no address hardware-address**.

Sintaxe: **address** *ip-address* **hardware-address** *hardware-address* **hardware-type** {ethernet | ieee802}
no address *ip-address*

Parâmetros:

» **ip-address:** especifica o IP estático para o vínculo no formato *A.B.C.D*.
» **mac-address:** especifica o endereço do hardware, no formato *XX:XX:XX:XX:XX:XX*.
» **ethernet | ieee802:** especifica o tipo de hardware.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: reserve o endereço IP 192.168.0.10 no pool de endereços "produto" para o dispositivo com o MAC 5e:4c:a6:31:24:01, o dispositivo é do tipo Ethernet:

INTELBRAS(config)# ip dhcp server pool *produto*
INTELBRAS(config-dhcp)# address *192.168.0.10* **hardware-address** *5e:4c:a6:31:24:01* **hardware-type** ethernet

25.11. address cliente-identifier

Descrição: o comando **address cliente-identifier** é usado para especificar o endereço estático vinculado ao ID do cliente no pool de endereços. Para excluir a ligação use o comando **no address**.

Sintaxe: **address** *ip-address* **cliente-identifier** *cliente-id* **[ascii]**
no address *ip-address*

Parâmetros:

» **ip-address:** especifica o endereço de IP para o vínculo.
» **client-id:** especifica o ID do cliente no formato de valor hexadecimal.
» **ascii:** o ID do cliente é inserido com caracteres ASCII.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: reserve o endereço IP 192.168.0.10 no pool de endereços "produto" para o dispositivo com o ID de cliente como "abc" na ASCII:

INTELBRAS(config)# ip dhcp server pool produto
INTELBRAS(config-dhcp)# address 192.168.0.10 **client-identifier** abc ascii

25.12. default-gateway

Descrição: o comando **default-gateway** é usado para indicar o gateway padrão para o pool de endereços. Para excluir a configuração correspondente, use o comando **no default-gateway**.

Sintaxe: **default-gateway** *gateway-list*
no default-gateway

Parâmetros:

» **gateway-list:** especifica a lista de gateway, no formato *A.B.C.D, E.F.G.H.* podem ser configurados até 8 gateways separados por vírgula.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique para o pool de endereços "produto" os gateways padrões como 192.168.0.1 e 192.168.1.1:

INTELBRAS(config)# ip dhcp server pool produto
INTELBRAS(config-dhcp)# default-gateway 192.168.0.1,192.168.1.1

25.13. dns-server

Descrição: o comando **dns-server** é usado para indicar o servidor de DNS para o pool de endereços. Para excluir a configuração correspondente, use o comando **no dns-server**.

Sintaxe: **dns-server** *dns-list*
no dns-server

Parâmetros:

» **dns-list:** especifica a lista de servidor DNS, no formato *A.B.C.D, E.F.G.H.* podem ser configurados até 8 servidores DNS separados por vírgula.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique para o pool de endereços "produto" os seguintes servidores de DNS 192.168.0.1 e 192.168.1.1:

INTELBRAS(config)# ip dhcp server pool *produto*
INTELBRAS(config-dhcp)# dns-server *192.168.0.1,192.168.1.1*

25.14. netbios-name-server

Descrição: o comando **netbios-name-server** é usado para especificar o endereço do servidor de NETBIOS. Para excluir a configuração correspondente, use o comando **no netbios-name-server**.

Sintaxe: **netbios-name-server** *NBNS-list*
no netbios-name-server

Parâmetros:

» **NBNS-list:** especifica a lista de servidores NETBIOS, no formato *A.B.C.D, E.F.G.H.* podem ser configurados até 8 servidores NETBIOS separados por vírgula.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique para o pool de endereços "produto" os seguintes servidores NETBIOS 192.168.0.1 e 192.168.1.1:

INTELBRAS(config)# ip dhcp server pool produto
INTELBRAS(config-dhcp)# netbios-name-server 192.168.0.1,192.168.1.1

25.15. netbios-node-type

Descrição: o comando **netbios-node-type** é usado para especificar o tipo de resolução de nomes do servidor de NETBIOS. Para excluir a configuração correspondente, use o comando **no netbios-node-type**.

Sintaxe: **netbios-node-type** *type*
no netbios-node-type

Parâmetros:

» **type:** especifica o tipo resolução do servidor NETBIOS, podem ser *b-node, h-node, m-node* ou *p-node*.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique para o pool de endereços "produto" o tipo do servidor NETBIOS como b-node:

INTELBRAS(config)# ip dhcp server pool produto
INTELBRAS(config-dhcp)# netbios-node-type b-node

25.16. next-server

Descrição: o comando **next-server** é usado para especificar o endereço do próximo servidor DHCP durante o processo de inicialização do DHCP. Para excluir esta configuração utilize o comando **no next-server.**

Sintaxe: **next-server** *ip-address*
no next-server

Parâmetros:

» **ip-address:** especifica o endereço de IP do próximo servidor.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o endereço IP 192.168.2.10 como próximo servidor para o pool de endereços "produto":

INTELBRAS(config)# ip dhcp server pool produto
INTELBRAS(config-dhcp)# next-server 192.168.2.10

25.17. domain-name

Descrição: o comando **domain-name** é usado para especificar o nome do domínio para o cliente DHCP. Para excluir esta configuração utilize o comando **no domain-name**.

Sintaxe: **domain-name** *domain-name*
no domain-name

Parâmetros:

» **domain-name:** especifica o nome do domínio DHCP.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o nome do domínio "edu" para o pool de endereços "produto":

INTELBRAS(config)# ip dhcp server pool produto
INTELBRAS(config-dhcp)# domain-name edu

25.18. bootfile

Descrição: o comando **bootfile** é usado para especificar o nome do arquivo de inicialização do cliente DHCP. Para excluir o arquivo de inicialização utilize o comando **no bootfile**.

Sintaxe: **bootfile** *file-name*
no bootfile

Parâmetros:

» **file-name:** especifica o nome do arquivo de inicialização do cliente DHCP.

Modo de comando: DHCP Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o nome do arquivo de inicialização do cliente DHCP como boot1:

INTELBRAS(config)# ip dhcp server pool produto
INTELBRAS(config-dhcp)# bootfile boot1

25.19. show ip dhcp server status

Descrição: o comando **show ip dhcp server status** é usado para mostrar o status do serviço de DHCP.

Sintaxe: **show ip dhcp server status**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o status do serviço DHCP:

INTELBRAS# show ip dhcp server status

25.20. show ip dhcp server statistics

Descrição: o comando **show ip dhcp server statistics** é usado para mostrar as estatísticas do serviço de DHCP, pacotes recebidos e enviados.

Sintaxe: **show ip dhcp server statistics**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as estatísticas do DHCP em relação aos pacotes enviados e recebidos pelo servidor:

INTELBRAS# show ip dhcp server statistics

25.21. show ip dhcp server extend-option

Descrição: o comando **show ip dhcp server extend-option** é usado para exibir a configuração dos servidores DHCP remotos.

Sintaxe: **show ip dhcp server extend-option**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações dos servidores DHCP remotos:

INTELBRAS# show ip dhcp server extend-option

25.22. show ip dhcp server pool

Descrição: o comando **show ip dhcp server pool** é usado para exibir a configuração do pool de endereços.

Sintaxe: **show ip dhcp server pool**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações do pool de endereços:

INTELBRAS# show ip dhcp server pool

25.23. show ip dhcp server excluded-address

Descrição: o comando s**how ip dhcp server excluded-address** é usado para exibir a configuração dos endereços reservados.

Sintaxe: **show ip dhcp server excluded-address**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração dos endereços reservados:

INTELBRAS# show ip dhcp server excluded-address

25.24. show ip dhcp server manual-binding

Descrição: o **comando show ip dhcp server manual-binding** é usado para exibir a configuração dos endereços vinculados estaticamente.

Sintaxe: **show ip dhcp server manual-binding**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração dos endereços vinculados estaticamente:

```
INTELBRAS# show ip dhcp server manual-binding
```

25.25. show ip dhcp server binding

Descrição: o comando **show ip dhcp server binding** é usado para exibir as entradas de vínculo.

Sintaxe: **show ip dhcp server binding** [**ip** *ip-address*]

Parâmetro:

» **ip-address:** especifica o endereço IP vinculado.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as entradas com endereços vinculados:

```
INTELBRAS# show ip dhcp server binding
```

25.26. clear ip dhcp server statistics

Descrição: o comando **clear ip dhcp server statistics** é usado para limpar as informações estatísticas dos pacotes DHCP.

Sintaxe: **clear ip dhcp server statistics**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: limpe as estatísticas dos pacotes DHCP:

```
INTELBRAS# clear ip dhcp server statistics
```

25.27. clear ip dhcp server binding

Descrição: o comando **clear ip dhcp server binding** é usado para limpar as informações de vínculos.

Sintaxe: **clear ip dhcp server binding** [*ip-address*]

Parâmetro:

» **ip-address:** especifica o endereço IP vinculado.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: limpe todos os endereços vinculados:

```
INTELBRAS# clear ip dhcp server binding
```

26. Comandos de retransmissão DHCP

Um agente de transmissão DHCP Relay é um dispositivo de layer 3 que encaminha pacotes DHCP entre clientes e servidores. O DHCP Relay encaminha solicitações e respostas entre clientes e servidores quando eles não estão na mesma sub-rede física.

26.1. service dhcp relay

Descrição: o comando **service dhcp relay** é utilizado para ativar o serviço de DHCP Relay de forma global. Para desabilitar o serviço de DHCP Relay utilize o comando **no service dhcp relay.**

Sintaxe: **service dhcp relay**
no service dhcp relay

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o serviço de DHCP Relay de forma global:

```
INTELBRAS(config)# service dhcp relay
```

26.2. ip dhcp relay hops

Descrição: o comando **ip dhcp relay hops** é usado para especificar os saltos máximos (agente de retransmissão DHCP) aos quais os pacotes DHCP podem ser retransmitidos. Para restaurar o valor padrão utilize o comando **no ip dhcp relay hops**.

Sintaxe: **ip dhcp relay hops** *hops*
no ip dhcp relay hops

Parâmetros:

» **hops:** especifique o máximo de saltos para o agente de retransmissão DHCP, aos quais os pacotes DHCP podem ser retransmitidos. Se a contagem de saltos de um pacote for maior que o valor definido aqui, o pacote será descartado. O valor varia de 1 a 16 e o valor padrão é *4*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o número máximo de saltos possíveis para 6:

```
INTELBRAS(config)# ip dhcp relay hops 6
```

26.3. ip dhcp relay time

Descrição: o comando **ip dhcp relay time** é usado para especificar o limite de tempo de retransmissão DHCP. O tempo de retransmissão DHCP é o tempo decorrido desde que o cliente iniciou o processo de aquisição ou renovação de endereço. Quando o tempo decorrido do pacote DHCP é maior que o valor definido aqui, o pacote DHCP será descartado pelo. Para restaurar o valor padrão utilize o comando **no ip dhcp relay time**.

Sintaxe: **ip dhcp relay time** *time*
no ip dhcp relay time

Parâmetros:

» **time:** especifique o tempo limite. O valor válido varia entre 1 e 65535. O valor padrão é *0* o que representa que o switch não examina esse campo para pacotes DHCP, por padrão.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure tempo limite para o DHCP Relay como 30 segundos:

```
INTELBRAS(config)# ip dhcp relay time 30
```

26.4. ip helper-address

Descrição: o comando **ip helper-address** é usado para adicionar o endereço do servidor DHCP à interface de layer 3. Para restaurar o valor padrão utilize o comando **no ip helper-address**.

Sintaxe: **ip helper-address** *ip-address*
no ip helper-address [*ip-address***]**

Parâmetros:

» **ip-address:** endereço do servidor DHCP.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: adicione o Servidor de DHCP 192.168.2.1 à intervace VLAN1:

```
INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ip helper-address 192.168.2.1
```

26.5. ip dhcp relay information

Descrição: o comando **ip dhcp relay information** é usado para habilitar a option 82 do suporte no DHCP Relay. Para desabilitar essa função utilize o comando **no ip dhcp relay information**.

Sintaxe: **ip dhcp relay information**
no ip dhcp relay information

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a option 82 do suporte no DHCP Relay da porta 2:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp relay information
```

26.6. ip dhcp relay information strategy

Descrição: o comando **ip dhcp relay information strategy** é usado é usado para especificar a operação do campo para Option 82 dos pacotes de solicitação DHCP do Host. Para restaurar essa função para o padrão utilize o comando **no ip dhcp relay information strategy.**

Sintaxe: **ip dhcp relay information strategy** {drop | keep | replace}
no ip dhcp relay information strategy

Parâmetros:

» **drop | keep | replace:** as operações do campo *Option 82* dos pacotes de solicitação DHCP do Host. A operação padrão é *keep*.
  » **drop:** descarta o pacote com o campo *Option 82*.
  » **keep:** mantenha o campo *Option 82* no pacote.
  » **replace:** substitua o campo da option 82 pela opção do sistema definida pelo comutador.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique a estratégia da option 82 como replace a porta 2:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp relay information strategy replace
```

26.7. ip dhcp relay information format

Descrição: o comando **ip dhcp relay information format** é usado é usado para escolher o formato do campo para a subopção da Option 82 dos pacotes de solicitação DHCP do Host. Para restaurar essa função para o padrão utilize o comando **no ip dhcp relay information format**.

Sintaxe: **ip dhcp relay information format** {normal | private}
no ip dhcp relay information format

Parâmetros:

» **normal | private:** formato do tipo da subopção da option 82.
  » **normal:** indica que o formato da subopção é TLV (*type-length-value*).
  » **private:** indica que o formato do campo de valor de subopção é o valor que você configura para a subopção relacionada.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o formato da subopção da option 82 como TLV para a porta 2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp relay information format normal

26.8. ip dhcp relay information circuit-id

Descrição: o comando **ip dhcp relay information circuit-id** é usado para especificar o ID do circuito quando a option 82 customizada está ativada. Para limpar a ID do circuito utilize o comando **no ip dhcp relay information circuit-id**.

Sintaxe: **ip dhcp relay information circuit-id** *circuitID*
no ip dhcp relay information circuit-id

Parâmetros:

» **circuitID:** especifica a ID do circuito, até 64 caracteres.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique a id do circuito como "Intelbras" para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp relay information circuit-id Intelbras

26.9. ip dhcp relay information remote-id

Descrição: o comando **ip dhcp relay information remote-id** é usado para especificar o ID do remota quando a option 82 customizada está ativada. Para limpar a ID remota utilize o comando **no ip dhcp relay information remote-id**.

Sintaxe: **ip dhcp relay information remote-id** *remoteID*
no ip dhcp relay information remote-id

Parâmetros:

» **remoteID:** especifica a ID remota, até 64 caracteres.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique a id remota como "Intelbras" para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp relay information remote-id Intelbras

26.10. ip dhcp relay default-interface

Descrição: o **ip dhcp relay default-interface** é usado para configurar a interface do agente de retransmissão padrão. Quando o switch trabalha no modo DHCP VLAN Relay e não há interface IP na VLAN, o switch usa o IP da interface do Relay Agent padrão para preencher o campo de endereço IP na retransmissão dos pacotes DHCP. Para retornar a configuração da interface do Relay Agent para padrão utilize o comando **no ip dhcp relay default-interface**.

Sintaxe: **ip dhcp relay default-interface**
no ip dhcp relay default-interface

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configura a interface VLAN 1 como interface padrão para o Relay Agent:

```
INTELBRAS(config)# interface vlan 1
INTELBRAS(config-if)# ip dhcp relay default-interface
```

26.11. ip dhcp relay vlan

Descrição: o comando **ip dhcp relay vlan** é usado para adicionar o endereço do servidor DHCP à VLAN especificada. Se houver uma interface IP na VLAN e ela tiver configurado um endereço de servidor DHCP no nível da interface, a configuração no nível da interface terá maior prioridade. Nesse caso, o servidor DHCP configurado na VLAN não será usado para encaminhar os pacotes DHCP. Para excluir o endereço do servidor utilize o comando **no ip dhcp relay vlan**.

Sintaxe: **ip dhcp relay vlan** *vid* **helper-address** *ip-address*
no ip dhcp relay vlan *vid* **helper-address** [*ip-address*]

Parâmetros:

- **vid:** VLAN ID.
- **Ip-adress:** endereço IP do servidor DHCP.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: adicione o servidor DHCP de endereço 192.168.2.1 à VLAN 1:

```
INTELBRAS(config)# ip dhcp relay vlan 1 helper-address 192.168.2.1
```

26.12. show ip dchp relay

Descrição: o comando **show ip dchp relay** é usado para exibir o status global e a configuração da Option 82 do DHCP Relay.

Sintaxe: **show ip dchp relay**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração do DHCP Relay:

```
INTELBRAS(config)# show ip dhcp relay
```

27. Comandos de retransmissão DHCP L2

27.1. ip dhcp l2relay

Descrição: o comando **ip dhcp l2relay** é utilizado para ativar o serviço de DHCP L2 Relay de forma global. Para desabilitar o serviço de DHCP L2 Relay utilize o comando **no ip dhcp l2relay**.

Sintaxe: **ip dhcp l2relay**
no ip dhcp l2relay

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o serviço DHCP L2 Relay de forma global:

```
INTELBRAS(config)# ip dhcp l2relay
```

27.2. ip dhcp l2relay vlan

Descrição: o comando **ip dhcp l2relay vlan** é utilizado para ativar o serviço de DHCP L2 Relay em uma vlan específica. Para desabilitar o serviço de DHCP L2 Relay utilize o comando **no ip dhcp l2relay vlan**.

Sintaxe: **ip dhcp l2relay vlan** *vid*
no ip dhcp l2relay vlan *vid*

Parâmetro:

» **vid:** especifica qual VLAN será habilitada o DHCP L2 Relay.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o serviço DHCP L2 Relay para a VLAN 2:

```
INTELBRAS(config)# ip dhcp l2relay vlan 2
```

27.3. ip dhcp l2relay information

Descrição: o comando **ip dhcp l2relay information** é usado para ativar o suporte da option 82 no DHCP Relay. Para desabilitar esta função utilize o comando **no ip dhcp l2relay information**.

Sintaxe: **ip dhcp l2relay information**
no ip dhcp l2relay information

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o suporte à option 82 no DHCP L2 Relay da porta 2:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp l2relay information
```

27.4. ip dhcp l2relay information strategy

Descrição: o comando **ip dhcp l2relay information strategy** é usado é usado para especificar a operação do campo para Option 82 dos pacotes de solicitação DHCP do Host. Para restaurar essa função para o padrão utilize o comando **no ip dhcp l2relay information strategy**.

Sintaxe: **ip dhcp l2relay information strategy** {drop | keep | replace}
no ip dhcp l2relay information strategy

Parâmetros:

» **drop | keep | replace:** as operações do campo *Option 82* dos pacotes de solicitação DHCP do Host. A operação padrão é *keep*.
  » **drop:** descarta o pacote com o campo *Option 82*.
  » **keep:** Mantenha o campo *Option 82* no pacote.
  » **replace:** substitua o campo da option 82 pela opção do sistema definida pelo comutador.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique a estratégia da option 82 como replace a porta 2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp l2relay information strategy replace

27.5. ip dhcp l2relay information format

Descrição: o comando **ip dhcp l2relay information format** é usado é usado para escolher o formato do campo para a subopção da Option 82 dos pacotes de solicitação DHCP do Host. Para restaurar essa função para o padrão utilize o comando **no ip dhcp l2relay information format**.

Sintaxe: **ip dhcp l2relay information format** {normal | private}
no ip dhcp l2relay information format

Parâmetros:

- **normal | private:** formato do tipo da subopção da option 82.
  - **normal:** indica que o formato da subopção é TLV (*type-length-value*).
  - **private:** indica que o formato do campo de valor de subopção é o valor que você configura para a subopção relacionada.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o formato da subopção da option 82 como TLV para a porta 2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp l2relay information format normal

27.6. ip dhcp l2relay information circuit-id

Descrição: o comando **ip dhcp l2relay information circuit-id** é usado para especificar o ID do circuito quando a option 82 customizada está ativada. Para limpar a ID do circuito utilize o comando **no ip dhcp l2relay information circuit-id**.

Sintaxe: **ip dhcp l2relay information circuit-id** *circuitID*
no ip dhcp l2relay information circuit-id

Parâmetro:

- **circuitID:** especifica a ID do circuito, até 64 caracteres.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique a id do circuito como "Intelbras" para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp l2relay information circuit-id Intelbras

27.7. ip dhcp l2relay information remote-id

Descrição: o comando **ip dhcp l2relay information remote-id** é usado para especificar o ID do remota quando a option 82 customizada está ativada. Para limpar a ID remota utilize o comando **no ip dhcp l2relay information remote-id**.

Sintaxe: **ip dhcp l2relay information remote-id** *remoteID*
no ip dhcp l2relay information remote-id

Parâmetro:

- **remoteID:** especifica a ID remota, até 64 caracteres.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique a id remota como "Intelbras" para a porta 1/0/2:

INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp relay information remote-id Intelbras

27.8. show ip dchp l2relay

Descrição: o comando **show ip dchp l2relay** é usado para exibir o status global e a configuração da Option 82 do DHCP Relay.

Sintaxe: **show ip dchp l2relay**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração do DHCP Relay:

INTELBRAS(config)# show ip dhcp l2relay

27.9. show ip dchp l2relay interface

Descrição: o comando **show ip dchp l2relay** é usado para exibir o status DHCP L2 Relay para a(s) porta(as).

Sintaxe: **show ip dchp l2relay interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração do DHCP L2 Relay:

INTELBRAS(config)# show ip dhcp l2relay interface

28. Comandos QoS

A função QoS (*Quality of Service*) é usada para otimizar a performance da rede. Ela proporciona para você uma melhor qualidade e experiência de serviço. O switch implementa três modos de prioridade sendo eles baseado na porta, baseado na 802.1p e DSCP.

28.1. qos trust mode

Descrição: o comando **qos trust mode** é utilizado para configurar a função de Trust Mode (modo de confiabilidade) do CoS (*Class of Service*) para as portas. Por padrão o Trust Mode vem configurado como trust port priority.

Sintaxe: **qos trust mode** {dot1p | dscp | untrust}

Parâmetros:

- **dot1p:** modo de confiabilidade 802.1p. Nesse modo os dados serão classificados em diferentes serviços baseados na prioridade 802.1p.
- **dscp:** modo de confiabilidade DSCP. Neste modo os dados serão classificados baseados na prioridade dscp.
- **untrust:** modo de confiabilidade de porta. Os dados serão classificados baseados na prioridade da porta.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de confiabilidade da porta 1/0/3 como DSCP:

INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# qos trust mode dscp

28.2. qos port-priority

Descrição: o comando **qos port-priority** é usado para configurar a porta para o mapeamento de prioridade do 802.1p. Para retornar à configuração padrão utilize o comando **no qos port-priority**. Quando a prioridade da porta está ativa, os pacotes serão mapeados com diferentes prioridades baseadas no ingresso das portas.

Sintaxe: **qos port-priority** {*dot1p-priority*}
no qos port-priority

Parâmetro:

» **dot1p-priority:** prioridade de mapeamento para a porta, valores variam entre 0 e 7, os quais representam a prioridade 802.1p 0-7 respectivamente. Por padrão vem configurada como *0*.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a prioridade da porta 1/0/5 como 3:

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# qos port-priority 3

28.3. qos cos-map

Descrição: o comando **qos cos-map** é usado para configurar o mapeametno queue 802.1p de forma global. Para retornar à configuração padrão utilize o comando **no qos cos-map**. Quando a prioridade 802.1p está ativa os pacotes com TAG 802.1q são mapeados com diferentes leveis de prioridade baseados na prioridade 802.1p.

Sintaxe: **qos cos-map** {*dot1p-priority* } {*tc-queue*}
no qos cos-map

Parâmetros:

» **dot1p-priority:** prioridade de mapeamento para a porta, valores variam entre 0 e 7, os quais representam a prioridade 802.1p 0-7 respectivamente.

» **tc-queue:** representa o número do TC queue que a prioridade 802.1p irá ser mapeada. Varia entre 0 e 7.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: mapeie o 802.1p com prioridade 5 para o TC-2:

INTELBRAS(config)# qos cos-map 5 2

28.4. qos dot1p-remap

Descrição: o comando **qos dot1p-remap** é usado para configurar o mapeamento de 802.1p para 802.1p. Para retornar à configuração padrão utilize o comando **no qos dot1-remap**. Quando a o remapeamento 802.1p é configurado, os pacotes com a específica prioridade serão alterado para a nova prioridade 802.1p.

Sintaxe: **qos dot1p-remap** {*dot1p-priority* } {*new-dot1p-priority*}
no qos dot1p-remap

Parâmetros:

» **dot1p-priority:** prioridade original de mapeamento para a porta, valores variam entre 0 e 7, os quais representam a prioridade 802.1p 0-7 respectivamente.

» **new-dot1p-priority:** nova prioridade que será mapeada. Varia entre 0 e 7.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: altere o mapeamento 802.1p da prioridade 5 para 6:

INTELBRAS(config)# qos dot1p-remap 5 6

28.5. qos dscp-map

Descrição: o comando **qos dscp-map** é usado para configurar o mapeamento DSCP para o 802.1p. Para retornar à configuração padrão utilize o comando **no qos dscp -map**. DSCP (*DiffServ Code Point*) é uma nova definição para o campo *IP ToS* dado pelo IEEE. Esse campo é usado para dividir o datagrama IP em 64 prioridades. Quando a prioridade DSCP está ativa o datagrama será mapeamento em diferentes níveis de prioridade baseados no DSCP.

Sintaxe: **qos dscp -map** {*dscp-value-list*} {*dot1p-priority*}
no qos dscp -map

Parâmetros:

- **dscp-value-list:** representa o a lista de valores para o DSCP no formato *1-3,5,7*. Os valores variam entre 0 e 63.
- **dot1p-priority:** prioridade de mapeamento para a porta, valores variam entre 0 e 7, os quais representam a prioridade 802.1p 0-7 respectivamente.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: mapeie a prioridade DSCP 5 para a prioridade 2 do 802.1p:

```
INTELBRAS(config)# qos dscp -map 5 2
```

28.6. qos dscp-remap

Descrição: o comando **qos dscp-remap** é usado para configurar o mapeamento de DSCP para DSCP. Para retornar à configuração padrão utilize o comando **no qos dscp-remap**. Quando a o remapeamento DSCP é configurado, os pacotes com a específica prioridade serão alterado para a nova prioridade DSCP.

Sintaxe: **qos dscp-remap** {*dscp-value-list*} {*dscp-remap-value*}
no qos dscp-remap

Parâmetros:

- **dscp-value-list:** prioridade original de mapeamento para o DSCP no formato *1-3,5,5*. Os valores variam entre 0 e 63.
- **dscp-rempa-value:** nova prioridade que será mapeada. Varia entre 0 e 63.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: altere o mapeamento DSCP 10-12 para 2:

```
INTELBRAS(config)# qos dscp-remap 10-12 2
```

28.7. qos queue mode

Descrição: o comando **qos queue mode** é utilizado para configurar o Scheduler Mode (modo de agendamento). Quando uma rede está congestionada, é necessário resolver os recursos para os pacotes, usualmente um modo de agendamento de filas é utilizado para isto. O switch irá controlar a sequência de encaminhamento de acordo com a prioridade das filas e dos algoritmos de agendamento. No switch os níveis de prioridades são rotulados como TC0, TC1, TC2... TC7.

Sintaxe: **qos queue** {*tc-queue*} **mode** {sp | wrr} [**weight** *weitght*]

Parâmetros:

- **tc-queue:** ID de ingresso à fila, varia entre 0 e 7, qual representa a fila TC respetivamente entre TC0 e TC7.
- **sp:** Strict-Priority (prioridade restrita). Nesse modo, a fila com maior prioridade irá ocupar toda a largura de banda. Pacotes em filas de menor prioridade só serão encaminhados quando a fila com prioridade maior estiver fazia.
- **wrr:** Weight Round Robin Mode. Neste modo os pacotes em todas as filas são enviados ordenadamente baseados no valor de cada fila. Se você selecionar este modo será necessário especificar o *peso* de cada fila ao mesmo tempo.
- **weight:** configura o valor *peso* da fila TC especificada. Quando o modo de agendamento é especificado como WRR, o valor do peso varia entre 1 e 127. As 8 filas irão se adequar a largura de banda de acordo com o seu valor.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o modo de agendamento da TC1 como WRR e determine o "peso" da fila como 10 para a port 1/0/1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# qos queue 1 mode wrr weight 10
```

28.8. show qos cos-map

Descrição: o comando **show qos cos-map** é usado para mostrar o mapeamento da prioridade das filas TC do 802.1p.

Sintaxe: **show qos cos-map**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o mapeamento das filas 802.1p:

```
INTELBRAS# show qos cos-map
```

28.9. show qos dot1p-map

Descrição: o comando **show qos dot1p-map** é usado para mostrar o mapeamento da prioridade do 802.1p.

Sintaxe: **show qos dot1p-map**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o remapeamento das filas 802.1p:

```
INTELBRAS# show qos dot1p-map
```

28.10. show qos dscp-map

Descrição: o comando **show qos dscp-map** é usado para mostrar a configuração de prioridade do DSCP.

Sintaxe: **show qos dscp-map**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração de prioridade DSCP:

```
INTELBRAS# show qos dscp-map
```

28.11. show qos dscp-remap

Descrição: o comando **show qos dscp-remap** é usado para mostrar o mapeamento de prioridade do DSCP.

Sintaxe: **show qos dscp-remap**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o mapeamento de prioridade DSCP:

```
INTELBRAS# show qos dscp-remap
```

28.12. show qos port-priority interface

Descrição: o comando **show qos port-priority interface** é usado para mostrar a configuração de prioridade do 802.1p de todas as portas ou de uma em específico.

Sintaxe: **show qos port-priority interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta.
- **port-channel-id:** identificação da port-channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o mapeamento de prioridade 802.1p de todas as portas:

```
INTELBRAS# show qos port-priority interface
```

28.13. show qos trust interface

Descrição: o comando **show qos trust interface** é usado para mostrar o *trust mode* (modo de confiabilidade) das portas.

Sintaxe: **show qos trust interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta.
- **port-channel-id:** identificação da port-channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o trust mode de todas as portas:

```
INTELBRAS# show qos trust interface
```

28.14. show qos queue interface

Descrição: o comando **show qos trust interface** é usado para mostrar as definições de agendamento das portas.

Sintaxe: **show qos queue interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta.
- **port-channel-id:** identificação da port-channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as definições de agendamento de todas as portas:

```
INTELBRAS# show qos queue interface
```

29. Comandos de controle de banda

As funções de controle de largura de banda controlam a taxa de tráfego e o limite de tráfego em cada porta garantido a performance da rede. As funções de *Rate Limit* (taxa limite) limitam a taxa de tráfego de entrada e saída em cada porta. A função *Storm Control* permite monitorar pacotes de broadcast, multicast e quadros unicast desconhecidos na rede.

29.1. storm-control rate-mode

Descrição: o comando **storm-control rate-mode** é utilizado para configura o modo de Storm Control para a interface. Para retornar à configuração para o valor padrão utilize o comando **no storm-control rate-mode**. Este comando pode ser usado juntamente com o comando **storm-control** para habilitar funções de controle e especificar parâmetros.

Sintaxe: **storm-control rate-mode** {kbps | ratio}
no storm-control rate-mode

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o modo da função de Storm Control como Kbps para a porta 1/0/5:

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# storm-control rate-mode kbps

29.2. storm-control

Descrição: o comando **storm-control** é usado para habilitar a função de Storm Control para broadcast, multicast ou unicast desconhecido e determinar os níveis limites para uma interface. Para restaurar à configuração padrão utilize o comando **no storm-control**. Antes de configurar o tipo do Storm Control como kbps ou ratio garanta que a porta não está no modo pps.

Sintaxe: **storm-control** {broadcast | multicast | unicast} {*rate*}
no storm-control {broadcast | multicast | unicast}

Parâmetros:

- **broadcast | multicast | unicast:** seleciona o modo de Storm Control para a interface.
- **rate:** especifica a largura de banda que para receber os pacotes para esta porta. O tipo específico de pacote tratado no Storm Control que exceder essa largura de banda será processado de acordo com a configuração do comando **storm-control exceed**. Pra kpbs a taxa varia entre 1 e 1000000 kbps. Para *rate* (taxa), os valores variam entre 1 e 100 porcento.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o Storm Control de broadcast com a taxa de 1024 kbps para a porta 1/0/5:

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# storm-control rate-mode kbps
INTELBRAS(config-if)# storm-control broadcast 1024

29.3. storm-control exceed

Descrição: o comando **storm-control exceed** é usado para determinar a ação que o switch tomará quando o limite definido para a Storm for excedido na interface.

Sintaxe: **storm-control exceed** {drop | shutdown} [**recover-time** *time*]

Parâmetros:

- **drop:** determina a ação como descarte para os pacotes excedentes, ou seja a porta irá descartar os pacotes que excederem o limite do Storm Control.
- **shutdown:** determina a ação como desabilitar, a porta será desabilitada quando o limite do Storm Control for excedido.
- **time:** especifica o tempo de recuperação para a porta. Só toma efeito quando a ação de desabilitar a porta estiver em vigor. Os valores variam entre 0 e 3600 e por padrão vem configurado como *0*. Quando a porta estiver desabilitada ela pode se recuperar para o seu estado normal após passar o tempo de recuperação, se o tempo de recuperação for 0 (zero) significa que a porta não se recuperará para o seu estado normal automaticamente e você poderá recuperar a porta utilizando o comando **storm-control recover** de forma manual.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível admnistrador e operador têm acesso a esses comandos.

Exemplo: configure a ação de descarte para os pacotes que excederem o limite do Storm Control para a porta 1/0/5:

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# storm-control exceed drop

29.4. storm-control recover

Descrição: o comando **storm-control recover** é usado para recuperar a porta manualmente após a mesma ser desativada por uma Storm. Quando o tempo de recuperação for especificado como 0 (zero), a porta não se recuperará automaticamente. Nessa condição você deverá utilizar este comando para recuperar a porta manualmente.

Sintaxe: **storm-control recover**

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: recupere a porta 1/0/5:

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# storm-control recover

29.5. bandwidth

Descrição: o comando **bandwidth** é usado para configurar os limites de largura de banda para as portas Ethernet. Para desabilitar esse limite utilize o comando **no bandwidth**.

Sintaxe: **bandwidth** {[**ingress** *ingress-rate*] [**egress** *egress-rate*]}

Parâmetros:

- **ingress-rate:** especifica a largura de banda para o recebimento de pacotes, varia entre 1 e 1000000 Kbps para as portas Gigabit.
- **egress-rate:** especifica a largura de banda para o envio de pacotes, varia entre 1 e 1000000 Kbps para as portas Gigabit.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a taxa de recebimento de pacotes como 5120Kbps e envio de pacotes como 1024Kbps para a porta 1/0/5:

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# bandwidth ingress 5120 **egress** 1024

29.6. show storm-control

Descrição: o comando **show storm-control** é usado para mostrar as informações de Storm-Control das portas Ethernet.

Sintaxe: **show storm-control interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta.
- **port-channel-id:** identificação da port-channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as a informação de storm-control das portas 4, 5, 6 e 7:

INTELBRAS# show storm-control interface gigabitEthernet 1/0/4-7

29.7. show bandwitdth

Descrição: o comando **show bandwitdth** é usado para mostrar o limite de largura de banda das portas Ethernet.

Sintaxe: **show bandwitdth interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta.
- **port-channel-id:** identificação da port-channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as a informação de largura de banda da porta 1/0/4:

INTELBRAS# show bandwitdth interface gigabitEthernet 1/0/4

30. Comandos Voice VLAN

As Voice VLANs (VLAN de voz) são uma configuração especial para o stream de voz. Através da configuração da VLAN de voz e adição de portas à mesma você consegue configurar um QoS para dados de voz garantindo a prioridade da transmissão e qualidade da voz trafegada.

30.1. voice vlan

Descrição: o comando **voice vlan** é utilizado para ativar a função de VLAN de voz. Para desabilitar a função utilize o comando **no voice vlan**.

Sintaxe: **voice vlan** *vlan-id*
no voice vlan

Parâmetro:

» **vlan-id:** especifica a ID da VLAN do padrão *IEEE 802.1q*, varia entre 2 e 4094.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função VLAN de voz para a VLAN 10.

INTELBRAS(config)# voice vlan 10

30.2. voice vlan (interface)

Descrição: o comando **voice vlan** é utilizado para ativar o serviço de VLAN de voz em uma porta específica. Para desabilitar o serviço nas portas utilize o comando **no voice vlan**.

Sintaxe: **voice vlan**
no voice vlan

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de Voice Vlan para a porta 1/0/1:

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# voice vlan

30.3. voice vlan priority

Descrição: o comando **voice vlan priority** é usado para configurar a prioridade para a VLAN de voz. Para retornar à configuração padrão utilize o comando **no voice vlan priority**.

Sintaxe: **voice vlan priority** *pri*
no voice vlan priority

Parâmetro:

» **pri:** nível de prioridade, varia entre 0 e 7 e por padrão vem definido como *7*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a prioridade da VLAN de Voz como 5:

INTELBRAS(config)# voice vlan priority 5

30.4. voice vlan oui

Descrição: o comando **voice vlan oui** é usado para criar a VLAN OUI para voz. Para excluir esta VLAN utilize o comando **no voice vlan oui**.

Sintaxe: **voice vlan oui** *oui-prefix* **oui-desc** *string*
no voice vlan mac-address *oui-prefix*

Parâmetros:

- **oui-prefix:** endereço do dispositivo de voz no formato *XX:XX:XX*.
- **string:** identificação do OUI com até 16 caracteres.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie a VLAN OUI de voz descrita como Intelbras com o endereço OUI 00:11:11:11:11:11 e endereço de máscara FF:FF:FF:00:00:00:

```
INTELBRAS(config)# voice vlan oui 00:11:11 oui-desc Intelbras
```

30.5. show voice vlan

Descrição: o comando **show voice vlan** é usado para exibir o status global e a configuração da VLAN de voz.

Sintaxe: **show voice vlan**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: mostre a configuração da VLAN de voz de forma global:

```
INTELBRAS# show voice vlan
```

30.6. show voice vlan oui-table

Descrição: o comando **show voice vlan oui-table** é usado para exibir a configuração da VLAN OUI de voz.

Sintaxe: **show voice vlan oui-table**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: mostre a configuração do DHCP L2 Relay:

```
INTELBRAS# show voice vlan oui-table
```

30.7. show voice vlan interface

Descrição: o comando **show voice vlan interface** é usado para exibir a configuração e informação de todas as portas da VLAN voz.

Sintaxe: **show voice vlan interface**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: mostre a configuração da VLAN de voz de forma global.

```
INTELBRAS# show voice vlan interface
```

31. Comandos Auto VoIP

A função Auto VoIP é utilizada para priorizar a transmissão de tráfego de voz. VoIP ou voz sobre IP habilita chamadas de telefone através da rede de dados e a função de Auto VoIP ajuda a providenciar um mecanismo de classificação para os pacotes de voz. Quando a função *Auto VoIP* é configurada em uma porta que recebe tráfego de voz e dados essa função pode ajudar a garantir que a qualidade do som de um telefone IP não se deteriore quando o tráfego de dados para a porta for *pesado*.

31.1. auto-voip

Descrição: o comando **auto-voip** é utilizado para ativar a função de Auto VoIP globalmente. Para desabilitar a função utilize o comando **no auto-voip**.

Sintaxe: **auto-voip**
no auto-voip

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função Auto VoIP de forma global.

```
INTELBRAS(config)# auto-voip
```

31.2. auto-voip (interface)

Descrição: o comando **auto-voip** é utilizado para especificar uma ID de VLAN para as portas, ou seja, nesse modo os dispositivos de voz irão enviar pacotes de voz com as tags da VLAN desejada.

Sintaxe: **auto-voip** *vlan-id*

Parâmetro:

» **vlan-id:** especifica a identificação da VLAN de Auto VoIP. Os valores variam entre 2 e 2094.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: aponte a VLAN 3 para o Auto VoIP da porta 1/0/3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# auto-voip 3
```

31.3. auto-voip dot1p

Descrição: o comando **auto-voip dot1p** é utilizado para especificar o modo de interface dot1p para as portas, ou seja, nesse modo os dispositivos de voz irão enviar pacotes de voz com a prioridade 802.1p desejada.

Sintaxe: **auto-voip dot1p** *dot1p*

Parâmetro:

» **dot1p:** especifica a prioridade 802.1p desejada para a porta. Os valores variam entre 0 e 7.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: aponte a prioridade 5 do 802.1p para porta 1/0/3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# auto-voip dot1p 5
```

31.4. auto-voip untagged

Descrição: o comando **auto-voip untagged** é utilizado para especificar o modo sem tags para a porta, ou seja, nesse modo os dispositivos de voz irão enviar pacotes de voz sem tags.

Sintaxe: **auto-voip untagged**

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: aponte o modo de interface como untagged para a porta 3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# auto-voip untagged
```

31.5. auto-voip none

Descrição: o comando **auto-voip none** é utilizado para especificar o modo de interface como *none* para as portas, ou seja, nesse modo os dispositivos de voz poderão utilizar sua própria configuração para o envio de pacotes de voz.

Sintaxe: **auto-voip none**

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: instrua os dispositivos conectados a porta 1/0/3 a utilizarem suas próprias configurações para pacotes de voz:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# auto-voip none
```

31.6. no auto-voip

Descrição: o comando **no auto-voip** é utilizado para desabilitar a função de Auto VoIP para as porta correspondente.

Sintaxe: **no auto-voip**

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: desabilite a função Auto VoIP para a porta 3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# no auto-voip
```

31.7. auto-voip dscp

Descrição: o comando **auto-voip dscp** é utilizado para especificar valor DSCP para o Auto VoIP para as portas.

Sintaxe: **auto-voip dscp** *value*

Parâmetro:

» **value:** especifica o valor DSCP para o Auto VoIP. Os valores variam entre 0 e 63.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: aponte o valor 33 para o Auto VoIP da porta 1/0/3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# auto-voip dscp 33
```

31.8. auto-voip data priority

Descrição: o comando **auto-voip data priority** é utilizado para habilitar ou desabilitar o modo de substituição para o CoS (*Class of Servisse*) nas portas especificadas.

Sintaxe: **auto-voip data priority** {trust | untrust}

Parâmetros:

» **trust:** neste modo o switch colocará os pacotes de voz na fila TC correspondente de acordo com a prioridade 802.1p dos pacotes.

» **untrust:** neste modo o switch ignorará a prioridade 802.1p dos pacotes de voz e colocará os pacotes diretamente na TC 5.

Modo de comando: Interface Configuration (interface gigabitEthernet/interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o modo de substituição de CoS para a porta 3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# auto-voip data priority trust
```

31.9. show auto-voip

Descrição: o comando **show auto-voip** é usado para exibir a configuração do Auto VoIP.

Sintaxe: **show auto-voip** [*interface*]

Parâmetro:

» **interface:** mostra a configuração de Auto VoIP da porta determinada. Quando nenhum parâmetro é adicionado o comando mostrará a configuração global do Auto VoIP.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: mostre a configuração global do Auto VoIP:

```
INTELBRAS# show auto-voip
```

32. Comandos de controle de acesso

32.1. user access-control ip-based enable

Descrição: o comando **user access-control ip-based enable** é utilizado para configurar o modo de controle de acesso como baseado no IP. Para desabilitar a função utilize o comando **no user access-control**.

Sintaxe: **user access-control ip-based enable**
no user access-control

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de controle de acesso como baseado no IP:

```
INTELBRAS(config)# user access-control ip-based enable
```

32.2. user access-control ip-based

Descrição: o comando **user access-control ip-based** é utilizado para limitar a quantidade de endereços IP para login dos usuários. Somente os usuários que estiverem dentro do range de endereços que forem apontados aqui poderão realizar o login. Você pode adicionar até 30 entradas baseadas em IP. Para cancelar o limite de acesso para os usuários utilize o comando **no user access-control ip-based**.

Sintaxe: **user access-control ip-based** {*ip-addr ip-mask*} [snmp] [telnet] [ssh] [http] [https] [ping] [all]
no user access-control ip-based index *id*

Parâmetros:

» **ip-addr:** especifica o endereço IP de origem. Somente usuários com o endereço IP que você determinar aqui terão permissão para login.

» **ip-mask:** máscara de sub-rede do endereço IP.
» **[snmp] [telnet] [ssh] [http] [https] [ping] [all]:** especifica o tipo da interface de acesso. Por padrão todas as interfaces estão habilitadas.
» **id:** deleta a entrada especificada.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o controle de acesso somente para o endereço 192.168.0.148:

INTELBRAS(config)# user access-control ip-based 192.168.0.148 255.255.255.255

32.3. user access-control mac-based enable

Descrição: o comando **user access-control mac-based enable** é utilizado para configurar o modo de controle de acesso como baseado no endereço MAC. Para desabilitar essa função de controle de acesso utilize o comando **no user access-control**.

Sintaxe: **user access-control mac-based enable**
no user access-control

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de controle de acesso como baseado em endereço MAC:

INTELBRAS(config)# user access-control mac-based enable

32.4. user access-control mac-based

Descrição: o comando **user access-control mac-based** é utilizado para limitar a quantidade de endereços MAC para login dos usuários. Somente os usuários que tiverem os endereços que forem apontados aqui poderão realizar o login. Você pode adicionar até 30 entradas baseadas em MAC. Para cancelar o limite de acesso para os usuários utilize o comando **no user access-control mac-based.**

Sintaxe: **user access-control mac-based** {*mac-addr*} [snmp] [telnet] [ssh] [http] [https] [ping] [all]
no user access-control mac-based index *id*

Parâmetros:

» **mac-addr:** especifica o endereço MAC de origem. Somente usuários com o endereço MAC que você determinar aqui terão permissão para login.
» **[snmp] [telnet] [ssh] [http] [https] [ping] [all]:** especifica o tipo da interface de acesso. Por padrão todas as interfaces estão habilitadas.
» **id:** deleta a entrada especificada.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o controle de acesso somente para o endereço 00:00:13:0A:00:01:

INTELBRAS(config)# user access-control mac-based 00:00:13:0A:00:01

32.5. user access-control port-based enable

Descrição: o comando **user access-control port-based enable** é utilizado para configurar o modo de controle de acesso como baseado na porta Ethernet. Para desabilitar essa função de controle de acesso utilize o comando **no user access-control**.

Sintaxe: **user access-control port-based enable**
no user access-control

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de controle de acesso como baseado na porta Ethernet:

```
INTELBRAS(config)# user access-control port-based enable
```

32.6. user access-control port-based

Descrição: o comando **user access-control port-based** é utilizado para limitar as portas que podem fazer login. Somente os usuários que tiverem nas portas que forem apontados aqui poderão realizar o login. Você pode adicionar até 30 entradas baseadas em portas Ethernet. Para cancelar o limite de acesso para os usuários utilize o comando **no user access-control port-based.**

Sintaxe: **user access-control port-based** {**gigabitEthernet** *port-list*} [snmp] [telnet] [ssh] [http] [https] [ping] [all]
no user access-control port-based index *id*

Parâmetros:

- **port-list:** lista do grupo de portas Ethernet que serão habilitadas para login. No formato *1/0/1* ou *1/0/1-4*.
- **[snmp] [telnet] [ssh] [http] [https] [ping] [all]:** especifica o tipo da interface de acesso. Por padrão todas as interfaces estão habilitadas.
- **id:** deleta a entrada especificada.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o controle de acesso somente para as portas 2 à 6:

```
INTELBRAS(config)# user access-control port-based interface gigabitEthernet 1/0/2-6
```

33. Comandos HTTP e HTTPS

Com a ajuda do HTTP (*Hyper Text Transfer Protocol*) ou HTTPS (*Hyper Text Transfer Protocol over Secure Socket Layer*) você pode gerenciar o switch através de um navegador web.

HTTP é o protocolo de negociação e transferência de hypertext.

SSL (*Secure Sockets Layer*) é um protocolo que provê conexão segura para protocolos do Layer de aplicação (ex. HTTP) baseados em TCP. Adotando tecnologia de criptografia assimétrica o SSL utiliza um par de chaves para criptografar ou descriptografar a informação. Um par de chaves se refere à chave pública (contida no certificado) e uma chave privada. Por padrão o switch possui um certificado self-signed e uma chave privada correspondente. A função Certificate / Key Download permite que o usuário substitua o par de chaves padrão.

33.1. ip http server

Descrição: o comando **ip http server** é utilizado para habilitar o servidor HTTP dentro do switch. Para desabilitar utilize o comando **no ip http server**. Essa função vem habilitada por padrão. Os servidores HTTP e HTTPS não podem ser desabilitados ao mesmo tempo.

Sintaxe: **ip http server**
no ip http server

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: desabilite a função de http:

```
INTELBRAS(config)# no ip http server
```

33.2. ip http port

Descrição: o comando **ip http port** é utilizado para configurar o número da porta para o servidor HTTP do switch. Para retornar esse valor para o padrão utilize o comando **no ip http port**.

Sintaxe: **ip http port** *port-num*
no ip http port

Parâmetro:

» **port-num:** número da porta. Valor varia entre 1 e 65535.

Modo de comando: Global Configuration.

Requisito de privilégio: Somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: aponte o número da porta do servidor HTTP como 1800:

```
INTELBRAS(config)# ip http port 1800
```

33.3. ip http max-users

Descrição: o comando **ip http max-users** é utilizado para configurar o número máximo de usuários que podem conectar no servidor HTTP. Para retirar esta limitação utilize o comando **no ip http max-users**.

Sintaxe: **ip http max-users** *admin-num operator-num poweruser-num user-num*
no ip http max-users

Parâmetros:

» **admin-num:** número máximo de usuários administrares que podem fazer login no servidor HTTP, varia entre 1 e 16. O número total de usuários não pode passar de 16.

» **operator-num:** número máximo de usuários operadores que podem fazer login no servidor HTTP, varia entre 1 e 16. O número total de usuários não pode passar de 16.

» **poweruser-num:** número máximo de usuários administrares que podem fazer login no servidor HTTP, varia entre 1 e 16. O número total de usuários não pode passar de 16.

» **user-num:** número máximo de usuários administrares que podem fazer login no servidor HTTP, varia entre 1 e 16. O número total de usuários não pode passar de 16.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o número máximo de usuários para administrador, operador, usuário avançado (power user) e usuário como 5, 1, 1, 1 respectivamente:

```
INTELBRAS(config)# ip http max-user 5 1 1 1
```

33.4. ip http session timeout

Descrição: o comando **ip http session timeout** é utilizado para limitar o tempo de timeout para a conexão ao servidor HTTP. Para voltar esse tempo para o tempo padrão utilize o comando **no ip http session timeout**.

Sintaxe: **ip http session timeout** *time*
no ip http session timeout

Parâmetro:

» **time:** tempo para timeout, varia entre 5 e 30 minutos. Por padrão vem configurado como *10 minutos*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o tempo de timeout para a conexão HTTP como 15 minutos:

```
INTELBRAS(config)# ip http session timeout 15
```

33.5. ip http secure-server

Descrição: o comando **ip http secure-server** é utilizado para habilitar o servidor HTTPS dentro do switch. Para desabilitar utilize o comando **no ip http secure-server**. Essa função vem habilitada por padrão. Os servidores HTTP e HTTPS não podem ser desabilitados ao mesmo tempo.

Sintaxe: **ip http secure-server**
no ip http secure-server

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: desabilite o servidor HTTPS:

```
INTELBRAS(config)# no ip http secure-server
```

33.6. ip http secure-port

Descrição: o comando **ip http secure-port** é utilizado para configurar o número da porta para o servidor HTTP do switch. Para retornar esse valor para o padrão utilize o comando **no ip http secure-port.**

Sintaxe: **ip http secure-port** *port-num*
no ip http secure-port

Parâmetro:

» **port-num:** número da porta de acesso, varia entre 1 e 65535.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: aponte a porta de acesso ao servidor HTTPS como 2800:

```
INTELBRAS(config)# no ip http secure-port 2800
```

33.7. ip http secure-protocol

Descrição: o comando **ip http secure-protocol** é utilizado para configurar a versão do protocolo SSL. Para retornar esse valor para o padrão do SSL utilize o comando **no ip http secure-protocol**. Por padrão o switch suporta SSLv3 e TLSv1.

Sintaxe: **ip http secure-protocol** {[ssl3] [tls1]}
no ip http secure-protocol

Parâmetros:

» **ssl3:** Protocolo SSL 3.0.
» **tls1:** Protocolo TLS 1.0.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a conexão do protocolo SSL como SSL 3.0:

```
INTELBRAS(config)# ip http secure-protocol ssl3
```

33.8. ip http secure-ciphersuite

Descrição: o comando **ip http secure-ciphersuite** é utilizado para configurar a versão do protocolo SSL. Para retornar esse valor para o padrão do SSL utilize o comando **no ip http secure-ciphersuite**. Por padrão o switch suporta SSLv3 e TLSv1.

Sintaxe: **ip http secure-ciphersuite** {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}
no ip http secure-ciphersuite

Parâmetro:

» **[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]:** especifica o algoritmo de criptografia e o algoritmo de resumo para usar em uma conexão SSL. Por padrão o switch suporta todos esses cipher suites.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o cipher suite para ser utilizado para criptografia da conexão SSL como 3des-ede-cbc-sha:

INTELBRAS(config)# ip http secure-ciphersuite 3des-ede-cbc-sha

33.9. ip http secure-max-users

Descrição: o comando **ip http secure-max-users** é utilizado para configurar o número máximo de usuários que podem conectar no servidor HTTPS. Para retirar esta limitação utilize o comando **no ip http max-users**.

Sintaxe: **ip http secure-max-users** *admin-num operator-num poweruser-num user-num*
no ip http secure-max-users

Parâmetros:

- **admin-num:** número máximo de usuários administrares que podem fazer login no servidor HTTP, varia entre 1 e 16. O número total de usuários não pode passar de 16.
- **operator-num:** número máximo de usuários operadores que podem fazer login no servidor HTTP, varia entre 1 e 16. O número total de usuários não pode passar de 16.
- **poweruser-num:** número máximo de usuários administrares que podem fazer login no servidor HTTP, varia entre 1 e 16. O número total de usuários não pode passar de 16.
- **user-num:** número máximo de usuários administrares que podem fazer login no servidor HTTP, varia entre 1 e 16. O número total de usuários não pode passar de 16.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o número máximo de usuários para administrador, operador, usuário avançado (power user) e usuário como 5, 1, 1, 1 respectivamente para o servidor HTTPS:

INTELBRAS(config)# ip http secure-max-user 5 1 1 1

33.10. ip http secure-session timeout

Descrição: o comando **ip http secure-session timeout** é utilizado para limitar o tempo de timeout para a conexão ao servidor HTTP. Para voltar esse tempo para o tempo padrão utilize o comando **no ip http secure-session timeout**.

Sintaxe: **ip http secure-session timeout** *time*
no ip http secure-session timeout

Parâmetro:

- **time:** tempo para timeout, varia entre 5 e 30 minutos. Por padrão vem configurado como 10 minutos.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o tempo de timeout para a conexão HTTP como 15 minutos:

INTELBRAS(config)# ip http secure-session timeout 15

33.11. ip http secure-server download certificate

Descrição: o comando **ip http secure-server download certificate** é utilizado para fazer o download do certificado do servidor TFTP para o switch.

Sintaxe: **ip http secure-server download certificate** *ssl-cert* **ip-address** *ip-addr*

Parâmetros:

- **ssl-cert:** o nome do certificado SSl que será selecionado para baixar para o switch, com até 25 caracteres. O certificado deve ser um BASE64 encoded.
- **ip-addr:** endereço IP do servidor TFTP, pode ser IPv4 ou IPv6.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Baixe o certificado chamado ssl-cert do servidor TFTP com o endereço 192.168.0.146:

```
INTELBRAS(config)# ip http secure-server download certificate ssl-cert ip-address 192.168.0.146
```

Baixe o certificado chamado ssl-cert do servidor TFTP com o endereço fe80::1234:

```
INTELBRAS(config)# ip http secure-server download certificate ssl-cert ip-address fe80::1234
```

33.12. ip http secure-server download key

Descrição: o comando **ip http secure-server download key** é utilizado para fazer o download da chave do servidor TFTP para o switch.

Sintaxe: **ip http secure-server download key** *ssl-key* **ip-address** *ip-addr*

Parâmetros:

- **ssl-key:** o nome da chave SSl que será selecionado para baixar para o switch, com até 25 caracteres. O certificado deve ser um BASE64 encoded.
- **ip-addr:** endereço IP do servidor TFTP, pode ser IPv4 ou IPv6.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Baixe a chave chamada ssl-key do seridor TFTP com o endereço 192.168.0.146:

```
INTELBRAS(config)# ip http secure-server download key ssl-key ip-address 192.168.0.146
```

Baixe a chave chamada ssl-key do seridor TFTP com o endereço fe80::1234:

```
INTELBRAS(config)# ip http secure-server download key ssl-key ip-address fe80::1234
```

33.13. show ip http secure-server

Descrição: o comando **show ip http secure-server** é usado para mostrar a configuração global do SSL.

Sintaxe: **show ip http secure-server**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração global do SSL:

```
INTELBRAS# show ip http secure-server
```

34. Comandos SSH

O SSH (*Security Shell*) pode tornar um gerenciamento remoto não seguro em um gerenciamento com autenticações para garantir a segurança da informação gerenciada.

34.1. ip ssh server

Descrição: o comando **ip ssh server** é utilizado para habilitar a função SSH. Para desabilitar a função SSH utilize o comando **no ip ssh server**.

Sintaxe: **ip ssh server**
no ip ssh server

Modo de comando: Global Cofiguration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de SSH:

INTELBRAS(config)# ip ssh server

34.2. ip ssh port

Descrição: o comando **ip ssh port** é usado para configurar a porta para o serviço SSH. Para retornar o valor para o valor padrão utilize o comando **no ip ssh port**.

Sintaxe: **ip ssh port** *port*
no ip ssh port

Parâmetro:

» **port:** determina o número da porta, varia entre 1 e 65535. O valor padrão é *22*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a porta SSH como 22:

INTELBRAS(config)# ip ssh port 22

34.3. ip ssh version

Descrição: o comando **ip ssh version** é usado para habilitar a versão do protocolo SSH. Para desabilitar utilize o comando **no ip ssh version**.

Sintaxe: **ip ssh version** { v1 | v2 }
no ip ssh version

Parâmetros:

» **v1 | v2:** versão do protocolo à ser habilitada, representam respectiva mente SSH v1 e SSH v2.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o SSH v2.

INTELBRAS(config)# ip ssh version v2

34.4. ip ssh algorithm

Descrição: o comando **ip ssh algorithm** é usado para habilitar a versão do protocolo SSH. Para desabilitar utilize o comando **no ip ssh algorithm**.

Sintaxe: **ip ssh algorithm** {AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5}
no ip ssh algorithm

Parâmetros:

» **AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5:** especifica o algoritmo do SSH.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o algoritmo SSH como AES128-CBC.

INTELBRAS(config)# ip ssh algorithm AE128-CBC

34.5. ip ssh timeout

Descrição: o comando **ip ssh timeout** é usado para configurar o tempo de ociosidade da sessão SSH. Para restaurar ao padrão utilize o comando **no ip ssh timeout**.

Sintaxe: **ip ssh timeout** *value*
no ip ssh timeout

Parâmetro:

» **value:** representa o tempo de Idle-timeout, tempo limite para ociosidade.

Durante este período se não houver operação do cliente o sistema irá fechar a conexão automaticamente. Varia entre 1 e 120 segundos, por padrão vem configurado como *120 segundos*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o tempo de ociosidade em 30 segundos para a conexão ssh.

INTELBRAS(config)# ip ssh timeout 30

34.6. ip ssh max-client

Descrição: o comando **ip ssh max-client** é usado para especificar o número máximo de conexões SSH. Para retornar para o valor padrão utilize o comando **no ip ssh max-client**.

Sintaxe: **ip ssh max-client** *num*
no ip ssh max-client

Parâmetros:

» **num:** representa o máximo de conexões ao servidor SSH que serão permitidas. Varia entre 1 e 5 e por padrão vem configurado como *5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o limite de conexões para o servidor SSH como 3.

INTELBRAS(config)# ip ssh max-client 3

34.7. ip ssh download

Descrição: o comando **ip ssh download** é usado para baixar a chave SSH do servidor TFTP.

Sintaxe: **ip ssh download** {v1 | v2} *key-file* **ip-address** *ip-addr*

Parâmetros:

» **v1 | v2:** versão do protocolo para download, representam respectivamente SSH v1 e SSH v2.
» **key-file:** nome do arquivo chave selecionado para download. Com no máximo 25 caracteres. O tamanho da chave deve variar entre 512 e 3072 bits.
» **ip-addr:** endereço IP do servidor TFTP, pode ser IPv4 ou IPv6.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Baixe a chave SSH-1 ssh-key do servidor TFTP com o endereço 192.168.0.146:

INTELBRAS(config)# ip ssh download v1 ssh-key **ip-address** 192.168.0.146

Baixe a chave SSH-1 ssh-key do servidor TFTP com o endereço fe80::1234:

INTELBRAS(config)#)# ip ssh download v1 ssh-key **ip-address** fe80::1234

34.8. remove public-key

Descrição: o comando **remove public-key** é usado para remover a chave pública do SSH no switch.

Sintaxe: **remove public-key** {v1 | v2}

Parâmetros:

» **v1 | v2:** seleciona o tipo da chave pública do SSH, v1 e v2 que representam respectivamente SSH-1 e SSH-2.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente o administrador possui acesso a este comando.

Exemplo: retire a chave pública SSH-1 do switch:

```
INTELBRAS# remove public-key v1
```

34.9. show ip ssh

Descrição: o comando **show ip ssh** é usado para mostrar a configuração global do SSH.

Sintaxe: **show ip ssh**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as configurações do SSH:

```
INTELBRAS# show ip ssh
```

35. Comandos Telnet

35.1. telnet enable

Descrição: o comando **telnet enable** é utilizado para habilitar a função de Telnet. Para desabilitar esta função utilize o comando **telnet disable**. Esta função vem habilitada por padrão.

Sintaxe: **telnet enable**
telnet disable

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: desabilite a função de Telnet:

```
INTELBRAS(config)# telnet disable
```

35.2. telnet-port

Descrição: o comando **telnet port** é utilizado para configurar o número da porta Telnet. Para retornar este valor para o padrão utilize o comando **no telnet port**.

Sintaxe: **telnet port** *port*
no telnet port

Parâmetro:

» **port-num:** número da porta. Valor varia entre 1 e 65535.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: altere a porta Telnet para 556:

```
INTELBRAS(config)# telnet port 556
```

35.3. show telnet-status

Descrição: o comando **show telnet-status** é utilizado para mostrar as informações de configuração Telnet.

Sintaxe: **show telnet-status**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as a informação do telnet:

```
INTELBRAS# show telnet-status
```

36. Comandos AAA

AAA (*Authentication Authorization Accounting*) autenticação, autorização e contabilização. Essa função é utilizada para autenticar usuários tentando logar no switch ou tentando acesso com nível de privilégio de administrador.

» Applicable Access Apllication

A autenticação pode ser aplicada às aplicações de acesso como: Telnet, SSH e HTTP.

» Authentication Method List

A Method List (lista de método) descreve os métodos de autenticação e sua sequência para autenticar um usuário. O switch contém uma lista de Login para que os usuários tenham acesso ao switch e uma Enable List para os usuários normais obterem privilégio de administrador.

» RADIUS/TACACS+ server

O usuário pode configurar os servidores RADIUS/TACACS+ para a conexão entre o switch e o servidor.

» Server Group

O usuário pode definir um grupo de autenticação para os servidores com vários servidores executando os mesmos protocolos de segurança, tanto RADIUS como TACACS+. Os usuários podem definir uma ordem preferencial para os servidores. Quando um usuário tenta acessar o switch, o mesmo perguntará ao primeiro servidor uma lista de autenticação. Se nenhuma resposta for recebida o próximo servidor será consultado e assim sucessivamente.

36.1. tacacas-server host

Descrição: o comando **tacacas-server host** é utilizado para configurar um novo servidor TACACS+. Para deletar o servidor TACACS+ especificado utilize o comando **no tacacas-server host**. Os servidores TACACS+ que você configurar serão adicionados ao grupo de servidores como *tacacs* por padrão.

Sintaxe: **tacacas-server host** *ip-address* [**port** *port-id*] [**timeout** *time*] [**key** {[0] *string* | 7 *encrypted-string*}]
no tacacas-server host *ip-address*

Parâmetros:

» **ip-address:** especifica o endereço IP do servidor TACACS+.

» **port-id:** especifica o número da porta para o AAA. Por padrão é *49*.

» **time:** especifica o tempo em segundos que o switch aguardará a resposta do servidor antes do timeout. Valores variam entre 1 e 9 segundos e por padrão vem configurado como *5 segundos*.

» **[0] string | 7 encrypted-string:** 0 e 7 são os tipos de criptografia. 0 indica que uma chave será descriptografada. 7 indica que uma chave criptografada simétrica com um tamanho específico. Por padrão o tipo da criptografia é 0. O termo *string* é um chave compartilhada entre o switch e o servidor de autenticação para trocas de mensagens e contém no máximo 32 caracteres. O ponto de interrogação e espaço não são caracteres válidos. O termo *encrypted-string* é uma chave criptografada simétrica com um tamanho fixo a qual você pode copiar do arquivo de configuração de outros switchs. A chave ou chave criptografada configurada aparecerá no formulário de criptografia. Sempre configure as chaves como último item desse comando.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: apenas usuários do nível de administrador têm acesso a esses comandos.

Exemplo: configure um servidor TACACS+ com o IP 1.1.1.1 com a porta TCP 1500, 6 segundos para timeout e uma chave sem criptografia como 12345:

```
INTELBRAS(config)# tacacs-serer host 1.1.1.1 port 1500 timeout 6 key 12345
```

36.2. show tacacs-server

Descrição: o comando **show tacacs-server** é usado para exibir a informação sumarizada dos servidores TACACS+.

Sintaxe: **show tacacs-server**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: Somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: mostre a configuração de todos os servidores TACACS+:

```
INTELBRAS# show tacacs-server
```

36.3. radius-server host

Descrição: o comando **radius-server host** é usado para configurar um novo servidor RADIUS. Para excluir o servidor RADIUS especificado utilize o comando **no radius-server host**. Por padrão o servidor RADIUS configurado será adicionado ao grupo de servidores como *radius*.

Sintaxe: **radius-server host** *ip-address* [**auth-port** *port-id*] [**acct-port** *port-id*] [**timeout** *time*] [**retransmit** *number*] [**nas-id** *nas-id*] [**key** {[0] *string* | 7 *encrypted-string*}]
no radius-server host *ip-address*

Parâmetros:

- **ip-address:** especifica o endereço IP do servidor RADIUS.
- **auth-port port-id:** especifica o número da porta UDP de destino para a requisição de autenticação. Por padrão é *1812*.
- **acct-port port-id:** especifica o número da porta UDP de destino para contabilização de requisições . Por padrão é *1813*.
- **time:** especifica o tempo em segundos que o switch aguardará a resposta do servidor antes do timeout. Valores variam entre 1 e 9 segundos e por padrão vem configurado como *5 segundos*.
- **number:** especifica o número de vezes que a requisição RADIUS será retransmitida para o servidor caso o mesmo não responda a tempo. Por padrão é configurado como *2 vezes*.
- **nas-id:** especifica o nome do NAS (*Network Access Server*) que é o servidor de acesso à rede que estará contido no pacote RADIUS para identificação. Com no máximo 31 caracteres. Por padrão o endereço MAC do switch é o nome NAS. Ou seja, geralmente o NAS indica o próprio switch.
- **[0] string | 7 encrypted-string:** 0 e 7 são os tipos de criptografia. 0 indica que uma chave será descriptografada. 7 indica que uma chave criptografada simétrica com um tamanho específico. Por padrão o tipo da criptografia é *0*. O termo *string* é um chave compartilhada entre o switch e o servidor de autenticação para trocas de mensagens e contém no máximo 32 caracteres. O ponto de interrogação e espaço não são caracteres válidos. O termo *encrypted-string* é uma chave criptografada simétrica com um tamanho fixo a qual você pode copiar do arquivo de configuração de outros switchs. A chave ou chave criptografada configurada aparecerá no formulário de criptografia. Sempre configure as chaves como último item desse comando.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure o servidor RADIUS com o endereço IP 1.1.1.1, porta para autenticação 1200, com 6 segundos para timeout, com 3 retransmissões e uma chave sem criptografia 12345:

```
INTELBRAS(config)# radius-server host 1.1.1.1 auth-port 1200 timeout 6 retransmit 3 key 12345
```

36.4. show radius-server

Descrição: o comando **show radius-server** é usado para exibir a informação sumarizada dos servidores RADIUS.

Sintaxe: **show radius-server**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: mostre a configuração de todos os servidores RADIUS:

```
INTELBRAS# show radius-server
```

36.5. aaa group

Descrição: o comando **aaa group** é usado para criar grupos de servidores AAA para agrupar os grupos de servidores existentes de TACACS+ e RADIUS para autenticação. Esse comando coloca o switch no modo de Server Group Configuration. Para excluir um grupo AAA correspondente utilize o comando **no aaa group**.

Sintaxe: **aaa group** {radius | tacacs} *name*
no aaa group {radius | tacacs} *name*

Parâmetros:

» **radius | tacacs:** especifica o tipo de grupo RADIUS ou TACACS+.
» **name:** especifica o nome do grupo.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie um grupo de RADIUS com o nome radiusIntelbras:

INTELBRAS(config)# aaa group radius radiusIntelbras

36.6. server

Descrição: o comando **server** é usado para adicionar um servidor existente à um grupo de servidores definido. Para remover um servidor do grupo ode servidores utilize o **no server**.

Sintaxe: **server** *ip-address*
no server *ip-address*

Modo de comando: Server Group Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: crie o servidor RADIUS 1.1.1.1 para o grupo de servidor RADIUS "radiusIntelbras":

INTELBRAS(config)# aaa group radius *radiusIntelbras*
INTELBRAS(aaa-config)# server 1.1.1.1

36.7. show aaa group

Descrição: o comando **show aaa group** é usado para exibir as informações sumarizadas dos grupos AAA. Todos os servidores no grupo serão listados se não for especificado o nome do grupo.

Sintaxe: **show aaa group** [*group-name*]

Parâmetro:

» **group-name:** especifica o nome do grupo.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: mostre a configuração de todos os grupos de servidor:

INTELBRAS# show aaa group

36.8. aaa authentication login

Descrição: o comando **aaa authentication login** é usado para configurar a lista de métodos de autenticação para o login. A lista de métodos descreve os métodos de autenticação e sua respectiva sequencia para autenticar um usuário. Para deletar uma lista de métodos de autenticação utilize o comando **no aaa authentication login**.

Sintaxe: **aaa authentication login** {*method-list*} {method1} [method2] [method3] [method4]
no aaa authentication login *method-list*

Parâmetros:

» **method-list:** especifica o nome da lista.

» **method1, method2, method3, method4:** especifica os métodos de autenticação em ordem. A próxima autenticação só é aplicada se a anterior não responder ou falhar. Os métodos pré definidos são radius, tacacs, local e none. *radius* representa grupo de servidor RADIUS; *tacacs* representa os servidores TACACS+; *local* representa nome de usuário da base local; *none* representa sem autenticação para o login. Os usuários também podem definir novos métodos com o comando **aaa group**.

Modo de comando: Global Configuration.

Requisito de privilégio: apenas usuários do nível de administrador têm acesso a esses comandos.

Exemplo: configure uma lista de métodos de autenticação de login, list1, com a primeira prioridade radius e a segunda como local:

INTELBRAS(config)# aaa authentication login list1 radius local

36.9. aaa authentication enable

Descrição: o comando **aaa authentication enable** é usado para configurar a ordem dos métodos de autenticação. A lista de métodos descreve os métodos de autenticação e sua respectiva sequência para elevar os privilégios de usuários. Para deletar uma lista de métodos utilize o comando **no aaa authentication enable**. Por padrão vem configurado como *none* para o primeiro método.

Sintaxe: **aaa authentication enable** {*method-list*} {method1} [method2] [method3] [method4]
no aaa authentication enable *method-list*

Parâmetros:

» **method-list:** especifica o nome da lista.

» **method1, method2, method3, method4:** especifica os métodos de autenticação em ordem. A próxima autenticação só será aplicada se a anterior não responder ou falhar. Os métodos pré definidos são radius, tacacs, local e none. *radius* representa grupo de servidor RADIUS; *tacacs* representa os servidores TACACS+; *local* representa nome de usuário da base local; *none* representa sem autenticação para o login. Os usuários também podem definir novos métodos com o comando **aaa group**.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure uma lista de métodos de autenticação privilegiada, list2, com a primeira prioridade radius e a segunda como local:

INTELBRAS(config)# aaa authentication enable list2 radius local

36.10. aaa authentication dot1x default

Descrição: o comando **aaa authentication dot1x default** é usado para configurar uma lista de métodos de autenticação 802.1x. A lista de métodos descreve os métodos de autenticação e sua respectiva sequência de login dos usuários no 802.1x. Para deletar uma lista de métodos utilize o comando **no aaa authentication dot1x default**.

Sintaxe: **aaa authentication dot1x default** {method}
no aaa authentication dot1x default

Parâmetro:

» **method:** especifica o nome do método. Somente o grupo de servidor RADIUS é suportado, e o método padrão é o *radius.*

Modo de comando: Global Configuration.

Requisito de privilégio: Somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure o método de autenticação padrão para o 802.1x como "radius1":

INTELBRAS(config)# aaa authentication dot1x default radius1

36.11. aaa accounting dot1x default

Descrição: o comando **aaa accounting dot1x default** é usado para configurar a contabilidade de uma lista de métodos do 802.1x. Para deletar uma lista de métodos utilize o comando **no aaa accounting dot1x default**.

Sintaxe: **aaa accounting dot1x default** {method}
no aaa accounting dot1x default

Parâmetro:

» **method:** especifica o nome do método. Somente o grupo de servidor RADIUS é suportado, e o método padrão é o *radius*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure a contabilidade no método padrão para o 802.1x como "radius1":

```
INTELBRAS(config)# aaa accounting dot1x default radius1
```

36.12. show aaa authentication

Descrição: o comando **show aaa authentication** é usado para exibir as informações sumarizada das listas de métodos de autenticação de login, enable e dot1x.

Sintaxe: **show aaa authentication** [login | enable | dot1x]

Parâmetro:

» **login | enable | dot1x:** especifica o tipo da lista.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: mostre as configurações de todas as listas:

```
INTELBRAS# show aaa authentication
```

36.13. show aaa accounting

Descrição: o comando **show aaa accounting** é usado para exibir as informações sumarizada das contabilidades das listas de métodos.

Sintaxe: **show aaa accounting** [dot1x]

Parâmetro:

» **dot1x:** especifica o tipo da lista.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: mostre as configurações da lista padrão 802.1x:

```
INTELBRAS# show aaa accounting
```

36.14. line telnet

Descrição: o comando **line telnet** é utilizado para entrar no modo Line Configuration para configurar o terminal Telnet ao qual você deseja aplicar listas de autenticação.

Sintaxe: **line telnet**

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: entre no modo de Line Configuration.

```
INTELBRAS(config)# line telnet
```

36.15. login authentication (telnet)

Descrição: o comando **login authentication** é usado para aplicar uma lista de métodos de autenticação no login do terminal Telnet. Para restaurar a lista de métodos de autenticação padrão utilize o comando **no login authentication**.

Sintaxe: **login authentication** {*method-list*}
no login authentication

Parâmetro:

» **method-list:** especifica o nome da lista. Por padrão utiliza o método local.

Modo de comando: Line Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure uma lista de métodos de autenticação, list1, no terminal telnet chamado "list1":

```
INTELBRAS(config)# line telnet
INTELBRAS(config-line)# login authentication list1
```

36.16. line ssh

Descrição: o comando **line ssh** é utilizado para entrar no modo *Line Configuration* para configurar o terminal ssh ao qual você deseja aplicar listas de autenticação.

Sintaxe: **line ssh**

Modo de comando: Line Configuration Mode.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: entrar no modo de Line Configuration para ssh:

```
INTELBRAS(config)# line ssh
```

36.17. login authentication (ssh)

Descrição: o comando **login authentication** é usado para aplicar uma lista de métodos de autenticação para login no terminal ssh. Para restaurar a lista de métodos de autenticação padrão utilize o comando **no login authentication**.

Sintaxe: **login authentication** {*method-list*}
no login authentication

Parâmetro:

» **method-list:** especifica o nome da lista. Por padrão utiliza o método local.

Modo de comando: Line Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure uma lista de métodos de autenticação, list1, no terminal ssh:

```
INTELBRAS(config)# line ssh
INTELBRAS(config-line)# login authentication list1
```

36.18. enable authentication (telnet)

Descrição: o comando **enable authentication** é usado para aplicar a lista de métodos de autenticação privilegiada para o terminal Telnet. Para restaurar ao padrão utilize o comando **no enable authentication**.

Sintaxe: **enable authentication** {*method-list*}
no enable authentication

Parâmetro:

» **method-list:** especifica o nome da lista. Por padrão utiliza o método local.

Modo de comando: Line Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure a autenticação utilizando a lista de método list2, no terminal telnet:

```
INTELBRAS(config)# line telnet
INTELBRAS(config-line)# enable authentication list2
```

36.19. enable authentication (ssh)

Descrição: o comando **enable authentication** é usado para aplicar uma method-list para autenticação no terminal ssh. Para ao padrão utilize o comando **no enable authentication**.

Sintaxe: **enable authentication** {*method-list*}
no enable authentication

Parâmetro:

» **method-list:** especifica o nome da lista. Por padrão utiliza o método local.

Modo de comando: Line Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure a autenticação utilizando a lista de método, list2, no terminal ssh:

```
INTELBRAS(config)# line ssh
INTELBRAS(config-line)# enable authentication list2
```

36.20. ip http login authentication

Descrição: o comando **ip http login authentication** é usado para aplicar uma lista de métodos de autenticação para usuários que fazem login através do HTTP. Para restaurar ao padrão utilize o comando **no ip http login authentication**.

Sintaxe: **ip http login authentication** {*method-list*}
no ip http login authentication

Parâmetro:

» **method-list:** especifica o nome da lista. Por padrão utiliza o método local.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure uma lista de métodos para autenticação no HTTP, list1:

```
INTELBRAS(config)# ip http login authentication list1
```

36.21. ip http enable authentication

Descrição: o comando **ip http authentication** é usado para aplicar uma lista de métodos de autenticação para o acesso através do HTTP. Para restaurar ao padrão utilize o comando **no ip http enable authentication**.

Sintaxe: **ip http enable authentication** {*method-list*}
no ip http enable authentication

Parâmetro:

» **method-list:** especifica o nome da lista. Por padrão utiliza o método local.

Modo de comando: Line Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure uma lista de métodos de autenticação, list2, para o http:

```
INTELBRAS(config)# ip http enable authentication list2
```

36.22. show aaa global

Descrição: o comando **show aaa global** é usado para exibir o status global da função AAA e as listas de métodos dos diferentes métodos de aplicação: telnet, ssh e http.

Sintaxe: **show aaa global**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: mostre o status global da função AAA:

```
INTELBRAS# show aaa accounting
```

36.23. enable-admin

Descrição: o comando **enable-admin** é usado para adquirir privilégios de administrador através de uma conta que não é administradora.

Sintaxe: **enable-admin**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários, usuários avançados e operadores têm acesso a esse comando.

Exemplo: adquira privilégio administrador (a senha Enable é "123456"):

```
INTELBRAS# enable-admin
Password: 123456
```

37. Comandos IEEE 802.1x

A função do IEEE 802.1x é providenciar um controle de acesso para as portas LAN através de autenticação. Um sistema 802.1x inclui três entidades: Supplicant ou solicitante, autenticador e um servidor de autenticação.

- **Supplicant:** é o dispositivo que solicita acesso à LAN, no caso o solicitante.
- **Servidor de autenticação:** executa propriamente a solicitação do solicitante. Ele valida a identidade do solicitante e notifica o autenticador se o solicitante está ou não autorizado a acessar a LAN.
- **Autenticador:** controla o acesso físico da rede baseado no status de autenticador do solicitante. É um dispositivo de rede usual do 802.1x, esse atua como um intermediário (proxy) entre o solicitante e o servidor de autenticação, requisitando informações de identidade do solicitante, verificando essa informação com o servidor de autenticação e retransmitindo a resposta ao solicitante.

Este capítulo lida com o processo de autenticação entre solicitante e switch. Para realizar a autenticação e a função de accounting é necessário habilitar a função AAA e configurar o servidor de RADIUS. Para maiores detalhes vá para o capítulo *36. Comandos AAA*.

37.1. dot1x system-auth-control

Descrição: o comando **dot1x system-auth-control** é utilizado para habilitar o IEEE 802.1x de forma global. Para desabilitar esta função utilize o comando **no dot1x system-auth-control**.

Sintaxe: **dot1x system-auth-control**
no dot1x system-auth-control

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função do IEEE 802.1x:

```
INTELBRAS(config)# dot1x system-auth-control
```

37.2. dot1x handshake

Descrição: o comando **dot1x handshake** é usado para habilitar a função de handshake (aperto de mão). Essa função é utilizada para detectar o status da conexão entre o solicitante e o switch através do 802.1x. Desabilite a função de handshake caso você estiver utilizando um software cliente não compatível com o 802.1x. Essa função vem habilitada por padrão. Para desabilitar a mesma utilize o comando **no dot1x handshake**.

Sintaxe: **dot1x handshake**
no dot1x handshake

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: desabilite a função de hankshake:

```
INTELBRAS(config)# no dot1x handshake
```

37.3. dot1x auth-protocol

Descrição: o comando **dot1x auth-protocol** é utilizado para habilitar o IEEE 802.1x de forma global. Para retornar para a configuração padrão utilize o comando **no dot1x auth-protocol**.

Sintaxe: **dot1x auth-protocol** {pap | eap}
no dot1x auth-protocol

Parâmetros:

- **pap:** modo de terminação EAP. O sistema de autenticação IEEE 802.1x utiliza o EAP (*Extensible Authentication Protocol*), protocolo de autenticação extensível, ou seja, é utilizado para trocar informações entre o cliente e o switch. Os pacotes EAP chegam ao switch e são abertos e reempacotados no PAP (*Password Authentication Protocol*), protocolo de autenticação de senha, e então transferidos para o servidor de RADIUS.
- **eap:** modo de retransmissão EAP. O sistema de autenticação IEEE 802.1x utiliza o EAP (*Extensible Authentication Protocol*), protocolo de autenticação extensível, ou seja, é utilizado para trocar informações entre o cliente e o switch. Os pacotes do protocolo EAP com a informação de autenticação são encapsulados em um protocolo avançado, como o RADIUS, para então serem transmitidos para o servidor de autenticação.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o protocolo de autenticação 802.1x como PAP:

```
INTELBRAS(config)# dot1x auth-protocol pap
```

37.4. dot1x vlan-assignment

Descrição: o comando **dot1x vlan-assignment** é utilizado para habilitar a função de atribuição de VLAN. Para desabilitar esta função utilize o comando **no dot1x vlan-assignment**.

A tecnologia de atribuição de VLAN do 802.1x permite que o servidor RADIUS envie a atribuição da VLAN para a porta quando a porta estiver autenticada.

Se a VLAN atribuída não existir no switch automaticamente ele criará essa VLAN adicionando a porta autenticada à VLAN e alterando o PVID para a VLAN atribuída.

Se o servidor RADIUS não suportar as VLANs ou a autenticação 802.1x estiver desabilitada a porta permanecerá na sua VLAN original após autenticar com sucesso.

Sintaxe: **dot1x vlan-assignment**
no dot1x vlan-assignment

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a atribuição de VLAN:

```
INTELBRAS(config)# dot1x vlan-assignment
```

37.5. dot1x accounting

Descrição: o comando **dot1x accounting** é usado para habilitar a função de accounting do IEEE 802.1x de forma global. Para desabilitar a mesma utilize o comando **no dot1x accounting**.

Sintaxe: **dot1x accounting**
no dot1x accounting

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de accounting do IEEE 802.1x globalmente:

```
INTELBRAS(config)# dot1x accounting
```

37.6. dot1x mab

Descrição: o comando **dot1x mab** é usado para habilitar a função de MAB para a porta. Para desabilitar a mesma utilize o comando **no dot1x mab**.

Com a função de MAB (*MAC-based Authentication Bypass*) ativa, o switch envia automaticamente para o servidor de RADIUS requisições de acesso com o endereço MAC do cliente, nome de usuário e senha. Isso é algo necessário para configurar o servidor RADIUS com as configurações do usuário para a autenticação. Você pode habilitar a função nas portas IEEE 802.1x conectadas à dispositivos não compatíveis com o 802.1x. Por exemplo a maioria das impressoras e telefones IP não possuem a compatibilidade 802.1x.

Sintaxe: **dot1x mab**
no dot1x mab

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de MAB para a porta 1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x mab
```

37.7. dot1x guest-vlan

Descrição: o comando **dot1x guest-vlan** é utilizado para habilitar a função de convidado da VLAN para a porta. Para desabilitar esta função utilize o comando **no dot1x guest-vlan**.

Sintaxe: **dot1x guest-vlan** *vid*
no dot1x guest-vlan

Parâmetro:

» **vid:** a ID da VLAN que habilitará o Guest VLAN, viria entre 0 e 4094. 0 significa que o Guest VLAN está desabilitado. Os solicitantes dentro do Guest VLAN podem acessar as redes especificadas na origem.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de Guest VLAN para a porta 1 dentro da VLAn 5:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x guest-vlan 5
```

37.8. dot1x timeout quiet-period

Descrição: o comando **dot1x timeout quiet-period** é usado para habilitar a função quiet-period para a porta. Esta função determina o tempo qual as requisições da porta não serão processadas após a falha na autenticação da sequência 802.1x. Para desabilitar a mesma utilize o comando **no dot1x timeout quiet-period**.

Sintaxe: **dot1x timeout quiet-period** [*time*]
no dot1x timeout quiet-period

Parâmetro:

» **time:** duração do quiet-period. Varia entre 1 e 999 segundos e vem configurada como *10* por padrão.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função quiet-period e a configure para 5 segundos para a porta 1.

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x timeout quiet-period 5
```

37.9. dot1x timeout supp-timeout

Descrição: o comando **dot1x timeout supp-timeout** é usado para configurar o tempo de timeout para a porta solicitante. Para retornar para o valor padrão utilize o comando **no dot1x timeout supp-timeout**.

Sintaxe: **dot1x timeout supp-timeout** *time*
no dot1x timeout supp-timeout

Parâmetro:

» **time:** tempo máximo de espera até a resposta do solicitante que o switch aguardará até reenviar a solicitação ao solicitante. Varia entre 1 e 9 segundos e vem configurada como *3* por padrão.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função supp-timeout e a configure para 5 segundos para a porta 1.

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x timeout supp-timeout 5

37.10. dot1x max-req

Descrição: o comando **dot1x max-req** é usado para configurar o número máximo de requisições de autenticação que podem ser solicitadas quando o servidor não pode ser conectado. Para restaurar para a configuração padrão utilize o comando **no dot1x max-req**.

Sintaxe: **dot1x max-req** *times*
no dot1x max-req

Parâmetro:

» **times:** número máximo de vezes que uma requisição de autenticação pode ser repetida, varia entre 1 e 9. Por padrão vem configurada como *3*.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o máximo de vezes que a requisição de autenticação pode ser repetida para a porta 1 como 5:

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x max-req 5

37.11. dot1x

Descrição: o comando **dot1x** é usado para habilitar a função de IEEE 802.1 para a porta. Para desabilitar a mesma utilize o comando **no dot1x**.

Sintaxe: **dot1x**
no dot1x

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de IEEE 802.1x para a porta 1:

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x

37.12. dot1x port-control

Descrição: O comando **dot1x port-control** é usado para configurar o modo de controle para o IEEE 802.1x para uma porta específica. Por padrão o modo é *auto*. Para retornar a configuração padrão utilize o comando **no dot1x port-control**.

Sintaxe: **dot1x port-control** {auto | authorized-force | unauthorized-force}
no dot1x port-control

Parâmetros:

» **auto:** neste modo a porta só irá funcionar normalmente após a passar na autenticação 802.1x.
» **authorized-force:** neste modo a porta pode funcionar normalmente sem passar na autenticação 802.1x.
» **unauthorized-force:** neste modo a porta fixa proibida de funcionar pelo status fixo de não autorizada.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o modo de controle para a porta 1 como "authorize-force":

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x port-control authorized-force

37.13. dot1x port-method

Descrição: o comando **dot1x port-method** é usado para configurar o método de controle para o IEEE 802.1x para uma porta específica. Por padrão o modo é *mac-based*. Para retornar à configuração padrão utilize o comando **no dot1x port-method**.

Sintaxe: **dot1x port-method** {mac-based | port-based}
no dot1x port-method

Parâmetros:

» **mac-based:** neste método todos os clientes conectados à porta devem passar na autenticação 802.1x para obter acesso.
» **port-based:** neste método todos os clientes conectados a essa porta tem acesso à rede, nesta condição ao menos um dos clientes deve ter passado na autenticação 802.1x.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o método de controle para a porta 1 como *port-based*:

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x port-method port-based

37.14. dot1x auth-init

Descrição: o comando **dot1x auth-init** é usado para inicializar um cliente específico.

Sintaxe: **dot1x auth-init** [**mac** *mac-address*]

Parâmetro:

» **mac-address:** endereço MAC do cliente que será autorizado.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: inicialize o cliente de MAC 00:02:58:4f:6c:23 para a porta 1:

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x auth-init mac 00:02:58:4f:6c:23

37.15. dot1x auth-reauth

Descrição: o comando **dot1x auth-reauth** é usado para reautenticar um cliente específico.

Sintaxe: **dot1x auth-reauth** [**mac** *mac-address*]

Parâmetro:

» **mac-address:** endereço MAC do cliente que será reautenticado.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: reautentique o cliente de MAC 00:02:58:4f:6c:23 na porta 1.

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# dot1x auth-reauth mac 00:02:58:4f:6c:23

37.16. show dot1x global

Descrição: o comando **show dot1x global** é usado para exibir a informação global do 802.1x.

Sintaxe: **show dot1x global**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração do 802.1x:

INTELBRAS# show dot1x global

37.17. show dot1x interface

Descrição: o comando **show dot1x interface** é usado para exibir a informação de todas as portas ou de uma porta do 802.1x.

Sintaxe: **show dot1x interface** [**gigabtitEthernet** *port*]

Parâmetro:

» **port:** número da porta Ethernet. Se não especificada será mostrada informação de todas as portas.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração do 802.1x da porta 20:

INTELBRAS# show dot1x interface gigabitEthernet 1/0/20

37.18. show dot1x auth-state

Descrição: o comando s**how dot1x auth-state** é usado para exibir o status de autenticação de cada porta.

Sintaxe: **show dot1x auth-state**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a o status de autenticação de cada porta:

INTELBRAS# show dot1x auth-state

38. Comandos de segurança de porta

Você pode limitar o número de endereços MAC que podem ser aprendidos para cada porta, além de prevenir que a tabela de endereços MAC fique lotada devido à pacotes de ataque, impedindo que o switch atue como um ativo de rede.

38.1. mac address-table max-mac count

Descrição: o comando **mac address-table max-mac count** é utilizado para habilitar função segurança de porta e configurar os parâmetros relacionados. Para desabilitar a função e retornar os parâmetros para os valores padrão utilize o comando **no mac address-table max-mac count**.

Sintaxe: **mac address-table max-mac count** {[**max-number** *num*] [**exceed-max-learned** enable | disable] [**mode** {dynamic | static | permanent}] [**status** {forward | drop | disable}]}
no mac address-table max-mac count [max-number | mode | status]

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o número máximo de endereços MAC que podem ser aprendidos pela porta 1 como 30, habilite a função exceed-max-learned e configure o modo como permanente e o status como drop:

INTELBRAS(config)# interface gigabitEthernet 1/0/1

INTELBRAS(config-if)# mac address-table max-mac-count max-number 30 **exeed-maxlearned** enable **mode** permanente **status** drop

38.2. show mac address-table max-mac-count

Descrição: o comando **show mac address-table max-mac-count** é usado para exibir as configurações de segurança de porta.

Sintaxe: **show mac address-table max-mac-count interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*}

Parâmetro:

» **port:** determina o número da porta, varia entre 1 e 65539. O valor padrão é *22*.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração de segurança de porta para a porta 1:

```
INTELBRAS(config)# show mac address-table max-mac-count interface gigabitEthernet 1/0/1
```

39. Comandos de espelhamento de porta

Port Mirroring ou espelhamento de portas, permite que o switch envie uma cópia do tráfego que passa através de fontes específicas (porta, LAGs ou CPU) para uma porta destino. Isso não afeta o fluxo do tráfego da rede nas portas de origem, LAGs ou CPU. Geralmente, a porta de monitoramento é conectada ao sniffer para analisar os pacotes monitorados e troubleshooting da rede.

39.1. monitor session destination interface

Descrição: o comando **monitor session destination interface** é utilizado configurar a porta de monitoramento. Cada sessão de m possui uma única porta de monitoramento. Para alterar a porta de monitoramento utilize este comando alterando o valor da porta. Para desabilitar esta função utilize o comando **no monitor session**.

Sintaxe: **monitor session** *session_num* **destination interface gigabitEthernet** *port*
no monitor session *session_num* **destination interface gigabitEthernet** *port*
no monitor session *session_num*

Parâmetros:

» **session_num:** número da sessão de monitoria, só pode ser especificado como 1.

» **port:** número da porta de monitoramento.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Crie a sessão de monitoria 1 e configure a porta 1 como porta de monitoramento:

```
INTELBRAS(config)# monitor session 1 destination interface gigabitEthernet 1/0/1
```

Delete a porta de monitoramento 2 da sessão 1:

```
INTELBRAS(config)# no monitor session 1 destination interface gigabitEthernet 1/0/2
```

Delete a sessão de monitoramento 1:

```
INTELBRAS(config)# monitor session 1
```

39.2. monitor session source

Descrição: o comando **monitor session source** é utilizado para configurar as interfaces monitoradas. Para deletar este monitoramento utilize o comando **no monitor session source**.

O monitoramento de portas é correspondente à configuração corrente do modo de interface. Não há limite para as portas monitoradas, mas não há como monitorar portas ao mesmo tempo.

A porta de monitoramento e a monitorada não necessariamente precisam estar na mesma VLAN, isso não é uma exigência. A porta de monitoramento e a monitorada não podem ser membros de link-aggregation.

Sintaxe: **monitor session** *session_num* **source** {**cpu** *cpu_number* |**interface gigabitEthernet** *port-list* | **interface port-channel** *port-channel-id*} *mode*
no monitor session *session_num* **source** {**cpu** *cpu_number* | **interface gigabitEthernet** *port-list* | **interface port-channel** *port-channel-id*} *mode*

Parâmetro:

- **session_num:** número da sessão de monitoramento. Só pode ser 1.
- **cpu_number:** número da CPU. Só pode ser 1.
- **port-list:** lista de número de portas. É multiopcional.
- **port-channel-id:** lista de número de port-channel, varia entre 1 e 8.
- **mode:** modo de monitoramento. Existem 3 opções: *rx, tx* e *both*. Rx, modo de monitoramento de entrada, significa que os pacotes que estão sendo recebidos pela interface de monitoramento serão copiados para a porta de monitoramento. Tx, modo de monitoramento de saída, indica que os pacotes que estão saindo da interface de monitoramento serão copiados para a porta de monitoramento. Both representa que ambos os pacotes recebidos e enviados serão copiados para a interface de monitoramento.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo:

Crie a sessão de monitoramento 1 e então monitore as portas 4 e 5 monitorando os pacotes de entrada:

```
INTELBRAS(config)# monitor session 1 source interface gigabitEthernet 1/0/4-5 rx
```

Delete o monitoramento da porta 4 da sessão 1 e suas configurações:

```
INTELBRAS(config)# no monitor session 1 source interface gigabitEthernet 1/0/4 rx
```

39.3. show monitor session

Descrição: o comando **show monitor session** é utilizado para mostrar as informações de configuração do monitoramento de portas.

Sintaxe: **show monitor session** [*session_num*]

Parâmetro:

- **session_num:** sessão de monitoramento, só pode ser 1. É opcional.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as informações do monitoramento de portas.

```
INTELBRAS# show monitor session 1
```

40. Comandos ACL

O ACL (*Access Control List*) é usado para filtrar pacotes de dados configurando uma série de condições de correspondência, operações e intervalos de tempo. Isso provê flexibilidade e segurança à política de controle de acesso além de facilitar controle da segurança de rede.

40.1. access-list create

Descrição: O comando **access-list create** é utilizado para criar uma lista de controle de acesso, uma ACL.

Sintaxe: **access-list create** *acl-id* [*name acl-name*]
no access-list create { *acl-id* }

Parâmetros:

- **acl-id:** especifica a ID da ACL. Varia entre 0 e 499 para MAC ACL. Para IP ACL viria entre 500 e 999. Para IPv6 ACL varia entre 1500 e 1999.
- **acl-name:** nome para identificar a ACL.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie a IP ACL 523:

```
INTELBRAS(config)# access-list create 523
```

40.2. access-list resequence

Descrição: o comando **access-list resequence** é utilizado para ressequenciar as regras, fornecendo um ID de regra inicial e um valor de Step (passo).

Sintaxe: **access-list resequence** *acl-id-or-name* **start** *start-rule-id* **step** *rule-id-step-value*

Parâmetro:

- **acl-id-or-name:** especifica a ID da ACL ou nome.
- **start-rule-id:** ID da regra inicial.
- **rule-id-step-value**: valor do Step (passo).

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ressequencie as regas da ACL 12 com a ID inicial 1 e valor de Step 5:

```
INTELBRAS(config)# access-list resequence 12 start 1 step 5
```

40.3. access-list mac

Descrição: o comando **access-list mac** é usado para criar uma MAC ACL. Para excluir a mesma utilize o comando **no access-list mac**.

Sintaxe: **access-list mac** *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [**smac** *source-mac* **smask** *source-mac-mask*] [**dmac** *destination-mac* **dmask** *destination-mac-mask*] [**type** *ether-type*] [**pri** *dot1p-priority*] [**vid** *vlan-id*] [**tseg** *time-range-name*]
no access-list mac *acl-id-or-name* **rule** *rule-id*

Parâmetros:

- **acl-id-or-name:** especifica o nome ou a ID de uma ACL a qual a regra será adicionada.
- **auto:** a ID da regra será atribuída automaticamente e o intervalo entre as regras será 5.
- **rule-id:** especifica o número da ID da regra.
- **deny | permit:** especifica a ação que será tomada com o pacote que corresponder à essa regra. Por padrão vem configurado como *permit*. Os pacotes serão descartados se *deny* for selecionado e encaminhados caso *permit* for selecionado.
- **enable | disable:** habilita ou desabilita a função de Log para a regra ACL. Se *enable* for selecionado as vezes que a regra for acionada será feito relatório a cada 5 minutos. Com o contador de ACL Trap ativado uma Trap relacionada será gerada se o número de correspondências mudar.

» **source-mac:** especifica o endereço MAC de origem no formato *XX:XX:XX:XX:XX:XX*.
» **source-mac-mask:** especifica a máscara do endereço MAC de origem. É obrigatório se um endereço MAC de origem foi apontado. O formato é *XX:XX:XX:XX:XX:XX*.
» **destination-mac:** especifica o endereço MAC de destino. No formato *XX:XX:XX:XX:XX:XX*.
» **destination-mac-mask:** especifica a máscara do endereço MAC de destino. É obrigatório se um endereço MAC de destino foi apontado. No formato *XX:XX:XX:XX:XX:XX*.
» **ether-type:** especifica o tipo da Ethernet com 4 números hexadecimais.
» **dot1p-priority:** especifica a prioridade, varia entre 0 e 7. Por padrão *sem prioridade*.
» **vlan-id:** Id da VLAN, varia entre 1 e 4094.
» **time-range-name:** o nome do time-range, por padrão vem desabilitado.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie a ACL MAC 50 e configure a regra 5 para permitir pacotes com o endereço MAC de origem 00: 34: a2: 4: 34: b5:

INTELBRAS(config)# access-list create 50
INTELBRAS(config)# access-list mac 50 **rule** 5 **permit logging** disable **smac**
00:34:a2:d4:34:b5 **smask** ff:ff:ff:ff:ff:ff

40.4. access-list ip

Descrição: o comando **access-list ip** é usado para criar uma regra ACL IP. Para excluir a mesma utilize o comando **no access-list ip**. Uma ACL IP analisa e processa os pacotes de dados baseados em uma série de condições de correspondência, os quais podem ser endereço IP de origem e destino quais os pacotes carregam consigo.

Sintaxe: **access-list ip** *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [**sip** *sip-address* **sip-mask** *sip-address-mask*] [**dip** *dip-address* **dip-mask** *dip-address-mask*] [**dscp** *dscp-value*] [**tos** *tos-value*] [**pre** *pre-value*] [**protocol** *protocol* [**s-port** *s-port-number*] [**s-port-mask** *s-port-mask*] [**d-port** *d-port-number*] [**d-port-mask** *d-port-mask*] [**tcpflag** *tcpflag*]] [**tseg** *time-range-name*]
no access-list ip *acl-id-or-name* **rule** *rule-id*

Parâmetros:

» **acl-id-or-name:** especifica o nome ou a ID de uma ACL a qual a regra será adicionada.
» **auto:** a ID da regra será atribuída automaticamente e o intervalo entre as regras será 5.
» **rule-id:** especifica o número da ID da regra.
» **deny | permit:** especifica a ação que será tomada com o pacote que corresponder à essa regra. Por padrão vem configurado como *permit*. Os pacotes serão descartados se *deny* for selecionado e encaminhados caso *permit* for selecionado.
» **enable | disable**: habilita ou desabilita a função de Log para a regra ACL. Se *enable* for selecionado as vezes que a regra for acionada será feito relatório a cada 5 minutos. Com o contador de ACL Trap ativado uma Trap relacionada será gerada se o número de correspondências mudar.
» **sip-address**: especifica o endereço IP de origem.
» **sip-address-mask**: especifica a máscara do endereço IP de origem. É obrigatório se um endereço IP de origem foi apontado.
» **dip-address**: especifica o endereço IP de destino.
» **dip-address-mask:** especifica a máscara do endereço IP de destino. É obrigatório se um endereço IP de destino foi apontado.
» **dscp-value**: especifica o valor DSCP varia entre 0 e 63.
» **tos-value:** especifica um valor ToS IP para ser correspondido, varia entre 0 e 15.
» **pre-vaule:** especifica o valor precedente do IP para ser correspondido, varia entre 0 e 7.
» **protocol**: especifica o tipo de protocolo.
» **s-port-number:** especifica o número da porta de origem.
» **s-port-mask:** especifica a máscara da porta com 4 números hexadecimais.
» **d-port-number:** especifica o número de destino da porta.
» **d-port-mask:** especifica a máscara da porta de destino com 4 números hexadecimais.
» **tcpflag**: para o protocolo TCP, especifique o valor da FLAG usando números binários ou * (por exemplo, 01 * 010 *). O padrão é *, o que indica que a Flag não será correspondida. As flags são URG (*Urgent flag*), ACK (*acknowledge flag*), PSH (*push flag*), RST (*reset flag*),SYN (*synchronize flag*), and FIN (*finish flag*).
» **time-range-name:** o nome do time-range, por padrão vem desabilitado.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie uma IP ACL 600, e configure a regra 1 para permitir pacotes com o endereço IP de origem 192.168.1.100:

INTELBRAS(config)# access-list create 600

INTELBRAS(config)# access-list ip 600 **rule** 1 **permit logging** disable **sip** 192.168.1.100 **sip-mask** 255.255.255.255

40.5. access-list ipv6

Descrição: o comando **access-list ipv6** é usado para criar uma regra ACL IPv6. Para excluir a mesma utilize o comando **no access-list ipv6**. Uma ACL IPv6 analisa e processa os pacotes de dados baseados em uma série de condições de correspondência, os quais podem ser endereço IP de origem e destino.

Antes de criar uma ACL IPv6 e vinculá-la a uma interface você deve configurar os modelos SDM como *enterpriseV6* e salvar suas configurações.

Sintaxe: **access-list ipv6** *acl-id-or-name* **rule** {auto | *rule-id*} {deny | permit} **logging** {enable | disable} [**class** *class-value*] [**flow-label** *flow-label-value*] [**sip** *source-ip-address* **sip-mask** *source-ip-mask*] [**dip** *destination-ip-address* **dip-mask** *destination-ip-mask*] [**s-port** *source-port-number*] [**d-port** *destination-port-number*] [**tseg** *time-range-name*]
no access-list ipv6 *acl-id-or-name* **rule** *rule-id*

Parâmetros:

- **acl-id-or-name:** especifica o nome ou a ID de uma ACL a qual a regra será adicionada.
- **auto:** a ID da regra será atribuída automaticamente e o intervalo entre as regras será 5.
- **rule-id:** especifica o número de ID da regra.
- **deny | permit:** especifica a ação que será tomada com o pacote que corresponder à essa regra. Por padrão vem configurado como *permit*. Os pacotes serão descartados se *deny* for selecionado e encaminhados caso *permit* for selecionado.
- **enable | disable:** habilita ou desabilita a função de Log para a regra ACL. Se *enable* for selecionado as vezes que a regra for acionada será feito relatório a cada 5 minutos. Com o contador de ACL Trap ativado uma Trap relacionada será gerada se o número de correspondências mudar.
- **class-value:** especifica o valor de classe para ser correspondido, varia entre 0 e 63.
- **flow-label-value:** especifica um valor de Flow Label para ser correspondido.
- **source-ip-address:** especifica o endereço IP de origem, Todos os tipos de endereço IPv6 serão confirmados. Você pode adicionar um endereço IPv6 completo de 128 bits, porém somente os primeiros 64 bits serão válidos.
- **sip-address-mask:** especifica a máscara do endereço IPv6 de origem. É obrigatório se um endereço IPv6 de origem foi apontado. Adicione a máscara em seu formato completo, por exemplo ffff:ffff:0000:ffff. A máscara especificará quais bits do endereço de origem corresponderão à regra.
- **destination-ip-address:** especifica o endereço IP de destino, Todos os tipos de endereço IPv6 serão confirmados. Você pode adicionar um endereço IPv6 completo de 128 bits, porém somente os primeiros 64 bits serão válidos.
- **destination-ip-mask:** especifica a máscara do endereço IPv6 de destino. É obrigatório se um endereço IPv6 de origem foi apontado. Adicione a máscara em seu formato completo, por exemplo ffff:ffff:0000:ffff. A máscara especificará quais bits do endereço de origem corresponderão à regra;
- **source-port-number:** especifica o número da porta de origem do TCP/UDP caso um desses protocolos seja escolhido.
- **destination-port-number:** especifica o número da porta de destino do TCP/UDP caso um desses protocolos seja escolhido.
- **time-range-name:** o nome do time-range, por padrão vem desabilitado.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie uma IPv6 ACL 1600, e configure a regra 1 para bloquear pacotes com o endereço de origem CDCD:910A:2222:5498:8475:1111:3900:2020:

INTELBRAS(config)# access-list create 1600

INTELBRAS(config)# access-list ipv6 1600 **rule** 1 **deny logging** disable **sip**
CDCD:910A:2222:5498:8475:1111:3900:2020 **sip-mask** ffff:ffff:ffff:ffff

40.6. access-list action

Descrição: o comando **access-list action** é usado para especificar uma regra para ser configurada com novas políticas (s-condition, s-mirror, qos-remark) e entrar no modo de Action Configuration. Para deletar as políticas de uma regra utilize o comando **no access-list action**.

Sintaxe: **access-list action** *acl-id-or-name* **rule** *rule-id*
no access-list action *acl-id-or-name* **rule** *rule-id*

Parâmetros:

- **acl-id-or-name:** especifica a ID ou nome da ACL a ser configurada ou excluída.
- **rule-id:** especifica a ID da regra a ser alterada ou excluída.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique a regra 1 da ACL 200 para ter suas regras alteradas:

INTELBRAS(config)# access-list action 200 **rule** 1

40.7. redirect interface

Descrição: o comando **redirect interface** é usado para redirecionar os pacotes que corresponderem a uma regra ACL para uma porta específica. Para desabilitar essa política utilize o comando **no redirect interface**.

Sintaxe: **redirect interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*}
no redirect interface {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*}

Parâmetros:

- **port:** especifica a porta que o pacote será redirecionado. Por padrão são todas.

Modo de comando: Action Configuration.

Requisito de privilégio: Somente usuários do nível admnistrador e operador têm acesso a esses comandos.

Exemplo: defina uma política de redirecionamento para porta 1 os pacotes que corresponderem a ACL 6:

INTELBRAS(config)# access-list action 6 rule 1
INTELBRAS(config-action)# redirect interface gigabitEthernet 1/0/1

40.8. s-condition

Descrição: o comando **s-condition** é usado para limitar a taxa para os pacotes que corresponderem a regra ACL. Para retornar para o valor padrão utilize o comando **no s-condition**.

Sintaxe: **s-condition rate** *rate* **burst** *burst-size* **osd** {none | discard}
no s-condition

Parâmetros:

- **rate:** especifica a taxa, varia entre 0 e 1000000 kbps.
- **burst-size:** especifica o número de bytes permitidos em um segundo variando entre 1 e 128.
- **osd:** especifica a ação a ser tomada para os pacotes cuja a taxa estão além da taxa especificada. Por padrão é configurado como *none* representa nenhuma ação, e *discard* representa que os pacotes serão descartados.

Modo de comando: Action Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a política para a regra 1 da ACL 6 para limitar a transmissão dos pacotes com correspondência para 1000Kbps e se o número de bytes por segundo for maior que 100, os mesmos devem ser descartados:

INTELBRAS(config)# access-list action 6 **rule** 1
INTELBRAS(config-action)# s-condition rate 1000 **burst** 100 **osd** discard

40.9. s-mirror

Descrição: o comando **s-mirror** é usado para definir uma política para espelhar os pacotes que corresponderem a uma ACL para uma porta destino. Para desabilitar essa política utilize o comando **no s-mirror**.

Sintaxe: **s-mirror interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port*}
no s-mirror

Parâmetros:

» **port:** especifica a porta para a qual os pacotes serão espelhados.

Modo de comando: Action Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a política para a regra 1 da ACL 6 para espelhar os pacotes com correspondência para a porta gigabit 1/0/2:

```
INTELBRAS(config)# access-list action 6 rule 1
INTELBRAS(config-action)# s-mirror interface gigabitEthernet 1/0/2
```

40.10. qos-remark

Descrição: o comando **qos-remark** é usado para configurar a função QoS Remark como política de ação. Para restaurar os valores padrões utilize o comando **no qos-remark**.

Dentro deste comando não é possível configurar DSCP e o dot1p ao mesmo tempo.

Sintaxe: **qos-remark** [**dscp** *dscp*] [**priority** *pri*] [**dot1p** *dot1p-pri*]
no qos-remark

Parâmetros:

» **dscp:** DSCP do QoS Remark. Especifica a região DSCP para os dados dos pacotes que corresponderem a ACL, varia entre 0 e 63.

» **pri:** prioridade local do QoS Remark. Especifica a prioridade local para os dados dos pacotes com correspondência no ACL, via entre 0 e 7.

» **dot1p-pri:** prioridade 802.1p do QoS Remark. Esta configuração de Remark irá alterar o campo de prioridade do pacote para a nova prioridade que você determinar aqui. Varia entre 0 e 7.

Modo de comando: Action Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure a política para a regra 1 da ACL 6 para especificar a região do DSCP como 30 para a prioridade local 2 para os pacotes que corresponderem a esta regra:

```
INTELBRAS(config)# access-list action 6 rule 1
INTELBRAS(config-action)# qos-remark dscp 30 priority 2
```

40.11. access bind

Descrição: o comando **access bind** é usado para vincular uma porta à uma regra ACL. Para desabilitar esse vínculo utilize o comando **no access bind**.

Sintaxe: **access bind** *acl-id-or-name* **interface** {[**vlan** *vlan-list*] [**fastEthernet** *port-list*] [**gigabitEthernet** *port-list*] [**ten-gigabitEthernet** *port-list*]}
no access bind *acl-id-or-name* **interface** {[**vlan** *vlan-list*] [**fastEthernet** *port-list*] [**gigabitEthernet** *port-list*] [**ten-gigabitEthernet** *port-list*]}

Parâmetros:

» **acl-id-or-name:** nome ou ID da ACL que será vinculada.

» **vlan-list:** especifica a VLAN ou lista de VLAN à qual será vinculada a ACL, varia entre 1 e 4094.

» **port-list:** especifica a porta ou conjunto de portas para a qual será vinculada a ACL.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: vincule a VLAN 4 e porta 3 para a ACL 1:

```
INTELBRAS(config)# access-list bind 1 interface vlan 4 gigabitEthernet 1/0/3
```

40.12. show access-list

Descrição: o comando **show access-list** é usado para exibir as configurações de ACL.

Sintaxe: **show access-list** *acl-id-or-name*

Parâmetro:

» **acl-id-or-name:** ID ou nome da ACL a qual você quer mostrar as informações.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações da ACL MAC 20:

```
INTELBRAS# show access-list 20
```

40.13. show access-list bind

Descrição: o comando **show access-list bind** é usado para exibir as configurações de vínculo ACL.

Sintaxe: **show access-list bind**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações das políticas de vínculos:

```
INTELBRAS# show access-list bind
```

40.14. show access-list status

Descrição: o comando **show access-list status** é usado para exibir as configurações dos recursos de entrada da ACL.

Sintaxe: **show access-list status**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações da ACL MAC 20:

```
INTELBRAS# show access-list status
```

40.15. show access-list counter

Descrição: o comando **show access-list counter** é usado para exibir a contagem de pacotes que corresponderam a uma regra de uma ACL.

Sintaxe: **show access-list** *acl-id-or-name* **counter**

Parâmetro:

» **acl-id-or-name:** ID ou nome da ACL a qual você quer mostrar as informações.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a contagem de pacotes correspondidos da ACL 20:

```
INTELBRAS# show access-list 20 counter
```

40.16. clear access-list

Descrição: o comando **clear access-list** é usado para limpar a contagem de pacotes de um ACL.

Sintaxe: **clear access-list** *acl-id-or-name* [**rule** *rule-id*]

Parâmetro:

» **acl-id-or-name:** ID ou nome da ACL a qual você quer limpar as informações.

» **rule-id:** ID da regra.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: limpe a contagem de pacotes da ACL 100:

INTELBRAS# clear access-list 100

41. Comandos IPv4 IMPB

Você pode vincular endereço IP, endereço MAC, VLAN e uma porta conectada à um host, este vínculo pode seguir condição de verificação de inspeção de ARP e detecção de origem IP (ip verify source) para filtrar de pacotes.

41.1. ip source binding

Descrição: o comando **ip source binding** é utilizado para criar um vínculo entre endereço IP, endereço MAC, VLAN e número de porta de forma manual. Você pode criar o vínculo manualmente uma vez que você tenha as informações relacionadas dos Host na LAN. Para excluir a entrada de vínculo utilize o comando **no ip source binding**.

Sintaxe: **ip source binding** *hostname ip-addr mac-addr* **vlan** *vlan-id* **interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*} {none | arp-detection | ip-verify-source | both}
no ip source binding *ip-addr*

Parâmetros:

- **hostname:** nome do Host com até 20 caracteres.
- **ip-addr:** endereço IP do Host.
- **mac-addr:** endereço MAC do Host.
- **vlan-id:** ID da VLAN que necessita ser vinculada, variando entre 1 e 4094.
- **port:** número da porta a qual o Host está conectado.
- **none | arp-detection | ip-verify-source | both:** tipo de proteção da entrada; *arp-detection* indica detecção de ARP; *ip-verify-source* indica que haverá filtro na origem IP; *none* indica que nenhuma aplicação será definida; *both* indica a aplicação de ambas.

Modo de comando: Interface Cofiguration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplos:

Crie uma entrada de vínculo entre o IP 192.168.0.1, MAC 00:00:00:00:00:01, VLAN ID 2 e com a porta 5 e por fim habilite a detecção de ARP:

INTELBRAS(config)# ip source binding host1 192.168.0.1 00:00:00:00:00:01 **vlan** 2 **interface gigabitEthernet** 1/0/5 arp-detection

Delete o Vínculo para o IP 192.168.0.1:

INTELBRAS(config-if)# no source binding 192.168.0.1

41.2. ip dhcp snooping

Descrição: o comando **ip dhcp snooping** é usado para habilitar a função de DHCP Snooping de forma global. Para desabilitar essa função utilize o comando **no ip dhcp snooping**. A função DHCP Snooping fica monitorando o processo de obtenção de endereço IP entre um host e um servidor DHCP, registrando as informações de endereço IP, endereço MAC, VLAN e porta, para poder criar uma tabela de vínculo automático.

Sintaxe: **ip dhcp snooping**
no ip dhcp snooping

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função DHCP Snooping de forma global:

INTELBRAS(config)# ip dhcp snooping

41.3. ip dhcp snooping vlan

Descrição: o comando **ip dhcp snooping vlan** é usado para habilitar a função de DHCP Snooping para uma VLAN específica. Para desabilitar essa função utilize o comando **no ip dhcp snooping vlan**.

Sintaxe: **ip dhcp snooping vlan** *vlan-range*
no ip dhcp snooping vlan *vlan-range*

Parâmetro:

» **vlan-range:** especifica as VLANs as quais terão a função DHCP Snooping habilitada, no formato *1-3, 5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função DHCP Snooping de nas VLANs 1, 4, 6 e 7:

INTELBRAS(config)# ip dhcp snooping vlan 1,4,6-7

41.4. ip dhcp snooping max-entries

Descrição: o comando **ip dhcp snooping max-entries** é usado para configurar o número máximo de entradas que podem ser aprendidas em uma porta através do DHCP Snooping. Para retornar para os valores padrões utilize o comando **no ip dhcp snooping max-entries**.

Sintaxe: **ip dhcp snooping max-entries** *value*
no ip dhcp snooping max-entries

Parâmetro:

» **value:** valor máximo de entradas que podem ser aprendidos pela porta através do DHCP Snooping.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure como 100 o número máximo de entradas que podem ser aprendidas pela porta 1:

INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# ip dhcp snooping max-entries 100

41.5. show ip source binding

Descrição: o comando **show ip source binding** é utilizado para mostrar as a tabela de entradas de vínculo IP-MAC-VID-PORT.

Sintaxe: **show ip source binding**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a tabela de entradas de vínculo:

INTELBRAS# show ip source binding

41.6. show ip dhcp snooping

Descrição: o comando **show ip dhcp snooping** é utilizado para mostrar as status de execução do DHCP Snooping.

Sintaxe: **show ip dhcp snooping**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as a informação do DHCP snooping:

INTELBRAS# show ip dhcp snooping

41.7. show ip dhcp snooping interface

Descrição: o comando **show ip dhcp snooping interface** é utilizado para mostrar as informações de configuração do DHCP Snooping de uma determinada porta ou Port Channel.

Sintaxe: **show ip dhcp snooping interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetro:

- **port:** número da porta Ethernet.
- **port-channel-id:** ID da Port Channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Mostre a configuração DHCP Snooping de todas as portas Ethernet:

```
INTELBRAS# show ip dhcp snooping interface
```

Mostre a configuração DHCP Snooping da porta gigabit 5:

```
INTELBRAS# show ip dhcp snooping interface gigabitEthernet 1/0/5
```

42. Comandos IPv6 IMPB

Você pode vincular endereço IPv6, endereço MAC, VLAN e uma porta conectada à um host, este vínculo pode seguir condição de verificação de inspeção de ARP e detecção de origem IP (ip verify source) para filtrar de pacotes.

42.1. ipv6 source binding

Descrição: o comando **ipv6 source binding** é utilizado para criar um vínculo entre endereço IP, endereço MAC, VLAN e número de porta de forma manual. Você pode criar o vínculo manualmente uma vez que você tenha as informações relacionadas dos Host na LAN. Para excluir a entrada de vínculo utilize o comando **no ipv6 source binding**.

Sintaxe: **ipv6 source binding** *hostname ipv6-addr mac-addr* **vlan** *vlan-id* **interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*} {none | nd-detection | ipv6-verify-source | both}
no ip source binding *ipv6-addr*

Parâmetros:

- **hostname:** nome do Host com até 20 caracteres.
- **ipv6-addr:** endereço IPv6 do Host.
- **mac-addr:** endereço MAC do Host.
- **vlan-id:** ID da VLAN que necessita ser vinculada, variando entre 1 e 4094.
- **port:** número da porta a qual o Host está conectado.
- **none | nd-detection | ipv6-verify-source | both:** tipo de proteção da entrada; *nd-detection* indica detecção de ND; *ipv6-verify-source* indica que haverá filtro na origem IPv6; *none* indica que nenhuma aplicação será definida; *both* indica a aplicação de ambas.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie um vínculo de entrada entre 2001:0:9d38:90d5::34, MAC address AA-BB-CC-DD-EE-FF, VLAN ID 10, na porta 1/0/5, e habilitar a ND Detection:

```
INTELBRAS(config)# ipv6 source binding host1 2001:0:9d38:90d5::34 aa:bb:cc:dd:ee:ff vlan 10 interface gigabitEthernet 1/0/5 nd-detection
```

42.2. ipv6 dhcp snooping

Descrição: o comando **ipv6 dhcp snooping** é usado para habilitar a função de DHCPv6 Snooping de forma global. Para desabilitar essa função utilize o comando **no ipv6 dhcp snooping**. A função DHCP Snooping monitora o processo de obtenção de endereço IP dos hosts através do servidor DHCPv6, e grava o endereço IPv6, o endereço MAC, a VLAN e o número da porta do Host para criação de vínculo automática.

Sintaxe: **ipv6 dhcp snooping**
no ipv6 dhcp snooping

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função DHCPv6 Snooping de forma global:

```
INTELBRAS(config)# ipv6 dhcp snooping
```

42.3. ipv6 dhcp snooping vlan

Descrição: o comando **ipv6 dhcp snooping vlan** é usado para habilitar a função de DHCPv6 Snooping para uma VLAN específica. Para desabilitar essa função utilize o comando **no ipv6 dhcp snooping vlan**.

Sintaxe: **ipv6 dhcp snooping vlan** *vlan-range*
no ipv6 dhcp snooping vlan *vlan-range*

Parâmetro:

» **vlan-range:** especifica as VLANs as quais terão a função DHCPv6 Snooping habilitada, no formato *1-3, 5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função DHCPv6 Snooping de nas VLANs 1, 4, 6 e 7:

```
INTELBRAS(config)# ipv6 dhcp snooping vlan 1,4,6-7
```

42.4. ipv6 dhcp snooping max-entries

Descrição: O comando **ipv6 dhcp snooping max-entries** é usado para configurar o número máximo de entradas que podem ser aprendidas em uma porta através do DHCPv6 Snooping. Para retornar para os valores padrões utilize o comando **no ipv6 dhcp snooping max-entries**.

Sintaxe: **ipv6 dhcp snooping max-entries** *value*
no ipv6 dhcp snooping max-entries

Parâmetro:

» **value:** valor máximo de entradas que podem ser aprendidos pela porta através do DHCPv6 Snooping.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure como 100 o número máximo de entradas que podem ser aprendidas pela porta 1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# ipv6 dhcp snooping max-entries 100
```

42.5. ipv6 nd snooping

Descrição: o comando **ipv6 nd snooping** é usado para habilitar a função de ND Snooping de forma global. Para desabilitar essa função utilize o comando **no ipv6 nd snooping**. A função ND Snooping monitora o processo de detecção de endereços duplicados, e grava o endereço IPv6, o endereço MAC, a VLAN e o número da porta do Host para criação automática de vínculo.

Sintaxe: **ipv6 nd snooping**
no ipv6 nd snooping

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função ND Snooping de forma global:

```
INTELBRAS(config)# ipv6 nd snooping
```

42.6. ipv6 nd snooping vlan

Descrição: o comando **ipv6 nd snooping vlan** é usado para habilitar a função de ND Snooping para uma VLAN específica. Para desabilitar essa função utilize o comando **no ipv6 nd snooping vlan**.

Sintaxe: **ipv6 nd snooping vlan** *vlan-range*
no ipv6 nd snooping vlan *vlan-range*

Parâmetro:

» **vlan-range:** especifica as VLANs as quais terão a função ND Snooping habilitada, no formato *1-3, 5*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função ND Snooping de nas VLANs 1, 4, 6 e 7:

```
INTELBRAS(config)# ipv6 dhcp snooping vlan 1,4,6-7
```

42.7. ipv6 nd snooping max-entries

Descrição: o comando **ipv6 nd snooping max-entries** é usado para configurar o número máximo de entradas que podem ser vinculadas a uma porta. Para retornar para os valores padrões utilize o comando **no ipv6 nd snooping max-entries**.

Sintaxe: **ipv6 nd snooping max-entries** *value*
no ipv6 nd snooping max-entries

Parâmetro:

» **value:** valor máximo de entradas que podem ser vinculadas a uma porta.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure como 100 o número máximo vínculos para a porta 1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(config-if)# ipv6 nd snooping max-entries 100
```

42.8. show ipv6 source binding

Descrição: o comando **show ipv6 source binding** é utilizado para mostrar as a tabela de vínculo IPv6-MAC-VID-PORT.

Sintaxe: **show ipv6 source binding**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a tabela de vínculo:

```
INTELBRAS# show ipv6 source binding
```

42.9. show ipv6 dhcp snooping

Descrição: o comando **show ipv6 dhcp snooping** é utilizado para mostrar as status de execução do DHCPv6 Snooping.

Sintaxe: **show ipv6 dhcp snooping**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exibe o status de execução do DHCPv6 Snooping:

INTELBRAS# show ipv6 dhcp snooping

42.10. show ipv6 dhcp snooping interface

Descrição: o comando **show ipv6 dhcp snooping interface** é utilizado para mostrar as informações de configuração do DHCPv6 Snooping de uma determinada porta ou Port Channel.

Sintaxe: **show ipv6 dhcp snooping interface** [**gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta Ethernet.
- **port-channel-id:** ID da Port Channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Mostre a configuração DHCPv6 Snooping de todas as portas Ethernet:

INTELBRAS# show ipv6 dhcp snooping interface

Mostre a configuração DHCPv6 Snooping da porta gigabit 5:

INTELBRAS# show ipv6 dhcp snooping interface gigabitEthernet 1/0/5

42.11. show ipv6 nd snooping

Descrição: o comando **show ipv6 nd snooping** é utilizado para mostrar as status de execução do ND Snooping.

Sintaxe: **show ipv6 nd snooping**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o status do ND snooping:

INTELBRAS# show ipv6 nd snooping

43. Comandos IP Verify Source

A verificação do IP de origem é um filtro baseado nos endereços IP das entradas de vínculo IP-MAC. Somente pacotes com correspondência do respectivo vínculo ativo podem ser processados, os quais melhoram o uso da largura de banda.

43.1. ip verify source

Descrição: o comando **ip verify source** é utilizado para configurar o IP Verify Source (verificação do IP de origem) para uma determinada porta. Para desabilitar essa função utilize o comando **no ip verify source**.

Sintaxe: **ip verify source** {sip+mac | sip}
no ip verify source

Parâmetro:

- **sip+mac:** tipo de segurança, *sip+mac* indica que somente os pacotes com correspondência com endereço IP de origem, endereço MAC de origem e número de porta no vínculo IP-MAC podem ser processados.
- **sip:** tipo de segurança. *sip* indica que somente os pacotes com correspondência com endereço IP de origem e número da porta serão processados.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a verificação de endereço IP de origem para a portas 5 à 10. Configure que somente os pacotes com correspondência entre endereço IP, endereço MAC e número de porta serão processados:

INTELBRAS(config)# interface range gigabitEthernet 1/0/5-10
INTELBRAS(config-if-range)# ip verify source sip+mac

43.2. ip verify source logging

Descrição: o comando **ip verify source logging** é utilizado para habilitar a função de geração de log. Com essa função habilitada, o switch irá gerar registro de log quando pacotes *ilegais* forem recebidos. Para desabilitar essa função utilize o comando **no ip verify source logging**.

Sintaxe: **ip verify source logging**
no ip verify source logging

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de registro para fazer que o switch gere logs quando receber pacotes ilegais:

INTELBRAS(config)# ip verify source logging

43.3. show ip verify source logging

Descrição: o comando **show ip verify source logging** é usado para exibir as configurações do IP Verify Source.

Sintaxe: **show ip verify source logging**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações do IP Verify Source.

INTELBRAS# show ip verify source logging

43.4. show ip verify source logging interface

Descrição: o comando **show ip verify source logging interface** é usado para exibir as configurações de IP Verify Source de uma porta específica.

Sintaxe: **show ip verify source logging interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta Ethernet.
- **port-channel-id:** ID do Port Channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações IP Verify Source da porta gigabit 5:

INTELBRAS# show ip verify source logging interface gigabitEthernet 1/0/5

44. Comandos IPv6 Verify Source

O IPv6 Verify Source é uma ferramenta para filtrar os pacotes IPv6 com base nas entradas do vínculo IPv6-MAC. Apenas os pacotes marcados com as regras vinculadas IPv6-MAC podem ser processados, o que pode aumentar a utilidade da largura de banda.

Antes de configurar o IPv6 Verify Source feature, você deve configurar o template SDM como *enterpriseV6* e salvar as configurações.

44.1. ipv6 verify source

Descrição: o comando **ipv6 verify source** é usado para configurar o IPv6 Verify Source mode para uma porta especificada. Para desativar o IPv6 Verify Source, utilize o comando **no ipv6 verify source**.

Sintaxe: **ipv6 verify source** {sipv6+mac | sipv6}
no ipv6 verify source

Parâmetros:

» **sipv6+mac:** tipo de segurança. *sipv6+mac* indica que somente os pacotes com o seu endereço IPV6 de origem, MAC de origem, e número da porta correspondentes com a regra IPv6-MAC podem ser processados.

» **sipv6:** tipo de segurança. "sipv6" indica que somente os pacotes com seu endereço de origem IPv6 e o número da porta associados com as regras vinculada IPv6-MAC podem ser processados.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função IPv6 Verify Source nas portas Gigabit Ethernet 5-10. Configurar para que apenas os pacotes com o seu endereço de origem IPv6, MAC de origem e número de porta vinculados às regras associada ao IPv6-MAC sejam processados:

```
INTELBRAS(config)# interface range gigabitEthernet 1/0/5-10
INTELBRAS(config-if-range)# ipv6 verify source sipv6+mac
```

44.2. show ipv6 verify source

Descrição: o comando **show ipv6 verify source** é usado para exibir as informações de configuração do IPv6 Verify Source.

Sintaxe: **show ipv6 verify source**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações de configuração do IPv6 Verify Source:

```
INTELBRAS(config)# show ipv6 verify source
```

44.3. show ipv6 verify source interface

Descrição: o comando **show ipv6 verify source interface** é usado para exibir as configurações do IPv6 verify source de uma porta Gigabit Ethernet desejada.

Sintaxe: **show ipv6 verify source interface gigabitEthernet** *port*

Parâmetros:

» **port:** o número da porta Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as configurações IPv6 verify source da porta Gigabit Ethernet 1/0/5:

```
INTELBRAS# show ipv6 verify source interface gigabitEthernet 1/0/5
```

45. Comandos de filtro DHCPv4

O DHCPv4 Filter é uma ferramenta permite ao usuário não só restringir todos os pacotes DHCP Server, mas também receber qualquer pacote servidor DHCP configurado por qualquer cliente DHCP especificado, ele é útil quando um ou mais servidores DHCP estão presentes na rede, e ambos fornecem serviços DHCP a diferentes grupos com clientes distintos.

45.1. ip dhcp filter

Descrição: o comando **ip dhcp filter** é usado para habilitar a função de filtro de DHCP globalmente. Para desabilitar a função de DHCP Filter globalmente, utilize o comando **no ip dhcp filter.**

Sintaxe: **ip dhcp filter**
no ip dhcp filter

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative a função de DHCP Filter globalmente:

```
INTELBRAS(config)# ip dhcp filter
```

45.2. ip dhcp filter (interface)

Descrição: o comando **ip dhcp filter (interface)** é usado para ativar a função de filtro de DHCP em uma porta especificada. Para desabilitar a função DHCP Filter na porta, utilize o comando **no ip dhcp filter (interface)**.

Sintaxe: **ip dhcp filter**
no ip dhcp filter

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o DHCP Filter na porta 1/0/1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(Config-if)# ip dhcp filter
```

45.3. ip dhcp filter mac-verify

Descrição: o comando **ip dhcp filter mac-verify** é usado para permitir que a função MAC Verify seja habilitada. Para desativar o recurso MAC Verify use o comando **no ip dhcp filter mac-verify**. Existem dois campos no pacote DHCP contendo o endereço MAC do hospedeiro. O recurso MAC Verify é usado para comparar os dois campos, e descartar o pacote se os dois campos forem diferentes.

Sintaxe: **ip dhcp filter mac-verify**
no ip dhcp filter mac-verify

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o recurso MAC Verify na porta Gigabit Ethernet 10/2:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/2
INTELBRAS(config-if)# ip dhcp filter mac-verify
```

45.4. ip dhcp filter limit rate

Descrição: o comando **ip dhcp filter limit rate** é usado para ativar o controle de fluxo para os pacotes DHCP. Os pacotes DHCP excessivos serão descartados. Para restaurar a configuração padrão, utilize o comando **no ip dhcp filter limit rate**.

Sintaxe: **ip dhcp filter limit rate** *value*
no ip dhcp filter limit rate

Parâmetro:

» **value:** o valor do controle de fluxo. As opções podem ser 5/10/15/20/25/30 (pacotes / segundo). O valor padrão é *0*, que significa *desativado*.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: defina o controle de fluxo da porta GigabitEthernet 2 como 20 pps:

INTELBRAS (config)#interface gigabitEthernet *1/0/2*
INTELBRAS (config-if)#ip dhcp filter limit rate *20*

45.5. ip dhcp filter decline rate

Descrição: o comando **ip dhcp filter decline rate** é usado para ativar o recurso Decline Protect, e configurar uma taxa limite dos pacotes DHCP Decline. Os pacotes DHCP Decline excessivos serão descartados. Para desativar o recurso Decline Protect, utilize o comando **no ip dhcp filter decline rate**.

Sintaxe: **ip dhcp filter decline rate** *value*
no ip dhcp filter decline rate

Parâmetro:

» **value:** define o limite da taxa de pacotes do DHCP, e os valores opcionais podem ser 0, 5, 10, 15, 20, 25 e 30 (unidades: pacote / segundo). O valor padrão é *0*, que significa *desativado*.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o limite da taxa de pacotes DHCP como 20 pacotes por segundo na porta Gigabit Ethernet 1/0/2:

INTELBRAS(config)#interface gigabitEthernet *1/0/2*
INTELBRAS(config-if)#ip dhcp filter decline *20*

45.6. ip dhcp filter server permit-entry

Descrição: o comando **ip dhcp filter server permit-entry** é usado para adicionar um servidor DHCP confiável. Para restaurar o padrão de fábrica, utilize o comando **no ip dhcp filter server permit-entry server-ip**.

Sintaxe: **ip dhcp filter server permit-entry server-ip** *ipAddr* **client-mac** *macAddr* **interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **interface port-channel** *port-channel-id*}
no ip dhcp filter server permit-entry server-ip *ipAddr* **client-mac** macAddr **interface** {**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **interface port-channel** *port-channel-id*}

Parâmetros:

» **ipAddr:** define o endereço IP do servidor DHCPv4 confiável.
» **macAddr:** define o endereço MAC do cliente DHCP. O valor *all* significa todos os endereços MAC do cliente.
» **port-list | port-channel-id:** define a porta que o servidor DHCPv4 confiável está conectado.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie um filtro para o servidor DHCPv4 confiável cujo o endereço de IP é 192.168.0.100, e o número da porta conectado é 1/0/1, sem um endereço MAC restrito:

INTELBRAS(config)# ip dhcp filter server permit-entry server-ip 192.168.0.100 **client-mac all interface gigabitEthernet** *1/0/1*

45.7. show ip dhcp filter

Descrição: o comando **show ip dhcp filter** é usado para exibir as configurações do filtro de DHCP.

Sintaxe: **show ip dhcp filter**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as configurações do filtro DHCP:

INTELBRAS# show ip dhcp filter

45.8. show ip dhcp filter interface

Descrição: o comando **show ip dhcp filter interface** é usado para exibir as configurações do dhcp filter nas portas.

Sintaxe: **show ip dhcp filter interface** [**fastEtherne**t port | **gigabitEthernet** port | **ten-gigabitEthernet** port | **port-channel** port-channel-id]

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: Não há.

Exemplo: exiba as configurações do dhcp filter na porta 1/0/3:

```
INTELBRAS# show ip dhcp filter interface gigabitEthernet 1/0/3
```

45.9. show ip dhcp filter server permit-entry

Descrição: o comando **show ip dhcp filter server permit-entry** é usado para exibir a configuração do servidor confiável.

Sintaxe: **show ip dhcp filter server permit-entry**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as configurações do DHCP server confiável:

```
INTELBRAS# show ip dhcp filter server permit-entry
```

46. Comandos de filtro DHCPv6

A função DHCPv6 Filter permite que o usuário possa não só restringir todos os pacotes DHCPv6 server, mas também possa receber quaisquer pacotes de DHCPv6 server especificados por qualquer DHCPv6 client especificado. Esta função é útil quando um ou mais servidores DHCPv6 estão presentes na rede, e ambos fornecem serviços DHCPv6 para diferentes grupos de clientes distintos.

46.1. ipv6 dhcp filter

Descrição: o comando **ipv6 dhcp filter** é usado para habilitar a função DHCP Filter globalmente. Para desabilitar a função de DHCPv6 Filter globalmente, utilize o comando **no ipv6 dhcp filter**.

Sintaxe: **Ipv6 dhcp filter**
no ipv6 dhcp filter

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a função DHCPv6 Filter globalmente:

```
INTELBRAS(config)# ipv6 dhcp filter
```

46.2. ipv6 dhcp filter (interface)

Descrição: o comando **ipv6 dhcp filter (interface)** é usado para ativar a função DHCPv6 Filter em uma porta especifica. Para desabilitar a função DHCPv6v Filter nesta porta, utilize o comando **no ipv6 dhcp filter (interface)**.

Sintaxe: **ipv6 dhcp filter**
no ipv6 dhcp filter

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o DHCPv6 Filter na porta 1/0/1:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/1
INTELBRAS(Config-if)# ipv6 dhcp filter
```

46.3. ipv6 dhcp filter limit rate

Descrição: o comando **ipv6 dhcp filter limit rate** é usado para ativar o controle de fluxo nos pacotes DHCPv6. Os pacotes DHCPv6 excedentes serão descartados. Para restaurar a configuração padrão, utilize o comando **no ipv6 dhcp filter limit rate**.

Sintaxe: **Ipv6 dhcp filter limit rate** value
no ipv6 dhcp filter limit rate

Parâmetro:

» **value:** é o valor do controle de fluxo. As opções podem ser 5/10/15/20/25/30 (pacotes / segundo). O valor padrão é *0*, que significa *desativado*.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: defina o controle de fluxo da porta GigabitEthernet 2 como 20 pps:

INTELBRAS(config)#interface gigabitEthernet 1/0/2
INTELBRAS(config-if)#ipv6 dhcp filter limit rate 20

46.4. ipv6 dhcp filter decline rate

Descrição: o comando **ipv6 dhcp filter decline rate** é usado para ativar o recurso Decline Protect, e configurar a taxa limite dos pacotes DHCP Decline. Os pacotes DHCPv6 Decline excedentes serão descartados. Para desativar o recurso Decline Protect, utilize o comando **no ipv6 dhcp filter decline rate**.

Sintaxe: **Ipv6 dhcp filter decline rate** *value*
no ipv6 dhcp filter decline rate

Parâmetro:

» **value:** define o limite da taxa de pacotes Decline packets, e os valores opcionais são 0, 5, 10, 15, 20, 25 e 30 (unidades: pacote / segundo). O valor padrão é *0*, que significa *desativado*.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet / interface port-channel / interface range port-channel).

Requisito de privilégio: somente usuários do nível administrador e usuário avançado têm acesso a esses comandos.

Exemplo: configure o limite da taxa de pacotes DHCPv6 Decline como 20 pacotes por segundo na porta Gigabit Ethernet 1/0/2:

INTELBRAS(config)#interface gigabitEthernet 1/0/2
INTELBRAS(config-if)#ipv6 dhcp filter decline 20

46.5. ipv6 dhcp filter server permit-entry

Descrição: o comando **ipv6 dhcp filter server permit-entry** é usado para adicionar um DHCPv6 server confiável. Para restaurar a opção padrão, utilize o comando **no ipv6 dhcp filter server permit-entry server-ip**.

Sintaxe: **Ipv6 dhcp filter server permit-entry server-ip** *ipAddr* **interface** {**fastEthernet** port | **gigabitEthernet** port | **ten-gigabitEthernet** port | **interface port-channel** *port-channel-id*}
no ipv6 dhcp filter server permit-entry server-ip *ipAddr* **interface** {**fastEthernet** port | **gigabitEthernet** port | **ten-gigabitEthernet** port | **interface port-channel** *port-channel-id*}

Parâmetros:

» **ipAddr:** define o endereço IPv6 do DHCPv6 server confiável.
» **port-list | port-channel-id:** define a porta que o DHCPv6 server confiável está conectado.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie um filtro do DHCPv6 server confiável, cujo endereço de IPv6 é 2003::1 e o número da porta conectada é 1/0/1:

INTELBRAS(config)#ipv6 dhcp filter server permit-entry server-ip 2003::1 **interface gigabitEthernet** 1/0/1

46.6. show ipv6 dhcp filter

Descrição: o comando **show ipv6 dhcp filter** é usado para exibir as configurações do DHCPv6 Filter.

Sintaxe: **show ipv6 dhcp filter**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as configurações DHCPv6 Filter:

```
INTELBRAS# show ipv6 dhcp filter
```

46.7. show ipv6 dhcp filter interface

Descrição: o comando **show ipv6 dhcp filter interface** é utilizado para exibir as configurações do DHCPv6 Filter nas portas.

Sintaxe: **show ipv6 dhcp filter interface** [**fastEthernet** port | **gigabitEthernet** port | **ten-gigabitEthernet** port | **port-channel** port-channel-id]

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e usuário avançado têm acesso a esses comandos.

Exemplo: exiba as configurações DHCPv6 Filter na porta 1/0/3:

```
INTELBRAS# show ipv6 dhcp filter interface gigabitEthernet 1/0/3
```

46.8. show ip dhcp filter server permit-entry

Descrição: o comando **show ipv6 dhcp filter server permit-entry** é usado para exibir as configurações do servidor DHCPv6 confiável.

Sintaxe: **show ipv6 dhcp filter server permit-entry**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as configurações do DHCPv6 server confiável:

```
INTELBRAS# show ipv6 dhcp filter server permit-entry
```

47. Comandos DoS Defend

O DoS (*Denial of Service*) Attack ocupa a largura de banda da rede de forma maliciosa pelos atacantes de rede, ou programas maliciosos, com envio de uma grande quantidade de solicitações de serviços para o host. Com o DoS Defend habilitado, o switch pode analisar o campo específico dos pacotes recebidos, e fornecer medidas de defesa para assegurar o funcionamento normal da rede local.

47.1. ip dos-prevent

Descrição: o comando **ip dos-prevent** é usado para permitir que o DoS defend seja habilitado globalmente. Para desativar o DoS defend de defender use o comando **no ip dos-prevent**.

Sintaxe: **ip dos-prevent**
no ip dos-prevent

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o DoS defend globalmente:

```
INTELBRAS(config)# ip dos-prevent
```

47.2. ip dos-prevent type

Descrição: o comando **ip dos-prevent type** é usado para selecionar o tipo do **ip dos-prevent**. Para desativar o tipo correspondente do ip dos-prevent utilize o comando **no ip dos-prevent type**.

Sintaxe: **ip dos-prevent type** {land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf}
no ip dos-prevent type {land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf}

Parâmetros:

- **Land:** o atacante envia um pacote TCP falso com a flag SYN habilitada para um host de destino. Uma vez que este pacote possua os campos endereço IP de origem e destino configurados de acordo com o endereço IP do host atacado, este host ficará preso em um loop infinito, afetando drasticamente o desempenho da rede.
- **scan-synfin:** o atacante envia um pacote TCP com as flags SYN e FIN habilitadas. A flag SYN é utilizada para iniciar uma nova conexão, enquanto a flag FIN é utilizada para solicitar uma desconexão. Portanto o pacote deste tipo é falso. O switch pode se defender desse tipo de pacote.
- **xma-scan:** o atacante envia o pacote TCP com as seguintes flags habilitadas: FIN, URG e PSH.
- **null-scan:** o atacante envia o pacote TCP com todas as flags de controle como 0. Durante a conexão e a transmissão de dados, os pacotes com todos os controles definidos como 0 serão considerados pacotes ilegais.
- **port-less-1024:** o atacante envia o pacote falso com o campo *TCP SYN* definido para 1 e porta de origem menor do que 1024.
- **blat:** o atacante envia um pacote TCP falso com os campos de porta de origem e destino configurados com o mesmo valor, e com a flag URG habilitada para um host de destino. Semelhante ao Land Attack, o desempenho do host atacado cairá drasticamente, uma vez que o host sempre tentará iniciar uma nova conexão com o atacante.
- **ping-flood:** o atacante inunda o sistema destino com pacotes Ping, criando uma tempestade de broadcast que torna impossível para o sistema para responder à comunicação confiável.
- **syn-flood:** o atacante usa um endereço IP falso para enviar solicitações de pacotes TCP para o servidor. Ao receber os pacotes de solicitação, o servidor irá responder com pacotes SYN-ACK. Já que o endereço IP é falso, nenhuma resposta será devolvida. O servidor irá continuar a enviar pacotes SYN-ACK. Se o atacante enviar um overflowing de pacotes de pedidos falsos, o recurso de rede será ocupado de forma maliciosa, e as requisições dos clientes confiáveis serão negadas.
- **win-nuke:** como o Sistema Operacional com erros não pode processar corretamente o URG (*Urgent Pointer*) dos pacotes TCP, o atacante envia esse tipo de pacotes para a porta 139 TCP (NetBIOS) do host com os erros do sistema operacional, o que fará com que o host fique com uma tela azul.
- **ping-of-death:** o Ping da Morte significa que o atacante envia pacotes de ping anormais, sendo maiores do que 65.535 bytes para causar falha do sistema no computador de destino.
- **smurf:** o Ataque Smurf é um ataque de negação de serviço distribuído em que um grande número de pacotes ICMP (*Internet Control Message Protocol*) com o IP de origem falso da vítima são transmitidos para uma rede de computadores usando um endereço de broadcast. A maioria dos dispositivos em uma rede, por padrão, vão responder a solicitação enviando uma resposta para o endereço IP de origem. Se o número de máquinas na rede que receber e responder a esses pacotes for muito grande, o computador da vítima será inundado com o tráfego.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: ative o DoS Defend para previnir um Land attack:

```
INTELBRAS(config)# ip dos-prevent type land
```

47.3. show ip dos-prevent

Descrição: O comando **show ip dos-prevent** é usado para exibir as informações DoS do detected DoS attack, incluindo ativar ou desativar o status, o DoS Defend Type, a contagem de ataques, etc.

Sintaxe: **show ip dos-prevent**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: exiba as informações DoS dos ataques DoS attack globalmente:

```
INTELBRAS(config)# show ip dos-prevent
```

48. Comandos DLDP

DLCP (*Device Link Detection Protocol*) é utilizado para monitorar o estado do link de fibra óptica ou de cabo Ethernet de par trançado. Quando um link unidirecional é detectado, a porta correspondente irá se desativar automaticamente ou manualmente dependendo do modo de configuração.

48.1. dldp (global)

Descrição: o comando **dldp** é utilizado para habilitar a função de DLDP globalmente. Para desabilitar a função utilize o comando **no dldp**.

Sintaxe: **dldp**
no dldp

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de DLDP de forma global:

```
INTELBRAS(config)# dldp
```

48.2. dldp interval

Descrição: o comando **dldp interval** é utilizado para definir o intervalo de pacotes de advertisement nas portas que estão no estado de advertisement.

Sintaxe: **dldp interval** *interval-time*

Parâmetros:

» **Interval-time:** intervalo para envio de pacotes advertisement. Varia entre 1 e 30 segundos, por padrão vem configurado como *5 segundos*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique o intervalo para envio dos pacotes de advertisement como 10 segundos:

```
INTELBRAS(config)# dldp interval 10
```

48.3. dldp shut-mode

Descrição: o comando **dldp shut-mode** é utilizado para configurar o modo de shutdown quando a link unidirecional é detectado.

Sintaxe: **dldp shut-mode** {auto | manual}

Parâmetros:

» **auto:** o switch irá desativar a porta automaticamente quando um link unidirecional for detectado. Por padrão vem configurado nesse modo.

» **manual:** o switch exibirá um alerta quando um link unidirecional for detectado. A operação para desativar a porta com o link unidirecional é realizada pelo usuário.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: configure o shut-mode como manual:

```
INTELBRAS(config)# dldp shut-mode manual
```

48.4. dldp (interface)

Descrição: o comando **dldp** é utilizado para habilitar a função de DLDP para uma porta específica. Para desabilitar a função utilize o comando **no dldp**.

Sintaxe: **dldp**
no dldp

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a função do DLDP para as portas 2, 3 e 4:

```
INTELBRAS(config)# interface range gigabitEthernet 1/0/2-4
INTELBRAS(config-if-range)# dldp
```

48.5. show dldp

Descrição: o comando **show dldp** é utilizado para mostrar a configuração global, estado, intervalo e modo de shutdown do DLDP.

Sintaxe: **show dldp**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações globais da função DLDP:

```
INTELBRAS# show dldp
```

48.6. show dldp interface

Descrição: o comando **show dldp interface** é utilizado para mostrar a configuração e estado de uma determinada porta. Por padrão a configuração e estado de todas as portas é exibida.

Sintaxe: **show dldp interface** [**gigabitEthernet** *port*]

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração e o estado de todas as portas:

```
INTELBRAS# show dldp interface
```

Exemplo: mostre a configuração e o estado da porta 5:

```
INTELBRAS# show dldp interface gigabitEthernet 1/0/5
```

49. Comandos SNMP

As funções do SNMP (*Simple Network Management Protocolo*) são utilizadas para gerenciar os dispositivos de rede, a qual pode facilitar o monitoramento dos nós de rede pelos administradores e também facilitar a implementação de operações.

49.1. snmp-server

Descrição: o comando **snmp-server** é utilizado para habilitar a função de SNMP. Por padrão a mesma vem desabilitada. Para desabilitar a função utilize o comando **no snmp-server**.

Sintaxe: **snmp-server**
no snmp-server

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a função de SNMP:

```
INTELBRAS(config)# snmp-server
```

49.2. snmp-server view

Descrição: o comando **snmp-server view** é utilizado para adicionar uma view. Para excluir essa view utilize o comando **no snmp-server view**. O OID (identificador de objetos) dos pacotes SNMP é utilizado para descrever o objeto gerenciado do switch, e a MIB (Management Information Base) é o que determina os OID. O SNMP View é criado para a estação de gerenciamento para gerenciar os objetos MIB.

Sintaxe: **snmp-server view** *name mib-oid* {include | exclude}
no snmp-server view *name mib-oid*

Parâmetros:

- **name:** nome da visualização com até 16 caracteres. Cada view inclui várias entradas com o mesmo nome.
- **mib-oid:** ID do objeto MIB. É o identificador de objeto para a entrada da view (OID) com até 61 caracteres.
- **include | exclude:** tipo da visualização, com as opções para incluir ou excluir. Elas representam se a view pode ou não ser gerenciada através da estação de gerenciamento SNMP individualmente.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: adicione uma view chamada view1 configurada a OID como 1.3.6.1.6.3.20 e apontando que esse OID pode ser gerenciado pela estação de gerenciamento SNMP:

INTELBRAS(config)# snmp-server view view1 1.3.6.1.6.3.20 include

49.3. snmp-server group

Descrição: o comando **snmp-server group** é utilizado para configurar e gerenciar um grupo SNMP. Para excluir um grupo SNMP utilize o comando **no snmp-server group**. O SNMPv3 provê o VACM (*View-based Access Control Model*) e USM (*User-Based Security Modell*) como mecanismos de autenticação. O usuário no grupo SNMP pode gerenciar o dispositivo através do Read View, Write View e Notify View. O modo de autenticação e modo de privacidade garantem alta segurança para a comunicação entre a estação de gerenciamento e o dispositivo gerenciado.

Sintaxe: **snmp-server group** *name* [**smode** v3] [**slev** {noAuthNoPriv | authNoPriv | authPriv}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*]
no snmp-server group *name* **smode** v3 **slev** {noAuthNoPriv | authNoPriv |authPriv}

Parâmetros:

- **name:** nome para o grupo SNMP com até 16 caracteres. O nome do grupo, modelo de segurança e o nível de segurança compõem a identificação do grupo SNMP. Esses três itens deverão ser iguais para os usuários em um grupo.
- **v3:** modelo de segurança do grupo, 3 indica SNMPv3, mais alto nível de segurança.
- **slev:** nível de segurança para o grupo SNMPv3. São 3 as opções, noAuthNoPriv representa sem autorização e criptografia, authNoPriv representa autorização e sem criptografia e para authPriv representa autorização e criptografia. Por padrão o nível de segurança é *noAuthNoPriv*. Não há necessidade de configurar esse nível de segurança para o SNMPv1 e para o SNMPv2.
- **read-view:** seleciona uma View para ser do tipo Read View. Ou seja, o acesso de gerência é restrito à somente leitura para a View atribuída.
- **write-view:** seleciona uma View para ser do tipo Write View. Ou seja, o acesso de gerência é somente escrita, as alterações podem ser feitas para a View atribuída. As Views definidas como ambas Read View e Write View podem visualizar e modificar.
- **notify-view:** seleciona uma View para ser do tipo Notify View. Ou seja, configura para que a estação de gerenciamento receba mensagens de notificação da View atribuída geradas pelo agente SNMP do switch.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplos:

Adicione um grupo SNMP e configure o nome do mesmo como grupo1 com modelo de segurança SNMPv3, nível de segurança authNoPriv e configure o acesso de gerência para que a view permita a escrita e leitura para a viewDefault além de indicar que as mensagens de notificação enviadas podem ser recebidas pela viewDefault:

INTELBRAS(config)# snmp-server group grupo1 **smode** v3 **slev** authNoPriv **read** viewDefault **write** viewDefault **notify** viewDefault

Delete o grupo1:

INTELBRAS(config)# snmp-server group grupo1 **smode** v3 **slev** authNoPriv

49.4. snmp-server user

Descrição: o comando **snmp-server user** é utilizado para adicionar um usuário. Para excluir um usuário utilize o comando **no snmp-server user**. O usuário em um grupo SNMP pode gerenciar o switch através do software de estação de gerenciamento. O usuário e seu grupo tem o mesmo nível de segurança e permissão de acesso.

Sintaxe: **snmp-server user** *name* {local | remote} *group-name* [**smode** v3] [**slev** {noAuthNoPriv | authNoPriv | authPriv}] [**cmode** {none | MD5 | SHA}] [**cpwd** *configm-pwd*] [**emode** {none | DES}] [**epwd** *encrypt-pwd*]
no snmp-server user name

Parâmetros:

- **name:** nome do usuário com até 16 caracteres.
- **local | remote:** tipo do usuário, indica se o usuário estará conectado com SNMP engine local ou remota. Assim como a Engine ID remota e a senha do usuário são utilizadas para computar a autenticação e privacidade, antes de configurar um usuário remoto você precisa indicar uma Engine ID remota primeiro.
- **group-name:** nome do grupo do usuário. O usuário é classificado para um grupo correspondente de acordo com o nome do grupo, modo de segurança e nível de segurança.
- **v3:** modo de segurança para o usuário, v3 indica SNMPv3.
- **slev:** nível de segurança para o grupo SNMPv3. São 3 as opções, noAuthNoPriv representa sem autorização e criptografia, authNoPriv representa autorização e sem criptografia e para authPriv representa autorização e criptografia. Por padrão o nível de segurança é *noAuthNoPriv*. Não há necessidade de configurar esse nível de segurança para o SNMPv1 e para o SNMPv2.
- **cmode:** modo de autenticação para o usuário SNMPv3. "none" indica que nenhum método de autenticação será utilizado, "MD5" indica que a autenticação da porta é realizada através do algoritmo HMAC_MD5 e "SHA" indica que a autenticação da porta é realizada através do SHA (Secure Hash Algorithm). Autenticação SHA possui um nível de segurança maior que MD5. Por padrão o modo de autenticação é definido como *none*.
- **confirm-pwd:** senha para autenticação com até 16 caracteres. Não são permitidos porto de interrogação e espaços. Esta senha aparecerá na forma de criptografia simétrica no arquivo de configuração.
- **emode:** modo de privacidade do usuário SNMPv3. "none" indica que nenhum modo de privacidade será usado, "DES" indica que o método de criptografia DES será utilizado. Por padrão o modo de privacidade é definido como *none*.
- **encrypt-pwd:** senha de privacidade com até 16 caracteres. Não são permitidos poto de interrogação e espaços. Esta senha aparecerá na forma de criptografia simétrica no arquivo de configuração.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: adicione um usuário local administrador do grupo2, configure seu modelo de segurança como SNMPv3, com o nível de segurança do grupo como authPriv, modo de autenticação MD5, senha de autenticação 11111, modo de privacidade DES e senha de privacidade 22222:

INTELBRAS(config)# snmp-server user administrador local group2 **smode** v3 **slev** authPriv **cmode** MD5 **cpwd** 11111 **emode** DES **epwd** 22222

49.5. snmp-server community

Descrição: o comando **snmp-server community** é utilizado para adicionar uma comunidade. Para excluir uma comunidade utilize o comando **no snmp-server community.** SNMP versão 1 e 2 adotam autenticação por nome de comunidade. O nome da comunidade pode limitar o acesso ao agente SNMP através da estação de gerenciamento da rede SNMP funcionando como senha.

Sintaxe: **snmp-server community** *name* {read-only | read-write} *mib-view*
no snmp-server community name

Parâmetros:

- **name:** nome do usuário com até 16 caracteres.
- **read-only | read-write:** direito de acesso da comunidade, com as opções de somente leitura e leitura e escrita.

» **mib-view:** MIB View para o acesso da comunidade.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: adicione a comunidade public com permissão de leitura e escrita para a view viewDefault:

INTELBRAS(config)# snmp-server community public read-write viewDefault

49.6. snmp-server host

Descrição: o comando **snmp-server host** é utilizado para adicionar uma notificação. Para excluir uma notificação utilize o comando **no snmp-server host**.

Sintaxe: **snmp-server host** *ip udp-port user-name* [**smode** {v1 | v2 | v3}] [**slev** {noAuthNoPriv | authNoPriv | authPriv}] [**type** {trap | inform}] [**retries** *retires*] [**timeout** *timeout*]
no snmp-server host name

Parâmetros:

» **ip:** endereço IP do Host de gerenciamento, suporta tanto IPv4 como IPv6.

» **udp-port:** porta UDP, a qual é utilizada para enviar as notificações. Varia entre 1 e 65535.

» **user-name:** nome de usuário da estação de gerenciamento.

» **smode:** modelo de segurança da estação de gerenciamento. Pode ser v1, v2 e v3 que representam respectivamente as versões SMNP. Por padrão vem definida como *v1*.

» **slev:** nível de segurança para o grupo SNMPv3. São 3 as opções, noAuthNoPriv representa sem autorização e criptografia, authNoPriv representa autorização e sem criptografia e para authPriv representa autorização e criptografia. Por padrão o nível de segurança é *noAuthNoPriv.*

» **type:** indica o tipo das notificações. *trap* indica que armadilhas serão enviadas enquanto *inform* indica que informações serão enviadas. O tipo *inform* possui nível de segurança maior que o tipo *trap* e as opções retries e timeout precisam ser configuradas para essa opção. Para o SNMPv1 só é possível selecionar a opção *trap*. Por padrão o tipo das notificações é *trap.*

» **retries:** a quantidade de vezes que o switch tenta enviar uma solicitação de *inform*, varia entre 1 e 255. O switch irá reenviar a solicitação de *infrom* se não obtiver resposta da estação de gerenciamento durante o intervalo de Timeout, e irá encerrar as tentativas de reenvio se o número de vezes alcançar a quantidade especificada aqui.

» **timeout:** tempo máximo que o switch pode aguardar por uma resposta da estação de gerenciamento antes de reenviar as solicitações, varia entre 1 e 3600 segundos.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplos:

Adicione uma notificação e configure o endereço IP do host de gerenciamento como 192.168.0.146, na porta UDP 162, nome de usuário da estação de gerenciamento como admin, modelo de segurança da estação v2, tipo de notificações como "inform", o tempo máximo de espera como 1000 segundos e máximo número de reenvio como 100:

INTELBRAS(config)# snmp-server host 192.168.0.146 162 admin **smode** v2 **type** inform **retries** 100 **timeout** 1000

Adicione uma notificação e configure o endereço IP do host de gerenciamento como fe80::1234, na porta UDP 162, nome de usuário da estação de gerenciamento como admin, modelo de segurança da estação v2, tipo de notificações como "inform", o tempo máximo de espera como 1000 segundos e máximo número de reenvio como 100:

INTELBRAS(config)# snmp-server host fe80::1234 admin **smode** v2 **type** inform **retries** 100 **timeout** 1000

49.7. snmp-server engineID

Descrição: o comando **snmp-server engineID** é utilizado para configurar a engineID local e remota do switch. Para retornar para a configuração padrão utilize o comando **no snmp-server engineID**.

Sintaxe: **snmp-server engineID** {[**local** *local-engineID*] [**remote** *remote-engineID*]}

no snmp-server engineID

Parâmetros:

» **local-engineID:** EngineID para clientes locais. Essa ID é um campo alfanumérico único utilizado para identificar o engine SNMP no swtich. Varia entre 10 e 64 caracteres hexadecimais, o qual deve ser um número par.

» **remote-engineID:** EngineID remota para o switch. Essa ID é um campo alfanumérico único utilizado para identificar o engine SNMP em dispositivos remotos que recebem informações do switch. Varia entre 10 e 64 caracteres hexadecimais, os quais devem ser um número par. O comando snmp-server engineID ficará desabilitado se os campos local e remoto não forem configurados.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: especifique uma engineID local como 1234567890, e uma engineID remota com abcdef123456:

INTELBRAS(config)# snmp-server engineID local 1234567890 **remote** abcdef123456

49.8. snmp-server traps snmp

Descrição: o comando **snmp-server traps snmp** é utilizado para habilitar as Traps padrões do SNMP as quais são linkup, linkdown, warmstart e coldstart. O comando sem parâmetros habilita todas as Traps padrões. Todas as Traps padrões do SNMP estão habilitadas por padrão. Para desabilitar o envio dessas Traps utilize o comando **no snmp-server traps snmp**.

Sintaxe: **snmp-server traps snmp** [linkup | linkdown | warmstart | coldstart | auth-failure]
no snmp-server traps snmp [linkup | linkdown | warmstart | coldstart | auth-failure]

Parâmetros:

» **linkup:** indica que o estado da porta mudou de linkdown para linkup e pode ser disparada quando você conectar um dispositivo à porta.

» **linkdown:** indica que o estado da porta mudou de linkup para linkdown e pode ser disparada quando você desconecta um dispositivo à porta.

» **warmstart**: indica que a função SNMP do switch se reinicializará quando a configuração física não sofrer mudanças. Uma Trap pode ser dispara se você desabilitar a habilitar SNMP depois que ele esteja habilitado e completamente configurado.

» **coldstart:** indica uma inicialização do SNMP causada pela reinicialização do sistema do switch. Uma Trap pode ser disparada quando o switch é reiniciado.

» **auth-failure**: disparada quando uma solicitação SNMP com falha na autenticação é recebida.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a trap padrão do SNMP de linkup para o switch:

INTELBRAS(config)# snmp-server traps snmp linkup

49.9. snmp-server traps

Descrição: o comando **snmp-server traps** é utilizado para habilitar as Extended Traps do SNMP. Para desabilitar o envio dessas Traps utilize o comando **no snmp-server traps**. Todas as Extended Traps do SNMP são desabilitadas por padrão.

Sintaxe: **snmp-server traps** {rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory}
no snmp-server traps {rate-limit | cpu | flash | lldp remtableschange | lldp topologychange | loopback-detection | storm-control | spanning-tree | memory}

Parâmetros:

» **rate-limit:** monitora se a largura de banda alcança o limite de banda que você determinou. Essa Trap pode ser disparada quando a função de Rate Limite está ativa e os pacotes que forem enviados para a porta com uma taxa superior à indicada.

» **cpu**: monitora o estado de carga da CPU do switch. Essa Trap pode ser disparada quando a taxa de utilização da CPU exceder o limite que você determinar. O limite da taxa de utilização da CPU do switch é configurado como 80% por padrão.

» **flash**: é disparada quando há modificação na memória flash durante operações como backup, reset, firmware upgrade, importação de configuração entre outras.

» **lldp remtables change**: uma notificação LLDP RemTablesChanges é enviada quando o valor do LLDP StatsRemTableLastChangeTime muda. Pode ser utilizada por um host NMS e disparar o sistema de manutenção de tabelas do LLDP remoto.

» **lldp topology change**: uma notificação gerada pelo dispositivo local que sente uma mudança na topologia que indica um novo dispositivo remoto ligado à porta local, ou um dispositivo remoto desconectado da porta local ou movido para uma outra porta.

» **loopback-detection**: essa função é usada para detectar loopbacks. Quando ativada o sistema irá gerar a Trap quando um loopback é detectado ou limpo.

» **storm-control**: essa função é utilizada para monitorar as Storms na rede. O sistema irá gerar a Trap quando a taxa de broadcast ou multicast atingir o limite do Storm Control.

» **spanning-tree**: essa função é utilizada para monitorar o estado do Spanning Tree. O sistema irá gerar essa trap nas seguintes situações: mudança do estado da porta de não encaminhando para encaminhando, ou vice-versa; e quando a porta recebe pacotes com flags TC ou pacotes TCN.

» **memory**: essa função é utilizada para monitorar a memória. O sistema gerará essa Trap quando a utilização de memória exceder 80%.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a Trap extended do SNMP de controle de largura de banda:

```
INTELBRAS(config)# snmp-server traps rate-limit
```

49.10. snmp-server traps vlan

Descrição: o comando **snmp-server traps vlan** é utilizado para habilitar as Traps de VLAN. O comando sem parâmetros ativa todas as Traps VLAN. Para desabilitar o envio dessas Traps utilize o comando **no snmp-server traps vlan**. Todas as Traps VLAN do SNMP são desabilitadas por padrão.

Sintaxe: **snmp-server traps vlan** [create | delete]
no snmp-server traps vlan [create | delete]

Parâmetros:

» **create:** disparado quando certa VLAN é criada com sucesso.

» **delete:** disparada quando certa VLAN é excluída com sucesso.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplos:

Habilite todas as Traps VLAN:

```
INTELBRAS(config)# snmp-server traps vlan
```

Habilite somente a Trap de criação de VLAN para o switch:

```
INTELBRAS(config)# snmp-server traps vlan create
```

49.11. snmp-server traps security

Descrição: o comando **snmp-server traps security** é utilizado para habilitar as Traps de segurança. Para desabilitar essa função utilize o comando **no snmp-server traps security.** Todas as Traps de segurança do SNMP são desabilitadas por padrão.

Sintaxe: **snmp-server traps security** {dhcp-filter | ip-mac-binding}
no snmp-server traps security {dhcp-filter | ip-mac-binding}

Parâmetros:

» **dhcp-filter:** disparada quando o filtro DHCPv4 é ativo e o switch recebe pacotes DHCP de um servidor DHCP ilegal.

» **ip-mac-binding:** disparada quando a inspeção ARP é ativa e o switch recebe pacotes ARP ilegais, ou quando o IPv4 Source Guard estiver ativo e o switch receber pacotes IP ilegais.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a Trap de filtro DHCP:

```
INTELBRAS(config)# snmp-server traps security dhcp-filter
```

49.12. snmp-server traps acl

Descrição: o comando **snmp-server traps acl** é utilizado para habilitar a Trap de ACL. Para desabilitar essa função utilize o comando **no snmp-server traps acl**. A Trap de ACL do SNMP é desabilitada por padrão.

Essa Trap monitora as informações de correspondência ACL, incluindo as ACL ID, ID de regra e número de pacotes correspondentes. Com a função de relatório de log do ACL ativo e juntamente com essa Trap o switch irá verificar as informações e correspondência ACL a cada 5 minutos e enviará Traps SNMP se houver alguma informação de atualização.

Sintaxe: **snmp-server traps acl**
no snmp-server traps acl

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a Trap de ACL:

```
INTELBRAS(config)# snmp-server traps acl
```

49.13. snmp-server traps ip

Descrição: o comando **snmp-server traps ip** é utilizado para habilitar as Traps de IP. Para desabilitar essas funções utilize o comando **no snmp-server traps ip**. As Traps de IP do SNMP são desabilitadas por padrão.

Sintaxe: **snmp-server traps ip** {change | duplicate}
no snmp-server traps ip {change | duplicate}

Parâmetros:

- **change:** disparado quando existir alteração de endereço IP do switch.
- **duplicate:** disparado quando existir endereços IP duplicados.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a Trap de mudança do endereço IP para o switch:

```
INTELBRAS(config)# snmp-server traps ip change
```

49.14. snmp-server traps power

Descrição: o comando **snmp-server traps power** é utilizado para habilitar as Traps de PoE. O comando sem parâmetros habilita todas as Traps PoE. Para desabilitar essas funções utilize o comando **no snmp-server traps power**. As Traps de PoE do SNMP são desabilitadas por padrão.

Sintaxe: **snmp-server traps power** [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown]
no snmp-server traps power [over-max-pwr-budget | port-pwr-change | port-pwr-deny | port-pwr-over-30w | port-pwr-overload | port-short-circuit | thermal-shutdown]

Parâmetros:

- **over-max-pwr-budget:** disparado quando a potência solicitada pelos dispositivos for superior à máxima potência que o switch PoE pode fornecer.
- **port-pwr-change:** disparado quando houver alteração da potência solicitada pelo dispositivo conectado.
- **port-pwr-deny:** disparado quando o switch encerra o fornecimento de potência para as portas PoE de baixa prioridade. Quando o total de potência solicitada excede o limite do sistema de alimentação o switch irá encerrar o fornecimento de energia para as portas de baixa prioridade de PoE para garantir estabilidade de funcionamento.
- **port-pwr-over-30w:** disparado quando a potência solicitada pelo dispositivo conectado for superior a 30 Watts.
- **port-pwr-overload:** disparado quando a potência solicitada pelo dispositivo conectado exceder a potência que a porta pode fornecer.

» **port-short-circuit:** disparado quando um curto circuito for detectado na porta.
» **thermal-shutdown:** disparado quando o chip PSE superaquece. O switch encerra o fornecimento de potência nesse caso.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite todas as Traps PoE para o switch:

```
INTELBRAS(config)# snmp-server traps power
```

49.15. snmp-server traps link-status

Descrição: o comando **snmp-server traps link-status** é utilizado para habilitar as Traps de link SNMP para uma porta específica. Para desabilitar essas funções utilize o comando **no snmp-server traps link-status**. As Traps de Link SNMP é desabilitada por padrão.

Sintaxe: **snmp-server traps link-status**
no snmp-server traps link-status

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: habilite a Trap de status de link SNMP para a porta 3:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/3
INTELBRAS(config-if)# snmp-server traps link-status
```

49.16. rmon history

Descrição: o comando **rmon history** é utilizado para configurar a amostra de entrada de histórico. Para retornar para a configuração padrão utilize o comando **no rmon history**. RMON (Remote Monitoring) é baseado na arquitetura SNMP e sua função é monitorar a rede. Histórico de grupo é um dos grupos de RMON mais utilizados. Após o histórico ser configurado, o switch coleta informações estatísticas periodicamente baseada em qual estação de monitoramento pode monitorar a rede.

Sintaxe: **rmon history** *index* **interface gigabitEthernet** *port* [**interval** *interval*] [**owner** *owner-name*] [**buckets** *number*]
no rmon history *index*

Parâmetros:

» **index:** número de indexação da entrada, varia entra 1 e 12 no formato, *1-3, 5*.
» **port:** número da porta Ethernet.
» **interval:** intervalo da coleta de amostras, varia entre 10 e 3600 segundos e por padrão vem configurado como *1800*.
» **owner-name:** dono da entrada de amostra de histórico, com até 16 caracteres. Configurado por padrão como *monitor*.
» **number:** número máximo de buckets desejados para o grupo de histórico de RMON, variando de 1 a 130. O padrão é *50 buckets*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure a porta gigabit 2 para amostras com intervalo de 100 segundos para as entradas 1, 2 e 3:

```
INTELBRAS(config)# rmon history 1-3 interface gigabitEthernet 1/0/2 interval 100 owner owner1
```

49.17. rmon event

Descrição: o comando **rmon event** é utilizado para configurar as entradas de eventos SNMP-RMON. Para retornar para a configuração padrão utilize o comando **no rmon event**. Grupos de evento são grupos RMON comumente utilizados e servem para definir os eventos RMON. Alarmes ocorrem quando um evento é detectado.

Sintaxe: **rmon event** *index* [**user** *user-name*] [**description** *descript*] [**type** {none | log | notify | log-notify}] [**owner** *owner-name*]
no rmon event *index*

Parâmetros:

- **index:** número de indexação da entrada, varia entra 1 e 12 no formato, *1-3, 5*.
- **user-name:** nome de usuário ao qual os eventos pertencerão com até 16 caracteres. Por padrão é apontado como *public*.
- **descript:** descrição do evento com até 16 caracteres, vazio por padrão.
- **type:** tipo do evento, pode ser *none* que indica nenhum processamento, *log* indica evento de registro de log, *notify* indica envio de mensagens Trap para a aestação de gerenciamento e *both* que indica que tantos eventos de registro de log e envio de mensagens Trap para estação de gerenciamento ocorrerão.
- **owner-name:** dono da entrada de evento, com até 16 caracteres. Configurado por padrão como *monitor*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure as entradas 1, 2, 3 e 4 como user1, a descrição do evento como descricao1, tipo do evento como log e o dono da entrada como dono1:

INTELBRAS(config)# rmon event 1-4 **user** user1 **description** descricao1 **type** log **owner** dono1

49.18. rmon alarm

Descrição: o comando **rmon alarm** é utilizado para configurar o gerenciamento de alarmes SNMP-RMON. Para retornar para a configuração padrão utilize o comando **no rmon alarm**. Grupos de alarme são grupos RMON comumente utilizados e servem para definir os eventos RMON. Alarmes ocorrem quando um evento é detectado.

Sintaxe: **rmon alarm** *index* {**stats-index** *sindex*} [**alarm-variable** {revbyte | revpkt | bpkt | mpkt | crc-lign | undersize | oversize | jabber | collision | 64 | 65-127 | 128-511 |512-1023 | 1024-10240}] [**s-type** {absolute | delta}] [**rising-threshold** *r-hold*] [**rising-event-index** *r-event*] [**falling-threshold** *f-hold*] [f**alling-event-index** *f-event*] [**a-type** {rise | fall | all}] [**owner** *owner-name*] [**interval** *interval*]
no rmon alarm *index*

Parâmetros:

- **index:** número de indexação da entrada, varia entre 1 e 12 no formato, *1-3, 5*.
- **sindex:** específica a index das estatísticas.
- **alarm-variable:** variável do alarm. Por padrão a opção é *revbyte*.
- **s-type:** tipo da amostra, a qual é a amostragem para a variável e comparação com os valores limites. Existem duas opções absolute e delta. *Absolute* indica comparar os valores diretamente com os limites ao final do intervalo de amostragem. *Delta* indica subtrair da última amostra o valor atual e então comparar a diferença com os valores de limite. Por padrão o tipo da amostra é definida como *absoluta*.
- **r-hold:** contador de subida que dispara o alarme do Rising threshold. Varia entre 1 e 2147483647. Configurado como *100* por padrão.
- **r-event:** evento de subida, o qual é a index do evento correspondente que será disparado se o valor da amostra for maior que o Rising threshold. Varia entre 1 e 12.
- **f-hold:** contador de queda é o valor que dispara do alarme Falling threshold, varia entre 1 e 2147483647. Por padrão é *100*.
- **f-event:** evento de queda, o qual é a index do evento correspondente que será disparado se o valor da amostra for inferior ao Falling threshold. Varia entre 1 e 12.
- **a-type:** tipo do alarme, com as opções *rise*, *fall* e *all*. *Rise* indica que o evento de alarme irá ser disparado quando a amostra exceder o valor do limite máximo do threshold, *fall* indica que o evento de alarme será disparado quando o valor da amostra estiver abaixo do limite mínimo do threshold, e *all* indica que o alarme será disparado em ambos os casos. Por padrão o tipo do alarme é definido como *all*.
- **owner-name:** dono da entrada de evento, com até 16 caracteres. Configurado por padrão como *monitor*.
- **interval:** tempo de intervalo do alarm, varia entre 10 e 3600 segundos e por padrão é definido como *1800*.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure uma entrada de alarme RMON 1, 2 e 3 com a entradas de estatísticas 2, pertencente ao dono1 e com intervalo de 100 segundos:

INTELBRAS(config)# rmon alarm 1-3 **stats -index** 2 **owner** dono1 **interval** 100

49.19. rmon statistics

Descrição: o comando **rmon statistics** é utilizado para configurar as entradas de estatísticas do RMON. Para excluir a entrada correspondente utilize o comando **no rmon statistcs**. O valor máximo de entradas suportadas é 1000.

Sintaxe: **rmon statistcs** *index* **interface gigabitEthernet** *port* [**owner** *owner-name*] [**status** {underCreation | valid}]
no rmon statistics *index*

Parâmetros:

- **index:** número de indexação da entrada, varia entre 1 e 12 no formato, *1-3, 5*.
- **port:** número da porta Ethernet.
- **owner-name:** criador do evento da entrada, com até 16 caracteres. Configurado por padrão como *monitor*.
- **status:** estado da entrada de estatística, pode ser *underCreation* ou *valid*. *underCreation* significa que a entrada não terá efeito enquanto não for modificada para *valid*, *valid* significa que a entrada terá efeito imediatamente após ser criada.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esses comandos.

Exemplo: configure para a porta gigabit 1 entradas 1, 2 e 3 de estatística pertencente ao dono1 validas após serem criadas:

INTELBRAS(config)# rmon statistics 1-3 **interface gigabitEthernet** 1/0/1 **owner** dono1 **status** valid

49.20. show snmp-server

Descrição: o comando **show snmp-server** é utilizado para exibir a configuração global do SNMP.

Sintaxe: **show snmp-server**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a configuração do SNMP:

INTELBRAS# show snmp-server

49.21. show snmp-server view

Descrição: o comando **show snmp-server view** é utilizado para exibir a tabela de Views.

Sintaxe: **show snmp-server view**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: exiba a tabela de Views:

INTELBRAS# show snmp-server view

49.22. show snmp-server group

Descrição: o comando **show snmp-server group** é utilizado para exibir a tabela de grupos SNMP.

Sintaxe: **show snmp-server group**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a tabela de grupos:

INTELBRAS# show snmp-server group

49.23. show snmp-server user

Descrição: o comando **show snmp-server user** é utilizado para exibir a tabela de usuários.

Sintaxe: **show snmp-server user**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a tabela de usuários do SNMP:

```
INTELBRAS# show snmp-server user
```

49.24. show snmp-server community

Descrição: o comando **show snmp-server community** é utilizado para exibir a tabela de comunidades.

Sintaxe: **show snmp-server community**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a tabela de comunidades do SNMP:

```
INTELBRAS# show snmp-server community
```

49.25. show snmp-server host

Descrição: o comando **show snmp-server host** é utilizado para exibir a tabela de Hosts.

Sintaxe: **show snmp-server host**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a tabela de hosts do SNMP:

```
INTELBRAS# show snmp-server host
```

49.26. show snmp-server engineID

Descrição: o comando **show snmp-server engineID** é utilizado para exibir o EngineID do SNMP.

Sintaxe: **show snmp-server engineID**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: Mostre o EngineID:

```
INTELBRAS# show snmp-server engineID
```

49.27. show rmon history

Descrição: o comando **show rmon history** é utilizado para exibir a configuração de entrada de amostra de histórico.

Sintaxe: **show rmon history** [*index*]

Parâmetro:

» **Index:** número de index da entrada a ser exibida, varia entre 1 e 12. Você pode selecionar mais de uma entrada para cada comando. Se não for incluído o parâmetro todas as entradas serão exibidas.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a configuração de todas as amostras de histórico:

```
INTELBRAS# show rmon history
```

49.28. show rmon event

Descrição: o comando **show rmon event** é utilizado para exibir a configuração dos eventos SNMP-RMON.

Sintaxe: **show rmon event** [*index*]

Parâmetro:

» **Index:** número de index da entrada a ser exibida, varia entre 1 e 12. Você pode selecionar mais de uma entrada para cada comando. Se não for incluído o parâmetro todas as entradas serão exibidas.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a configuração das entradas 1, 2, 3 e 4:

```
INTELBRAS# show rmon event 1-4
```

49.29. show rmon alarm

Descrição: o comando s**how rmon alarm** é utilizado para exibir a configuração das entradas de alarme de gerenciamento.

Sintaxe: **show rmon alarm** [*index*]

Parâmetro:

» **Index:** número de index da entrada a ser exibida, varia entre 1 e 12. Você pode selecionar mais de uma entrada para cada comando. Se não for incluído o parâmetro todas as entradas serão exibidas.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a configuração de alarme das entradas 1 e 2:

```
INTELBRAS# show rmon alarm 1-2
```

49.30. show rmon statistics

Descrição: o comando **show rmon statistics** é utilizado para exibir a configuração de entrada de estatística.

Sintaxe: **show rmon statistics** [*index*]

Parâmetro:

» **Index:** número de index da entrada a ser exibida, varia entre 1 e 65535. Se não for incluído o parâmetro todas as entradas serão exibidas.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador têm acesso a esse comando.

Exemplo: mostre a configuração da entrada de estatística 1:

```
INTELBRAS# show rmon statistics 1
```

50. Comandos PoE

A tecnologia PoE (*Power over Ethernet*) descreve um sistema de transmissão de energia juntamente com a transmissão de dados para dispositivos remotos através de cabos de par trançado em redes Ethernet. É extremamente útil para fornecer alimentação para telefones IP, access points wireless, câmeras entre outros.

50.1. power inline consumption (global)

Descrição: o comando **power inline consumption** é utilizado para configurar o limite de potência que o switch poderá fornecer através do PoE de forma global.

Sintaxe: **power inline consumption** *power-limit*

Parâmetro:

» **power-limit:** potência máxima que o switch poderá fornecer variando de 1 até 192 watts. Por padrão é configurado como *192 watts*.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine a potência máxima que o switch pode fornecer via PoE como 160w:

INTELBRAS(config)# power inline consumption 160

50.2. power profile

Descrição: o comando **power profile** é usado para criar um perfil PoE para o switch. Para excluir esse perfil utilize o comando **no power profile**.

Sintaxe: **power profile** *name* [**suply** {enable | disable} [**priority** {low | middle | high} [**consumption** {*power-limit* | auto | class1 | class2 | class3 | class4}]]]
no power profile *name*

Parâmetros:

- **name:** nome do perfil PoE com até 16 caracteres. Se o nome tiver espaços coloque-o entre aspas.
- **supply:** estado PoE da porta para o perfil. Por padrão é habilitado (*enable*).
- **priority:** prioridade PoE da porta para o perfil. Os níveis de prioridade incluem *high*, *middle* e *low* em ordem decrescente. Quando o fornecimento de potência excede o limite do sistema o dispositivo conectado em uma porta com baixa prioridade será desconectado.
- **consumption:** a potência máxima que a porta pode fornecer com 5 opções.
- **power-limit:** indica que você pode apontar um valor manualmente entre 1 e 192, o valor representa 0.1 watt como unidade, para indicar 5w você deve indicar o valor 50. *auto* indica que o switch indicará automaticamente o valor. *class1* representa 4 watts, *class2* representa 7 watts, *class3* representa 15.4 watts e *class4* representa 30 watts.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: crie um perfil PoE chamado câmera ip, com o estado habilitada e com nível de prioridade baixo, com limite de 5 watts:

INTELBRAS(config)# power profile "câmera ip" **suplly** enable **priority** low **consumption** 50

50.3. power inline consumption (interface)

Descrição: o comando **power inline consumption** é utilizado para configurar o limite de potência que uma porta poderá fornecer através do PoE.

Sintaxe: **power inline consumption** {*power-limit* | auto | class1 | class2 | class3 | class4}

Parâmetro:

- **consumption:** a máxima potência que a porta pode fornecer com 5 opções.
  - **power-limit:** indica que você pode apontar um valor manualmente entre 1 e 192, o valor representa 0.1 watt como unidade, para indicar 5w você deve indicar o valor 50.
  - **auto:** indica que o switch indicará automaticamente o valor.
  - **class1:** representa 4 watts.
  - **class2:** representa 7 watts.
  - **class3:** representa 15.4 watts.
  - **class4:** representa 30 watts.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine a potência máxima que a porta 2 pode fornecer via PoE como 5:

INTELBRAS(config)# interface gigbatiEtherent 1/0/2
INTELBRAS(config-if)# power inline consumption 50

50.4. power inline priority

Descrição: o comando **power inline priority** é utilizado para configurar a prioridade do PoE que uma porta.

Sintaxe: **power inline priority** {low | middle | high}

Parâmetro:

» **low | middle | high:** prioridade PoE da porta para o perfil. Os níveis de prioridade incluem *high*, *middle* e *low* em ordem decrescente. Quando o fornecimento de potência excede o limite do sistema o dispositivo conectado em uma porta com baixa prioridade será desconectado.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine a prioridade da porta 2 como média:

INTELBRAS(config)# interface gigbatiEtherent 1/0/2
INTELBRAS(config-if)# power inline priority middle

50.5. power inline supply

Descrição: o comando **power inline supply** é utilizado para configurar o estado PoE da porta.

Sintaxe: **power inline supply** {enable | disable}

Parâmetro:

» **enable | disable:** estado PoE da porta para o perfil. Por padrão é habilitado (*enable*).

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: desabilite a função de PoE para a porta 2:

INTELBRAS(config)# interface gigbatiEtherent 1/0/2
INTELBRAS(config-if)# power inline supply disable

50.6. power inline profile

Descrição: o comando **power inline profile** é utilizado para vincular a porta a um perfil PoE existente. Para cancelar este vínculo utilize o comando **no power inline profile**.

Sintaxe: **power inline profile** *name*
no power inline profile

Parâmetro:

» **name:** nome do perfil PoE que será vinculado à porta. Se o nome contiver espaços escreva-o entre aspas.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: vincule o perfil câmera ip à porta 2:

INTELBRAS(config)# interface gigbatiEtherent 1/0/2
INTELBRAS(config-if)# power inline name "câmera ip"

50.7. power inline time-range

Descrição: o comando **power inline time-range** é utilizado para vincular a porta a um perfil Time-Range existente. Para cancelar este vínculo utilize o comando **no power inline time-range**.

Sintaxe: **power inline time-range** *name*
no power inline time-range

Parâmetro:

» **name:** nome do time range que será vinculado à porta.

Modo de comando: Interface Configuration Mode (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: vincule o time-range "tRange2" à porta 2:

```
INTELBRAS(config)# interface gigbatiEtherent 1/0/2
INTELBRAS(config-if)# power inline name tRange2
```

50.8. show power inline

Descrição: o comando **show power inline** é utilizado para mostrar as informações do sistema PoE de forma global.

Sintaxe: **show power inline**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a informação do sistema PoE:

```
INTELBRAS# show power inline
```

50.9. show power inline configuration interface

Descrição: o comando **show power inline configuration interface** é utilizado para mostrar as configurações do sistema PoE de uma porta específica ou de todas as portas.

Sintaxe: **show power inline configuration interface** [**gigabitEthernet** *port*]

Parâmetro:

» **port:** número da porta Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração PoE de todas as portas:

```
INTELBRAS# show power inline configuration interface
```

50.10. show power inline information interface

Descrição: o comando **show power inline information interface** é utilizado para mostrar as informações do sistema PoE de uma porta específica ou de todas as portas.

Sintaxe: **show power inline information interface** [**gigabitEthernet** *port*]

Parâmetro:

» **port:** número da porta Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as informações PoE de todas as portas:

```
INTELBRAS# show power inline information interface
```

50.11. show power profile

Descrição: o comando **show power profile** é utilizado para mostrar as informações dos perfis PoE.

Sintaxe: **show power profile**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as informações dos perfis PoE:

```
INTELBRAS# show power profile
```

51. Comandos de inspeção ARP

A função de detecção ARP (*Address Resoluition Protocol*) serve para proteger o switch de fraudes ARP como Network Gateway Spoofing e o ataque Man-In-The-Middle, entre outros.

51.1. ip arp inspection

Descrição: o comando **ip arp inspection** é utilizado para habilitar a detecção ARP de forma global. Para desabilitar essa função utilize o comando **no ip arp inspection**.

Sintaxe: **ip arp inspection**
no ip arp inspection

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de detecção ARP de forma global:

```
INTELBRAS(config)# ip arp inspection
```

51.2. ip arp inspection validate

Descrição: o comando **ip arp inspection validate** é usado para habilitar a verificação se pacotes ARP são ilegais quando forem recebidos. Para desabilitar essa função utilize o comando **no ip arp inspection validate**.

Sintaxe: **ip arp inspection validate** {src-mac | dst-mac | ip}
no ip arp inspection validate {src-mac | dst-mac | ip}

Parâmetros:

- **src-mac:** habilita que o switch verifique se o endereço MAC de origem e o endereço MAC do remetente os pacotes são os mesmos ao receber um pacote ARP. Quando habilitado se os endereços não forem o mesmo o pacote será descartado.
- **dst-mac:** habilita que o switch verifique se o endereço MAC de destino no cabeçalho Ethernet em relação ao endereço MAC de destino no corpo ARP para respostas ARP. O dispositivo classifica pacotes com endereços MAC diferentes como inválidos e os descarta.
- **ip:** habilita ou desabilita que o switch verifique se o endereço IP do remetente de todos os pacotes ARP e o endereço IP de destino dos pacotes ARP são válidos. Os pacotes ilegais serão descartados.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a verificação se endereço MAC de origem e do remetente são os mesmos quando receber um pacote ARP:

```
INTELBRAS(config)# ip arp inspection validate src-mac
```

51.3. ip arp inspection vlan

Descrição: o comando **ip arp inspection vlan** é usado para habilitar a função de detecção de ARP para uma ou mais VLANs. Para desabilitar essa função utilize o comando **no ip arp inspection vlan**.

Sintaxe: **ip arp inspection vlan** *vlan-list*
no ip arp inspection vlan *vlan-list*

Parâmetro:

- **vlan-list:** especifica as VLANs as quais terão a função DHCP Snooping habilitada, no formato *1-3, 5.*

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de detecção ARP nas VLANs 1, 4, 6 e 7:

```
INTELBRAS(config)# ip dhcp snooping vlan 1,4,6-7
```

51.4. ip arp inspection vlan logging

Descrição: o comando **ip arp inspection vlan logging** é usado para habilitar a função de log para uma ou mais VLANs. Para desabilitar essa função utilize o comando **no ip arp inspection vlan logging**.

Sintaxe: **ip arp inspection vlan** *vlan-list* **logging**
no ip arp inspection vlan *vlan-list* **logging**

Parâmetros:

» **vlan-list:** especifica as VLANs as quais terão a função DHCP Snooping habilitada, no formato *1-3, 5*.
» **logging:** habilita a função de registrar log quando um pacote ARP é descartado.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de log nas VLANs 1, 4, 6 e 7:

INTELBRAS(config)# ip dhcp snooping vlan 1,4,6-7 **logging**

51.5. ip arp inspection trust

Descrição: o comando **ip arp inspection trust** é utilizado para configurar uma porta como confiável a qual é desnecessário a função de detecção ARP. Para limpar a lista de confiabilidade utilize o comando **no ip arp inspection trust**. Portas específicas como porta de up-link, porta de roteamento e porta LAG, deveriam ser apontadas como portas confiáveis. Para garantir a comunicação normal do switch configure as portas ARP confiáveis antes de habilitar a função de detecção ARP.

Sintaxe: **ip arp inspection trust**
no ip arp inspection trust

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: aponte as portas 2, 3, 4 e 5 como portas Confiáveis:

INTELBRAS(config)# interface range gigabitEthernet 1/0/2-5
INTELBRAS(config-if-range)# ip arp inspection trust

51.6. ip arp inspection limit-rate

Descrição: o comando **ip arp inspection limit-rate** é utilizado para configurar a taxa ARP de uma determinada porta. Para retornar para o valor padrão utilize o comando **no ip arp inspection limit-rate**.

Sintaxe: **ip arp inspection limit-rate** *value*
no ip arp inspection limit-rate

Parâmetro:

» **value:** especifica o valor máximo para recebimento de pacotes ARP por segundo, varia entre 1 e 300 pps (pacotes por segundo). Por padrão é configurado como *100 segundos*.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o limite de pacotes ARP como 50 pps para a porta 5:

INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# ip arp inspection limit-rate 50

51.7. ip arp inspection burst-interval

Descrição: o comando **ip arp inspection burst-interval** é utilizado para configurar o intervalo de tempo de rajada de pacotes ARP para uma determinada porta. Para retornar para o valor padrão utilize o comando **no ip arp inspection burst-interval**.

Sintaxe: **ip arp inspection burst-interval** *value*
no ip arp inspection burst-interval

Parâmetro:

» **value:** especifica o intervalo de tempo. Se a velocidade de recebimento de pacotes ARP nesse intervalo de tempo atingir o limite, a porta irá se desabilitar. Varia entre 1 e 15 segundos e é definida como *1 segundo* por padrão.

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: determine o intervalo de rajada como 2 segundos para a porta 5:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# ip arp inspection burst-interval 2
```

51.8. ip arp inspection recover

Descrição: o comando **ip arp inspection recover** é utilizado para restaurar uma porta para o estado de transmitir ARP no filtro de ARP status.

Sintaxe: **ip arp inspection recover**

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: recupere a porta 5 para o estado de transmitir ARP:

```
INTELBRAS(config)# interface gigabitEthernet 1/0/5
INTELBRAS(config-if)# ip arp inspection recover
```

51.9. show ip arp inspection

Descrição: o comando **show ip arp inspection** é utilizado para mostrar as configurações da detecção ARP de forma global incluindo o estado "enable/disable" e a lista de confiabilidade.

Sintaxe: **show ip arp inspection**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações globais da detecção ARP:

```
INTELBRAS# show ip arp inspection
```

51.10. show ip arp inspection interface

Descrição: o comando **show ip arp inspection interface** é utilizado para mostrar as configurações da detecção ARP de uma porta.

Sintaxe: **show ip arp inspection interface** [**gigabitEthernet** *port*]

Parâmetro:

» **port:** número da porta Ethernet.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações de detecção ARP da porta 1:

```
INTELBRAS# show ip arp inspection interface gigabitEthernet 1/0/1
```

Exemplo: mostre a configuração de todas as portas:

```
INTELBRAS# show ip arp inspection interface
```

51.11. show ip arp inspection vlan

Descrição: o comando **show ip arp inspection vlan** é utilizado para mostrar as configurações da detecção ARP das VLANs.

Sintaxe: **show ip arp inspection vlan**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações de detecção ARP da VLAN:

```
INTELBRAS# show ip arp inspection vlan
```

51.12. show ip arp inspection statistics

Descrição: o comando **show ip arp inspection statistics** é utilizado para mostrar o número de pacotes ARP ilegais recebidos.

Sintaxe: **show ip arp inspection statistics**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre o número de pacotes ARP ilegais recebidos:

```
INTELBRAS# show ip arp inspection statistics
```

51.13. clear ip arp inspection statistics

Descrição: o comando **clear ip arp inspection statistics** é utilizado para limpar o número de pacotes ARP ilegais recebidos.

Sintaxe: **clear ip arp inspection statistics**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: limpe o número de pacotes ARP ilegais recebidos:

```
INTELBRAS# clear ip arp inspection statistics
```

52. Comandos ND Detection

A função de detecção ND permite que o switch detecte pacotes ND baseado nas entradas de vínculo da tabela de vínculo IPv6-MAC para filtrar pacotes ilegais. Antes de configurar a detecção ND complete a configuração de vínculo IPv6-MAC.

52.1. ipv6 nd detection

Descrição: O comando **ip nd detection** é utilizado para habilitar a função de detecção ND de forma global. Para desabilitar essa função utilize o comando **no ip nd detection**.

Sintaxe: **ipv6 nd detection**
no ipv6 nd detection

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a detecção ND de forma global:

```
INTELBRAS(config)# ipv6 nd detection
```

52.2. ipv6 nd detection vlan

Descrição: o comando **ipv6 nd detection vlan** é utilizado para habilitar a função de detecção ND para uma ou mais VLAN. Para desabilitar essa função utilize o comando **no ipv6 nd detection**.

Sintaxe: **ipv6 nd detection vlan** *vlan-range*
no ipv6 nd detection vlan *vlan-range*

Parâmetro:

» **vlan-range:** número de identificação da VLAN ou lista de VLANs no formato *1, 4-7*.

Modo de comando: Interface Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a detecção ND para as VLANs 1, 4, 6 e 7:

INTELBRAS(config)# ipv6 nd detection vlan 1,4,6-7

52.3. ipv6 nd detection vlan logging

Descrição: o comando **ipv6 nd detection vlan logging** é utilizado para habilitar a função Log para uma ou mais VLAN. Para desabilitar essa função utilize o comando **no ipv6 nd detection logging.**

Sintaxe: **ipv6 nd detection vlan** *vlan-range* **logging**
no ipv6 nd detection vlan *vlan-range* **logging**

Parâmetro:

» **vlan-range:** número de identificação da VLAN ou lista de VLANs no formato *1, 4-7*.

Modo de comando: Interface Cofiguration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de LOG para as VLANs 1, 4, 6 e 7:

INTELBRAS(config)# ipv6 nd detection vlan 1,4,6-7 **logging**

52.4. ipv6 nd detection trust

Descrição: o comando **ipv6 nd detection vlan** é utilizado para configurar uma porta como confiável a qual é desnecessário a função de detecção de ND. Para desabilitar essa função utilize o comando **no ipv6 nd detection**. Portas específicas como porta de up-link, porta de roteamento e porta LAG, deveriam ser apontadas como portas confiáveis. Para garantir a comunicação normal do switch configure as portas ARP confiáveis antes de habilitar a função de detecção ARP.

Sintaxe: **ipv6 nd detection trust**
no ipv6 nd detection trust

Modo de comando: Interface Configuration (interface gigabitEthernet / interface range gigabitEthernet).

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: aponte as portas 2, 3, 4 e 5 como portas Confiáveis:

INTELBRAS(config)# interface range gigabitEthernet 1/0/2-5
INTELBRAS(config-if-range)# ipv6 nd detection trust

52.5. show ipv6 nd detection

Descrição: o comando **show ipv6 nd detection** é utilizado para mostrar as configurações globais da detecção ND, incluindo o estado *enable/disable*.

Sintaxe: **show ipv6 nd detection**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações globais da detecção ND:

INTELBRAS# show ipv6 nd detection

52.6. show ipv6 nd detection interface

Descrição: o comando **show ipv6 nd detection interface** é utilizado para mostrar as configurações de interface da detecção ND.

Sintaxe: **show ipv6 nd detection interface** [**fastEthernet** *port* | **gigabitEthernet** *port* | **ten-gigabitEthernet** *port* | **port-channel** *port-channel-id*]

Parâmetros:

- **port:** número da porta Ethernet.
- **port-channel-id:** ID da Port-Channel.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplos:

Mostre as configurações da porta gigabit 1:

```
INTELBRAS# show ipv6 nd detection interface gigabitEthernet 1/0/1
```

Exemplo: mostre as configurações de todas as portas:

```
INTELBRAS# show ipv6 nd detection interface
```

52.7. show ipv6 nd detection vlan

Descrição: o comando **show ipv6 nd detection vlan** é utilizado para mostrar as configurações detecção ND de VLAN.

Sintaxe: **show ipv6 nd detection vlan**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre as configurações globais da detecção ND:

```
INTELBRAS# show ipv6 nd detection vlan
```

53. Comandos LOG sistema

A informação de Log irá gravar configurações e operações do switch respectivamente para você monitorar o estado das operações e diagnosticar mal funcionamentos.

53.1. logging buffer

Descrição: o comando **logging buffer** é utilizado para armazenar registros de log do sistema em um buffer interno. Para desabilitar essa função utilize o comando **no logging buffer**. Registro local é a informação salva de log do sistema a qual possuí dois canais de saída, o que significa que pode ser salvo em duas posições diferentes como log buffer e log em memória flash. O log buffer indica que o registro de log do sistema será salvo na memória RAM e pode ser exibido utilizando o comando **show logging buffer**, o qual é perdido quando o switch é reiniciado.

Sintaxe: **logging buffer**
no logging buffer

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de detecção ARP de forma global:

```
INTELBRAS(config)# logging buffer
```

53.2. logging buffer level

Descrição: o comando **logging buffer level** é utilizado para configurar o nível de severidade e estado das entradas de configuração no log buffer. Para retornar para a configuração padrão utilize o comando **no logging buffer level**.

Sintaxe: **logging buffer level** *level*
no logging buffer level

Parâmetro:

» **level:** nível de severidade da saída de registro de informação para cada canal. São 8 níveis e variam entre 0 e 7. Valores menores maior prioridade. Somente registros com nível de severidade igual ou menor serão exibidas. Por padrão é indicada como *6* então somente informações com nível entre 0 e 6 serão salvas no log buffer.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: indique o nível de severidade como 5:

```
INTELBRAS(config)# logging buffer level 5
```

53.3. logging file flash

Descrição: o comando **logging file flash** é usado para armazenar o registro de log em um arquivo na memória flash do switch. Para desabilitar essa função utilize o comando **no logging file flash**. Essa função vem desabilitada por padrão. O arquivo de log indica um setor falsh para salvar o registro de log do sistema. A informação no arquivo de log não será perdida quando o switch reiniciar e podem ser exibidos pelo comando **show logging flash**.

Sintaxe: **logging file flash**
no logging file flash

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite a função de log em arquivo flash:

```
INTELBRAS(config)# logging file flash
```

53.4. logging file flash frequency

Descrição: o comando **logging file flash frequency** é usado para especificar a frequência com que o arquivo de log em flash se sincronizará com o log em buffer. Para retornar a função para o valor padrão utilize o comando **no logging file flash frequency**.

Sintaxe: **logging file flash frequency** {**periodic** *periodic* | **immediate**}
no logging file flash frequency

Parâmetros:

» **periodic:** frequência de sincronização do log do sistema no buffer para o arquivo em flash, variando entre 1 e 48 horas. Por padrão o sincronismo acontece a cada *24 horas*.

» **immediate:** indica que o registro de log do sistema será sincronizado com o arquivo de flash imediatamente. Essa opção irá reduzir a vida útil do arquivo de flash e não é recomendada.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: especifique a sincronização do log para o arquivo flash a cada 10 horas:

```
INTELBRAS(config)# logging file flash frequency 10
```

53.5. logging file flash level

Descrição: o comando **logging file flash level** é utilizado para configurar o nível de severidade e estado das entradas de configuração no log buffer. Para retornar para a configuração padrão utilize o comando **no logging file flash level**.

Sintaxe: **logging file flash level** *level*
no logging file flash level

Parâmetro:

» **level:** nível de severidade da saída de registro de informação para cada canal. São 8 níveis e variam entre 0 e 7. Valores menores maior prioridade. Somente registros com nível de severidade igual ou menor serão exibidas. Por padrão é indicada como *6* então somente informações com nível entre 0 e 6 serão salvas no arquivo de log no flash.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: salve as mensagem com severidade igual ou maior que 5 no arquivo flash:

```
INTELBRAS(config)# logging file flash level 5
```

53.6. logging host index

Descrição: o comando **logging host index** é utilizado para configurar um log para o host. Para limpar a configuração de um host utilize o comando **no logging host index**. Log Host possibilita receber o log do sistema através de outro dispositivo. Você pode monitorar remotamente as configurações e o estado de operação por meio do Log Host.

Sintaxe: **logging host index** *idx host-ip level*
no logging host index *idx*

Parâmetros:

» **idx:** Index do Log Host. O switch suporta até 4 hosts.
» **host-ip:** endereço IP do Host.
» **level**: nível de severidade da saída de registro de informação para cada canal. São 8 níveis e variam entre 0 e 7. Valores menores maior prioridade. Somente registros com nível de severidade igual ou menor serão exibidas. Por padrão é indicada como *6* então somente informações com nível entre 0 e 6 serão salvas no log buffer.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o log host 2 para o endereço IP 192.168.0.148 com nível 5:

```
INTELBRAS(config)# logging host index 2 192.168.0.148 5
```

53.7. logging console

Descrição: o comando **logging console** é utilizado para enviar os logs do sistema para a porta console. Para desabilitar o registro para a porta console utilize o comando **no logging console**. Essa função é desabilitada por padrão.

Sintaxe: **logging console**
no logging console

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: habilite o registro de Log na porta console:

```
INTELBRAS(config)# logging console
```

53.8. logging console level

Descrição: o comando **logging console level** é utilizado para limitar o que é exibido no log da porta Console. Logs do sistema com níveis inferiores ao limite estipulado por esse comando serão mostrados na porta Console. Para retornar para a configuração padrão utilize o comando **no logging console level.**

Sintaxe: **logging console level** *level*
no logging console level

Parâmetro:

» **level:** nível de severidade da saída de registro de informação para cada canal. São 8 níveis e variam entre 0 e 7. Valores menores maior prioridade. Somente registros com nível de severidade igual ou menor serão exibidas. Por padrão é indicada como *6* então somente informações com nível entre 0 e 6 serão salvas no log buffer.

Modo de comando: Global Cofiguration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: indique que todas as mensagens de log serão exibidas na porta console:

```
INTELBRAS(config)# logging console level 7
```

53.9. logging monitor

Descrição: o comando **logging monitor** é utilizado para exibir as mensagens de log do sistema em um terminal. Para desabilitar essa função utilize o comando **no logging monitor**. Essa função é habilitada por padrão.

Sintaxe: **logging monitor**
no logging monitor

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: desabilite a função de log no terminal:

```
INTELBRAS(config)# no logging monitor
```

53.10. logging monitor level

Descrição: o comando **logging monitor level** é utilizado para limitar o que é exibido no log dos dispositivos terminais. Logs do sistema com níveis inferiores ao limite estipulado por esse comando serão mostrados para os dispositivos. Para retornar para a configuração padrão utilize o comando **no logging monitor level**.

Sintaxe: **logging monitor level** *level*
no logging monitor level

Parâmetro:

» **level:** nível de severidade da saída de registro de informação para cada canal. São 8 níveis e variam entre 0 e 7. Valores menores maior prioridade. Somente registros com nível de severidade igual ou menor serão exibidas. Por padrão é indicada como *6* então somente informações com nível entre 0 e 6 serão salvas no log buffer.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: indique o nível de severidade como 5:

```
INTELBRAS(config)# logging monitor level 5
```

53.11. clear logging

Descrição: o comando **clear logging** é utilizado para limpar as informações buffer e do arquivo de log.

Sintaxe: **clear logging** [buffer | flash]

Parâmetro:

» **buffer | flash:** canais de saída, buffer e flash. Se não houver parâmetro será limpo a informação dos dois canais.

Modo de comando: Global Configuration.

Requisito de privilégio: somente usuários do nível administrador e operador têm acesso a esses comandos.

Exemplo: limpe a informação do arquivo de Log:

INTELBRAS(config)#clear logging buffer

53.12. show logging local-config

Descrição: o comando **show logging local-config** é utilizado para mostrar as configurações locais de log, saída de log para a porta console, para o terminal, para o buffer e para o arquivo flash.

Sintaxe: **show logging local-config**

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração local do log:

INTELBRAS# show logging local-config

53.13. show logging loghost

Descrição: o comando **show logging loghost** é utilizado para mostrar as configurações do Log Host.

Sintaxe: **show logging loghost** [*index*]

Parâmetro:

» **index:** index do Log Host o qual terá a configuração exibida, varia entre 1 e 4. Se não houver parâmetro definido será exibido a configuração de todos os log host.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração do log host 2:

INTELBRAS# show logging loghost 2

53.14. show logging buffer

Descrição: o comando **show logging buffer** é utilizado para mostrar as configurações do Log que estão no buffer de acordo com o nível de severidade apontado.

Sintaxe: **show logging buffer** [**level** *level*]

Parâmetro:

» **level:** nível de severidade da saída de registro de informação para cada canal. São 8 níveis e variam entre 0 e 7. Valores menores maior prioridade. Somente registros com nível de severidade igual ou menor serão exibidas. Se não for definido um nível desejado será exibido toda a informação de Log.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração do log com severidade entre 0 e 5 que estão no buffer:

INTELBRAS# show logging buffer level 5

53.15. show logging flash

Descrição: o comando **show logging flash** é utilizado para mostrar as configurações do Log que estão no arquivo flash, de acordo com o nível de severidade apontado.

Sintaxe: **show logging flash** [**level** *level*]

Parâmetro:

» **level:** nível de severidade da saída de registro de informação para cada canal. São 8 níveis e variam entre 0 e 7. Valores menores maior prioridade. Somente registros com nível de severidade igual ou menor serão exibidas. Se não for definido um nível desejado será exibido toda a informação de Log.

Modo de comando: Configuration and Privileged EXEC.

Requisito de privilégio: nenhum.

Exemplo: mostre a configuração do log com severidade entre 0 e 5 que estão no buffer:

```
INTELBRAS# show logging flash level 5
```

Termo de garantia

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo: Nº de série:

Revendedor:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 3 (três) anos – sendo este de 90 (noventa) dias de garantia legal e 33 (trinta e três) meses de garantia contratual –, contado a partir da data da compra do produto pelo Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca expressa de produtos que apresentarem vício de fabricação. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.
2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.
3. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.
4. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.
6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.
7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.
8. Após sua vida útil, o produto deve ser entregue a uma assistência técnica autorizada da Intelbras ou realizar diretamente a destinação final ambientalmente adequada evitando impactos ambientais e a saúde. Caso prefira, a pilha/bateria assim como demais eletrônicos da marca Intelbras sem uso, pode ser descartado em qualquer ponto de coleta da Green Eletron (gestora de resíduos eletroeletrônicos a qual somos associados). Em caso de dúvida sobre o processo de logística reversa, entre em contato conosco pelos telefones (48) 2106-0006 ou 0800 704 2767 (de segunda a sexta-feira das 08 ás 20h e aos sábados das 08 ás 18h) ou através do e-mail suporte@intelbras.com.br.

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

Todas as imagens deste manual são ilustrativas.

intelbras

fale com a gente

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

Importado no Brasil por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br

02.22