Manual do usuário

S2300G

S2300G | Manual do usuário

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

Este manual contempla os seguinte modelos da serie S2300G :

- » S2310G-A
- » S2328G-A
- » S2328G-PA
- » S2328G-B
- » S2328G-PB
- » S2352G-A
- » S2352G-B
- » S2352G-PB

Este é um produto homologado pela Anatel, o número de homologação se encontra na etiqueta do produto, para consultas utilize o link sistemas.anatel.gov.br/sch (https://sistemas.anatel.gov.br/sch)

ÍNDICE

EXPORTAR PARA PDF

Para exportar este manual para o formato de arquivo PDF, utilize o recurso de impressão que navegadores como Google Chrome® e Mozilla Firefox® possuem. Para acessá-lo, pressione as teclas *CTRL + P* ou clique aqui. Se preferir, utilize o menu do navegador, acessando a aba *Imprimir*, que geralmente fica no canto superior direito da tela. Na tela que será aberta, execute os passos a seguir, de acordo com o navegador:

Google Chrome®: na tela de impressão, no campo *Destino*, clique em *Alterar*, selecione a opção *Salvar como PDF* na seção *Destinos locais* e clique em *Salvar*. Será aberta a tela do sistema operacional solicitando que seja definido o nome e onde deverá ser salvo o arquivo.

Mozilla Firefox®: na tela de impressão, clique em *Imprimir*, na aba *Geral*, selecione a opção *Imprimir para arquivo*, no campo *Arquivo*, defina o nome e o local onde deverá ser salvo o arquivo, selecione *PDF* como formato de saída e clique em *Imprimir*.

PROTEÇÃO E SEGURANÇA DE DADOS

Observar as leis locais relativas à proteção e uso de tais dados e as regulamentações que prevalecem no país. O objetivo da legislação de proteção de dados é evitar infrações nos direitos individuais de privacidade baseadas no mau uso dos dados pessoais.

Tratamento de dados pessoais

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

Diretrizes que se aplicam aos funcionários da Intelbras

- Os funcionários da Intelbras estão sujeitos a práticas de comércio seguro e confidencialidade de dados sob os termos dos procedimentos de trabalho da companhia.
- É imperativo que as regras a seguir sejam observadas para assegurar que as provisões estatutárias relacionadas a serviços (sejam eles serviços internos ou administração e manutenção remotas) sejam estritamente seguidas. Isso preserva os interesses do cliente e oferece proteção pessoal adicional.

Diretrizes que controlam o tratamento de dados

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

Uso indevido e invasão de hackers

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

> A Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo tratamento de dados pessoais a partir deste produto, com exceção aos dados necessários para funcionamento do próprio produto. Para mais informações, consulte o capítulo sobre métodos de

segurança do equipamento.

Visão Geral

Este guia do usuário fornece as seguintes informações:

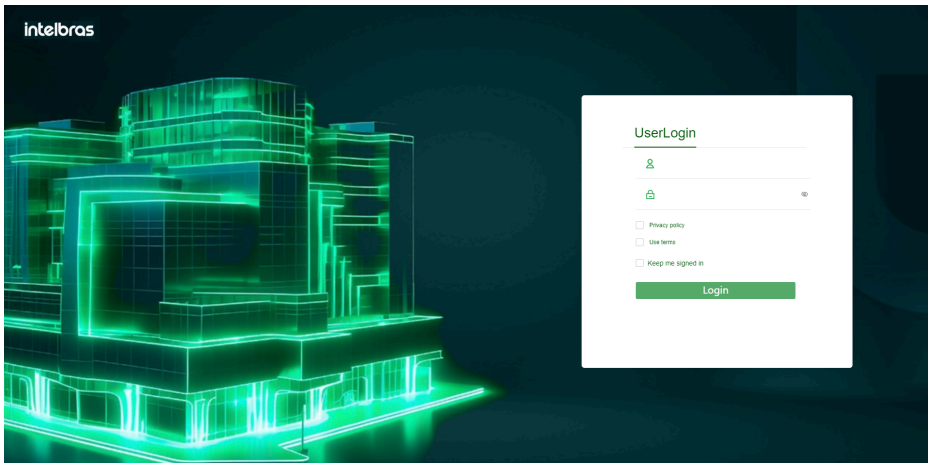
- Como se conectar à interface de rede pela primeira vez.
- Exploração da interface de rede pela primeira vez.
- Como usar a interface de rede.
- Quais recursos você pode configurar na interface de rede.

Este guia do usuário não inclui procedimentos de configuração passo a passo, pois as páginas da web são projetadas de maneira orientada por tarefas. Normalmente, uma página de configuração fornece links para as páginas necessárias para concluir a tarefa. Os usuários não precisam navegar por várias páginas. Para tarefas que exigem navegação por várias páginas, este guia do usuário fornece exemplos de configuração.

Este guia do usuário também não fornece informações detalhadas sobre os parâmetros. Você pode obter informações suficientes online, nas informações de recursos e nos parâmetros das páginas da web.

Exploração da Interface de Rede

Faça login na interface de rede por meio de HTTP ou HTTPS.



Exploração da Interface de Rede pela Primeira Vez

> O acesso à web é suportado por padrão de fábrica apenas para um dispositivo com endereço IP de gerenciamento, nome de usuário e senha no rótulo do dispositivo. Para outros dispositivos, a Conexão à Rede não é suportada por padrão de fábrica. Para efetuar login na web para esses dispositivos, você deve primeiro fazer login nos dispositivos através da porta do console e configurar as configurações conforme necessário.

Como prática recomendada, altere as informações de login e atribua permissões de acesso imediatamente após a primeira conexão bem-sucedida por motivos de segurança.

Configurações de Conexão Padrão

Item	Endereço IP do Dispositivo	Máscara de Sub-rede	Nome de Usuário	Senha	Papel do Usuário
Dispositivo PI (Interface VLAN 1)	192.168.0.1	255.255.255.0	admin	admin	administrador de rede

OBSERVAÇÃO:	A Interface VLAN 1 obtém endereços IP via DHCP por padrão. Se a interface obteve um endereço IP com sucesso, você deve usar o endereço IP do PI obtido para a conexão.

Exploração da Interface de Rede pela Primeira Vez

> O login na Web é suportado por padrão de fábrica apenas para um dispositivo com endereço IP de gerenciamento, nome de usuário e senha na etiqueta do dispositivo. Para outros dispositivos, a Conexão à Rede não é suportada por padrão de fábrica. Para fazer login na web para esses dispositivos, você deve primeiro fazer login nos dispositivos através da porta do console e configurar as configurações conforme necessário.

Como prática recomendada, altere as informações de login e atribua permissões de acesso imediatamente após a primeira conexão bem-sucedida por motivos de segurança.

Conexão à Rede Suportada por Padrão de Fábrica

Por padrão, o HTTP e o HTTPS estão habilitados. Para fazer login na interface de rede:

- Use um cabo Ethernet para conectar o terminal de configuração a uma porta Ethernet no dispositivo.
- Identifique o endereço IP e a máscara do dispositivo. O dispositivo usa o endereço IP padrão, conforme mostrado no guia de usuario. A máscara é 255.255.255.0.
- Figura 1: Endereço IP Padrão do PI no Dispositivo
- Endereço IP Padrão do PI: 192.168.0.1
- Atribua ao host de conexão um endereço IP na mesma sub-rede do dispositivo.
- Abra o navegador e digite as informações de conexão:
- Na barra de endereço, digite o endereço IP do dispositivo.
- Acesso HTTP: Digite o endereço em http:// (http://)*endereço IP*:*porta* ou *endereço IP*:*porta* formato.
- Acesso HTTPS: Digite o endereço em https:// *endereço IP*:*porta* formato.
- O argumento *endereço IP* representa o endereço IP do dispositivo. O argumento *da porta* representa a porta de serviço HTTP ou HTTPS. O número de porta padrão é 80 para HTTP e 443 para HTTPS. Você não precisa inserir o número da porta se não tiver alterado a porta de serviço.
- Na página de login, insira o nome de usuário padrão (admin), a senha (admin) e o código de verificação.
- Clique em Fazer Login.
- Para alterar as informações de conexão, clique no ícone do Administrador.
- Para adicionar novas contas de usuário e atribuir permissões de acesso a diferentes usuários, selecione Dispositivo > Manutenção > Administradores.

Conexão à Rede Não Suportada por Padrão de Fábrica

> Como prática recomendada, altere as informações de login e atribua permissões de acesso imediatamente após a primeira conexão bem-sucedida por motivos de segurança.

Para fazer login na interface de rede:

- Faça login no dispositivo através da porta do console e configure os parâmetros de Conexão à Rede conforme a seguir:
- Habilite os serviços HTTP e HTTPS.
- Crie um usuário local como administrador, atribua a função de administrador de rede ao usuário, selecione HTTP e HTTPS como serviços disponíveis e defina a senha do usuário local.
- Configure o endereço IP da interface VLAN 1.
- Use um cabo Ethernet para conectar o terminal de configuração a uma porta Ethernet no dispositivo.
- Identifique o endereço IP e a máscara do dispositivo da seguinte maneira:

- Se um servidor DHCP estiver em uso, o servidor DHCP atribuirá automaticamente um endereço IP ao dispositivo. Para identificar o endereço IP do dispositivo, use o comando mostrar IP interface apresentação da seguinte maneira:

  display ip interface brief mostrar IP interface apresentação

```
<Sysname> display ip interface brief
*down: administratively down (s): spoofing (l): loopback
Interface       Physical Protocol IP address    VPN instance Description
MGE0/0/0        up       up       192.168.1.137 --           --
Vlan1           up       up       169.254.0.255 --           --
```

- Se nenhum servidor DHCP estiver em uso, o dispositivo usará o endereço IP da interface VLAN 1.
- Atribua ao host de conexão um endereço IP na mesma sub-rede do dispositivo.
- Abra o navegador e digite as informações de conexão:
- Na barra de endereço, digite o endereço IP do dispositivo.
- Acesso HTTP: Digite o endereço em http:// (http://)*endereço IP*:*porta* formato.
- Acesso HTTPS: Digite o endereço em https:// *endereço IP*:*porta* formato.
- O argumento *endereço IP* representa o endereço IP do dispositivo. O argumento *da porta* representa a porta de serviço HTTP ou HTTPS. O número de porta padrão é 80 para HTTP e 443 para HTTPS. Você não precisa inserir o número da porta se não tiver alterado a porta de serviço.
- Na página de login, insira o nome de usuário e a senha.
- Clique em Fazer Login.
- Para alterar as informações de conexão, clique no ícone do Administrador.
- Para adicionar novas contas de usuário e atribuir permissões de acesso a diferentes usuários, selecione Dispositivo > Manutenção > Administradores.

Logout

> Por motivos de segurança, faça logout da interface de rede imediatamente após concluir suas tarefas. Você não pode fazer logout simplesmente fechando o navegador. O dispositivo não salva automaticamente a configuração quando você faz logout da interface de rede.

Para evitar a perda de configuração quando o dispositivo é reiniciado, você deve salvar a configuração.

Para fazer logout da interface de rede:

- Use um dos seguintes métodos para salvar a configuração atual.
- Clique no ícone Salvar no canto superior esquerdo.
- Selecione Dispositivo > Manutenção > Configuração para acessar a página de gerenciamento de configuração.
- Clique em Sair no canto superior esquerdo da interface de rede.

Utilizando a Interface de Rede

Conforme ilustrado na imagem, a interface de rede é composta pelas seguintes áreas:

Áreas:

(1) Área do Cabeçalho

Contém as seguintes unidades:

- Informações básicas, incluindo o logotipo da Intelbras, nome do dispositivo e informações sobre a conexão atual do usuário.
- Ícones de gerenciamento básico:

  Ícone de Administrador - Clique neste ícone para selecionar um idioma ou alterar a senha de conexão.

Ícone de Sair - Clique neste ícone para sair.

Ícone de Salvar - Clique neste ícone para salvar a configuração.

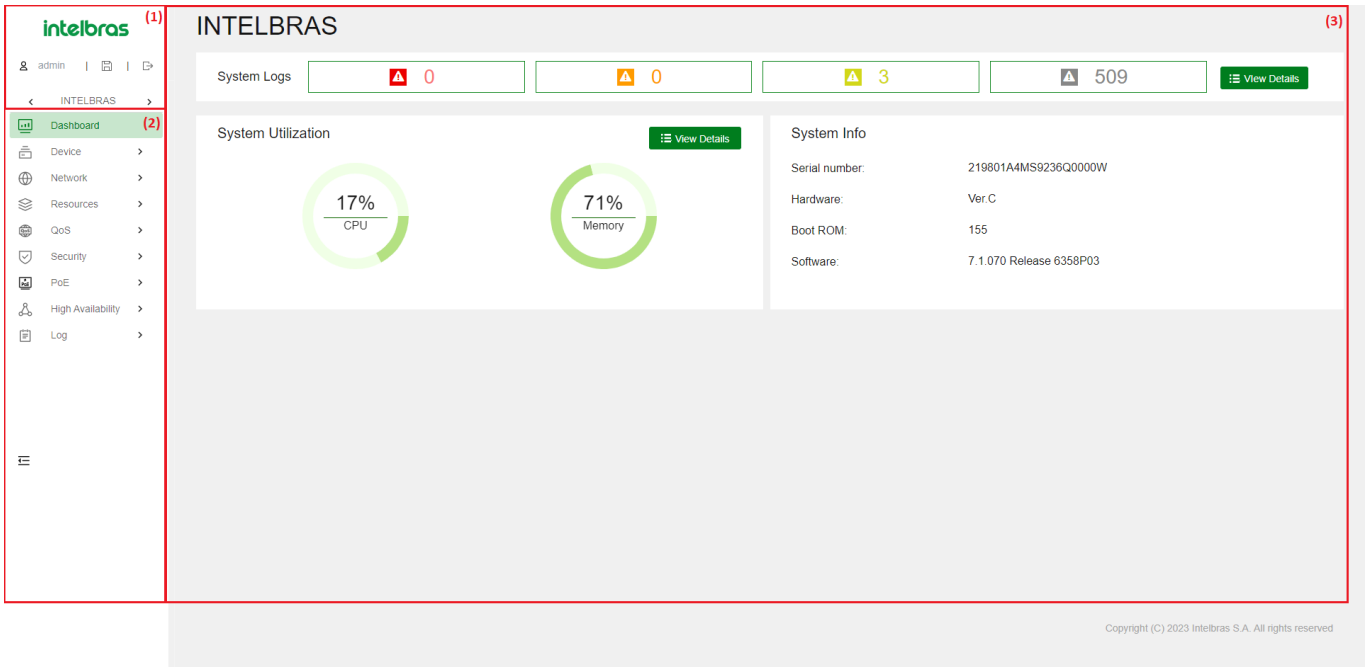
(2) Menu de navegação

Organiza os menus de recursos em uma árvore.

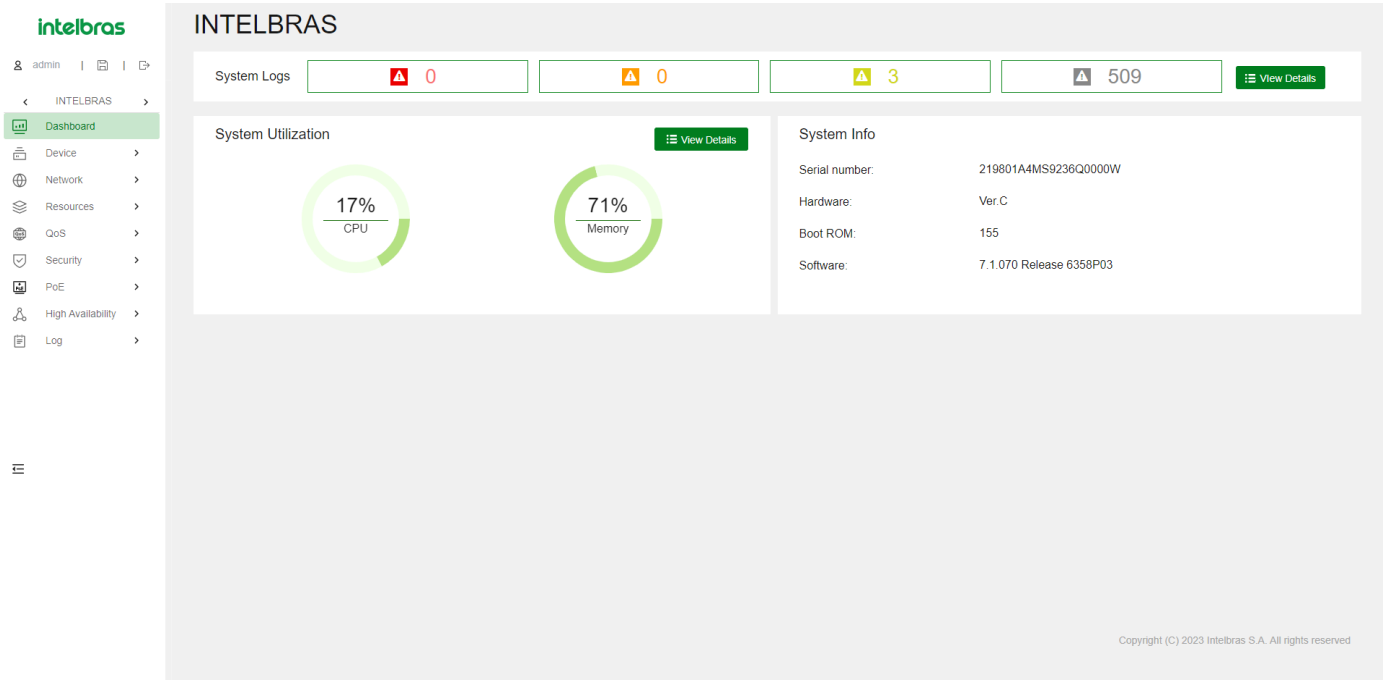
(3) Painel de Conteúdo

Exibe informações e fornece uma área para você configurar recursos. Dependendo do conteúdo neste painel, as páginas da web incluem os seguintes tipos:

- **Página de Recursos** - Contém funções ou recursos que um módulo de recursos pode oferecer (consulte "Usando uma Página de Recursos").
- **Página de Tabelas** - Exibe entradas em uma tabela (consulte "Usando uma Página de Tabelas").
- **Página de Configurações** - Contém parâmetros para configurar um recurso ou função (consulte "Usando uma Página de Configurações").



Layout da Interface de Rede



Tipos de Páginas da Web

As páginas da web incluem páginas de recursos, tabelas e configurações. Esta seção fornece informações básicas sobre essas páginas. Para mais informações sobre o uso dos ícones e botões nas páginas, consulte "Ícones e Botões".

Utilizando a Página de Recursos

Conforme mostrado na Figura 3, a página de recursos contém informações sobre o módulo de recursos, incluindo estatísticas de entrada da tabela, características e funções. A partir da página de recursos, você pode configurar as características oferecidas pelo módulo de recursos.

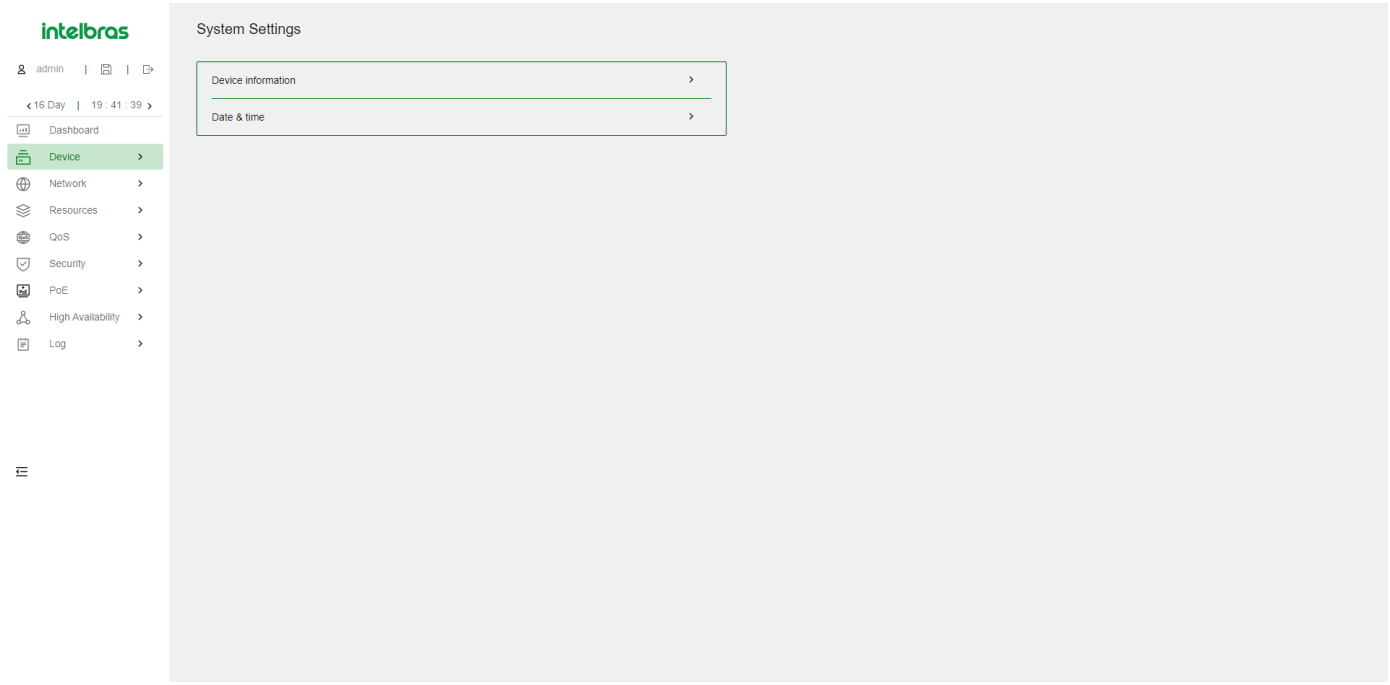


Figura 3: Exemplo de Página de Recursos

Utilizando a Página de Tabelas

Conforme mostrado na Figura 4, a página de tabelas exibe entradas em uma tabela. Para organizar as entradas por ordem crescente ou decrescente de um campo, clique no campo. Por exemplo, clique em **Endereço MAC** para classificar as entradas pelo endereço MAC.

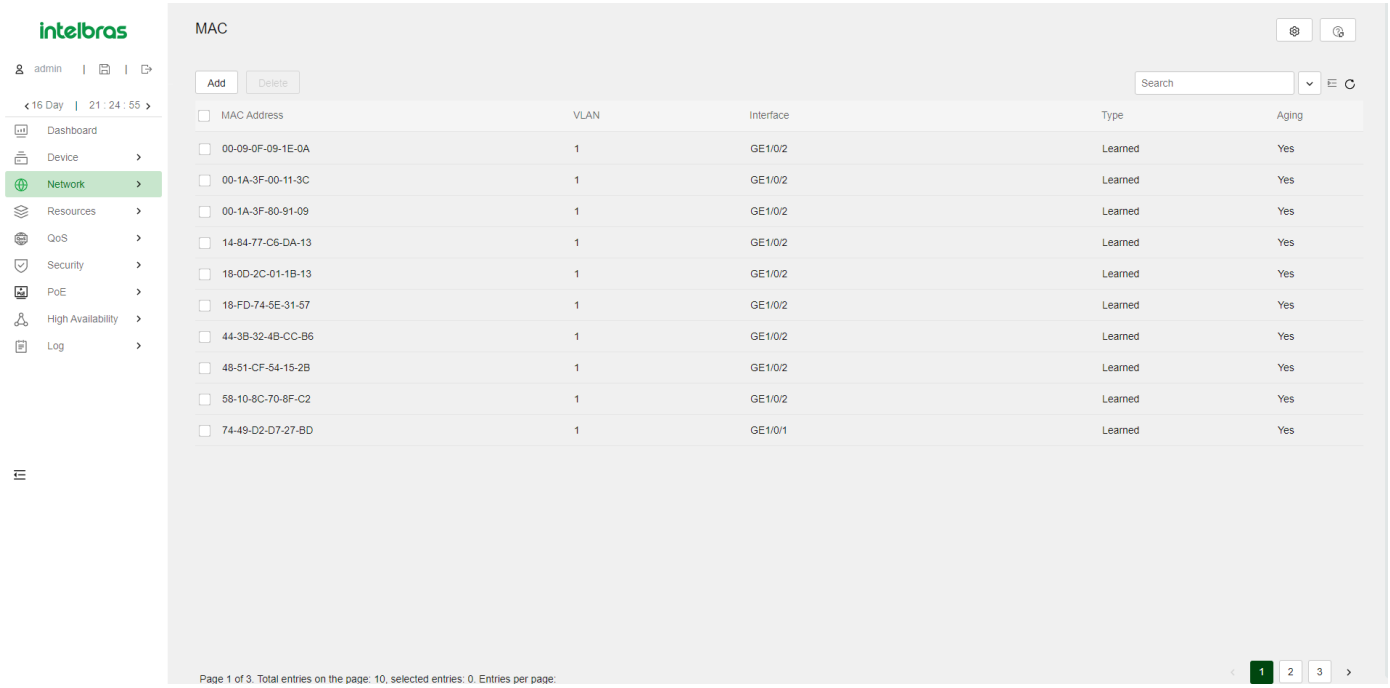


Figura 4: Exemplo de Página de Tabelas

Utilizando a Página de Configurações

Conforme mostrado na Figura 5, uma página de configuração contém todos os parâmetros para uma tarefa de configuração. Se um parâmetro deve ser configurado em outra página, a página de configuração geralmente fornece um link. Você não precisa navegar para a página de destino. Por exemplo, você pode usar uma ACL ao configurar um filtro de pacotes. Se nenhuma ACL estiver disponível quando você executa a

tarefa, você pode clicar no ícone **Adicionar** para criar uma ACL. Nesta situação, você não precisa navegar para a página de gerenciamento de ACL.

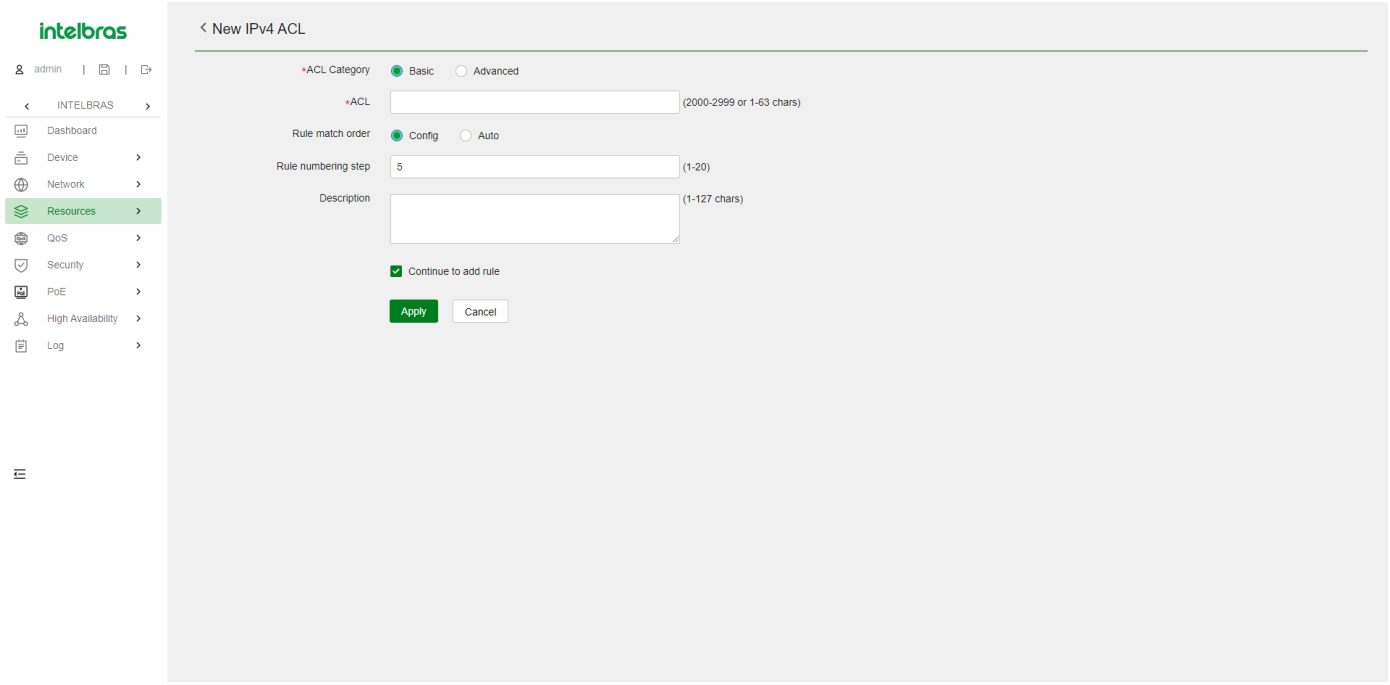


Figura 5: Exemplo de Página de Configurações

Realizando Tarefas Básicas

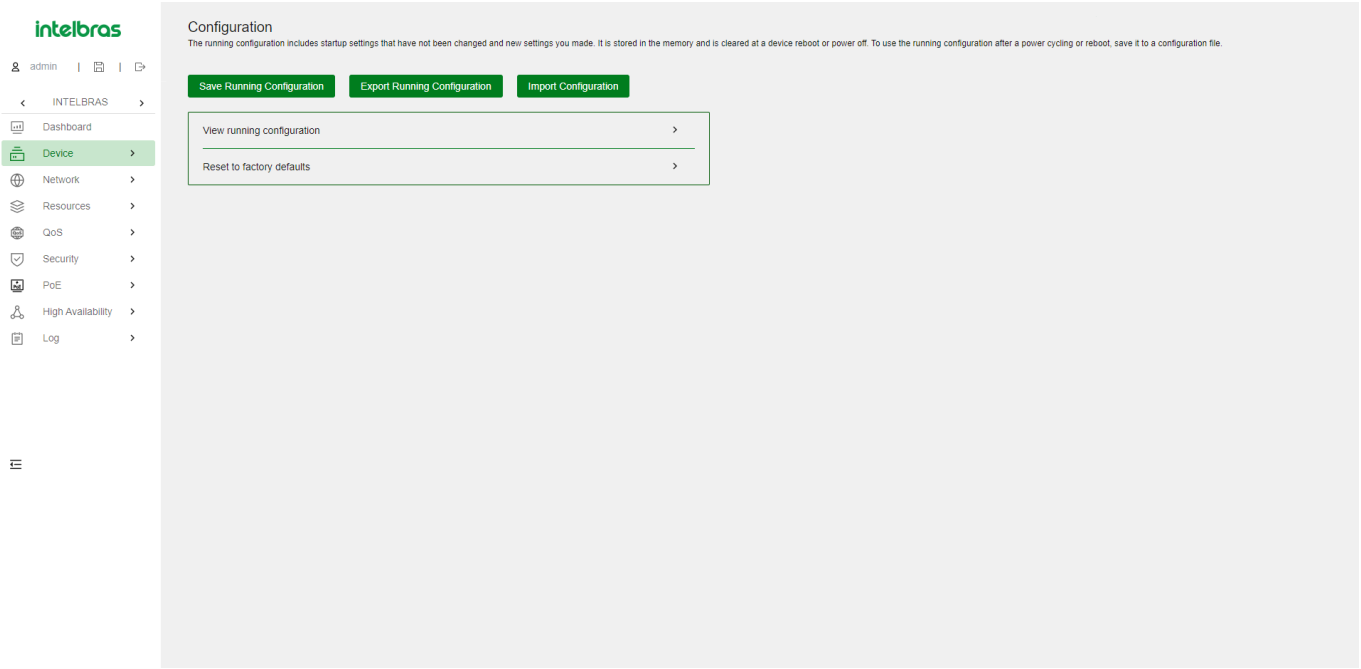
Esta seção descreve as tarefas básicas que você frequentemente precisa realizar ao configurar ou gerenciar o dispositivo.

Salvando a Configuração

Normalmente, as configurações entram em vigor imediatamente após você criá-las. No entanto, o sistema não salva automaticamente as configurações no arquivo de configuração. Elas serão perdidas quando o dispositivo for reiniciado.

Para evitar a perda das configurações, use um dos seguintes métodos para salvar a configuração:

- Clique no ícone no canto esquerdo.
- Selecione **Dispositivo > Manutenção > Configuração** para acessar a página de gerenciamento de configuração.



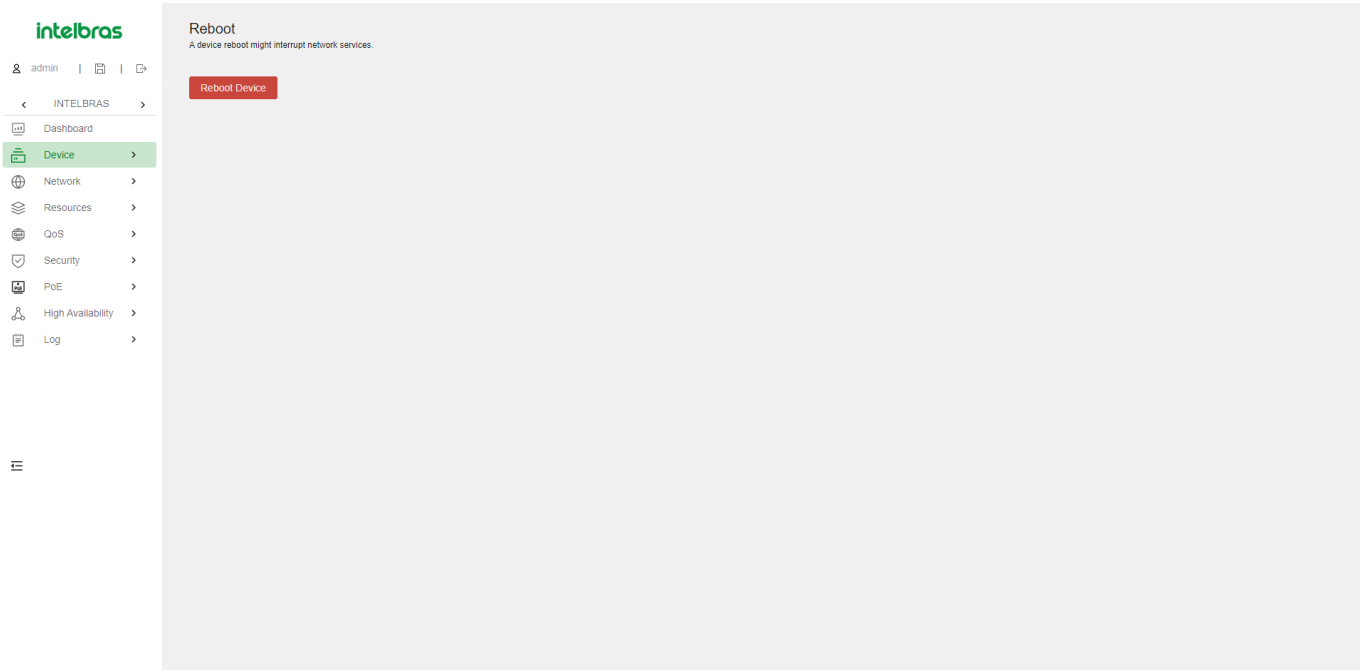
Exibindo ou Modificando Configurações

Passe o mouse sobre o menu. Clique no ícone no final do menu.

Reiniciando o Dispositivo

O reinício é necessário para que algumas configurações, como IRF, tenham efeito. Para reiniciar o dispositivo:

- Salve a configuração.
- Selecione **Dispositivo > Manutenção > Reiniciar**.
- Na página de reinício, clique no botão de reinício.



Recurso do Navegador

Os itens de menu e ícones disponíveis dependem das funções de usuário que você possui. Por padrão, você pode usar qualquer função de usuário para visualizar informações. Para configurar recursos, você deve ter a função de usuário de **Administrador de Rede**.

Este capítulo descreve todos os menus disponíveis para a função de usuário **Administrador de Rede**. O menu de nível superior inclui **Painel**, **Dispositivo**, **Rede**, **Recursos**, NAT, **QoS**, **Segurança**, **PoE** e **Log**. Para cada menu superior, é fornecida uma tabela de navegação. Use as tabelas de navegação para acessar as páginas e realizar as tarefas que você deseja.

Por exemplo:

- Para alterar o nome padrão do dispositivo, selecione **Dispositivo** > **Manutenção** > **Configurações** na Menu de navegação.
- Para excluir um LCA IPv4, selecione **Recursos** > **LCA** > **IPv4** na Menu de navegação.

OBSERVAÇÃO:

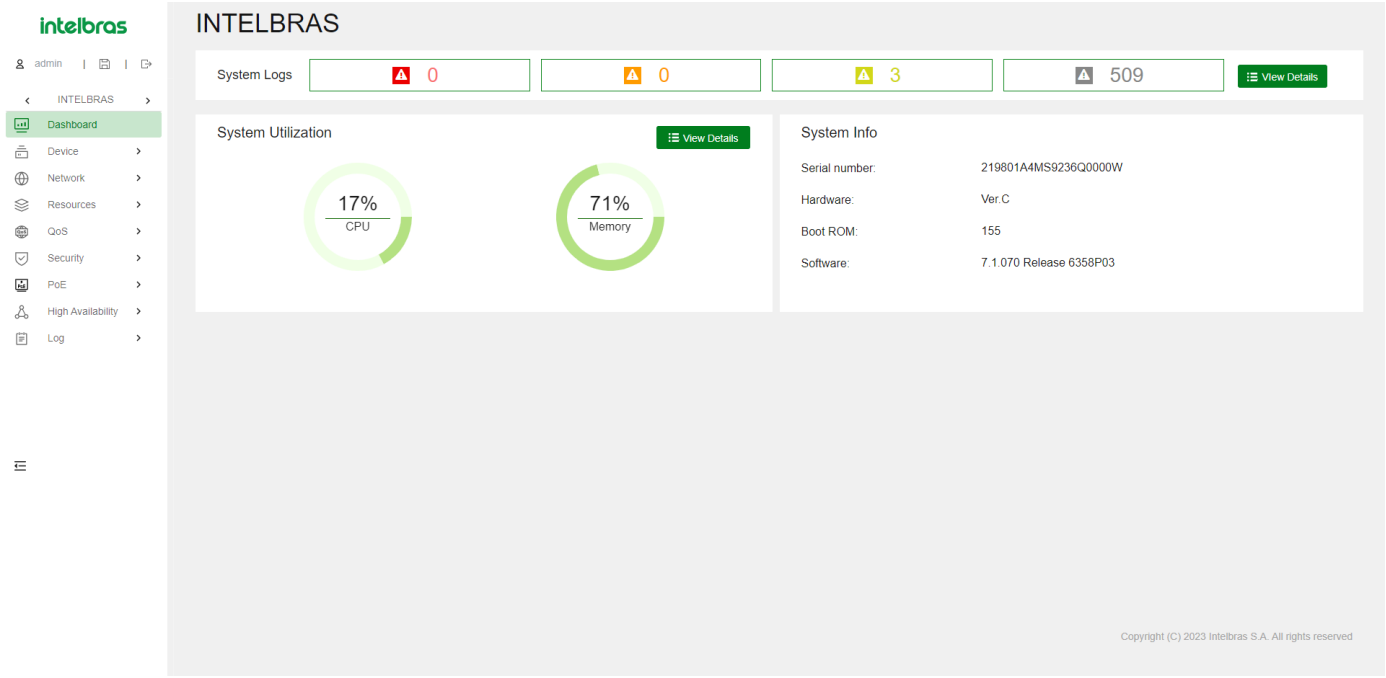
Nas tabelas de navegação, o menu está em negrito se houver submenus.

Dashboard

O Dashboard fornece uma visão geral do sistema e o status atual, incluindo:

- Registro do sistema.
- Uso da CPU e memória.
- Número de série do dispositivo.
- Informações da versão do hardware. Este menu não possui submenus.

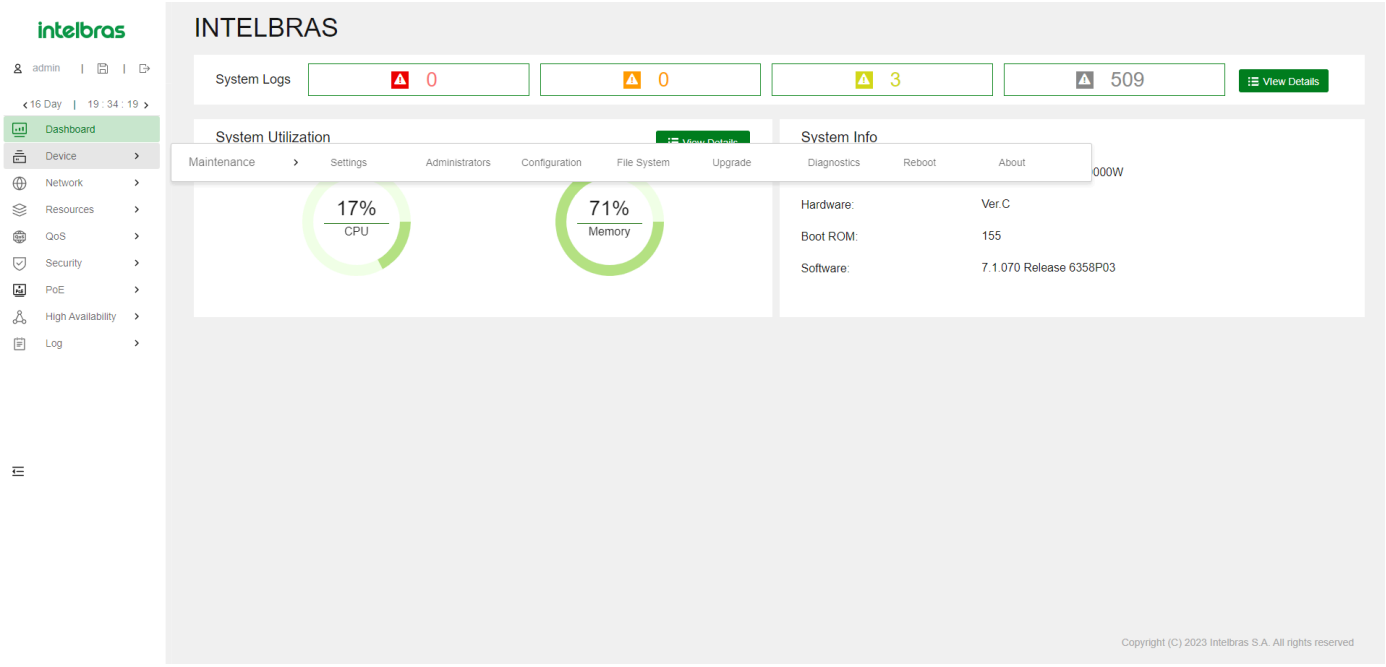
Esse Menu não faz conter submenus.



Menu do Dispositivo

As características e funções oferecidas no Menu do Dispositivo podem variar de acordo com o modelo do switch. Use a Tabela 3 para navegar nas tarefas que você pode executar no Menu do Dispositivo e obter informações sobre o suporte a recursos e funções no menu.

	Menu	Tarefa
Maintenance	Settings	Configure as configurações básicas do dispositivo, incluindo o nome do dispositivo, localização e informações de contato. Configure as configurações de hora do sistema. Você pode configurar manualmente o tempo do sistema ou configurar o dispositivo para obter a hora UTC de uma fonte confiável e calcular o tempo do sistema.
	Administrators	Crie, modifique ou exclua funções de usuário. Crie, modifique ou exclua contas de usuário. Os seguintes switches não têm a conta padrão e não suportam o primeiro login com um nome de usuário e senha padrão.
	Configuration	Salve a configuração atual. Importe a configuração e exporte a configuração em execução. Mostre a configuração atual. Restaure a configuração padrão de fábrica.
	File System	Mostre informações sobre o armazenamento de mídia. Mostre informações sobre arquivos e pastas. Exclua arquivos. Faça o download de arquivos.
	Upgrade	Exiba listas de imagens de software, incluindo: Imagens de programas atuais. Software de imagens de inicialização principal e de backup.
	Diagnóstics	Coleta de informações de diagnóstico usadas para diagnóstico do sistema e solução de problemas.
	Reboot	Reinicie o dispositivo.
	About	Mostre informações básicas do dispositivo, incluindo: Nome do dispositivo. Número de série. Informações de versão. Rótulo eletrônico. Declaração legal.



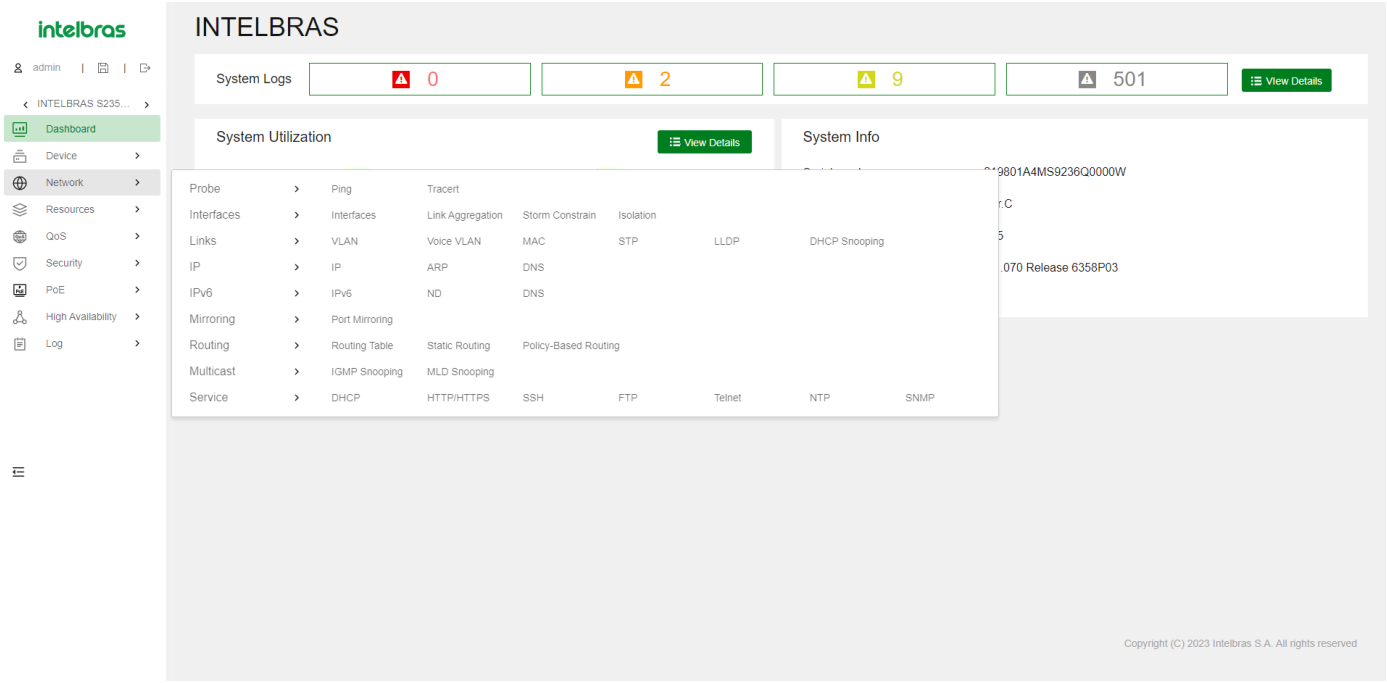
Menu de rede

	Menus	Tarefas
Probe	Ping	Testar a conectividade com um dispositivo em uma rede IPv4. Testar a conectividade com um dispositivo em uma rede IPv6.
	Tracert	Tracert IPv4. Tracert IPv6.
Interfaces	Interfaces	Exibir interfaces e seus atributos, incluindo: Status de link. Endereço IP. Velocidade e modo duplex. Descrição da interface. Alterar configurações da interface. Excluir interfaces lógicas.
	Link Aggregation	
	Storm Constrain	Definir o intervalo de coleta de estatísticas. Definir parâmetros de controle de Storm Constrain. Exibir informações de Storm controls.
	Isolamento	Criar grupos de isolamento. Modificar grupos de isolamento.

Links	VLAN	Configurar VLANs baseadas em porta. Criar interfaces de VLAN.
	Voice VLAN	
	MAC	Criar ou excluir entradas MAC estáticas, entradas MAC dinâmicas e entradas MAC blackhole. Exibir entradas MAC existentes.
	STP	Ativar ou desativar STP globalmente. Ativar ou desativar STP em interfaces. Configurar o modo de operação STP como STP, RSTP, PVST ou MSTP. Configurar prioridades de instância. Configurar regiões MST.
	LLDP	Ativar ou desativar LLDP. Modificar o modo LLDP e de ponte. Modificar o modo de operação da interface. Configurar o LLDP para anunciar os TLVs especificados.
	DHCP Snooping	
IP	IP	Configurar o método de obtenção de um endereço IP (DHCP ou estático). Configurar o endereço IP ou MTU de uma interface. Criar uma interface de loopback.
	ARP	Gerenciar entradas ARP dinâmicas e entradas ARP estáticas. Configurar proxy ARP. Configurar ARP gratuito. Configurar proteção contra ataque ARP.
	DNS	Gerenciar políticas de DNS dinâmico. Configurar uma interface associada à política de DNS dinâmico.

IPv6	IPv6	Configurar o método de obtenção de um endereço IPv6 (atribuição manual, atribuição dinâmica ou geração automática). Configurar o endereço IPv6 de uma interface. Definir o MTU de uma interface. Criar uma interface de loopback.
	ND	Gerenciar entradas ND dinâmicas e entradas ND estáticas. Configurar o tempo de envelhecimento para entradas ND obsoletas. Minimizar entradas ND link-local. Configurar limite de salvo. Configurar atributos de prefixo RA, incluindo: Prefixo de endereço. Comprimento do prefixo. Tempo de vida válido. Tempo de vida preferido. Configurar configurações RA para uma interface, incluindo: Supressão de mensagens RA. Intervalos máximos e mínimos para envio de mensagens RA. Limite de salto. M-flag. O-flag. Tempo de vida do roteador. Intervalo de retransmissão de NS. Preferência do roteador. Tempo de alcance do vizinho. Habilitar proxy ND comum e local em uma interface. Configurar regras ND para a interface.
	DNS	
Mirroring	Port Mirroring	Configurar grupos de espelhamento local. Configurar grupos de espelhamento remoto.
Routing	Routing Table	Exibir informações de tabela de roteamento IPv4 e IPv6, incluindo informações resumidas da tabela de roteamento e estatísticas de rota.
	Static Routing	Exibir entradas de rota estática IPv4 e IPv6. Criar, modificar e excluir entradas de rota estática IPv4 e IPv6.
	Policy-Based Routing	

Multicast	IGMP Snooping	Configurar funções de snooping IGMP, incluindo: Habilitar descarte de dados de multicast desconhecidos. Configurar o questionador de snooping IGMP. Habilitar processamento de saída rápida. Definir o número máximo de grupos de multicast em uma porta.
	MLD Snooping	Configurar funções de snooping MLD, incluindo: Habilitar descarte de dados de multicast IPv6 desconhecidos. Configurar o questionador de snooping MLD. Habilitar processamento de saída rápida. Definir o número máximo de grupos de multicast IPv6 em uma porta.
Service	DHCP	
	HTTP/HTTPS	Ativar ou desativar o serviço HTTP. Ativar ou desativar o serviço HTTPS. Definir o tempo limite de ociosidade da conexão da Web. Definir o número da porta do serviço HTTP. Definir o número da porta do serviço HTTPS. Especificar ACLs de controle de acesso da Web.
	SSH	Ativar os serviços Stelnet, SFTP e SCP. Definir o DSCP em pacotes enviados pelo dispositivo. Filtrar clientes SSH usando uma ACL. Definir o tempo limite de ociosidade da conexão SFTP.
	FTP	Ativar ou desativar o serviço FTP. Definir o valor DSCP para o dispositivo usar em pacotes FTP de saída. Especificar a ACL de controle de acesso FTP. Definir o tempo limite de ociosidade da conexão FTP. Associar o serviço FTP a uma política de servidor SSL.
	Telnet	Ativar ou desativar o serviço Telnet. Definir valores DSCP para o dispositivo usar em pacotes Telnet IPv4 ou IPv6 de saída. Especificar ACLs de controle de acesso Telnet.
	NTP	Configurar o dispositivo para usar o relógio local como relógio de referência.
	SNMP	Ativar SNMP. Configurar parâmetros SNMP, como versão, nome da comunidade, grupo e usuários. Configurar a função de envio de notificação.

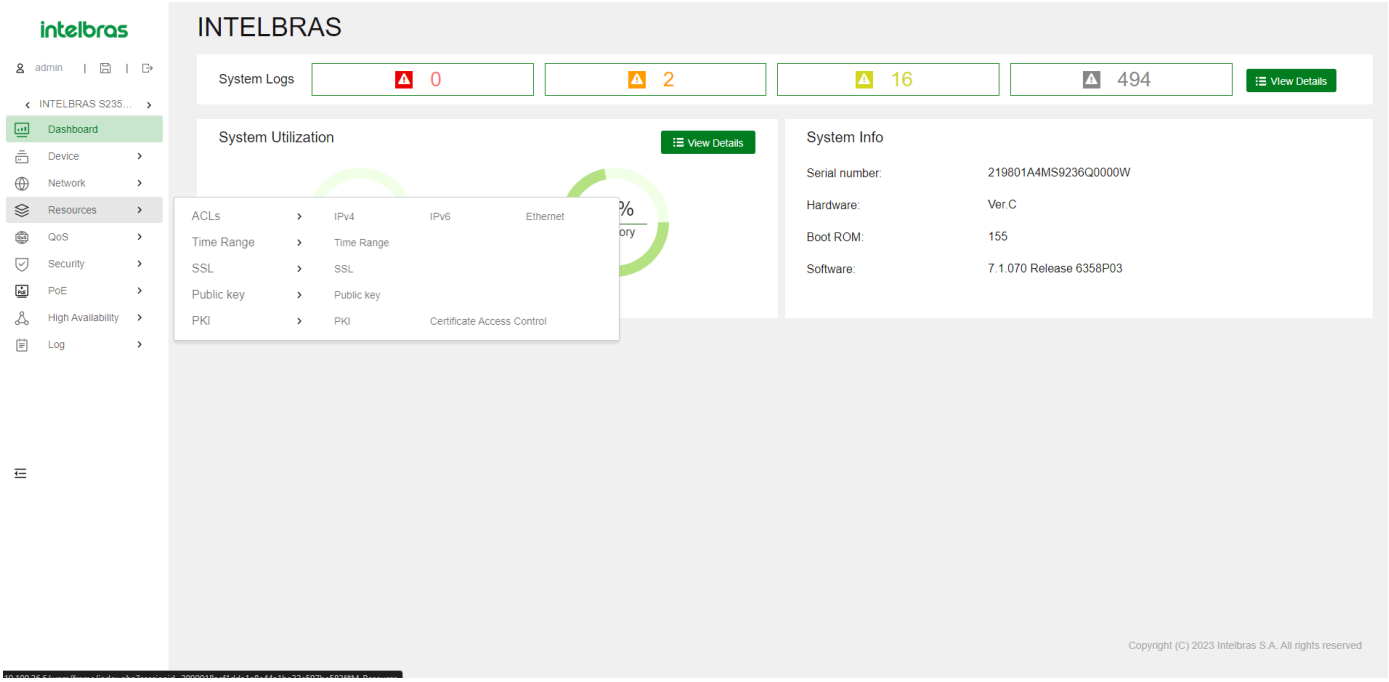


Menu de recursos

O menu *Recursos* contém recursos comuns que podem ser usados por várias funcionalidades. Por exemplo, você pode usar uma *ACL* tanto em um filtro de pacotes para filtrar o tráfego quanto em uma política de *QoS* para combinar o tráfego.

	Menu	Tarefas
ACLs	IPv4	Criar, modificar ou excluir uma ACL IPv4 básica e IPv4 avançada.
	IPv6	Criar, modificar ou excluir uma ACL IPv6 básica e IPv6 avançada.
	Ethernet	Criar, modificar ou excluir uma ACL de cabeçalho de quadro Ethernet.
Time Range	Time Range	Criar, modificar ou excluir um intervalo de tempo.
SSL	SSL	Criar, modificar ou excluir uma política de cliente SSL.
Public Key	Public Key	Gerenciar pares de chaves assimétricas locais. Gerenciar chaves públicas de hosts pares.
PKI	PKI	
	Certificate Access Control	

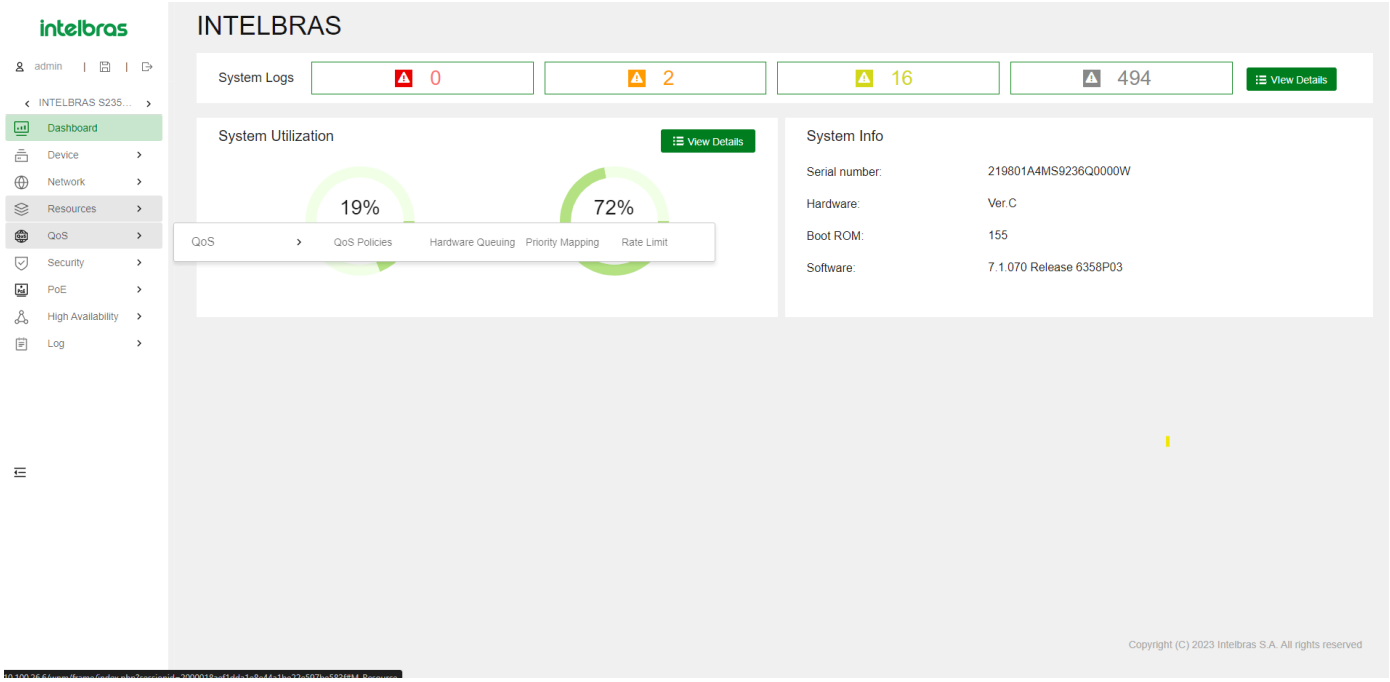
NOTA: Você pode criar ACLs a partir das páginas de ACL ou durante o processo de configuração de uma funcionalidade que utiliza ACLs. No entanto, para modificar ou excluir uma ACL, você deve acessar o menu de ACL.



Menu QoS

Navegador de Menu QoS (Tabela 6)

	Menus	Tarefas
QoS	QoS Policies	Criar, modificar ou excluir políticas de QoS de interface. Criar, modificar ou excluir políticas de QoS de VLAN. Criar, modificar ou excluir políticas de QoS globais.
	Hardware Queuing	Modificar a configuração de filas de hardware.
	Priority Mapping	Configurar a prioridade da porta. Configurar o modo de confiança de prioridade para uma porta. Configurar mapas de prioridade: Aplicar e redefinir o mapa de prioridade 802.1p local. Aplicar e redefinir o mapa de prioridade DSCP-to-802.1p. Aplicar e redefinir o mapa de prioridade DSCP-to-DSCP.
	Rate Limit	Criar, modificar ou excluir limites de taxa.



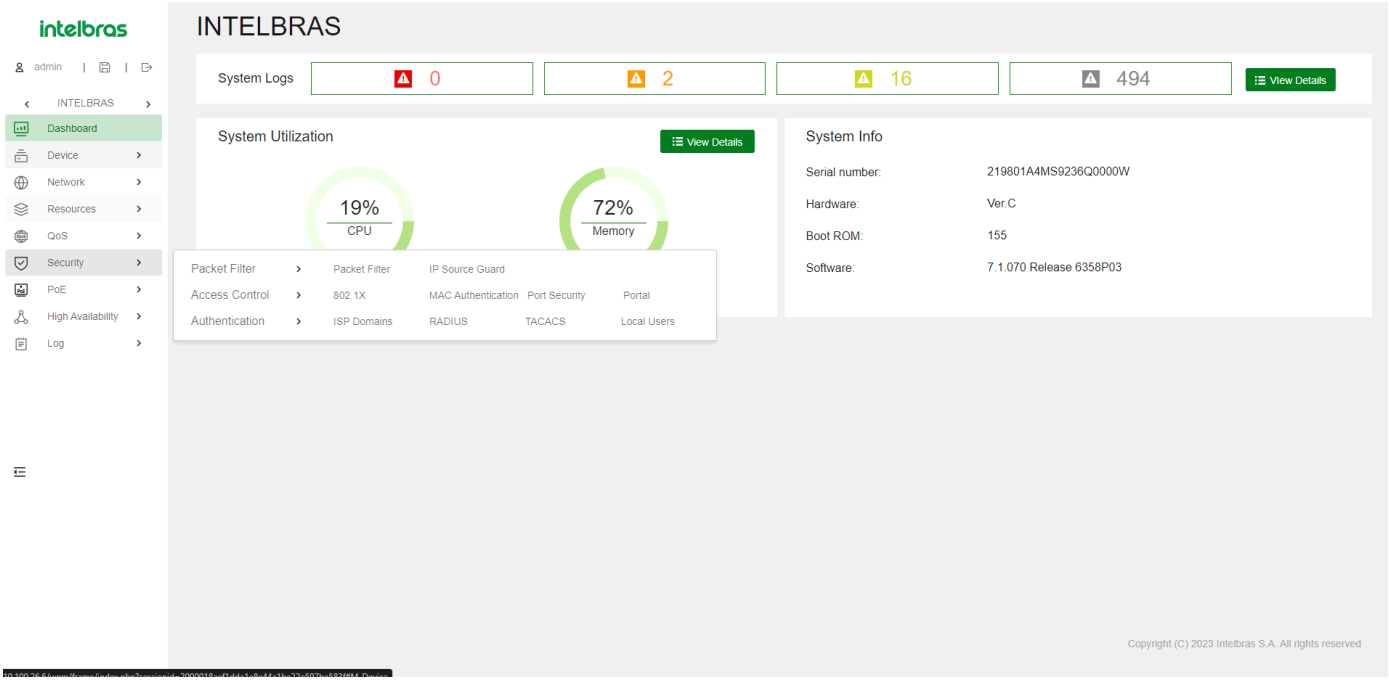
Menu de Segurança

Use a Tabela 7 para navegar nas tarefas que você pode executar a partir do menu de Segurança.

Tabela 7 - Navegador de Menu de Segurança

	Menus	Tarefas
Packet Filter	Packet Filter	
	IP Source Guard	Configurar uma associação estática de guarda de origem IPv4 específica de interface.
Access Control	802.1X	Ativar ou desativar o 802.1X. Configurar o método de autenticação 802.1X.
	MAC Authentication	Ativar ou desativar a autenticação MAC. Configurar o domínio ISP de autenticação MAC. Configurar o formato do nome de usuário.
	Port Security	Ativar ou desativar a segurança de porta. Configurar o modo de segurança de porta. Configurar a ação de proteção contra intrusões. Configurar o modo NTK. Configurar o modo seguro de envelhecimento do MAC.
	Portal	Configurar um servidor de autenticação de portal. Configurar um servidor Web de portal. Configurar um servidor Web de portal local. Criar regras de portal gratuito. Criar políticas de interface.

Authentication	ISP Domains	Configurar domínios ISP de autenticação.
	RADIUS	Configurar esquemas RADIUS.
	TACACS	Configurar esquemas TACACS.
	Local Users	Configurar usuários locais.



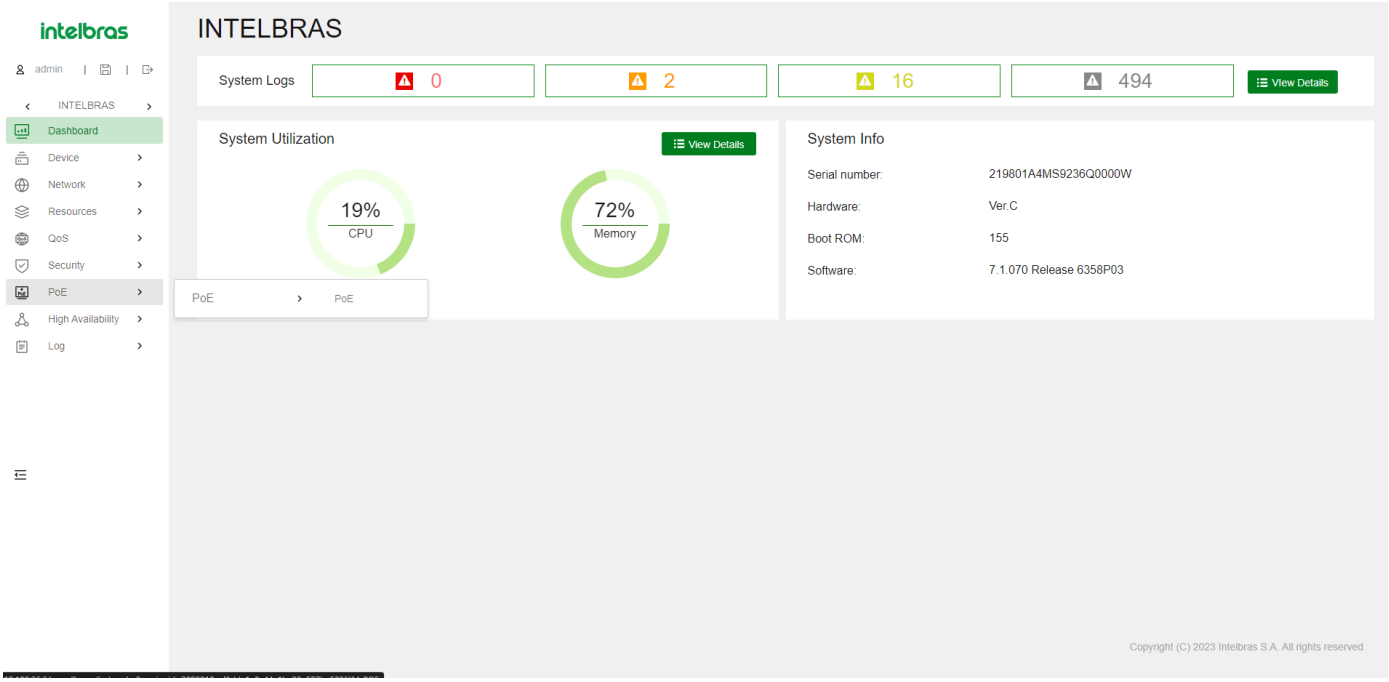
Menu PoE (Alimentação sobre Ethernet)

Este menu server apenas para os modelos PoE, S2328G-PA S2328G-PB e S2352G-PB.

Use a Tabela 8 para navegar nas tarefas que você pode executar a partir do menu PoE.

Tabela 8 - Navegador do Menu PoE

	Menus	Tarefas
PoE	PoE	Configurar a potência máxima PoE e o limite de alarme de potência para o dispositivo. Ativar ou desativar PoE em uma interface. Configurar a potência máxima PoE, a prioridade de fornecimento de energia, a descrição do PD e a descrição de falha para uma interface. Atualizar o firmware do PSE.

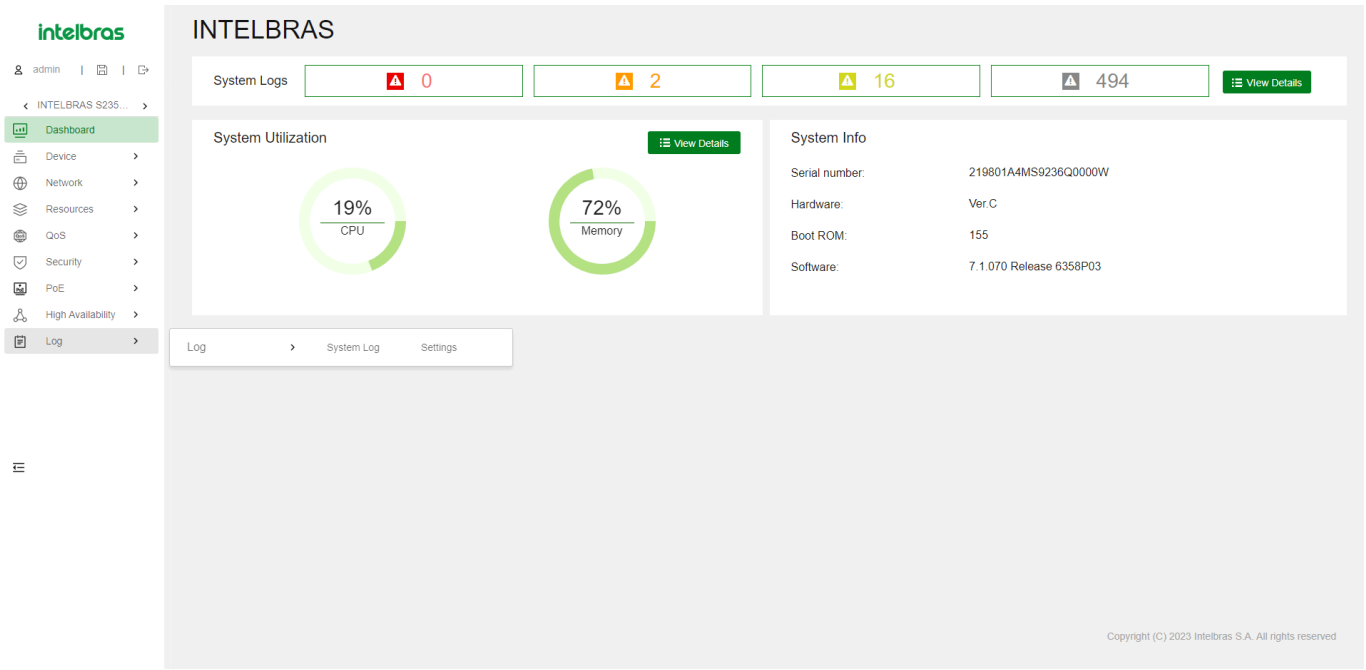


Menu de Logs

Use a Tabela 11 para navegar nas tarefas que você pode executar a partir do menu de Logs.

Tabela 11 - Navegador do Menu de Logs

	Menus	Tarefas
Log	System Log	Exibir informações de log. Consultar, coletar e excluir informações de log.
	Settings	Configurar destinos de saída de log. Ativar ou desativar a saída de log para o buffer de log e configurar o número máximo de logs no buffer. Configurar o endereço e número da porta dos hosts de log.



Gerenciamento de Dispositivos

Configurações

Acesse a página de **Configurações** para alterar o nome do dispositivo, localização e hora do sistema.

Hora do Sistema

A hora do sistema correta é essencial para o gerenciamento e comunicação em rede. Configure a hora do sistema corretamente antes de usar o dispositivo na rede.

O dispositivo pode usar a hora do sistema configurada manualmente ou obter a hora UTC de uma fonte de hora na rede e calcular a hora do sistema.

Quando usando a hora do sistema configurada localmente, o dispositivo utiliza os sinais de relógio gerados pelo seu oscilador de cristal interno para manter a hora do sistema.

Se você alterar o fuso horário ou as configurações de horário de verão sem alterar a data ou hora, o dispositivo ajusta a hora do sistema com base nas novas configurações.

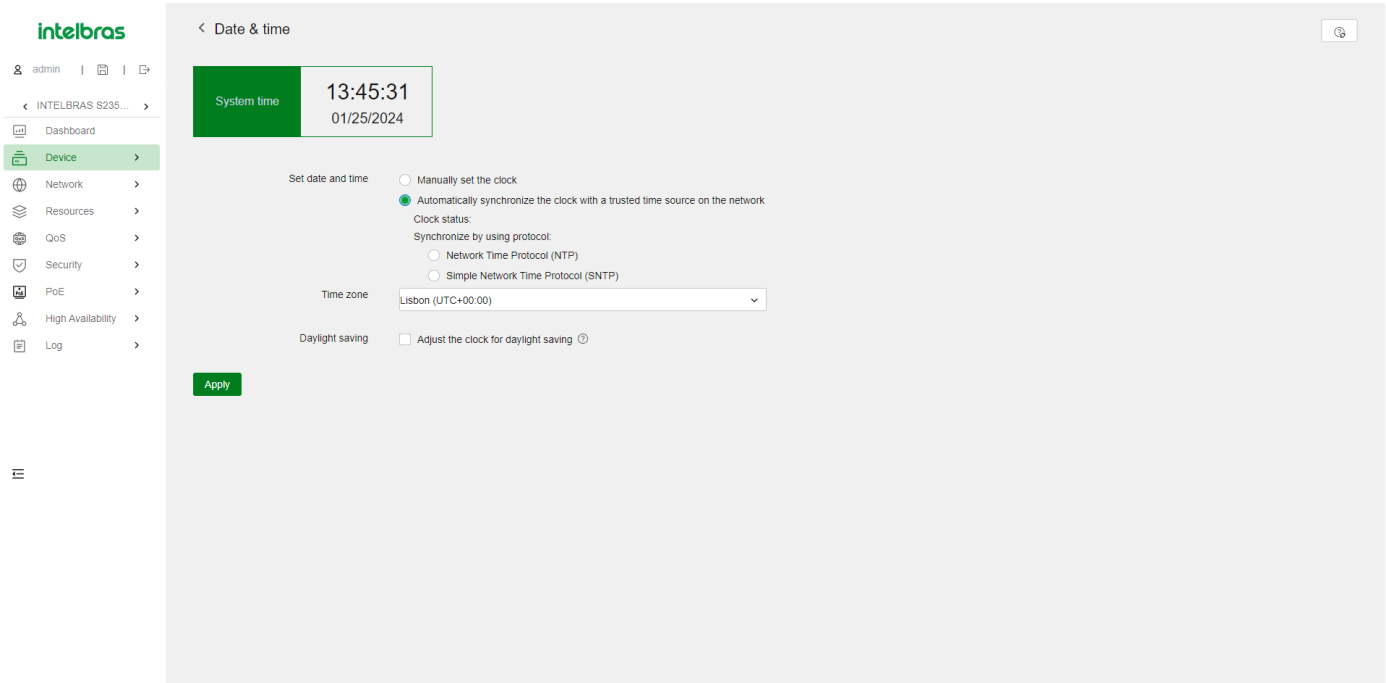
Após obter a hora UTC de uma fonte de hora, o dispositivo usa a hora UTC e as configurações de fuso horário e horário de verão para calcular a hora do sistema. Em seguida, o dispositivo sincroniza periodicamente a hora UTC e recalcula a hora do sistema.

Se você alterar o fuso horário ou as configurações de horário de verão, o dispositivo recalculará a hora do sistema.

A hora do sistema calculada a partir da hora UTC de uma fonte de hora é mais precisa.

Verifique se o fuso horário e as configurações de horário de verão correspondem aos parâmetros do local onde o dispositivo está localizado.

Se a hora do sistema não mudar conforme o período de horário de verão termina, atualize a interface da Web.



Protocolos de Sincronização de Relógio

O dispositivo suporta os seguintes protocolos de sincronização de relógio:

- **NTP** - Protocolo de Hora de Rede. O NTP é tipicamente usado em redes grandes para sincronizar dinamicamente o tempo entre dispositivos de rede. Ele fornece uma precisão de relógio superior à configuração manual da hora do sistema.
- **SNTP** - NTP Simples, uma implementação mais simples do NTP. O SNTP usa os mesmos formatos de pacote e procedimentos de troca que o NTP. No entanto, o SNTP simplifica o procedimento de sincronização de relógio. Comparado ao NTP, o SNTP utiliza menos recursos e implementa a sincronização de relógio em menos tempo, mas oferece uma precisão de tempo menor.

Modos de Operação NTP/SNTP

O NTP suporta dois modos de operação: modo cliente/servidor e modo ativo/passivo simétrico. O dispositivo pode atuar apenas como cliente no modo cliente/servidor ou como o par ativo no modo ativo/passivo simétrico.

O SNTP suporta apenas o modo cliente/servidor. O dispositivo pode atuar apenas como cliente.

Modos de Operação NTP/SNTP :

Modo	Processo de Funcionamento	Princípio	Cenário de Aplicação
Cliente/Servidor	1. Um cliente envia uma mensagem de sincronização de relógio para os servidores NTP. 2. Ao receber a mensagem, os servidores automaticamente entram no modo servidor e enviam uma resposta. 3. Se o cliente estiver sincronizado com vários servidores de hora, ele seleciona um relógio ideal e sincroniza seu relógio local com a fonte de referência ideal. Você pode configurar vários servidores de hora para um cliente. Este modo de operação requer que você especifique o endereço IP do servidor NTP no cliente.	Um cliente pode se sincronizar com um servidor, mas um servidor não pode se sincronizar com um cliente.	Este modo é destinado a cenários onde dispositivos de estrato superior se sincronizam com dispositivos de estrato inferior. É possível configurar vários servidores de tempo para um cliente. Este modo de operação requer que você especifique o endereço IP do servidor NTP no cliente.

Ativo/Passivo Simétrico	4. Um par ativo simétrico envia periodicamente mensagens de sincronização de relógio para um par passivo simétrico. 5. Um par ativo simétrico envia periodicamente mensagens de sincronização de relógio para um par passivo simétrico. 6. O par passivo simétrico opera automaticamente no modo passivo simétrico e envia uma resposta. 7. Se o par ativo simétrico puder se sincronizar com vários servidores de hora, ele seleciona um relógio ideal e sincroniza seu relógio local com a fonte de referência ideal. Este modo de operação requer que você especifique o endereço IP do par passivo simétrico no par ativo simétrico.	Um par ativo simétrico e um par passivo simétrico podem se sincronizar entre si. Se ambos estiverem sincronizados, o par com um estrato superior se sincroniza com o par de um estrato inferior.	Este modo é mais frequentemente usado entre servidores com o mesmo estrato para funcionar como backup um do outro. Se um servidor não conseguir se comunicar com todos os servidores de um estrato inferior, ele ainda poderá se sincronizar com os servidores do mesmo estrato. Este modo de operação requer que você especifique o endereço IP do par passivo simétrico no par ativo simétrico.

Autenticação da Fonte de Tempo NTP/SNTP

A função de autenticação da fonte de tempo permite que o dispositivo autentique os pacotes NTP ou SNTP recebidos. Essa função garante que o dispositivo obtenha o GMT correto.

Para uma autenticação bem-sucedida no modo cliente/servidor, você deve habilitar a autenticação tanto no cliente quanto no servidor e configurar o mesmo ID de chave e chave neles.

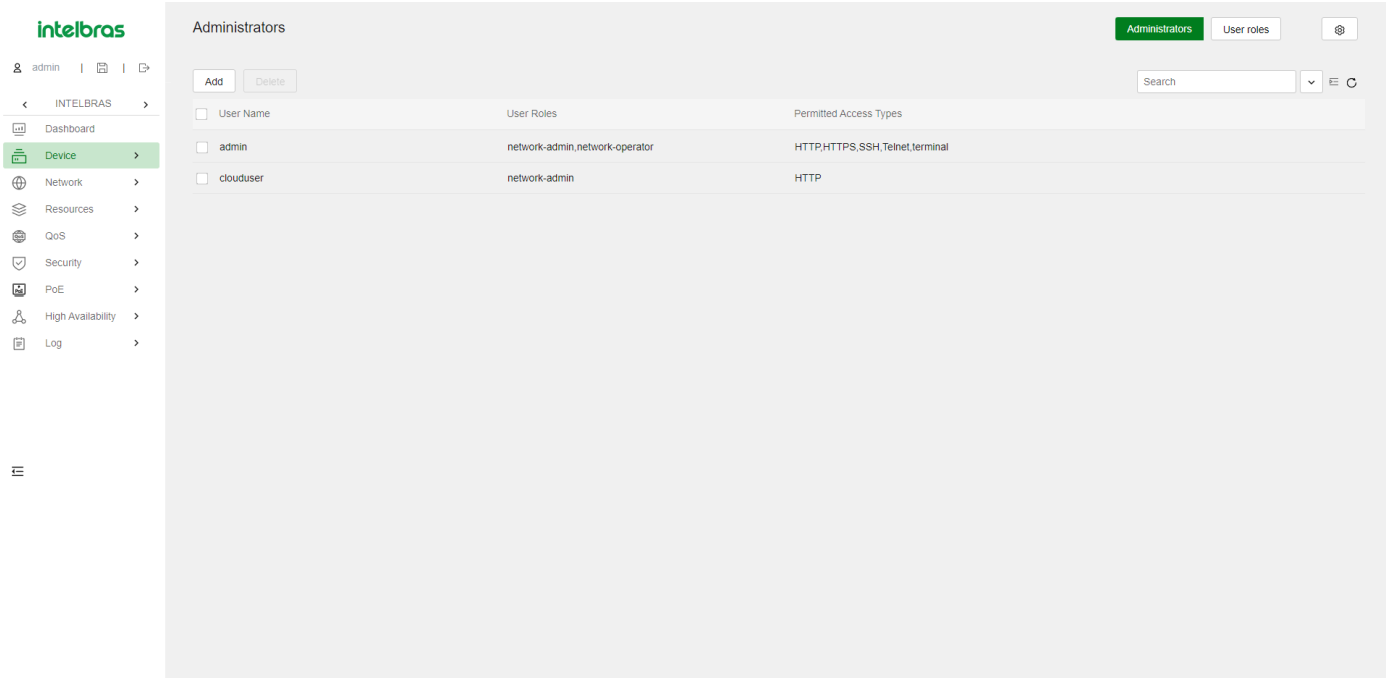
Para uma autenticação bem-sucedida no modo ativo/passivo simétrico, você deve habilitar a autenticação tanto nos pares ativos quanto nos pares passivos e configurar o mesmo ID de chave e chave neles.

Administradores

Um administrador configura e gerencia o dispositivo a partir dos seguintes aspectos:

- Gerenciamento de contas de usuário: Gerencia informações e atributos de contas de usuário (por exemplo, nome de usuário e senha).
- Controle de acesso com base em funções: Gerencia permissões de acesso do usuário com base na função do usuário.
- Controle de senha: Gerencia senhas de usuário e controla o status de login do usuário com base em políticas predefinidas.

O tipo de serviço de um administrador pode ser SSH, Telnet, FTP, HTTP, HTTPS ou terminal.



Gerenciamento de Contas de Usuário

Uma conta de usuário no dispositivo gerencia atributos para usuários que fazem login no dispositivo com o mesmo nome de usuário. Os atributos incluem nome de usuário, senha, serviços e parâmetros de controle de senha.

Controle de Acesso com Base em Funções

Atribua funções de usuário aos usuários para controlar o acesso dos usuários a funções e recursos do sistema. Atribuir permissões a uma função de usuário inclui o seguinte:

- Define um conjunto de regras para determinar funções acessíveis ou inacessíveis para a função de usuário.
- Configura políticas de acesso a recursos para especificar quais interfaces, VLANs e instâncias VRF são acessíveis para a função de usuário.

Para configurar uma função relacionada a um recurso (uma interface ou VLAN), a função de usuário deve ter acesso tanto à função quanto ao recurso.

Regras de Função de Usuário

Regras de função de usuário permitem ou negam o acesso a funções específicas. Na interface web, uma regra de função de usuário controla o acesso a elementos específicos em páginas da web. As páginas da web são organizadas em menus web estruturados em árvore. Você pode controlar o acesso aos menus web com base nos seguintes atributos:

- Leitura: Menus web que exibem informações de configuração e manutenção.
- Escrita: Menus web que configuram o recurso no sistema.
- Execução: Menus web que executam funções específicas.

Uma função de usuário pode acessar o conjunto de menus web permitidos especificados nas regras de função de usuário.

Políticas de Acesso a Recursos

Políticas de acesso a recursos controlam o acesso de funções de usuário a recursos do sistema e incluem os seguintes tipos:

- Política de interface: Controla o acesso a interfaces.
- Política de VLAN: Controla o acesso a VLANs.

Você pode realizar as seguintes tarefas em uma interface ou VLAN acessível:

- Criar ou remover a interface ou VLAN.

- Configurar atributos para a interface ou VLAN.
- Aplicar a interface ou VLAN a outros parâmetros.

Funções de Usuário Predefinidas

O sistema fornece funções de usuário predefinidas. Essas funções de usuário têm acesso a todos os recursos do sistema (interfaces, VLANs e instâncias VRF). Suas permissões de acesso são diferentes.

Se as funções de usuário predefinidas não atenderem aos requisitos de acesso, você pode definir novas funções de usuário para controlar as permissões de acesso dos usuários.

> O perfil de usuário security-audit tem acesso apenas aos menus de registro de segurança. Os menus de registro de segurança não são suportados na interface web atual, portanto, não atribua o perfil de usuário security-audit a nenhum usuário.

Atribuição de Perfis de Usuário

Dependendo do método de autenticação, a atribuição de perfil de usuário tem os seguintes métodos:

- Autorização local - Se o usuário passar na autorização local, o dispositivo atribuirá os perfis de usuário especificados na conta de usuário local.
- Autorização remota - Se o usuário passar na autorização remota, o servidor AAA remoto atribuirá os perfis de usuário especificados no servidor.

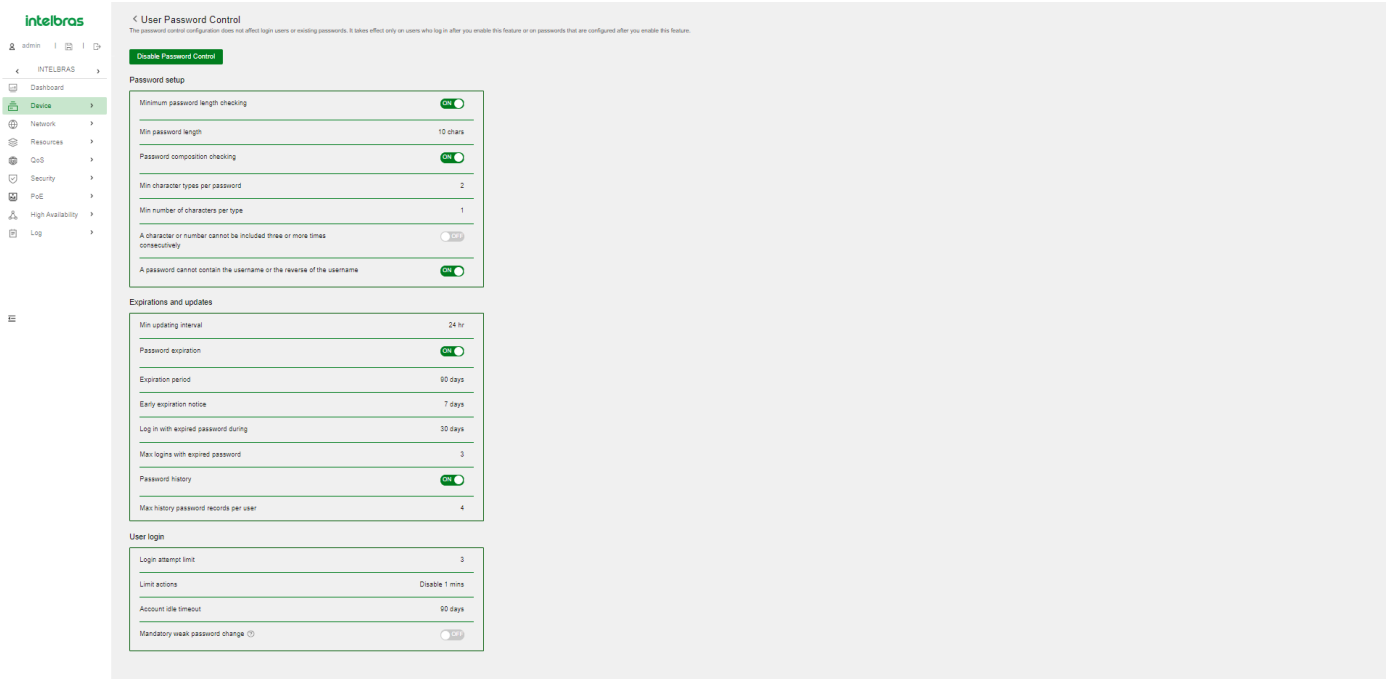
Um usuário que não obtém um perfil de usuário é desconectado do dispositivo. Se vários perfis de usuário forem atribuídos a um usuário, o usuário poderá usar o conjunto de funções e recursos acessíveis a todos os perfis de usuário.

Controle de Senha

O controle de senha permite implementar as seguintes funcionalidades:

- Gerenciar configurações de senha de login e super senha, expirações e atualizações para usuários de gerenciamento de dispositivo.
- Controlar o status de login do usuário com base em políticas predefinidas.

Os usuários locais são divididos em dois tipos: usuários de gerenciamento de dispositivo e usuários de acesso à rede. Esta funcionalidade se aplica apenas aos usuários de gerenciamento de dispositivo.



Comprimento Mínimo da Senha

Você pode definir o comprimento mínimo das senhas de usuário. Se um usuário inserir uma senha mais curta que o comprimento mínimo, o sistema rejeitará a senha.

Política de Composição de Senha

Uma senha pode ser uma combinação de caracteres dos seguintes tipos:

- Letras maiúsculas de A a Z.
- Letras minúsculas de a a z.
- Dígitos de 0 a 9.
- Caracteres especiais. Consulte a Tabela 15.

Aqui estão alguns exemplos de caracteres especiais:

Nome do Caractere	Símbolo	Nome do Caractere	Símbolo
Menos	-	Porcentagem	%
Mais	+	Cerquilha	#
Aspas Duplas	"	Sinal de Maior	>
Chave Direita	}	Colchete Direito	]
Parêntese Direito	)	Ponto e Vírgula	;
Barra	/	Til	~
Sublinhado	_	Barra Vertical	|

Com base nos requisitos de segurança do sistema, você pode definir o número mínimo de tipos de caracteres que uma senha deve conter e o número mínimo de caracteres para cada tipo, como mostrado na - Política de composição de senha.

Nível de Combinação de Senha	Número Mínimo de Tipos de Caracteres	Número Mínimo de Caracteres para Cada Tipo
Nível 1	Um	Um
Nível 2	Dois	Um
Nível 3	Três	Um
Nível 4	Quatro	Um

No modo não-FIPS, todos os níveis de combinação estão disponíveis para uma senha. No modo FIPS, apenas o nível 4 de combinação está disponível para uma senha. Quando um usuário define ou altera uma senha, o sistema verifica se a senha atende ao requisito de combinação. Se a senha não atender ao requisito, a operação falhará.

Política de Verificação de Complexidade de Senha

Uma senha menos complexa, como uma senha que contenha o nome de usuário ou caracteres repetidos, tem mais chances de ser quebrada. Para uma segurança mais alta, você pode configurar uma política de verificação de complexidade de senha para garantir que todas as senhas dos usuários sejam relativamente complexas. Com essa política configurada, quando um usuário configura uma senha, o sistema verifica a complexidade da senha. Se a senha não for complexa o suficiente, a configuração falhará.

Controle de Login com Senha Fraca

O sistema verifica senhas fracas para usuários de gerenciamento de dispositivo Telnet, SSH, HTTP ou HTTPS. Uma senha é considerada fraca se não atender aos seguintes requisitos:

- Restrição de composição de senha.
- Restrição de comprimento mínimo de senha.
- Verificação de nome de usuário.

Dependendo dos requisitos de segurança do sistema, você pode definir o número mínimo de tipos de caracteres que uma senha deve conter e o número mínimo de caracteres para cada tipo, conforme mostrado na .

Política de Composição de Senhas

Primeiro Login com Nome de Usuário e Senha Padrão

As configurações padrão de fábrica incluem um nome de usuário e senha padrão. Se o dispositivo iniciar com as configurações padrão de fábrica, os usuários de gerenciamento de dispositivo Telnet, SSH, HTTP ou HTTPS devem alterar a senha padrão no primeiro login antes de acessar o sistema.

Atualização de Senha

Essa função permite definir o intervalo mínimo em que os usuários podem alterar suas senhas. Se um usuário fizer login para alterar a senha, mas o tempo decorrido desde a última alteração for menor que esse intervalo, o sistema negará a solicitação. Por exemplo, se você definir esse intervalo para 48 horas, um usuário não poderá alterar a senha duas vezes em 48 horas.

Expiração de Senha

A expiração de senha impõe um ciclo de vida a uma senha de usuário. Após a expiração da senha, o usuário precisa alterar a senha.

Se um usuário inserir uma senha expirada durante o login, o sistema exibirá uma mensagem de erro. O usuário será solicitado a fornecer uma nova senha e confirmá-la digitando-a novamente. A nova senha deve ser válida, e o usuário deve inserir exatamente a mesma senha ao confirmá-la.

Notificação Antecipada de Expiração de Senha Pendente

Quando um usuário faz login, o sistema verifica se a senha expirará em um período igual ou menor ao período de notificação especificado. Se for esse o caso, o sistema notifica o usuário quando a senha expirará e oferece a opção de alterar a senha. Se o usuário definir uma nova senha que esteja em conformidade com a complexidade da senha, o sistema registrará a nova senha e o horário de configuração. Se o usuário optar por não alterar a senha ou falhar na alteração, o sistema permitirá que o usuário faça login usando a senha atual.

Entrar com Senha Expirada

Você pode permitir que um usuário faça login um certo número de vezes dentro de um período de tempo após a expiração da senha. Por exemplo, se você definir o número máximo de logins com senha expirada para 3 e o período de tempo para 15 dias, um usuário pode fazer login três vezes dentro de 15 dias após a senha expirar.

Histórico de Senhas

Com essa funcionalidade habilitada, o sistema armazena as senhas que um usuário usou. Quando um usuário altera a senha, o sistema verifica se a nova senha é diferente da atual e daquelas armazenadas nos registros de histórico de senha por pelo menos quatro caracteres. Os quatro caracteres devem ser diferentes entre si. Caso contrário, o sistema exibirá uma mensagem de erro, e a senha não será alterada.

Você pode definir o número máximo de registros de histórico de senha que o sistema deve manter para cada usuário. Quando o número de registros de histórico de senha excede a sua configuração, o registro mais recente sobrescreve o mais antigo.

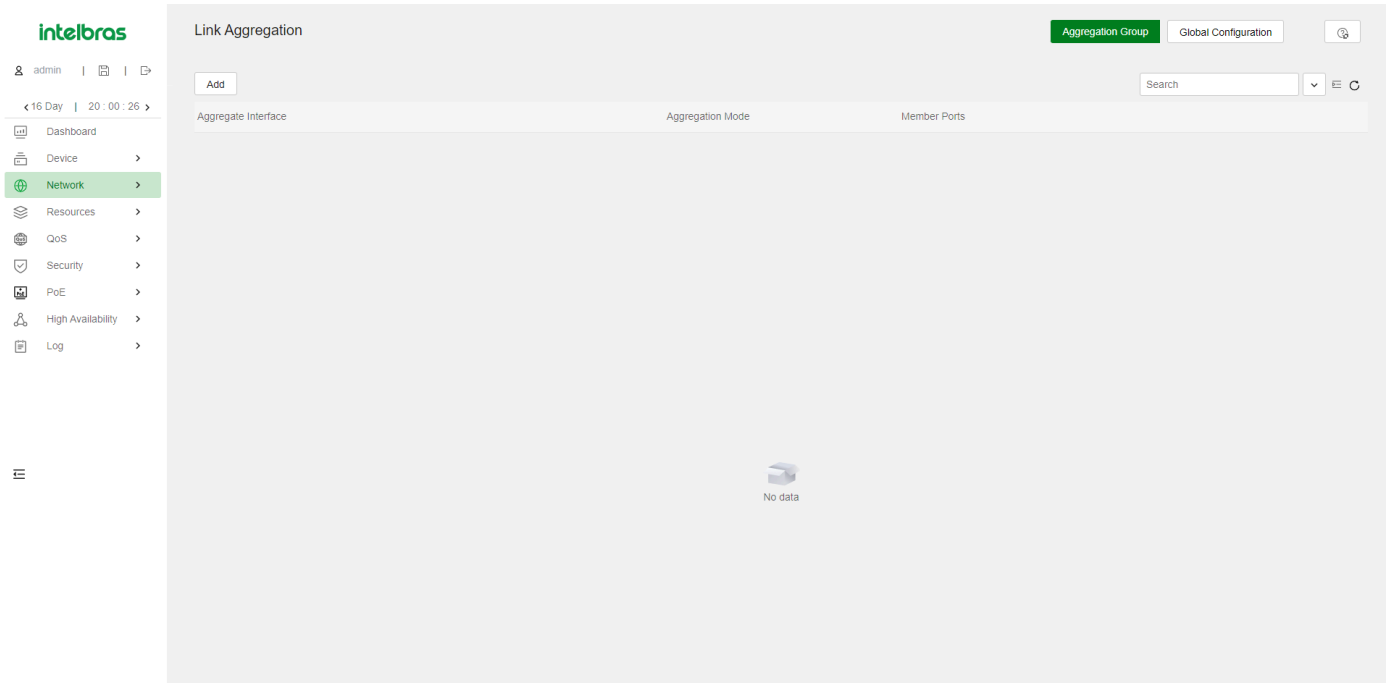
As senhas de login atuais dos usuários de gerenciamento de dispositivos não são armazenadas no histórico de senhas, porque a senha do usuário de gerenciamento de dispositivos é salva em texto cifrado e não pode ser recuperada para uma senha em texto simples.

Recursos de Serviços de Rede

Link Aggregation

Link aggregation combina várias conexões Ethernet físicas em uma única conexão lógica, chamada de link agregado. Link aggregation oferece os seguintes benefícios:

- Aumento da largura de banda além dos limites de uma única conexão. Em um link agregado, o tráfego é distribuído entre as portas de membros.
- Melhor confiabilidade na conexão. As portas de membros se complementam dinamicamente. Quando uma porta de membro falha, o tráfego é automaticamente redirecionado para outras portas de membros.



Grupo de Agregação

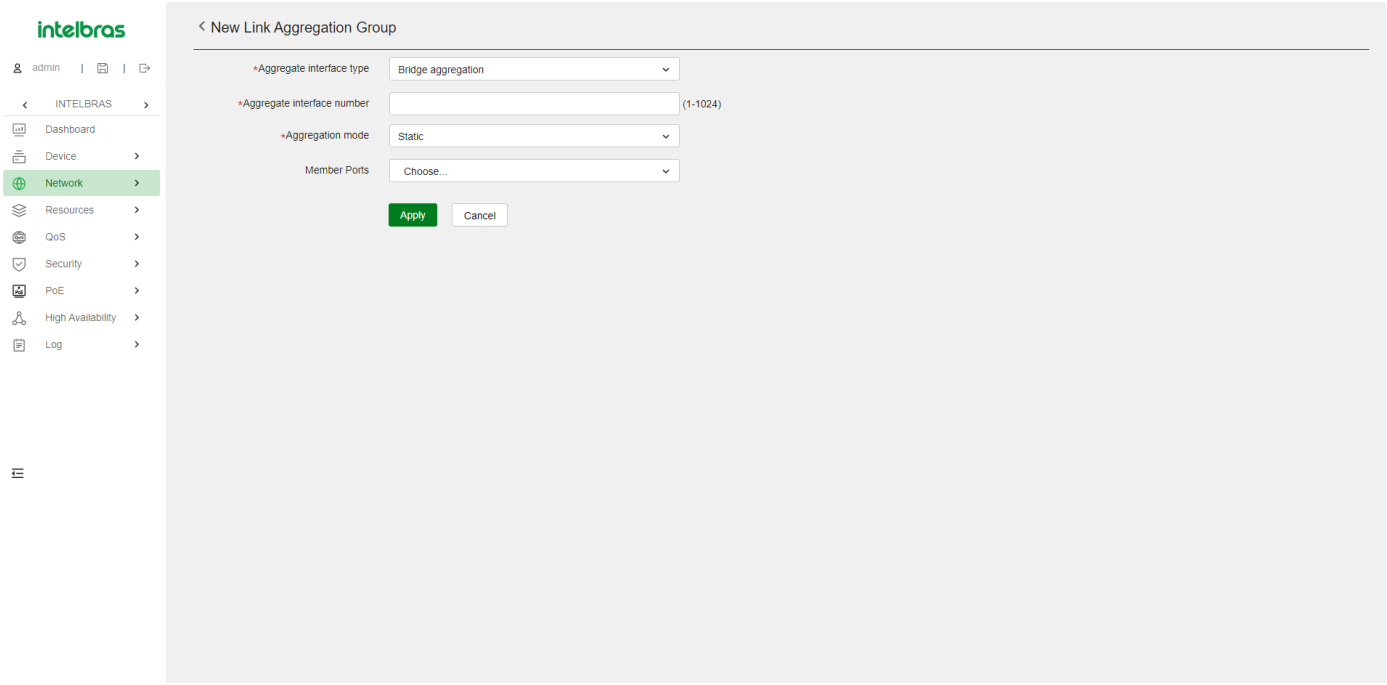
O agrupamento de links é implementado por meio do agrupamento de interfaces. Um grupo de agregação é um conjunto de interfaces Ethernet agrupadas. Essas interfaces Ethernet são conhecidas como portas de membros do grupo de agregação. Cada grupo de agregação possui uma interface lógica correspondente (chamada de interface agregada).

Ao criar uma interface agregada, o dispositivo cria automaticamente um grupo de agregação do mesmo tipo e número que a interface agregada. Por exemplo, ao criar a interface agregada de Camada 2 número 1, o grupo de agregação de Camada 2 número 1 é criado.

Uma interface agregada pode ser de um dos seguintes tipos:

- Camada 2—As portas de membros em um grupo de agregação de Camada 2 podem ser apenas interfaces Ethernet de Camada 2.
- Camada 3—As portas de membros em um grupo de agregação de Camada 3 podem ser apenas interfaces Ethernet de Camada 3.

A taxa de porta de uma interface agregada é igual à taxa total de suas portas de membros Selecionadas. O modo de duplexação é o mesmo que o das portas de membros Selecionadas.



Estados de Agregação das Portas em um Grupo de Agregação

Uma porta de membro em um grupo de agregação pode estar em qualquer um dos seguintes estados de agregação:

- Selecionada—Uma porta Selecionada pode encaminhar tráfego.
- Não Selecionada—Uma porta Não Selecionada não pode encaminhar tráfego.

Chave Operacional

Ao agregar portas, o sistema atribui automaticamente a cada porta uma chave operacional com base em informações da porta, como taxa da porta e modo de duplexação. Qualquer alteração nessas informações aciona um recálculo da chave operacional.

Configurações de Atributo

Para se tornar uma porta Selecionada, uma porta de membro deve ter as mesmas configurações de atributo que a interface agregada.

Considerações sobre Recursos

Isolamento de Porta—Indica se a porta se juntou a um grupo de isolamento e a que grupo de isolamento a porta pertence.

VLAN

As configurações de atributo da VLAN incluem:

- IDs de VLAN permitidos.
- PVID (ID da VLAN da Porta).
- Modo de marcação de VLAN.

Modos de Agregação de Links

Um grupo de agregação opera em um dos seguintes modos:

- Estático—A agregação estática é estável. Um grupo de agregação em modo estático é chamado de grupo de agregação estático. Os estados de agregação das portas de membros em um grupo de agregação estático não são afetados pelas portas pares.
- Dinâmico—Um grupo de agregação em modo dinâmico é chamado de grupo de agregação dinâmico. O sistema local e o sistema par têm automaticamente os estados de agregação das portas de membros por meio do LACP, o que reduz a carga de trabalho dos administradores.

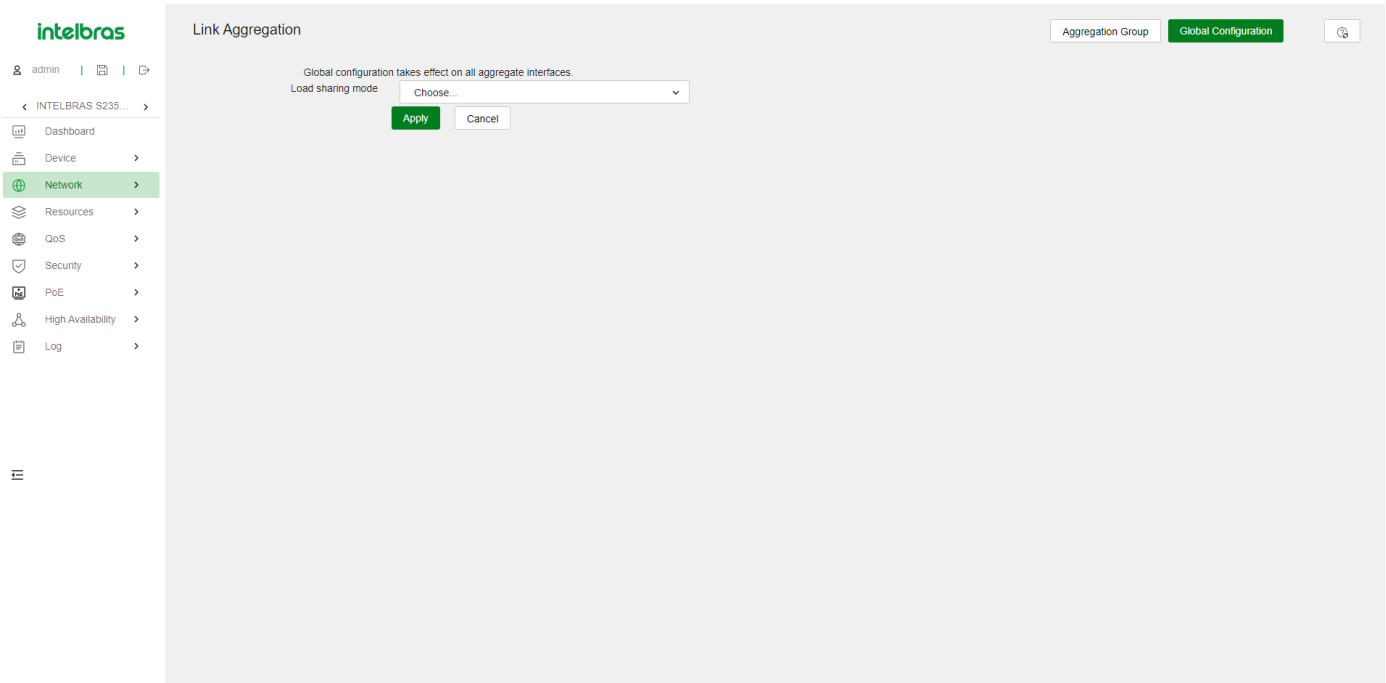
Modos Globais de Compartilhamento de Carga

Em um grupo de agregação de links, o tráfego pode ser compartilhado entre as portas Selecionadas com base em qualquer um dos seguintes modos:

- Compartilhamento de carga por fluxo — Distribui o tráfego com base em fluxos.

  O modo de compartilhamento de carga classifica os pacotes em fluxos e encaminha os pacotes do mesmo fluxo na mesma conexão. Este modo pode ser baseado em um ou uma combinação dos seguintes critérios de classificação de tráfego:

- IP de Origem.
- IP de Destino.
- MAC de Origem.
- MAC de Destino.
- Compartilhamento de carga por pacote — Distribui o tráfego por pacote.
- Compartilhamento de carga automático — Seleciona automaticamente um modo de compartilhamento de carga dependendo do tipo de pacote.



Storm control

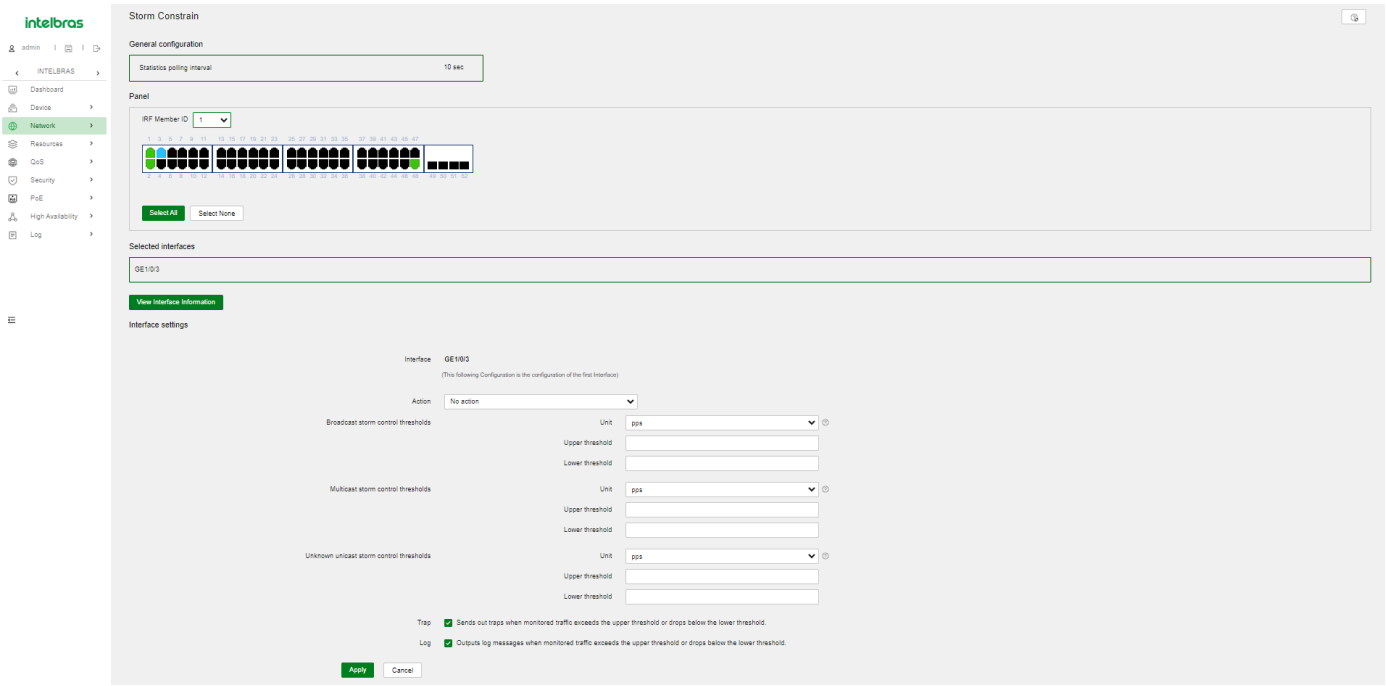
O Storm control compara o tráfego de broadcast, multicast e unicast desconhecido regularmente com os respectivos limites de tráfego em uma interface Ethernet. Para cada tipo de tráfego, o Storm control fornece um limite inferior e um limite superior. Dependendo da sua configuração, quando um determinado tipo de tráfego excede o limite superior, a interface executa uma das seguintes ações:

- Nenhuma ação—Não executa nenhuma ação na interface.
- Bloqueio — Bloqueia esse tipo de tráfego e encaminha outros tipos de tráfego. Mesmo que a interface não encaminhe o tráfego bloqueado, ela ainda conta o tráfego. Quando o tráfego bloqueado cai abaixo do limite inferior, a interface começa a encaminhar o tráfico.
- Desligamento — A interface é desativada automaticamente e para de encaminhar qualquer tráfego. Quando o tráfego bloqueado cai abaixo do limite inferior, a interface não volta a ser ativada automaticamente. Para ativar a interface, ative-a manualmente ou desative a função de Storm control.

  É possível configurar uma interface Ethernet para emitir armadilhas de eventos de limite e mensagens de log quando o tráfego monitorado atende a uma das seguintes condições:

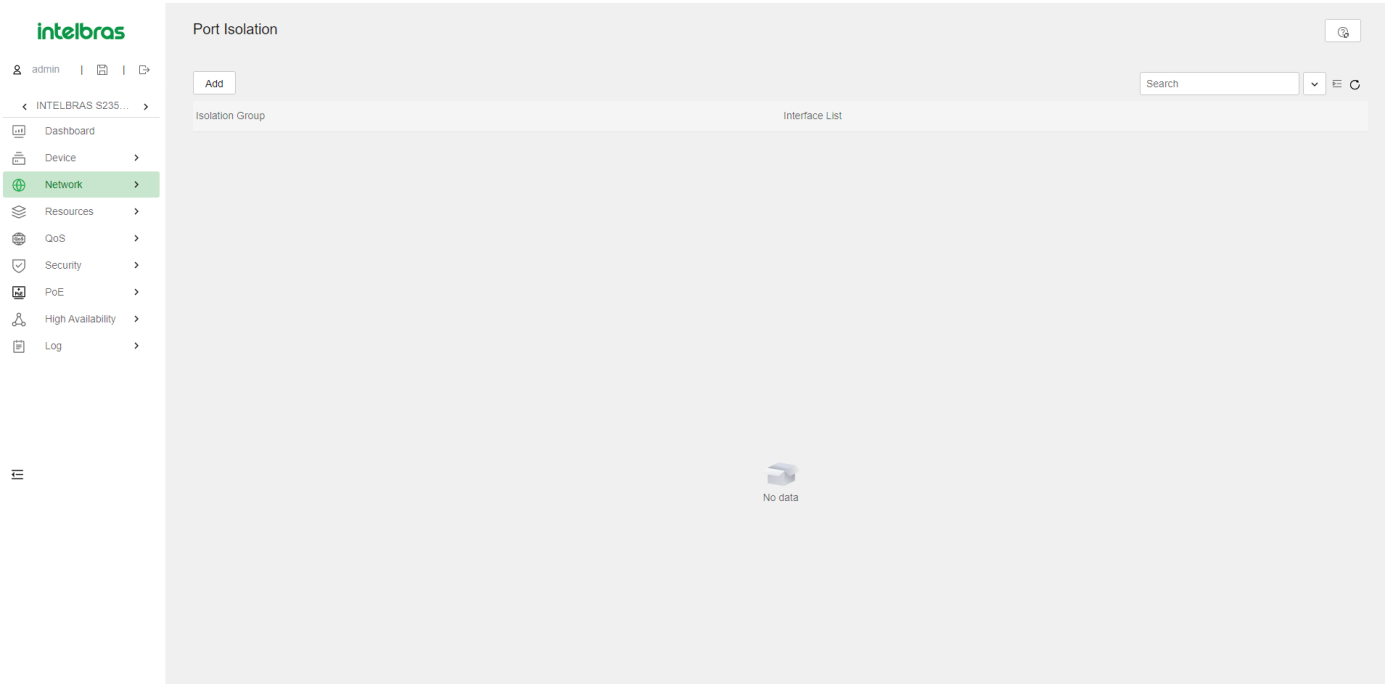
- Excede o limite superior.

- Desce abaixo do limite inferior.



Isolamento de Porta

O recurso de isolamento de porta isola o tráfego da Camada 2 para garantir a privacidade e a segurança de dados sem o uso de VLANs. As portas em um grupo de isolamento não podem se comunicar entre si. No entanto, elas podem se comunicar com portas fora do grupo de isolamento.



VLAN

A tecnologia de Rede Local Virtual (VLAN) divide uma LAN em várias LANs lógicas, chamadas de VLANs. Cada VLAN é um domínio de broadcast. Dispositivos na mesma VLAN podem se comunicar diretamente entre si. Dispositivos em VLANs diferentes são isolados uns dos outros na Camada 2.

VLANs Baseadas em Porta

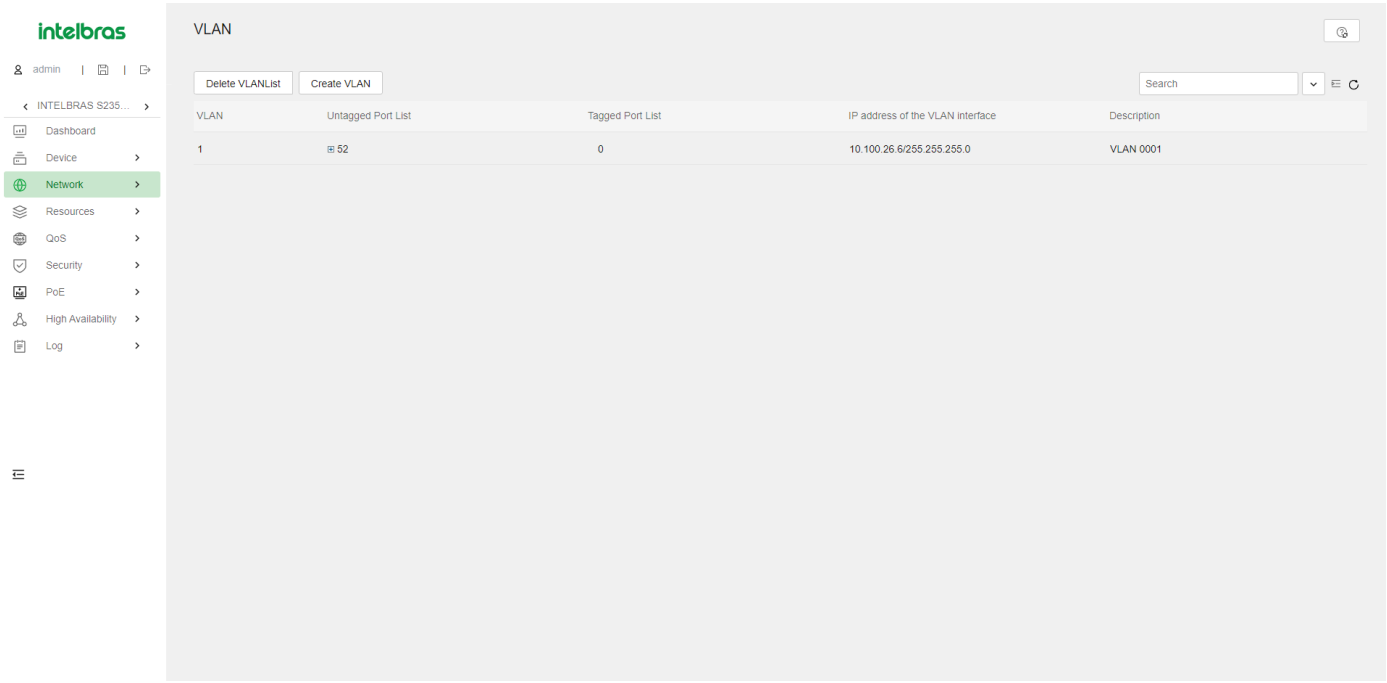
As VLANs baseadas em porta agrupam membros de VLANs por porta. Uma porta encaminha pacotes de uma VLAN somente após ser atribuída à VLAN. É possível configurar uma porta como uma porta desmarcada ou marcada de uma VLAN.

- Para configurar a porta como uma porta desmarcada de uma VLAN, atribua-a à lista de portas desmarcadas da VLAN. A porta desmarcada de uma VLAN encaminha pacotes da VLAN sem marcadores de VLAN.

- Para configurar a porta como uma porta marcada de uma VLAN, atribua-a à lista de portas marcadas da VLAN. A porta marcada de uma VLAN encaminha pacotes da VLAN com marcadores de VLAN.

  É possível configurar o tipo de link de uma porta como acesso, tronco ou híbrido. Portas de diferentes tipos de link utilizam métodos diferentes de manipulação de marcadores de VLAN.

- Acesso—Uma porta de acesso pode encaminhar pacotes de apenas uma VLAN e enviá-los sem marcadores. Atribua uma porta de acesso somente à lista de portas desmarcadas de uma VLAN.
- Tronco—Uma porta de tronco pode encaminhar pacotes de várias VLANs. Exceto pacotes do ID de VLAN da porta (PVID), pacotes enviados de uma porta de tronco são marcados com VLAN. Atribua uma porta de tronco à lista de portas desmarcadas do PVID da porta e à lista de portas marcadas de outras VLANs.
- Híbrido—Uma porta híbrida pode encaminhar pacotes de várias VLANs. É possível atribuir uma porta híbrida à lista de portas desmarcadas de algumas VLANs e à lista de portas marcadas de outras VLANs. Uma porta híbrida desmarcada de uma VLAN encaminha pacotes da VLAN sem marcadores de VLAN. Uma porta híbrida marcada de uma VLAN encaminha pacotes da VLAN com marcadores de VLAN.



Interface de VLAN

Para permitir que dispositivos de VLANs diferentes se comuniquem na Camada 3, é possível usar interfaces de VLAN. As interfaces de VLAN são interfaces virtuais usadas para a comunicação na Camada 3 entre diferentes VLANs. Elas não existem como entidades físicas nos dispositivos. Para cada VLAN, é possível criar uma interface de VLAN e atribuir a ela um endereço IP. A interface de VLAN age como o gateway da VLAN para encaminhar pacotes destinados a outro sub-rede IP.

Voice VLAN

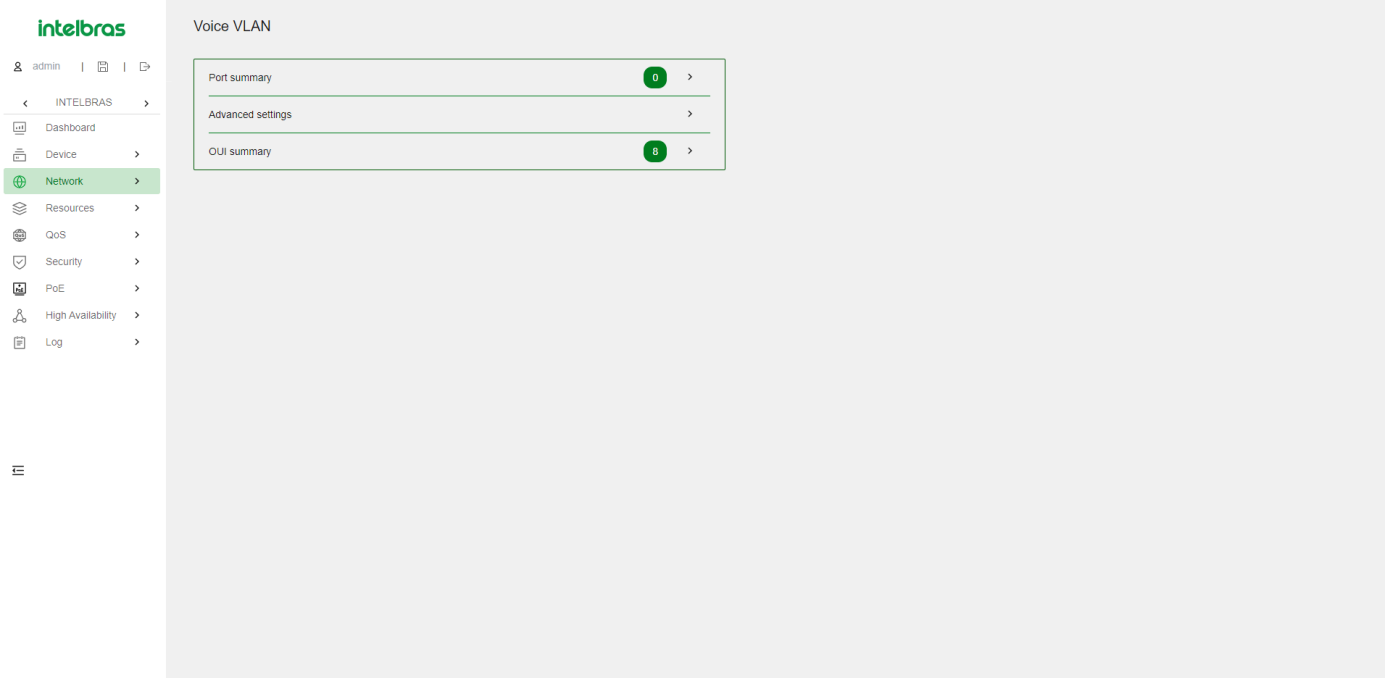
Uma Voice Vlan é usada para transmitir tráfego de voz. O dispositivo pode configurar parâmetros de QoS para pacotes de voz para garantir maior prioridade de transmissão para esses pacotes.

Endereços OUI

Um dispositivo identifica pacotes de voz com base em seus endereços MAC de origem. Um pacote cujo endereço MAC de origem esteja em conformidade com um endereço OUI (Identificador Único da Organização) do dispositivo é considerado um pacote de voz. Os endereços OUI são resultados lógicos AND de endereços MAC e máscaras OUI. A tabela a seguir mostra os endereços OUI padrão.

Número	Endereço OUI	Fabricante
1	0001-E300-0000	Telefone Siemens
2	0003-6B00-0000	Telefone Cisco

3	0004-0D00-0000	Telefone Avaya
4	000F-E200-0000	Telefone Intelbras Aolynk
5	0060-B900-0000	Telefone Philips/NEC
6	00D0-1E00-0000	Telefone Pingtel
7	00E0-7500-0000	Telefone Polycom
8	00E0-BB00-0000	Telefone 3Com



Modo de Configuração de Prioridade de QoS para Tráfego de Voz

As configurações de prioridade de QoS transportadas no tráfego de voz incluem os valores CoS e DSCP. É possível configurar o dispositivo para confiar ou modificar as configurações de prioridade de QoS para o tráfego de voz. Se o dispositivo confia nas configurações de prioridade de QoS em pacotes de Voice Vlan de entrada, o dispositivo não modifica seus valores CoS e DSCP.

Modos de Atribuição de Voice Vlan

Uma porta pode ser atribuída automaticamente ou manualmente a uma Voice Vlan.

Modo Automático

Quando um telefone IP é ligado, ele envia pacotes de protocolo. Após receber esses pacotes de protocolo, o dispositivo usa o endereço MAC de origem dos pacotes de protocolo para fazer correspondência com seus endereços OUI. Se a correspondência for bem-sucedida, o dispositivo realiza as seguintes operações:

- Atribui a porta receptora dos pacotes de protocolo à Voice Vlan.
- Emite regras de ACL e define a precedência do pacote.
- Inicia o temporizador de envelhecimento da Voice Vlan.

Se nenhum pacote de voz for recebido da porta antes que o temporizador de envelhecimento expire, o dispositivo removerá a porta da Voice Vlan. O temporizador de envelhecimento também é configurável.

Modo Manual

É necessário atribuir manualmente a porta que se conecta ao telefone IP a uma Voice Vlan. O dispositivo usa o endereço MAC de origem dos pacotes de voz recebidos para fazer correspondência com seus endereços OUI. Se a correspondência for bem-sucedida, o dispositivo emite regras de ACL e define a precedência do pacote.

Modo de Segurança e Modo Normal de Voice Vlan

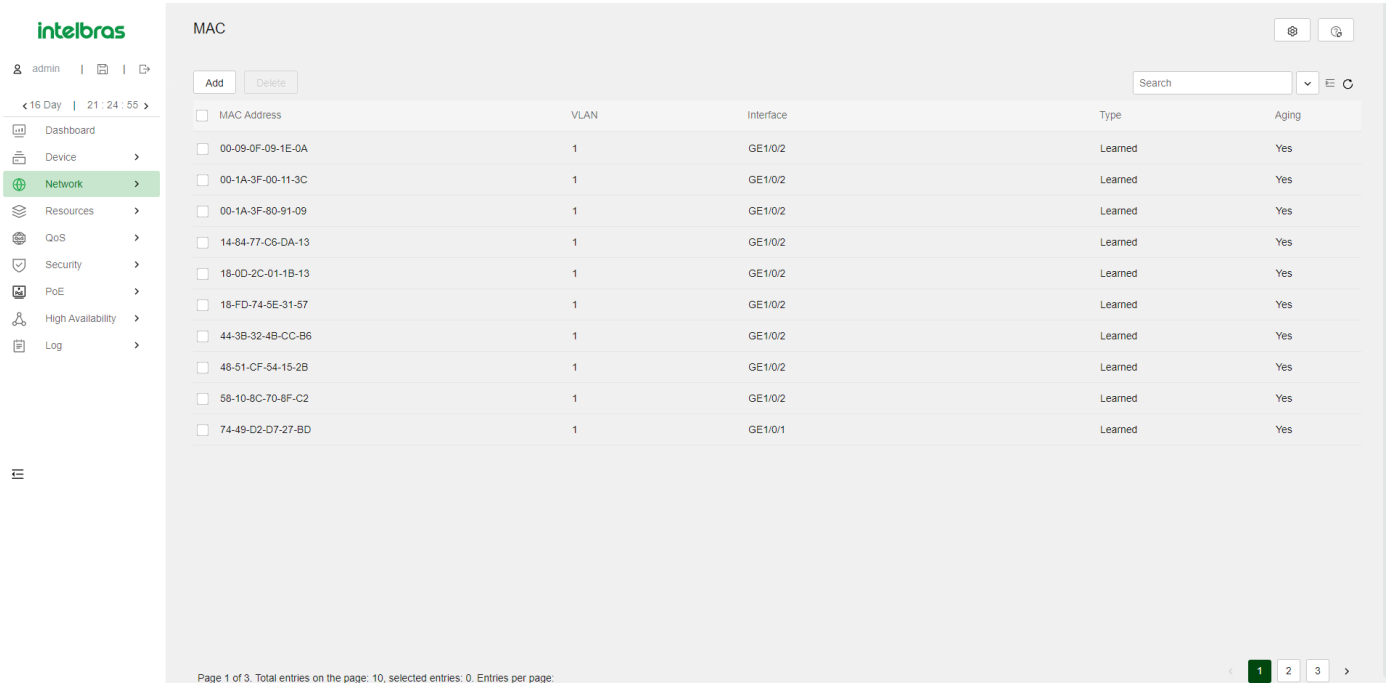
Dependendo dos mecanismos de filtragem de pacotes de entrada, uma porta habilitada para Voice Vlan pode operar em um dos seguintes modos:

- Modo Normal—A porta recebe pacotes marcados com Voice Vlan e os encaminha na Voice Vlan sem examinar seus endereços MAC. Se o PVID da porta for a Voice Vlan e a porta operar no modo de atribuição de VLAN manual, a porta encaminhará todos os pacotes não marcados recebidos na Voice Vlan.
- Modo de Segurança—A porta usa os endereços MAC de origem dos pacotes recebidos para fazer correspondência com os endereços OUI do dispositivo. Os pacotes que não correspondem serão descartados.

MAC (Endereço de Controle de Acesso à Mídia)

Um dispositivo Ethernet utiliza uma tabela de endereços MAC para encaminhar quadros. Uma entrada de endereço MAC inclui um endereço MAC de destino, uma interface de saída (ou egress RB) e um ID de VLAN. Quando o dispositivo recebe um quadro, ele usa o endereço MAC de destino do quadro para procurar uma correspondência na tabela de endereços MAC.

- O dispositivo encaminha o quadro para a interface de saída na entrada correspondente se encontrar uma correspondência.
- O dispositivo faz um flood do quadro na VLAN do quadro se não encontrar correspondência.



Tipos de Entradas de Endereços MAC

Uma tabela de endereços MAC pode conter os seguintes tipos de entradas:

- Entradas Dinâmicas—Uma entrada dinâmica pode ser configurada manualmente ou aprendida dinamicamente para encaminhar quadros com um endereço MAC de destino específico pela interface associada. Uma entrada dinâmica pode expirar. Uma entrada dinâmica configurada manualmente tem a mesma prioridade que uma aprendida dinamicamente.
- Entradas Estáticas—Uma entrada estática é adicionada manualmente para encaminhar quadros com um endereço MAC de destino específico pela interface associada, e ela nunca expira. Uma entrada estática tem prioridade mais alta do que uma entrada aprendida dinamicamente.
- Entradas de Buraco Negro—Uma entrada de buraco negro é configurada manualmente e nunca expira. Uma entrada de buraco negro é configurada para filtrar quadros com um endereço MAC de origem ou de destino específico. Por exemplo, para bloquear todos os quadros destinados a um usuário, é possível configurar o endereço MAC do usuário como uma entrada de endereço de buraco negro.
- Entradas de Segurança—Uma entrada de segurança pode ser configurada manualmente ou aprendida dinamicamente para encaminhar quadros com um endereço MAC específico pela interface associada. Uma entrada de segurança nunca expira.

Temporizador de Envelhecimento para Entradas de Endereços MAC Dinâmicos

Para segurança e uso eficiente do espaço na tabela, a tabela de endereços MAC utiliza um temporizador de envelhecimento para entradas dinâmicas aprendidas em todas as interfaces. Se uma entrada de endereço MAC dinâmica não for atualizada antes que o temporizador de envelhecimento expire, o dispositivo exclui a entrada. Esse mecanismo de envelhecimento garante que a tabela de endereços MAC possa ser atualizada prontamente para acomodar as alterações mais recentes na topologia da rede.

Para uma rede estável, é necessário um intervalo de envelhecimento mais longo, enquanto uma rede instável requer um intervalo de envelhecimento mais curto. Um intervalo de envelhecimento muito longo pode fazer com que a tabela de endereços MAC retenha entradas desatualizadas. Como resultado, os recursos da tabela de endereços MAC podem se esgotar, e a tabela de endereços MAC pode não ser atualizada para acomodar as alterações mais recentes na rede. Um intervalo muito curto pode resultar na remoção de entradas válidas, o que causaria inundações desnecessárias e afetaria possivelmente o desempenho do dispositivo. Para reduzir as inundações em uma rede estável, defina um temporizador de envelhecimento longo ou desative o temporizador para evitar que as entradas dinâmicas envelheçam desnecessariamente. A redução das inundações melhora o desempenho da rede. A redução das inundações também melhora a segurança, pois reduz as chances de um quadro de dados atingir destinos não desejados.

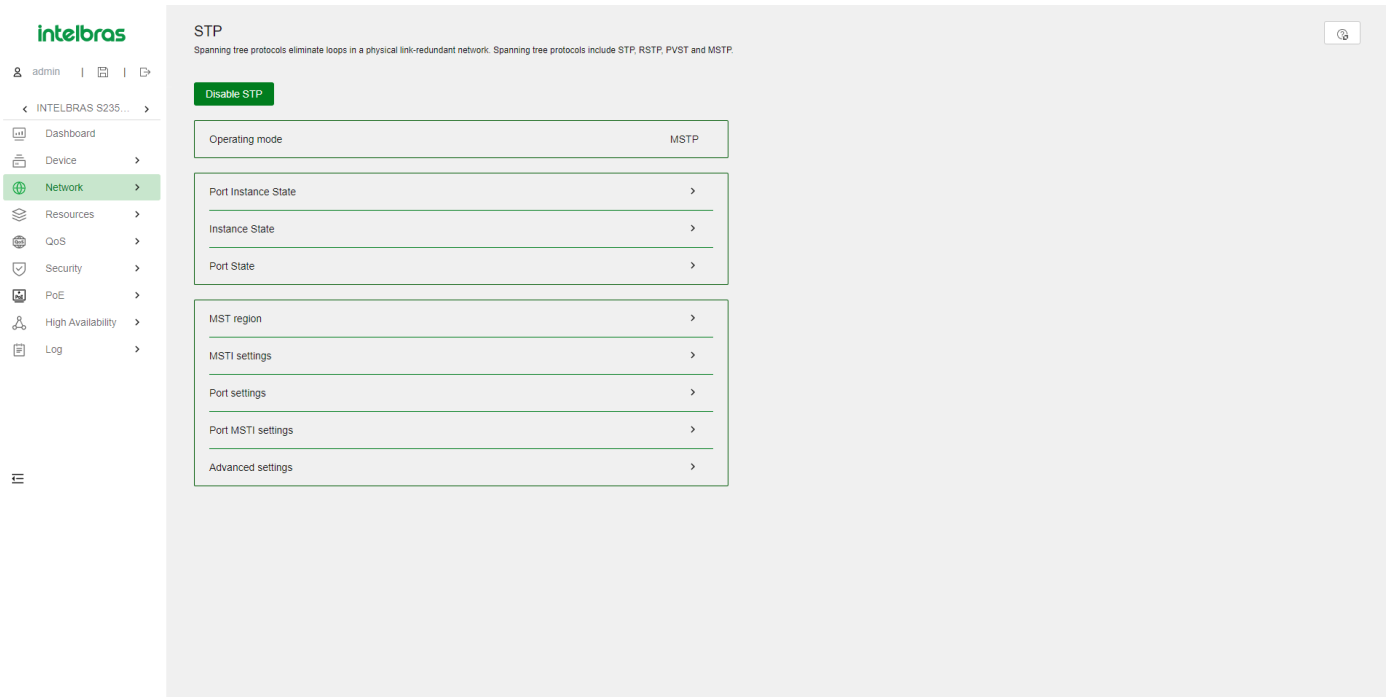
Aprendizado de Endereços MAC

O aprendizado de endereços MAC é habilitado por padrão. Para evitar que a tabela de endereços MAC seja saturada quando o dispositivo estiver sofrendo ataques, desative o aprendizado de endereços MAC. Por exemplo, você pode desativar o aprendizado de endereços MAC para evitar que o dispositivo seja atacado por uma grande quantidade de quadros com diferentes endereços MAC de origem. Quando o aprendizado global de endereços MAC está habilitado, é possível desativar o aprendizado de endereços MAC em uma única interface. Também é possível configurar o limite de aprendizado de MAC em uma interface para limitar o tamanho da tabela de endereços MAC. Uma grande tabela de endereços MAC degradará o desempenho de encaminhamento. Quando o limite é atingido, a interface para de aprender quaisquer endereços MAC. Você também pode configurar se deseja encaminhar quadros cujo endereço MAC de origem não esteja na tabela de endereços MAC.

Protocolos de Spanning tree (STP)

Os protocolos de Spanning tree realizam as seguintes tarefas:

- Podam a estrutura de loop em uma estrutura de árvore livre de loops para uma rede de Camada 2 bloqueando seletivamente portas.
- Mantêm a estrutura da árvore para a rede ativa. Os protocolos de Spanning tree incluem STP, RSTP e MSTP:



Modos de Spanning tree

Os modos de Spanning tree incluem:

- Modo STP—Todas as portas do dispositivo enviam BPDUs STP. Selecione este modo quando o dispositivo de porta peer suportar apenas STP.

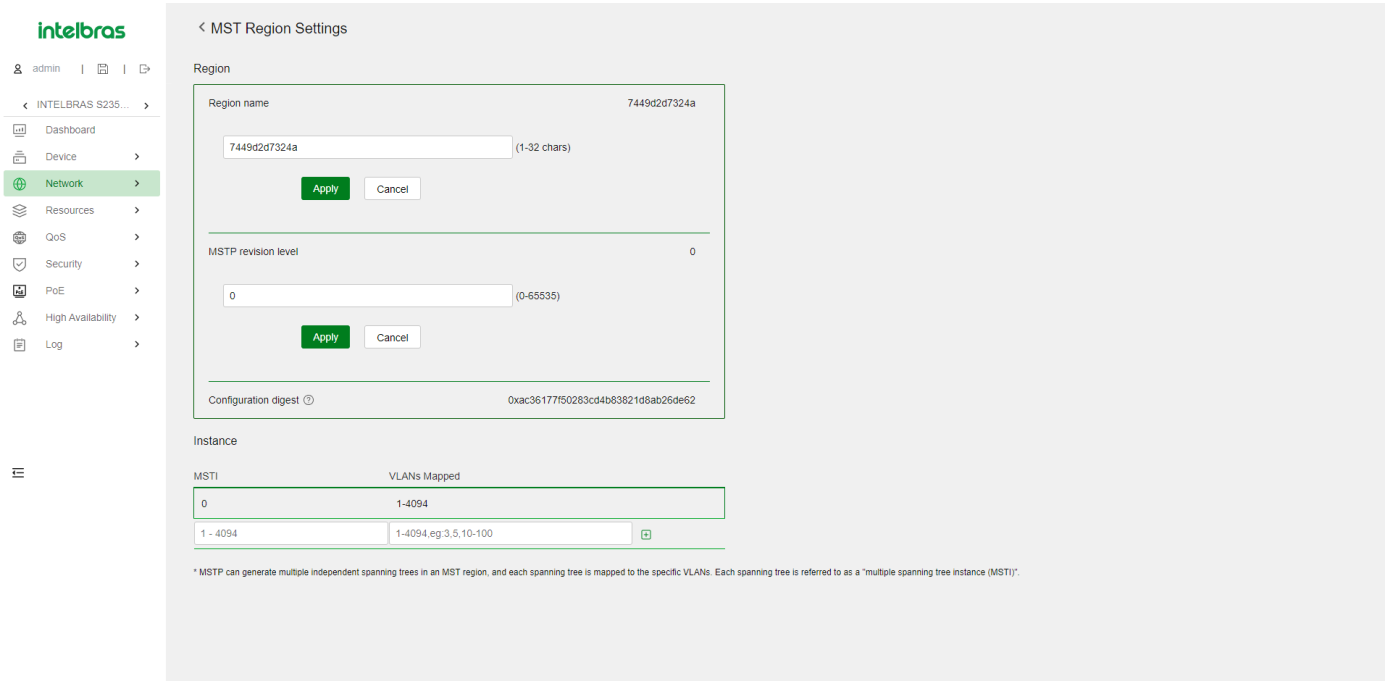
- Modo RSTP—Todas as portas do dispositivo enviam BPDUs RSTP. Uma porta neste modo faz automaticamente a transição para o modo STP quando recebe BPDUs STP de um dispositivo peer. A porta não faz a transição para o modo MSTP quando recebe BPDUs MSTP de um dispositivo peer.

Conceitos Básicos de MSTP

O MSTP divide uma rede comutada em várias regiões de Spanning tree (regiões MST). O MSTP mantém várias árvores de abrangência independentes em uma região MST e cada Spanning tree é mapeada para VLANs específicas. Essa Spanning tree é chamada de instância de Spanning tree múltipla (MSTI). A Spanning tree comum (CST) é uma única Spanning tree que conecta todas as regiões MST na rede comutada. Uma Spanning tree interna (IST) é uma Spanning tree que opera em uma região MST. Também é chamada de MSTI 0, uma MSTI especial para a qual todas as VLANs são mapeadas por padrão. A Spanning tree comum e interna (CIST) é uma única Spanning tree que conecta todos os dispositivos na rede comutada. Ela consiste nas ISTs em todas as regiões MST e no CST.

Dispositivos em uma região MST têm as seguintes características:

- Protocolo de Spanning tree habilitado.
- Mesmo nome de região.
- Configuração de mapeamento de VLAN para instância idêntica.
- Mesmo nível de revisão MSTP.
- Fisicamente conectados.



Funções das Portas

O cálculo da Spanning tree envolve as seguintes funções das portas:

- Porta raiz—Encaminha dados para uma ponte não raiz na ponte raiz. A ponte raiz não tem porta raiz.
- Porta designada—Encaminha dados para o segmento ou dispositivo de rede a jusante.
- Porta alternativa—Serve como porta de backup para uma porta raiz ou porta mestra. Quando a porta raiz ou porta mestra está bloqueada, a porta alternativa assume.
- Porta de backup—Serve como porta de backup de uma porta designada. Quando a porta designada é inválida, a porta de backup se torna a nova porta designada.
- Porta mestra—Serve como porta no caminho mais curto da região MST local para a ponte raiz comum. A porta mestra nem sempre está localizada na raiz regional. Ela é uma porta raiz na IST ou CIST e ainda é uma porta mestra nas outras MSTIs. O cálculo STP envolve portas raiz, portas designadas e portas alternativas. O cálculo RSTP envolve portas raiz, portas designadas, portas alternativas e portas de backup. O cálculo MSTP envolve todas as funções de porta.

Estados de Porta

O RSTP e o MSTP definem os seguintes estados de porta:

Estado	Descrição
Encaminhando	O porto recebe e envia BPDUs (Bridge Protocol Data Units) e encaminha o tráfego do usuário.
Aprendendo	O porto recebe e envia BPDUs, mas não encaminha o tráfego do usuário. O estado de aprendizado é um estado intermediário do porto.
Descartando	O porto recebe e envia BPDUs, mas não encaminha o tráfego do usuário.

Temporizadores STP

Os parâmetros de tempo mais importantes no cálculo do STP são atraso direto, intervalo de hello e idade máxima.

Forward delay - O atraso direto é o tempo de atraso para a transição do estado da porta. As portas recém-eleitas como portas raiz ou portas designadas devem passar pelos estados de escuta e aprendizado antes de passarem para o estado de encaminhamento. Isso requer o dobro do tempo de atraso direto e permite que o novo BPDU de configuração seja propagado por toda a rede. **Hello time** - O dispositivo envia BPDU de configuração no intervalo de hello para os dispositivos vizinhos, a fim de garantir que as rotas estejam livres de falhas. Se o dispositivo não receber BPDU de configuração no período de tempo limite, ele recalcula a Spanning tree. A fórmula para calcular o período de tempo limite é período de tempo limite = fator de tempo limite x 3 x intervalo de hello. O fator de tempo limite é 3 por padrão. **Idade máxima** - O dispositivo usa a idade máxima para determinar se uma BPDU de configuração armazenada expirou e a descarta se a idade máxima for excedida.
Para garantir uma rápida convergência topológica, certifique-se de que as configurações de tempo atendam às seguintes fórmulas:

2 x (atraso direto - 1 segundo) e idade máxima - Idade máxima e 2 x (intervalo de hello + 1 segundo)

Padrões para o cálculo do custo de caminho padrão

Três padrões estão disponíveis para o cálculo do custo de caminho padrão. Em uma rede de Spanning tree com dispositivos de vários fornecedores, você pode especificar um padrão para que o dispositivo use no cálculo automático do custo de caminho padrão para compatibilidade com dispositivos de outros fornecedores.

dot1d-1998 - O dispositivo calcula o custo de caminho padrão para portas com base no IEEE 802.1d-1998. **dot1t** - O dispositivo calcula o custo de caminho padrão para portas com base no IEEE 802.1t. **legacy** - O dispositivo calcula o custo de caminho padrão para portas com base em um padrão privado.

Taxa de transmissão de BPDU

O número máximo de BPDUs que uma porta pode enviar dentro de cada intervalo de hello é a taxa de transmissão de BPDU. Quanto maior a taxa de transmissão de BPDU, mais BPDUs são enviados dentro de cada intervalo de hello, e mais recursos do sistema são usados. Definindo uma taxa de transmissão de BPDU apropriada, você pode

limitar a taxa na qual a porta envia BPDUs. Definir uma taxa apropriada também evita que os protocolos de Spanning tree usem recursos de rede excessivos quando a topologia da rede muda.

Para evitar que uma porta de borda afete a estabilidade da topologia da Spanning tree na rede central quando ela recebe BPDUs, você pode habilitar o BPDU guard. Com o BPDU guard habilitado em uma porta de borda, a porta de borda é desativada quando ela recebe BPDUs, e o sistema notifica o NMS que a porta foi desativada pelo protocolo de Spanning tree. A porta desativada será reativada após um período de tempo.

Número máximo de saltos de uma região MST

Restrinja o tamanho da região definindo o número máximo de saltos de uma região MST. O limite de salto configurado na ponte raiz regional é usado como limite de salto para a região MST.

As BPDUs de configuração enviadas pela ponte raiz regional sempre têm um contador de saltos configurado com o valor máximo. Quando um dispositivo recebe esta BPDU de configuração, ele decrementa o contador de saltos em um e usa o novo contador de saltos nas BPDUs que ele propaga. Quando o contador de saltos de uma BPDU atinge zero, o dispositivo que a recebeu a descarta. Dispositivos além do alcance dos saltos máximos não podem mais participar dos cálculos da Spanning tree, portanto, o tamanho da região MST é limitado.

Recursos de proteção de Spanning tree

O protocolo de Spanning tree suporta vários recursos de proteção para garantir a estabilidade da topologia da Spanning tree.

Loop guard - Quando ocorre congestão de link ou falhas de link unidirecionais na rede da Spanning tree, uma porta bloqueada pode passar para o estado de encaminhamento. Como resultado, ocorrem loops. O estado inicial de uma porta habilitada para loop guard é **discarding** em todos os MSTIs. Quando a porta recebe BPDUs em um MSTI, ela passa seu estado apenas no MSTI. Caso contrário, permanece no estado de descarte para evitar loops temporários.

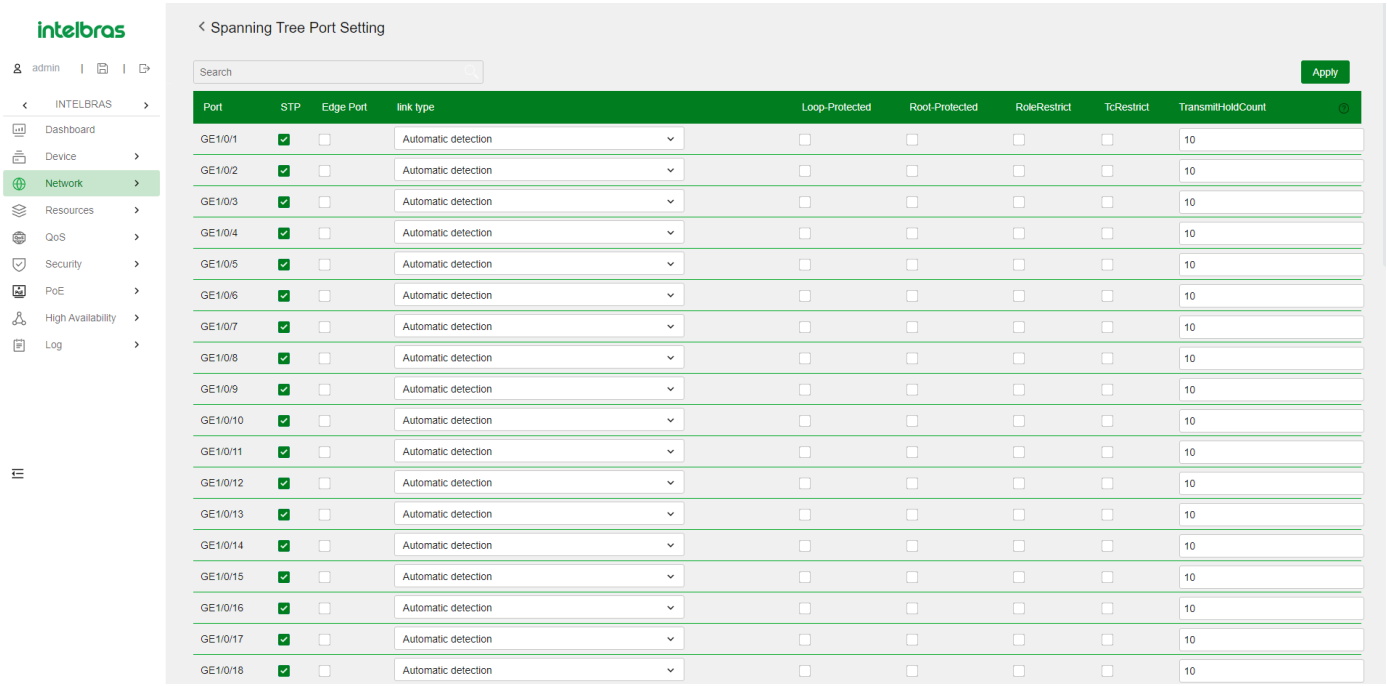
Root guard - Devido a erros de configuração possíveis ou ataques maliciosos na rede, a ponte raiz legal pode receber uma BPDU de configuração com uma prioridade mais alta. Outro dispositivo substitui a ponte raiz legal atual, causando uma mudança indesejada na topologia da rede. O tráfego que deveria passar por links de alta velocidade é redirecionado para links de baixa velocidade, resultando em congestão de rede. Para evitar essa situação, o MSTP fornece o recurso de root guard. Se o root guard estiver habilitado em uma porta de uma ponte raiz, essa porta desempenha o papel de porta designada em todos os MSTIs. Depois que esta porta recebe uma BPDU de configuração com uma prioridade mais alta de um MSTI, ela imediatamente define essa porta como estado de escuta no MSTI e não encaminha a BPDU de configuração recebida. Isso é equivalente a desconectar o link conectado a esta porta no MSTI. Se a porta não receber BPDUs com uma prioridade mais alta dentro de um determinado período de tempo, ela volta ao seu estado original.

Restrição de função da porta - A mudança do ID da ponte de um dispositivo na rede de acesso do usuário pode causar uma mudança na topologia da Spanning tree na rede central. Para evitar esse problema, você pode habilitar a restrição de função da porta em uma porta. Com esse recurso habilitado, quando a porta recebe uma BPDU superior, ela se torna uma porta alternativa em vez de uma porta raiz.

Restrição de transmissão TC-BPDU - A mudança de topologia na rede de acesso do usuário pode causar alterações no endereço de encaminhamento na rede central. Quando a topologia da rede de acesso do usuário está instável, a rede de acesso do usuário pode afetar a rede central. Para evitar esse problema, você pode habilitar a restrição de transmissão TC-BPDU em uma porta. Com esse recurso habilitado, quando a porta recebe uma TC-BPDU, ela não encaminha a TC-BPDU para outras portas.

Guarda TC-BPDU - Quando um dispositivo recebe TC-BPDUs (as BPDUs que notificam dispositivos de mudanças na topologia), ele limpa as entradas de endereçamento de encaminhamento. Se alguém usa TC-BPDUs para atacar o dispositivo, o dispositivo receberá um grande número de TC-BPDUs em um curto período de tempo. Em seguida, o dispositivo está ocupado com a limpeza de entradas de endereçamento de encaminhamento. Isso afeta a estabilidade da rede. A guarda TC-BPDU permite que você defina o número máximo de limpezas imediatas de entradas de endereçamento de encaminhamento realizadas dentro do período de tempo especificado após o dispositivo receber o primeiro TC-BPDU. Para as TC-BPDUs recebidas acima do limite, o dispositivo executa uma limpeza de entradas de endereçamento de encaminhamento

quando o período de tempo expira.

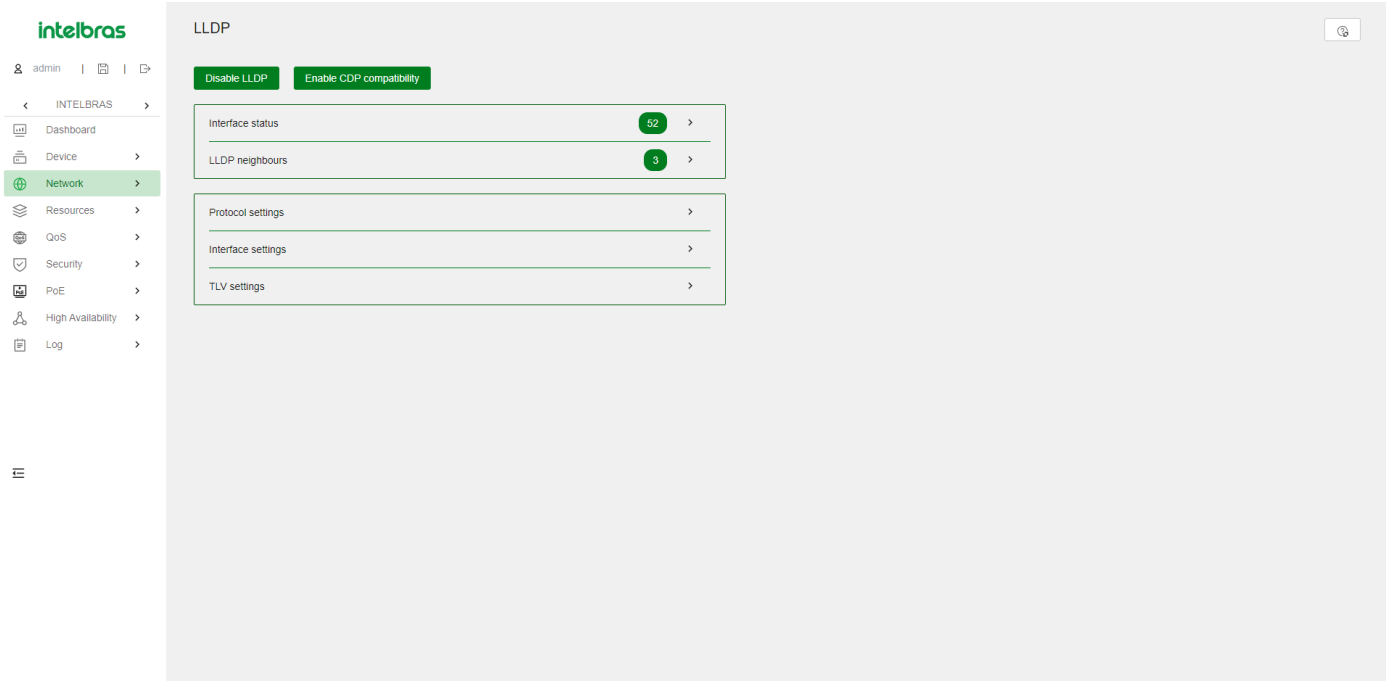


TC snooping

Quando o protocolo da Spanning tree está desabilitado, o dispositivo transmite BPDUs de forma transparente. Como resultado, quando a topologia de outra rede de usuário muda, o dispositivo pode levar muito tempo para aprender novamente as entradas corretas de endereço MAC e entradas ARP. Durante esse período, o tráfego na rede pode ser interrompido. Para evitar a interrupção do tráfego, você pode habilitar o TC snooping. Após receber uma TC-BPDU por meio de uma porta, o dispositivo atualiza as entradas de endereço MAC e entradas ARP associadas à VLAN da porta. Dessa forma, o TC snooping impede que a mudança na topologia interrompa o encaminhamento do tráfego na rede.

LLDP

O Protocolo de Descoberta da Camada de Link (LLDP) opera na camada de link de dados para trocar informações sobre dispositivos entre dispositivos diretamente conectados. Com o LLDP, um dispositivo envia informações locais do dispositivo como triplos TLV (tipo, comprimento e valor) em unidades de dados LLDP (LLDPDUs) para os dispositivos diretamente conectados. As informações locais do dispositivo incluem as capacidades do sistema, endereço IP de gerenciamento, ID do dispositivo, ID da porta e assim por diante. O dispositivo armazena as informações do dispositivo nas LLDPDUs dos vizinhos LLDP em um MIB padrão. O LLDP permite que um sistema de gerenciamento de rede detecte e identifique rapidamente as alterações na topologia de rede da Camada 2.



Agente LLDP

Um agente LLDP é um mapeamento de uma entidade onde o LLDP é executado. Vários agentes LLDP podem ser executados na mesma interface.

Os agentes LLDP são divididos nos seguintes tipos:

- Agente de ponte mais próxima.
- Agente de ponte de cliente mais próxima.
- Agente de ponte mais próxima que não é TPMR.

O LLDP troca pacotes entre agentes vizinhos e cria e mantém informações de vizinhos para eles.

Transmissão de quadros LLDP

Um agente LLDP operando no modo TxRx ou Tx envia quadros LLDP periodicamente e quando a configuração local muda para os dispositivos conectados diretamente. Para evitar que os quadros LLDP sobrecarreguem a rede durante períodos de mudanças frequentes nas informações do dispositivo local, o LLDP usa o mecanismo de balde de tokens para limitar a taxa de quadros LLDP.

O LLDP ativa automaticamente o mecanismo de transmissão rápida de quadros LLDP em um dos seguintes casos:

1. Um novo quadro LLDP é recebido e carrega informações do dispositivo novas para o dispositivo local.

2. O modo de operação do LLDP agente muda de Desabilitado ou Rx para TxRx ou Tx.

O mecanismo de transmissão rápida de quadros LLDP envia sucessivamente o número especificado de quadros LLDP em um intervalo configurável de transmissão rápida de quadros LLDP. O mecanismo ajuda os vizinhos LLDP a descobrir o dispositivo local o mais rápido possível. Em seguida, o intervalo de transmissão normal de quadros LLDP é retomado.

Recebimento de quadros LLDP

Um agente LLDP operando nos modos TxRx ou Rx confirma a validade dos TLVs (Tipos, Tamanhos e Valores) carregados em cada quadro LLDP recebido. Se os TLVs forem válidos, o agente LLDP salva as informações e inicia um temporizador de envelhecimento. Quando o valor TTL (Tempo de Vida) no TLV Tempo de Vida do quadro LLDP se torna zero, as informações envelhecem imediatamente.

Ao definir o multiplicador TTL, você pode configurar o TTL dos LLDPDUs enviados localmente. O TTL é expresso usando a seguinte fórmula:

TTL = Mín (65535, (multiplicador TTL * intervalo de transmissão de quadros LLDP + 1))

Conforme a expressão mostra, o TTL pode chegar a 65535 segundos. TTLs superiores a 65535 serão arredondados para 65535 segundos.

Atraso de reinicialização LLDP

Quando o modo de operação do LLDP muda em uma porta, a porta reinicializa as máquinas de estado do protocolo após um atraso de reinicialização LLDP. Ajustando o atraso, você pode evitar inicializações frequentes causadas por mudanças frequentes no modo de operação do LLDP em uma porta.

Armadilhamento LLDP

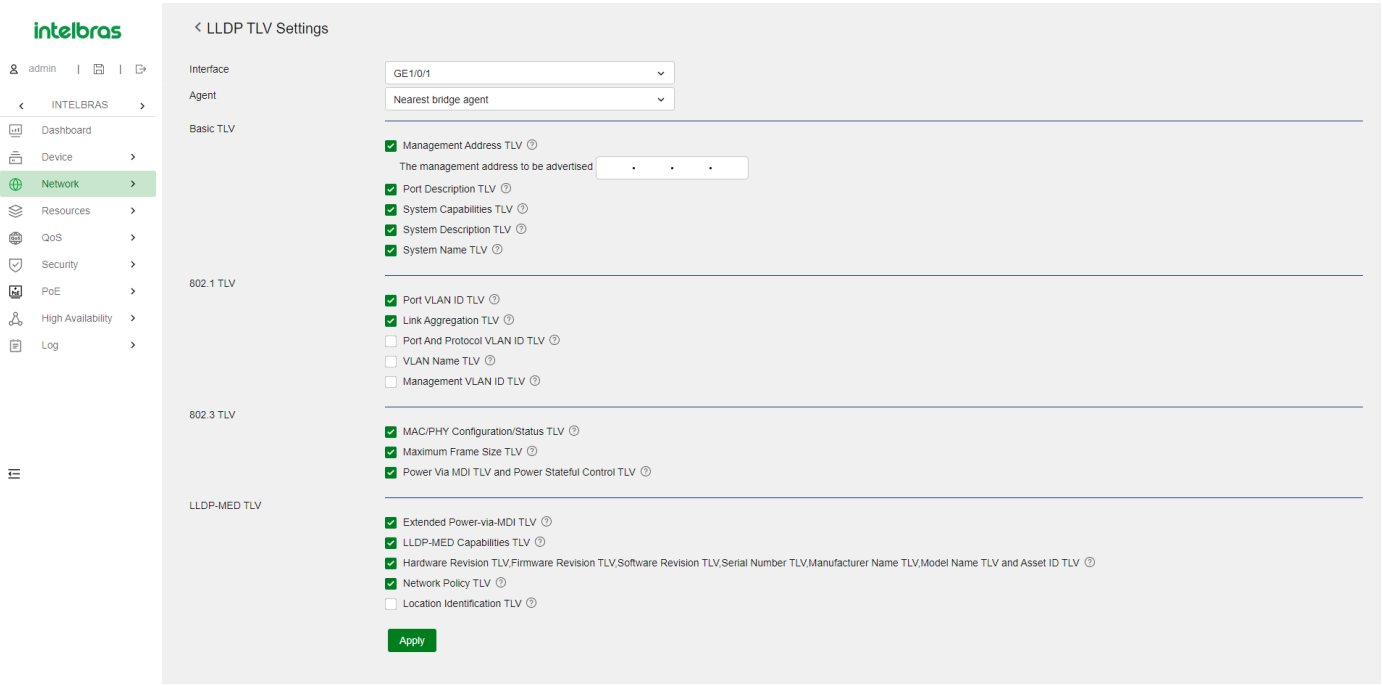
O armadilhamento LLDP notifica o sistema de gerenciamento de rede de eventos, como dispositivos vizinhos recém-detectados e falhas de link.

TLVs LLDP

Um TLV é um elemento de informação que contém os campos de tipo, tamanho e valor. Os TLVs LLDPDU incluem as seguintes categorias:

TLVs de gerenciamento básico TLVs específicos da organização (IEEE 802.1 e IEEE 802.3) TLVs LLDP-MED (descoberta de ponto de extremidade de mídia)
TLVs de gerenciamento básico são essenciais para o gerenciamento de dispositivos.

TLVs específicos da organização e TLVs LLDP-MED são usados para o gerenciamento aprimorado de dispositivos. Eles são definidos por padronização ou outras organizações e são opcionais para LLDPDUs.



Compatibilidade com CDP

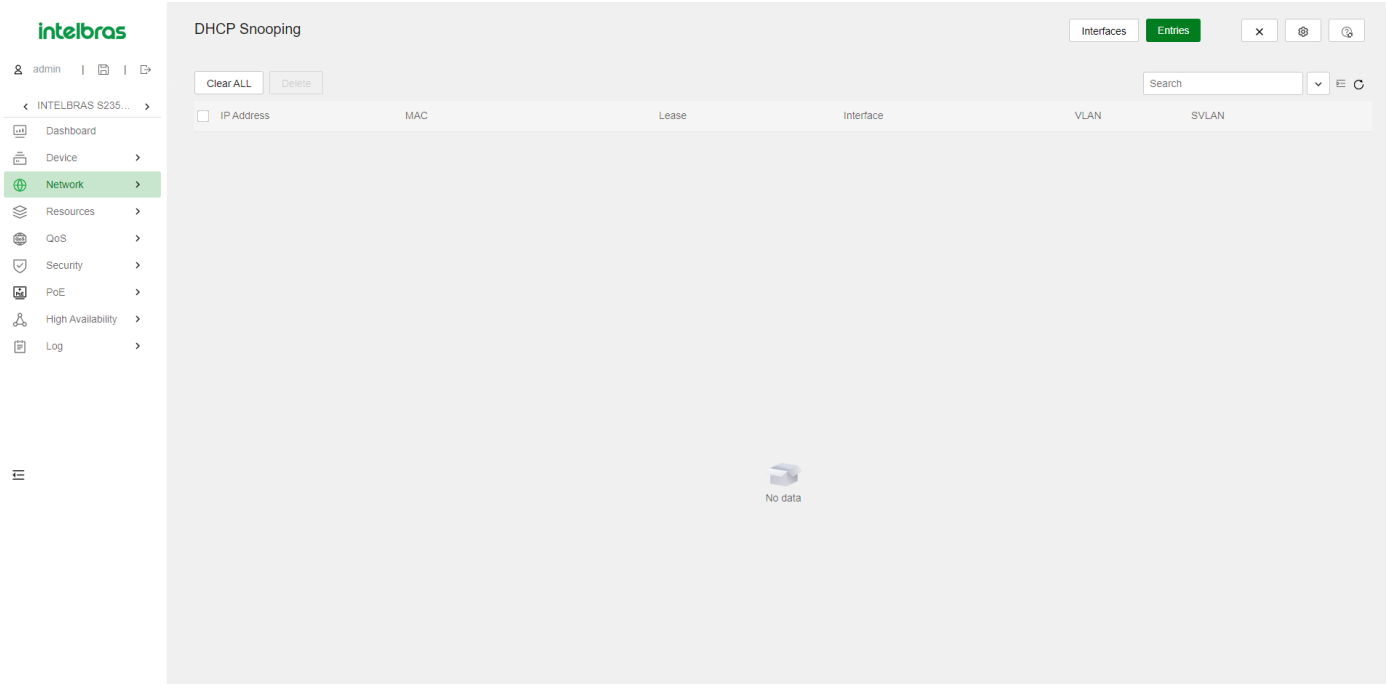
A compatibilidade com CDP permite que seu dispositivo receba e reconheça pacotes CDP de um dispositivo conectado diretamente e responda com pacotes CDP.

DHCP Snooping

O snooping de DHCP funciona entre o cliente DHCP e o servidor ou entre o cliente DHCP e o agente de retransmissão de DHCP. O snooping de DHCP fornece as seguintes funções:

Garante que os clientes DHCP obtenham endereços IP apenas de servidores DHCP autorizados.
O snooping de DHCP define portas confiáveis e não confiáveis para garantir que os clientes obtenham endereços IP apenas de servidores DHCP autorizados.

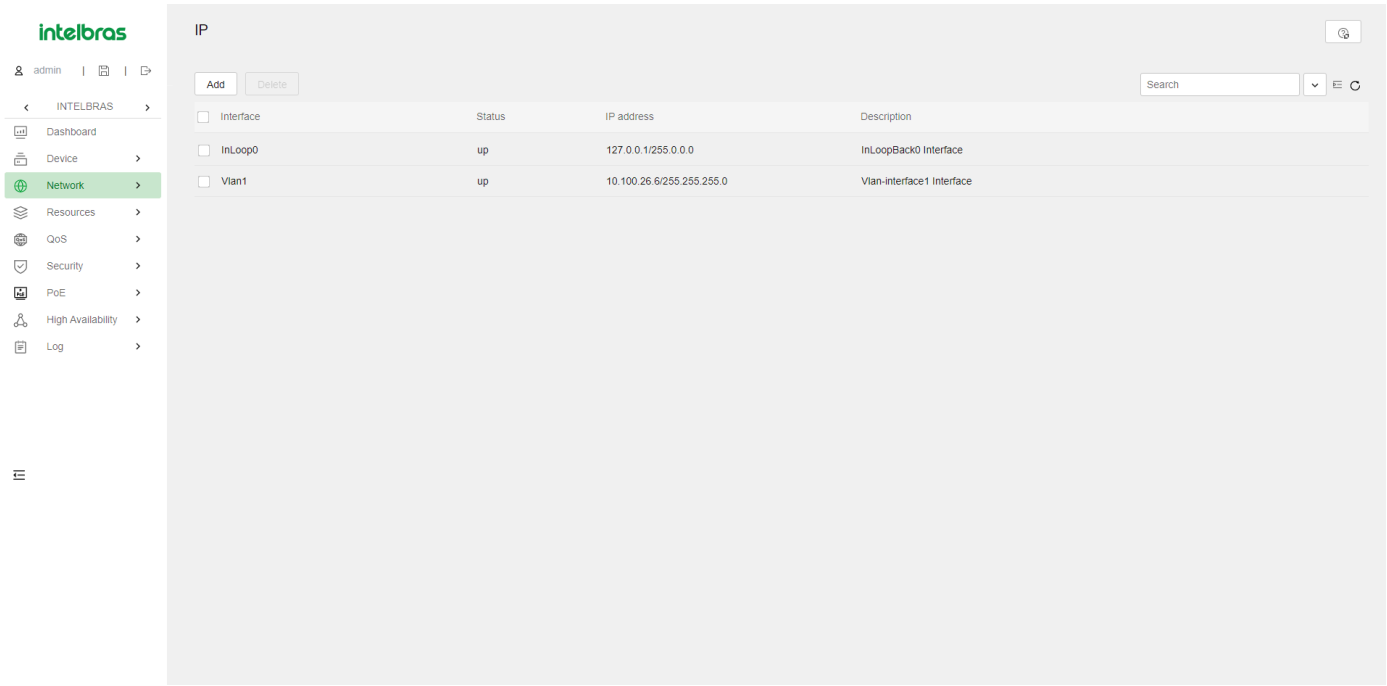
Confiável: Uma porta confiável pode encaminhar mensagens DHCP corretamente para garantir que os clientes obtenham endereços IP de servidores DHCP autorizados.



IP

Classes de endereços IP

A atribuição de endereços IP usa um endereço de 32 bits para identificar cada host em uma rede IPv4. Para facilitar a leitura, eles são escritos em notação decimal pontuada, com cada endereço tendo quatro octetos de comprimento. Por exemplo, o endereço 00001010000000010000000100000001 em binário é escrito como 10.1.1.1.



Cada endereço IP se divide nas seguintes seções:

- **ID de rede** - Identifica uma rede. Os primeiros bits de um ID de rede, conhecidos como campo de classe, identificam a classe do endereço IP.
- **ID do host** - Identifica um host em uma rede.

Os endereços IP são divididos em cinco classes. A tabela a seguir mostra as classes de endereços IP e os intervalos. As três primeiras classes são as mais comuns.

Classe	Intervalo de Endereços	Observações

A	0.0.0.0 a 127.255.255.255	O endereço IP 0.0.0.0 é usado por um host ao inicializar para comunicação temporária. Este endereço nunca é um endereço de destino válido.
B	128.0.0.0 a 191.255.255.255	N/A
C	192.0.0.0 a 223.255.255.255	N/A
D	224.0.0.0 a 239.255.255.255	Endereços de multicast.
E	240.0.0.0 a 255.255.255.255	Reservado para uso futuro, exceto o endereço de transmissão 255.255.255.255.

Sub-rede e máscara

A sub-rede divide uma rede em sub-redes menores chamadas sub-redes, usando alguns bits do ID do host para criar um ID de sub-rede.

A máscara identifica a fronteira entre o ID do host e a combinação de ID de rede e ID de sub-rede.

Cada máscara de sub-rede possui 32 bits que correspondem aos bits em um endereço IP. Em uma máscara de sub-rede, uns consecutivos representam o ID de rede e o ID de sub-rede, e zeros consecutivos representam o ID do host.

Antes de serem subdivididas, as redes Classe A, B e C usam essas máscaras padrão (também chamadas de máscaras naturais): 255.0.0.0, 255.255.0.0 e 255.255.255.0, respectivamente.

A subdivisão aumenta o número de endereços que não podem ser atribuídos a hosts. Portanto, o uso de sub-redes significa acomodar menos hosts.

Por exemplo, uma rede Classe B sem subdivisão pode acomodar 1022 hosts a mais do que a mesma rede subdividida em 512 sub-redes.

- **Sem sub-rede** - 65534 (216 - 2) hosts. (Os dois endereços deduzidos são o endereço de transmissão, que tem um ID de host todo em uns, e o endereço de rede, que tem um ID de host todo em zeros.)
- **Com sub-rede** - O uso dos primeiros nove bits do ID de host para subdivisão fornece 512 (29) sub-redes. No entanto, apenas sete bits permanecem disponíveis para o ID do host. Isso permite 126 (27 - 2) hosts em cada sub-rede, totalizando 64512 (512 * 126) hosts.

Métodos de configuração de endereço IP

Você pode usar os seguintes métodos para habilitar uma interface a obter um endereço IP:

Atribuir manualmente um endereço IP à interface. Configurar a interface para obter um endereço IP por meio do DHCP.

MTU para uma interface

Quando um pacote excede o MTU da interface de saída, o dispositivo processa o pacote de uma das seguintes maneiras:

Se o pacote não permitir fragmentação, o dispositivo o descarta. Se o pacote permitir fragmentação, o dispositivo o fragmenta e encaminha os fragmentos.
A fragmentação e a recombinação consomem recursos do sistema, portanto, defina um MTU apropriado para uma interface com base no ambiente de rede para evitar a fragmentação.

ARP

O ARP (Address Resolution Protocol) resolve endereços IP em endereços MAC em redes Ethernet.

Tipos de Entradas na Tabela ARP

Uma tabela ARP armazena entradas ARP dinâmicas e estáticas.

Entrada ARP Dinâmica

O ARP cria e atualiza automaticamente as entradas dinâmicas. Uma entrada ARP dinâmica é removida quando seu temporizador de envelhecimento expira ou a interface de saída é desativada. Além disso, uma entrada ARP dinâmica pode ser substituída por uma entrada ARP estática.

Entrada ARP Estática

Uma entrada ARP estática é configurada manualmente e mantida pelo administrador. Ela não expira e não pode ser sobrescrita por nenhuma entrada ARP dinâmica.

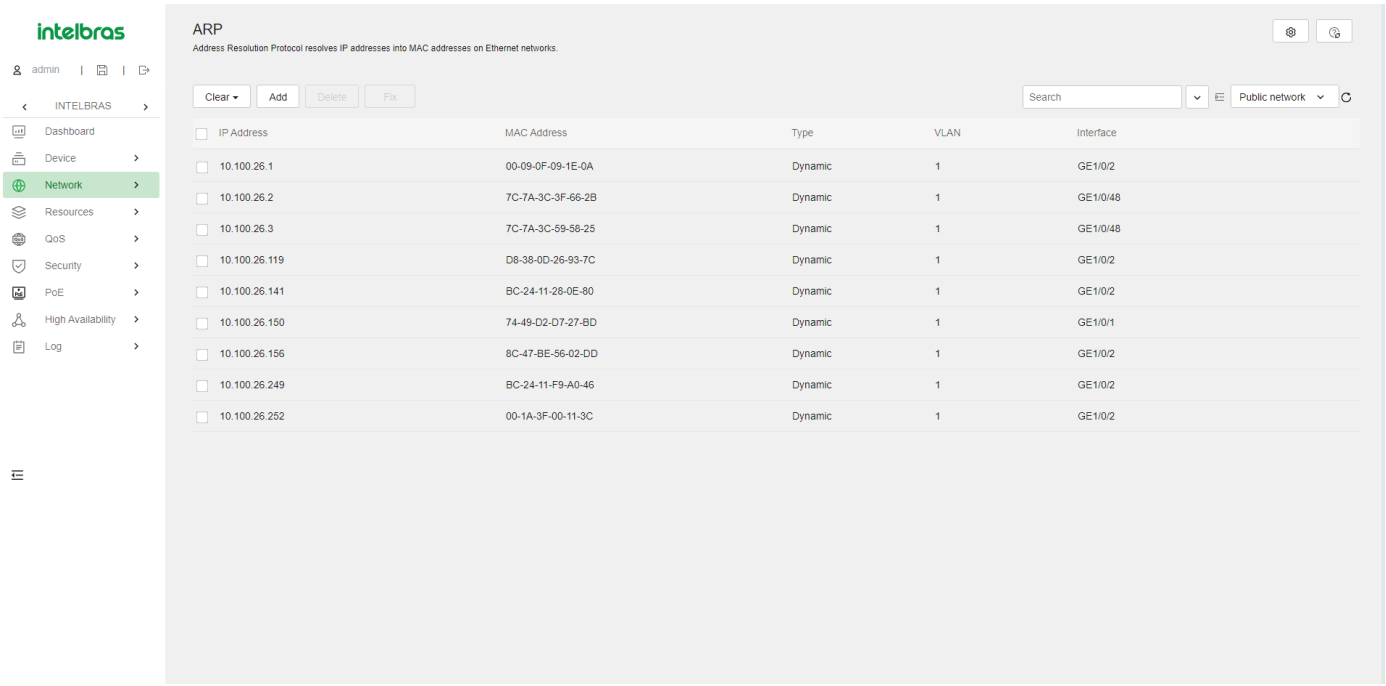
As entradas ARP estáticas protegem a comunicação entre dispositivos, pois pacotes maliciosos não podem modificar o mapeamento IP-para-MAC em uma entrada ARP estática.

O dispositivo suporta os seguintes tipos de entradas ARP estáticas:

- **Entrada ARP Estática Longa** - Ela contém o endereço IP, endereço MAC, VLAN e interface de saída. É usada diretamente para encaminhar pacotes.
- **Entrada ARP Estática Curta** - Ela contém apenas o endereço IP e o endereço MAC.

Se a interface de saída for uma interface Ethernet de Camada 3, a entrada ARP curta pode ser usada diretamente para encaminhar pacotes. Se a interface de saída for uma interface de VLAN, o dispositivo envia uma solicitação ARP com o endereço IP de destino na entrada ARP curta. Se o endereço IP e os endereços MAC do remetente na resposta ARP coincidirem com a entrada ARP estática curta, o dispositivo realiza as seguintes tarefas: Adiciona a interface que recebeu a resposta ARP à entrada ARP estática curta. Usa a entrada ARP estática curta resolvida para encaminhar pacotes IP.

Para comunicar com um host usando um mapeamento IP-para-MAC fixo, configure uma entrada ARP estática curta no dispositivo. Para comunicar com um host usando um mapeamento IP-para-MAC fixo por meio de uma interface em uma VLAN, configure uma entrada ARP estática longa no dispositivo.

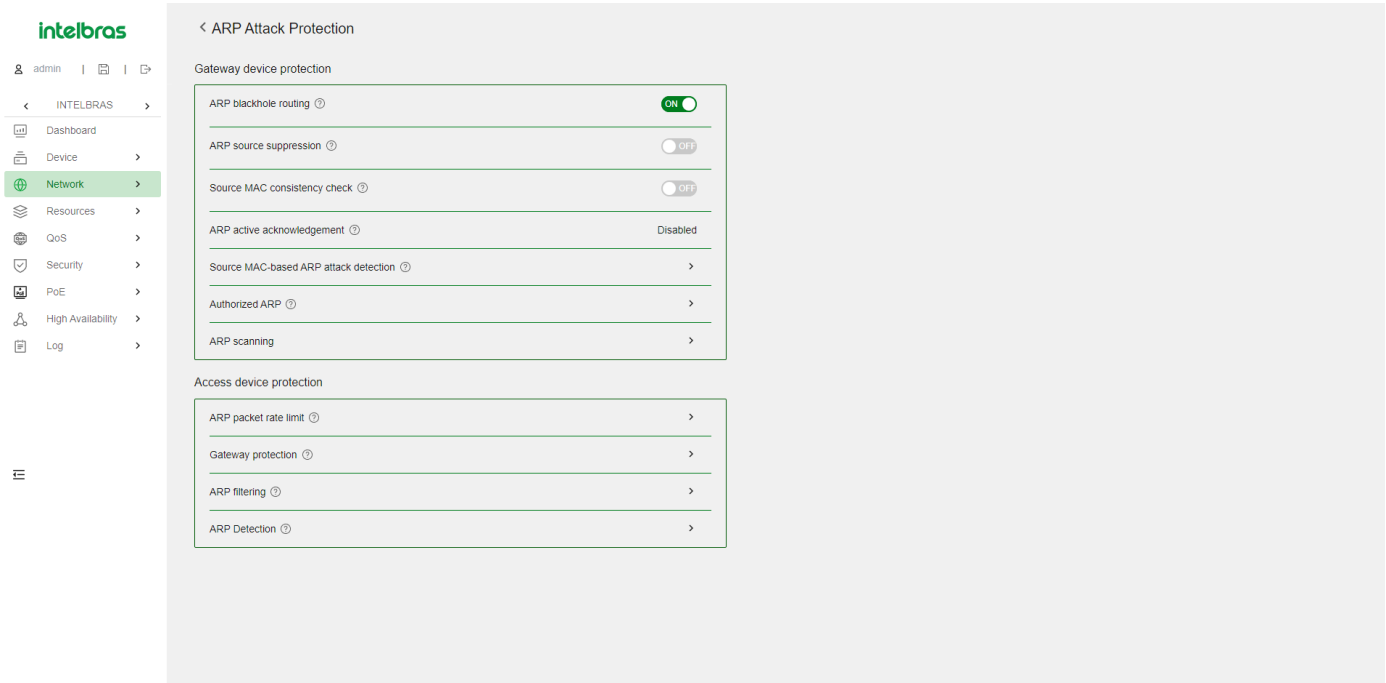


Proteção contra Ataques ARP

Ataques ARP e vírus representam ameaças à segurança de redes locais. Embora o ARP seja fácil de implementar, ele não possui mecanismos de segurança e é vulnerável a ataques de rede. Várias funcionalidades são usadas para detectar e prevenir ataques ARP.

O gateway oferece suporte às seguintes funcionalidades:

- Roteamento para buraco de ARP (ARP blackhole).
- Supressão de origem ARP (ARP source suppression).
- Verificação de consistência de MAC de origem de pacotes ARP (ARP packet source MAC consistency check).
- Reconhecimento ativo de ARP (ARP active acknowledgement).
- Detecção de ataque ARP com base no MAC de origem (Source MAC-based ARP attack detection).
- ARP autorizado (Authorized ARP).
- Varredura ARP e ARP fixo (ARP scanning and fixed ARP).
- O dispositivo de acesso oferece suporte às seguintes funcionalidades:
- Limite de taxa de pacotes ARP (ARP packet rate limit).
- Proteção de gateway ARP (ARP gateway protection).
- Filtragem ARP (ARP filtering).
- Detecção ARP (ARP detection).



Proteção contra Ataques com IP Irresolvível

Se um dispositivo recebe um grande número de pacotes IP irresolvíveis de um host, podem ocorrer as seguintes situações:

- O dispositivo envia um grande número de solicitações ARP, sobrecarregando as sub-redes de destino.
- O dispositivo continua tentando resolver os endereços IP de destino, sobrecarregando sua CPU.

Para proteger o dispositivo contra tais ataques IP, você pode configurar as seguintes funcionalidades:

- **Supressão de Origem ARP (ARP source suppression)** - Para de resolver pacotes de um host se o número de pacotes irresolvíveis do host exceder o limite superior dentro de 5 segundos. O dispositivo retoma a resolução ARP quando o intervalo expira. Essa funcionalidade é aplicável se os pacotes de ataque tiverem os mesmos endereços de origem.
- **Roteamento para Buraco de ARP (ARP blackhole routing)** - Cria uma rota para um buraco de ARP destinada a um endereço IP irresolvível. O dispositivo descarta todos os pacotes correspondentes até que a rota de buraco de ARP envelheça. Essa funcionalidade é aplicável, independentemente de os pacotes de ataque terem os mesmos endereços de origem.

Verificação de Consistência de MAC de Origem de Pacotes ARP

Essa funcionalidade permite que um gateway filtre pacotes ARP cujo endereço MAC de origem no cabeçalho Ethernet é diferente do endereço MAC do remetente no corpo da mensagem. Isso permite que o gateway aprenda entradas ARP corretas.

Reconhecimento Ativo de ARP

Configure essa funcionalidade nos gateways para evitar spoofing de usuário.

O reconhecimento ativo de ARP impede que um gateway crie entradas ARP incorretas. No modo estrito, um gateway realiza verificações de validade mais estritas antes de criar uma entrada ARP:

Ao receber uma solicitação ARP destinada ao gateway, o gateway envia uma resposta ARP, mas não cria uma entrada ARP. Ao receber uma resposta ARP, o gateway determina se resolveu o endereço IP do remetente:

- Se sim, o gateway realiza um reconhecimento ativo. Quando a resposta ARP é verificada como válida, o gateway cria uma entrada ARP.
- Se não, o gateway descarta o pacote.

Detecção de Ataque ARP com Base no MAC de Origem

Essa funcionalidade verifica o número de pacotes ARP entregues à CPU. Se o número de pacotes do mesmo endereço MAC dentro de 5 segundos exceder um limite, o dispositivo adiciona o endereço MAC a uma entrada de ataque ARP. Antes que a entrada envelheça, o dispositivo lida com o ataque usando um dos seguintes métodos:

- **Monitoramento** - Gera apenas mensagens de log.
- **Filtragem** - Gera mensagens de log e filtra os pacotes ARP subsequentes desse endereço MAC.

Você pode excluir os endereços MAC de alguns gateways e servidores dessa detecção. Essa funcionalidade não inspeciona pacotes ARP desses dispositivos, mesmo que eles sejam atacantes.

ARP Autorizado

As entradas ARP autorizadas são geradas com base nos arrendamentos de endereços dos clientes DHCP no servidor DHCP ou nas entradas de clientes dinâmicos no agente de retransmissão DHCP.

Com o ARP autorizado ativado, uma interface é desativada para aprender entradas ARP dinâmicas. Isso impede spoofing de usuário e permite que apenas clientes autorizados acessem os recursos de rede.

Varredura ARP e ARP Fixo

A varredura ARP é tipicamente usada em conjunto com a funcionalidade de ARP fixo em redes de pequena escala.

A varredura ARP cria automaticamente entradas ARP para dispositivos em uma faixa de endereços. O dispositivo realiza a varredura ARP usando as seguintes etapas:

- Envia solicitações ARP para cada endereço IP na faixa de endereços.
- Obtém os endereços MAC por meio das respostas ARP recebidas.
- Cria entradas ARP dinâmicas.

O ARP fixo converte entradas ARP dinâmicas existentes (incluindo aquelas geradas por meio da varredura ARP) em entradas ARP estáticas. Essa funcionalidade impede que as entradas ARP sejam modificadas por atacantes.

Limite de Taxa de Pacotes ARP

A funcionalidade de limite de taxa de pacotes ARP permite limitar a taxa de pacotes ARP entregues à CPU. Um dispositivo com detecção ARP ativada enviará todos os pacotes ARP recebidos à CPU para inspeção. O processamento excessivo de pacotes ARP pode fazer com que o dispositivo apresente mau funcionamento ou mesmo travamento. Para resolver esse problema, configure o limite de taxa de pacotes ARP.

Configure essa funcionalidade quando a detecção ARP estiver ativada ou quando forem detectados ataques de inundação ARP.

Se a geração de log para o limite de taxa de pacotes ARP estiver ativada, o dispositivo enviará a taxa de pacotes ARP cruzando o limite superior no intervalo de envio em uma mensagem de log para o centro de informações. Você pode configurar o módulo do centro de informações para definir as regras de saída de log.

Proteção de Gateway ARP

Configure essa funcionalidade em interfaces não conectadas a um gateway para evitar ataques de spoofing de gateway.

Quando uma interface desse tipo recebe um pacote ARP, verifica se o endereço IP do remetente no pacote é consistente com o de qualquer gateway protegido. Se sim, o pacote é descartado. Se não, o pacote é tratado corretamente.

Filtragem ARP

A funcionalidade de filtragem ARP pode evitar ataques de spoofing de gateway e de usuário.

Uma interface habilitada com essa funcionalidade verifica os endereços IP e MAC do remetente em um pacote ARP recebido em relação às entradas permitidas. Se encontrar uma correspondência, o pacote é tratado corretamente. Caso contrário, o pacote é descartado.

Detecção ARP

A detecção ARP permite que dispositivos de acesso bloqueiem pacotes ARP de clientes não autorizados para evitar ataques de spoofing de usuário e de gateway. A detecção ARP não verifica pacotes ARP recebidos de portas ARP confiáveis.

A detecção ARP fornece as seguintes funções:

- Verificação de validade do usuário
- Se você habilitar a detecção ARP apenas para uma VLAN, ela fornecerá apenas a verificação de validade do usuário.

  Ao receber um pacote ARP de uma interface ARP não confiável, o dispositivo compara os endereços IP e MAC do remetente com as seguintes entradas:

- Entradas de vinculação do IP de origem estático.
- Entradas de DHCP snooping.
- Se uma correspondência for encontrada, o pacote ARP é considerado válido e encaminhado. Caso contrário, o pacote ARP é considerado inválido e descartado.
- Verificação de validade do pacote ARP

Ative a verificação de validade para pacotes ARP recebidos em portas não confiáveis e especifique os seguintes objetos a serem verificados:

- **MAC de Origem** — Verifica se o endereço MAC do remetente no corpo da mensagem é idêntico ao endereço MAC de origem no cabeçalho Ethernet. Se forem idênticos, o pacote é encaminhado. Caso contrário, o pacote é descartado.
- **MAC de Destino** — Verifica o endereço MAC de destino nas respostas ARP. Se o endereço MAC de destino for tudo-zero, tudo-um ou inconsistente com o endereço MAC de destino no cabeçalho Ethernet, o pacote é considerado inválido e descartado.
- **IP** — Verifica os endereços IP de origem e destino das respostas ARP, e o endereço IP de origem das solicitações ARP. Endereços IP de tudo-um ou multicast são considerados inválidos e os pacotes correspondentes são descartados.

Encaminhamento Restrito ARP

O encaminhamento restrito ARP controla o encaminhamento de pacotes ARP recebidos em interfaces não confiáveis que passaram na verificação de validade do usuário da seguinte forma:

Se os pacotes forem solicitações ARP, eles serão encaminhados pela interface confiável. Se os pacotes forem respostas ARP, eles serão encaminhados de acordo com o endereço MAC de destino. Se não houver correspondência na tabela de endereços MAC, eles serão encaminhados pela interface confiável. O ARP não possui mecanismos de segurança e é vulnerável a ataques de rede. Para proteger a rede contra ataques ARP, o dispositivo oferece as funcionalidades de varredura ARP e ARP fixo.

A varredura ARP é tipicamente usada em conjunto com a funcionalidade de ARP fixo em redes de pequena escala.

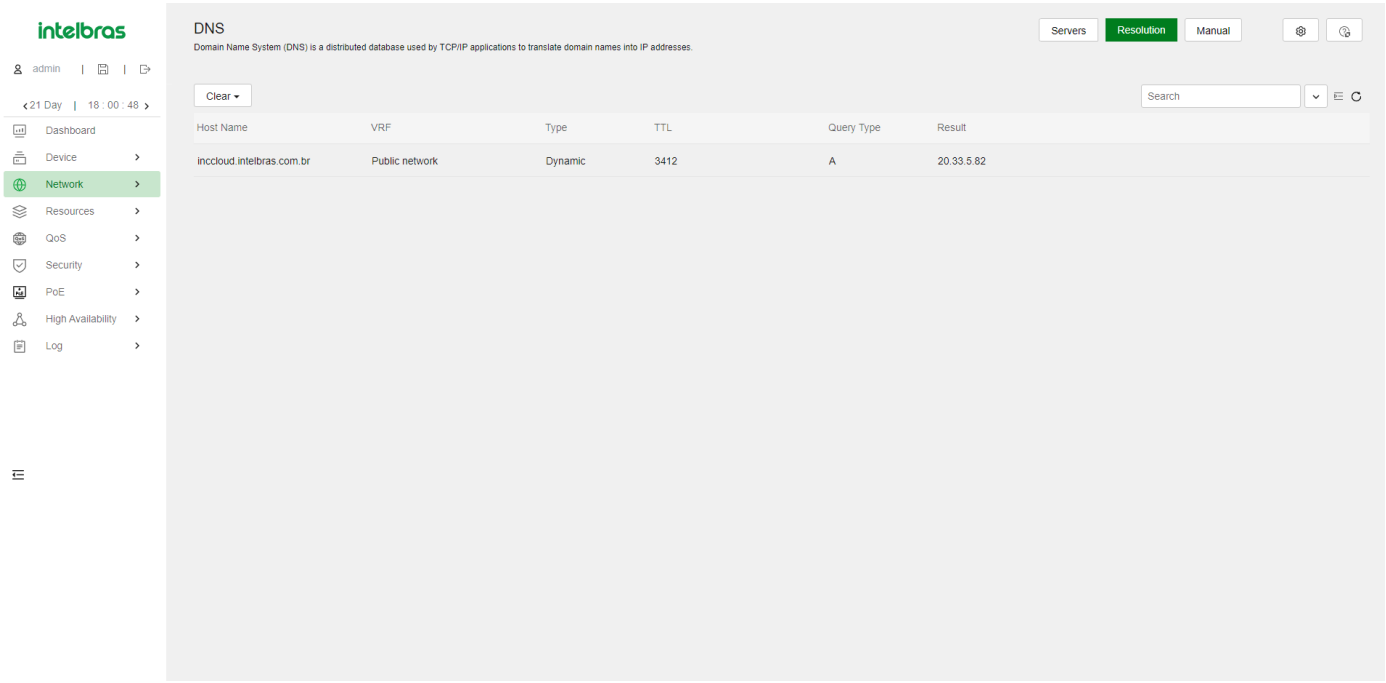
A varredura ARP cria automaticamente entradas ARP para dispositivos em uma faixa de endereços. O dispositivo realiza a varredura ARP usando as seguintes etapas:

- Envia solicitações ARP para cada endereço IP na faixa de endereços.
- Obtém os endereços MAC por meio das respostas ARP recebidas.
- Cria entradas ARP dinâmicas.

O ARP fixo converte entradas ARP dinâmicas existentes (incluindo aquelas geradas por meio da varredura ARP) em entradas ARP estáticas. Essa funcionalidade impede que as entradas ARP sejam modificadas por atacantes.

Sistema de Nomes de Domínio (DNS)

O Sistema de Nomes de Domínio (DNS) é um banco de dados distribuído usado por aplicativos TCP/IP para traduzir nomes de domínio em endereços IP. O DNS IPv4 traduz nomes de domínio em endereços IPv4. O DNS IPv6 traduz nomes de domínio em endereços IPv6. O mapeamento de nome de domínio para endereço IP é chamado de entrada DNS.



Resolução dinâmica de nomes de domínio

Para usar a resolução dinâmica de nomes de domínio, você deve especificar um endereço de servidor DNS para um dispositivo. O dispositivo envia consultas DNS para o servidor DNS para resolução de nomes de domínio.

Você pode configurar uma lista de sufixos de nomes de domínio para que o resolvedor possa usar a lista para fornecer a parte ausente de um nome incompleto. Por exemplo, você pode configurar **com** como sufixo para aabbcc.com. O usuário só precisa inserir **aabbcc** para obter o endereço IP de **aabbcc.com**. O resolvedor adiciona o sufixo e o delimitador antes de passar o nome para o servidor DNS.

O resolvedor de nomes lida com as consultas com base nos nomes de domínio que o usuário insere:

- Se o usuário inserir um nome de domínio sem um ponto (.) (por exemplo, aabbcc), o resolvedor considera o nome de domínio como um nome de host. Ele adiciona um sufixo DNS ao nome do host antes de realizar a operação de consulta. Se nenhuma correspondência for encontrada para qualquer combinação de nome de host e sufixo, o resolvedor usará o nome de domínio inserido pelo usuário (por exemplo, aabbcc) para a consulta de endereço IP.
- Se o usuário inserir um nome de domínio com um ponto (.) entre as letras (por exemplo, www.aabbcc), o resolvedor usará diretamente esse nome de domínio para a operação de consulta. Se a consulta falhar, o resolvedor adicionará um sufixo DNS para outra operação de consulta.

- Se o usuário inserir um nome de domínio com um ponto (.) no final (por exemplo, aabbcc.com.), o resolvedor considera o nome de domínio como um FQDN e retorna o resultado da consulta com sucesso ou falha. O ponto no final do nome de domínio é considerado um símbolo de terminação.

Resolução estática de nomes de domínio

A resolução estática de nomes de domínio significa criar manualmente mapeamentos entre nomes de domínio e endereços IP. Por exemplo, você pode criar um mapeamento DNS estático para um dispositivo para que possa acessar o dispositivo por Telnet usando o nome de domínio.

Depois que um usuário especifica um nome, o dispositivo verifica a tabela de resolução de nome estático em busca de um endereço IP. Se nenhum endereço IP estiver disponível, ele entra em contato com o servidor DNS para a resolução dinâmica de nomes, o que leva mais tempo do que a resolução estática de nomes. Para melhorar a eficiência, você pode colocar mapeamentos de nome para endereço IP frequentemente consultados na tabela local de resolução de nome estático.

Proxy DNS

O proxy DNS realiza as seguintes operações:

Encaminha a solicitação do cliente DNS para o servidor DNS designado.

Convey a resposta do servidor DNS para o cliente.

O proxy DNS simplifica a gestão de rede. Quando o endereço do servidor DNS é alterado, você pode alterar a configuração apenas no proxy DNS em vez de em cada cliente DNS.

IPv6

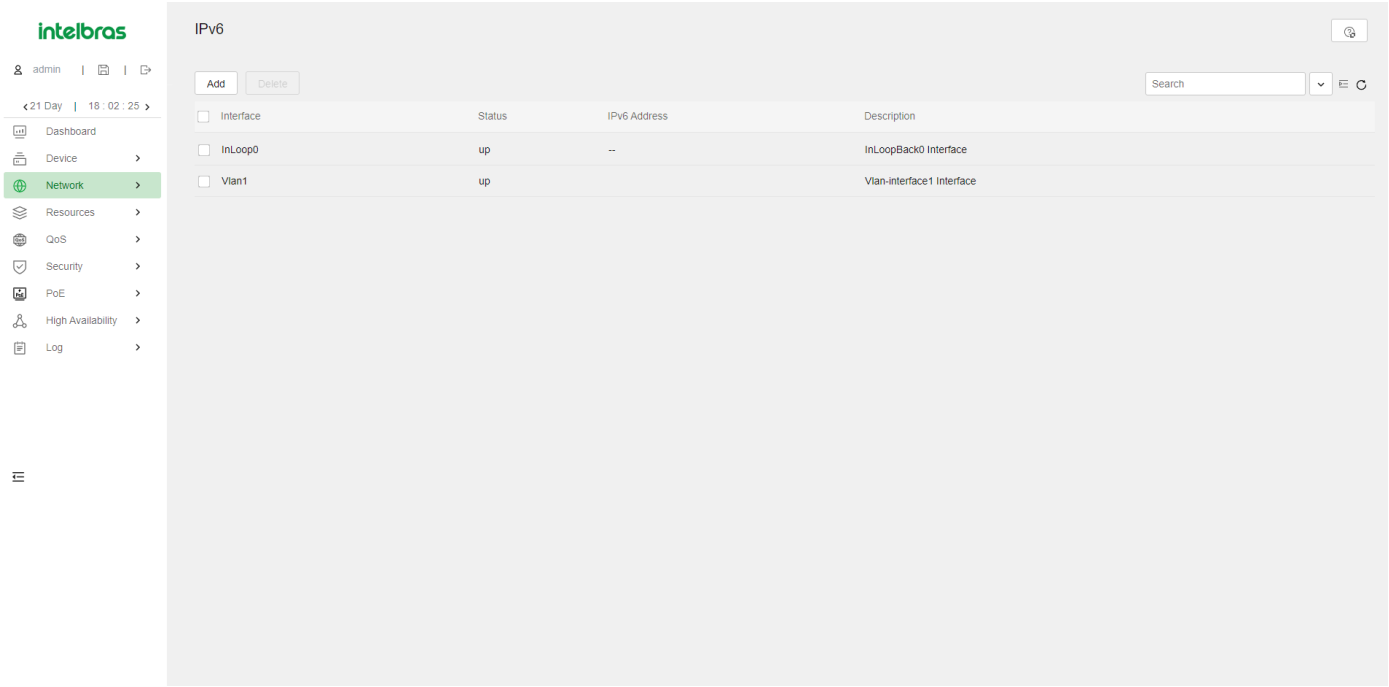
O DNS fornece apenas os mapeamentos estáticos entre nomes de domínio e endereços IP. Quando o endereço IP de um nó é alterado, o acesso ao nó falha.

O Sistema de Nomes de Domínio Dinâmico (DDNS) pode atualizar dinamicamente os mapeamentos entre nomes de domínio e endereços IP para servidores DNS.

Para usar o DDNS, você deve primeiro fazer login no servidor DDNS para registrar uma conta. O dispositivo age como cliente DDNS e envia uma solicitação de atualização DDNS para o servidor DNS quando o endereço IP do dispositivo é alterado. A solicitação contém o mapeamento mais recente do nome de domínio e endereço IP e as credenciais da conta do usuário (nome de usuário e senha). Após a autenticação do cliente DDNS, o servidor DDNS informa o servidor DNS para atualizar o nome de domínio e o endereço IP do cliente DDNS.

Nesta versão de software atual, o DDNS é suportado apenas pelo DNS IPv4. Ele é usado para atualizar os mapeamentos entre nomes de domínio e endereços IPv4.

Uma política DDNS contém o endereço do servidor DDNS, nome de usuário, senha, política associada de cliente SSL e intervalo de tempo de atualização. Após criar uma política DDNS, você pode aplicá-la a várias interfaces para simplificar a configuração DDNS.



IPv6

O IPv6, também chamado de Próxima Geração do IP (IPng), foi projetado pela IETF como o sucessor do IPv4. Uma diferença significativa entre o IPv6 e o IPv4 é que o IPv6 aumenta o tamanho do endereço IP de 32 bits para 128 bits.

Formatos de endereços IPv6

Um endereço IPv6 é representado como um conjunto de hexadecimais de 16 bits separados por dois pontos (:). Um endereço IPv6 é dividido em oito grupos, e cada grupo de 16 bits é representado por quatro números hexadecimais, por exemplo, 2001:0000:130F:0000:0000:09C0:876A:130B.

Para simplificar a representação de endereços IPv6, você pode lidar com zeros em endereços IPv6 usando os seguintes métodos:

Os zeros à esquerda em cada grupo podem ser removidos. Por exemplo, o endereço acima pode ser representado em um formato mais curto como 2001:0:130F:0:0:9C0:876A:130B. Se um endereço IPv6 contiver um ou mais grupos consecutivos de zeros, eles podem ser substituídos por dois pontos duplos (::). Por exemplo, o endereço acima pode ser representado no formato mais curto como 2001:0:130F::9C0:876A:130B. Um endereço IPv6 é composto por um prefixo de endereço e um identificador de interface, que são equivalentes ao ID de rede e ao ID de host de um endereço IPv4.

Um prefixo de endereço IPv6 é escrito na notação de endereço IPv6/prefixo. O prefixo do endereço é um número decimal que indica quantos bits à esquerda do endereço IPv6 estão no prefixo do endereço.

Tipos de endereços IPv6

Os endereços IPv6 incluem os seguintes tipos:

- **Endereço unicast** Um identificador para uma única interface, semelhante a um endereço IPv4 unicast. Um pacote enviado para um endereço unicast é entregue à interface identificada por esse endereço.
- **Endereço multicast** Um identificador para um conjunto de interfaces (geralmente pertencentes a diferentes nós), semelhante a um endereço multicast IPv4. Um pacote enviado para um endereço multicast é entregue a todas as interfaces identificadas por esse endereço. Os endereços de transmissão são substituídos por endereços multicast no IPv6.
- **Endereço anycast** Um identificador para um conjunto de interfaces (geralmente pertencentes a diferentes nós). Um pacote enviado para um endereço anycast é entregue à interface mais próxima entre as interfaces identificadas por esse endereço. A interface mais próxima é escolhida de acordo com a medida de distância do protocolo de roteamento.

O tipo de um endereço IPv6 é designado pelos primeiros bits, chamados prefixo de formato. A tabela a seguir mostra as correspondências entre tipos de endereço e prefixos de formato:

	Tipo	Prefixo de Formato (binário)	ID de Prefixo IPv6	Observações
Endereço unicast	Endereço não especificado	00...0 (128 bits)	::/128	Não pode ser atribuído a nenhum nó. Antes de adquirir um endereço IPv6 válido, um nó preenche esse endereço no campo de endereço de origem dos pacotes IPv6. O endereço não especificado não pode ser usado como um endereço de destino IPv6.
	Endereço de loopback	00...1 (128 bits)	::1/128	Tem a mesma função que o endereço de loopback no IPv4. Não pode ser atribuído a nenhuma interface física. Um nó usa este endereço para enviar um pacote IPv6 para si mesmo.
	Endereço de link local	1111111010	FE80::/10	Usado para comunicação entre nós de link local para descoberta de vizinho e autoconfiguração sem estado. Pacotes com endereços de origem ou destino de link local não são encaminhados para outros links.
	Endereço global unicast	Outras formas	N/A	Equivalente a endereços IPv4 públicos, os endereços globais unicast são fornecidos para provedores de serviços de Internet. Este tipo de endereço permite a agregação de prefixos para restringir o número de entradas de roteamento global.
	Endereço multicast	11111111	FF00::/8	N/A
	Endereço anycast	Endereços anycast usam o espaço de endereço unicast e têm a mesma estrutura de endereços unicast.	N/A	N/A

Identificadores de interface baseados em endereço EUI-64

Um identificador de interface tem 64 bits de comprimento e identifica exclusivamente uma interface em um link. As interfaces geram identificadores de interface baseados em endereço EUI-64 de maneiras diferentes.

Em uma interface IEEE 802 (como uma interface Ethernet e uma interface VLAN)O identificador de interface é derivado do endereço de camada de link (normalmente um endereço MAC) da interface. O endereço MAC tem 48 bits de comprimento.
Para obter um identificador de interface baseado em endereço EUI-64, siga estas etapas:

- Insira o número binário de 16 bits 1111111111111110 (valor hexadecimal de FFFE) após o 24º bit de alta ordem do endereço MAC.
- Inverta o bit universal/local (U/L) (o sétimo bit de alta ordem). Essa operação faz com que o identificador de interface tenha o mesmo significado local ou global que o endereço MAC.
- Em uma interface de tunelamento - Os 32 bits inferiores do identificador de interface baseado em endereço EUI-64 são o endereço IPv4 de origem da interface de tunelamento. Os 32 bits superiores do identificador de interface baseado em endereço EUI-64 de uma interface de tunelamento ISATAP são 0000:5EFE, enquanto os de outras interfaces de tunelamento são todos zeros.

- Em uma interface de outro tipo (como uma interface serial) - O identificador de interface baseado em endereço EUI-64 é gerado aleatoriamente pelo dispositivo.

Métodos de configuração de endereços globais unicast IPv6

Use um dos seguintes métodos para configurar um endereço global unicast IPv6 para uma interface:

- **Endereço IPv6 EUI-64** - O prefixo de endereço IPv6 da interface é configurado manualmente, e o identificador de interface é gerado automaticamente pela interface.
- **Configuração manual** - O endereço global unicast IPv6 é configurado manualmente.
- **Autoconfiguração de endereço sem estado** - O endereço global unicast IPv6 é gerado automaticamente de acordo com as informações do prefixo de endereço contidas na mensagem RA e o identificador de interface baseado em endereço EUI-64.
- **Autoconfiguração de endereço com estado** - Permite que um host adquira um endereço IPv6 de um servidor DHCPv6.

Você pode configurar vários endereços globais unicast IPv6 em uma interface.

Métodos de configuração de endereços de link local IPv6

Configure endereços de link local IPv6 usando um dos seguintes métodos para uma interface:

- **Geração automática** - O dispositivo gera automaticamente um endereço de link local para uma interface de acordo com o prefixo de endereço de link local (FE80::/10) e o identificador de interface baseado em endereço EUI-64.
- **Atribuição manual** - Um endereço de link local IPv6 é configurado manualmente.

Uma interface pode ter apenas um endereço de link local. Como boa prática, use o método de geração automática para evitar conflitos de endereço de link local. Se ambos os métodos forem usados, a atribuição manual tem precedência sobre a geração automática.

Se você usar a geração automática primeiro e, em seguida, a atribuição manual, o endereço de link local atribuído manualmente substituirá o gerado automaticamente.

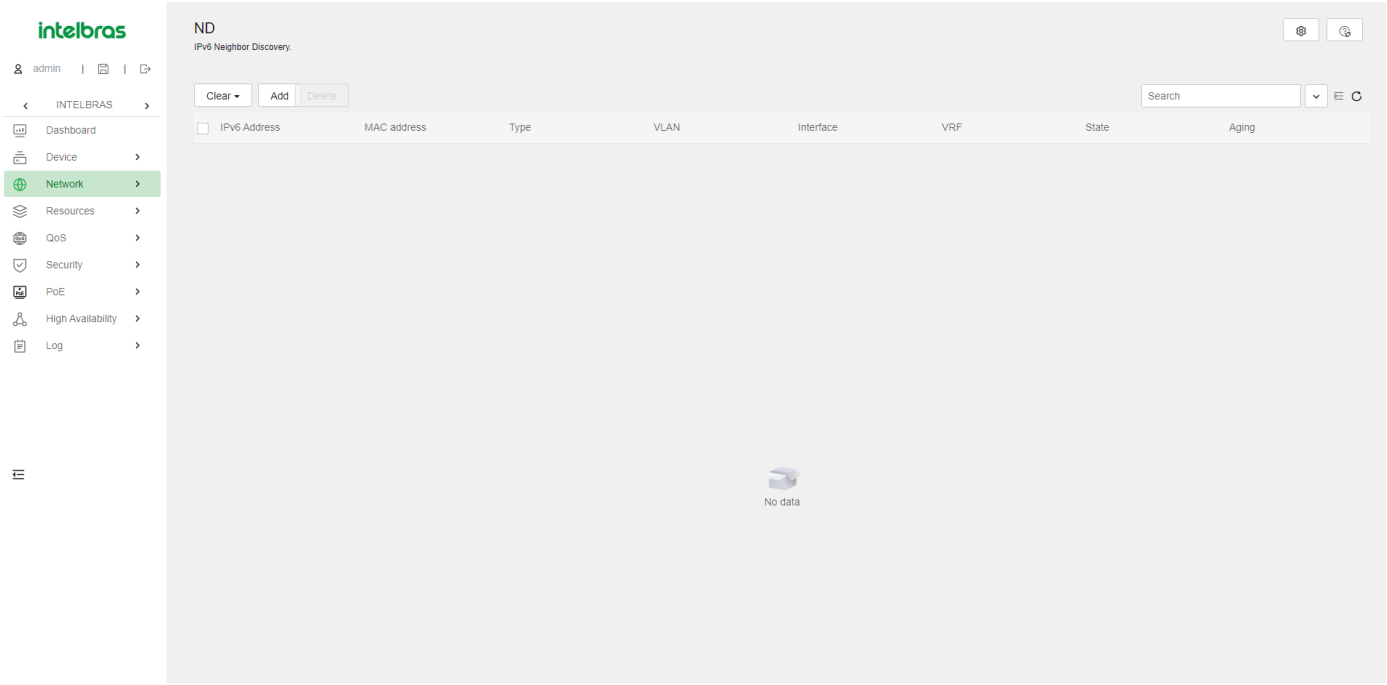
Se você usar a atribuição manual primeiro e, em seguida, a geração automática, ambos os seguintes ocorrem:

- O endereço de link local ainda é o atribuído manualmente.
- O endereço de link local gerado automaticamente não entra em vigor. Se você excluir o endereço atribuído manualmente, o endereço de link local gerado automaticamente entra em vigor.

ND - Neighbor Discovery

O protocolo de Descoberta de Vizinhos IPv6 (ND - Neighbor Discovery) usa mensagens ICMPv6 para fornecer as seguintes funções:

- Resolução de endereços
- Deteção de acessibilidade de vizinhos
- DAD (Duplicated Address Detection)
- Descoberta de roteador/prefixo
- Autoconfiguração de endereço sem estado
- Redirecionamento



A Tabela 17 descreve as mensagens ICMPv6 usadas pelo ND.

Mensagem ICMPv6	Tipo	Função
Solicitação de Vizinho (NS - Neighbor Solicitation)	135	Obtém o endereço da camada de enlace de um vizinho.
Anúncio de Vizinho (NA - Neighbor Advertisement)	136	Responde a uma mensagem NS.
Solicitação de Roteador (RS - Router Solicitation)	133	Solicita um prefixo de endereço e outras informações de configuração para autoconfiguração após a inicialização.
Anúncio de Roteador (RA - Router Advertisement)	134	Responde a uma mensagem RS.
Redirecionamento	137	Informa o host de origem de um próximo salto melhor no caminho para um destino específico quando certas condições são atendidas.

Entradas de Vizinhos

Uma entrada de vizinho armazena informações sobre um nó vizinho na rede. As entradas de vizinhos podem ser configuradas dinamicamente por meio de mensagens NS e NA ou configuradas manualmente.

Você pode configurar uma entrada de vizinho estática usando um dos seguintes métodos:

Método 1 - Associe o endereço IPv6 de um vizinho e o endereço de camada de enlace com a interface de camada 3 local.
Se você usar o Método 1, o dispositivo encontra automaticamente a porta de camada 2 conectada ao vizinho.

Método 2 - Associe o endereço IPv6 de um vizinho e o endereço de camada de enlace com uma porta de camada 2 em uma VLAN.
Se você usar o Método 2, certifique-se de que a interface de VLAN correspondente exista e que a porta de camada 2 pertença à VLAN.

Mensagens RA (Anúncio de Roteador)

Uma mensagem RA é anunciada por um roteador para todos os hosts na mesma rede. A mensagem RA contém o prefixo de endereço e outras informações de configuração para permitir que os hosts gerem endereços IPv6 por meio da autoconfiguração de endereço sem estado.

Você pode habilitar uma interface para enviar mensagens RA, especificar os intervalos de envio máximo e mínimo e configurar parâmetros nas mensagens RA. O dispositivo envia mensagens RA em intervalos aleatórios entre os intervalos máximo e mínimo. O intervalo mínimo deve ser menor ou igual a 0,75 vezes o intervalo máximo.

A Tabela 18 descreve os parâmetros configuráveis em uma mensagem RA.

Parâmetro	Descrição
Prefixo IPv6/comprimento do prefixo	O prefixo IPv6/comprimento do prefixo para um host gerar um endereço global unicast IPv6 por meio da autoconfiguração sem estado.
Tempo de vida válido	Especifica o tempo de vida válido de um prefixo. O endereço IPv6 gerado é válido dentro do tempo de vida válido e se torna inválido quando o tempo de vida válido expira.
Tempo de vida preferido	Especifica o tempo de vida preferido de um prefixo usado para a autoconfiguração sem estado. Após o término do tempo de vida preferido, o nó não pode usar o endereço IPv6 gerado para estabelecer novas conexões, mas pode receber pacotes destinados ao endereço IPv6. O tempo de vida preferido não pode ser maior do que o tempo de vida válido.
Flag de Não Autoconfiguração	Informa aos hosts que não usem o prefixo de endereço para autoconfiguração sem estado.
Flag Fora da Rede (Off-link)	Especifica o endereço com o prefixo para ser indiretamente acessível na rede.
MTU	Garante que todos os nós na rede usem o mesmo MTU.
Flag de Saltos Ilimitados	Especifica saltos ilimitados nas mensagens RA.
Flag M	Determina se um host usa a autoconfiguração com estado para obter um endereço IPv6.
Flag O	Determina se um host usa a autoconfiguração com estado para obter informações de configuração diferentes do endereço IPv6.
Vida do Roteador	Informa sobre a vida útil de um roteador anunciante. Se a vida útil for 0, o roteador não pode ser usado como o gateway padrão.
Temporizador de Retransmissão	Especifica o intervalo para retransmitir a mensagem NS após o dispositivo não receber uma resposta para uma mensagem NS dentro de um período de tempo.
Preferência do Roteador	Especifica a preferência do roteador em uma mensagem RA. Um host seleciona um roteador como o gateway padrão de acordo com a preferência do roteador. Se as preferências dos roteadores forem iguais, o host seleciona o roteador do qual recebeu a primeira mensagem RA.
Tempo Alcançável	Especifica o período alcançável para um vizinho após o dispositivo detectar que um vizinho está alcançável. Se o dispositivo precisar enviar um pacote para o vizinho após o período alcançável, o dispositivo reconfirma se o vizinho está alcançável.

ND Proxy

O ND Proxy permite que um dispositivo responda a uma mensagem NS que solicita o endereço de hardware de um host em outra rede. Com o ND Proxy, hosts em diferentes domínios de broadcast podem se comunicar entre si como se estivessem na mesma rede.

O ND Proxy inclui o ND Proxy comum e o ND Proxy local.

ND Proxy Comum

Conforme mostrado na Figura 6, a Interface A com endereço IPv6 4:1::96/64 e a Interface B com endereço IPv6 4:2::99/64 pertencem a sub-redes diferentes. O Host A e o Host B estão na mesma rede, mas em domínios de broadcast diferentes.

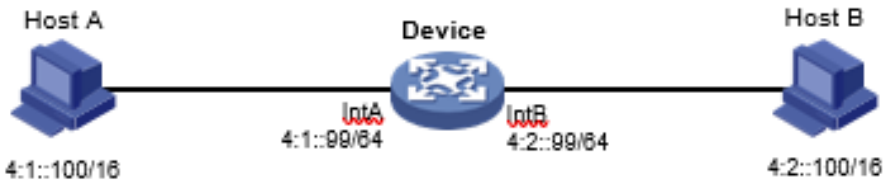


Figura 6 Ambiente de aplicação do ND Proxy comum

Devido ao endereço IPv6 do Host A estar na mesma sub-rede que o Host B, o Host A envia diretamente uma mensagem NS para obter o endereço MAC do Host B. No entanto, o Host B não pode receber a mensagem NS porque eles pertencem a domínios de broadcast diferentes.

Para resolver esse problema, habilite o ND Proxy comum na Interface A e na Interface B do dispositivo. O dispositivo responde à mensagem NS do Host A e encaminha pacotes de outros hosts para o Host B.

ND Proxy Local

Conforme mostrado na Figura 7, o Host A pertence à VLAN 2 e o Host B pertence à VLAN 3. O Host A e o Host B estão conectados à Interface A e à Interface C, respectivamente.

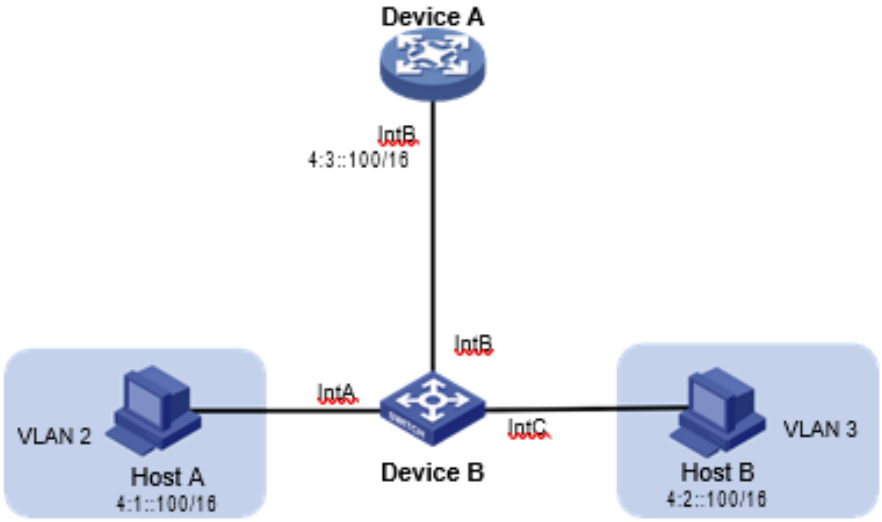


Figura 7 Ambiente de aplicação do ND Proxy local

Devido ao endereço IPv6 do Host A estar na mesma sub-rede que o Host B, o Host A envia diretamente uma mensagem NS para obter o endereço MAC do Host B. No entanto, o Host B não pode receber a mensagem NS porque eles estão em VLANs diferentes.

Para resolver esse problema, habilite o ND Proxy local na Interface B do roteador, para que o roteador possa encaminhar mensagens entre o Host A e o Host B.

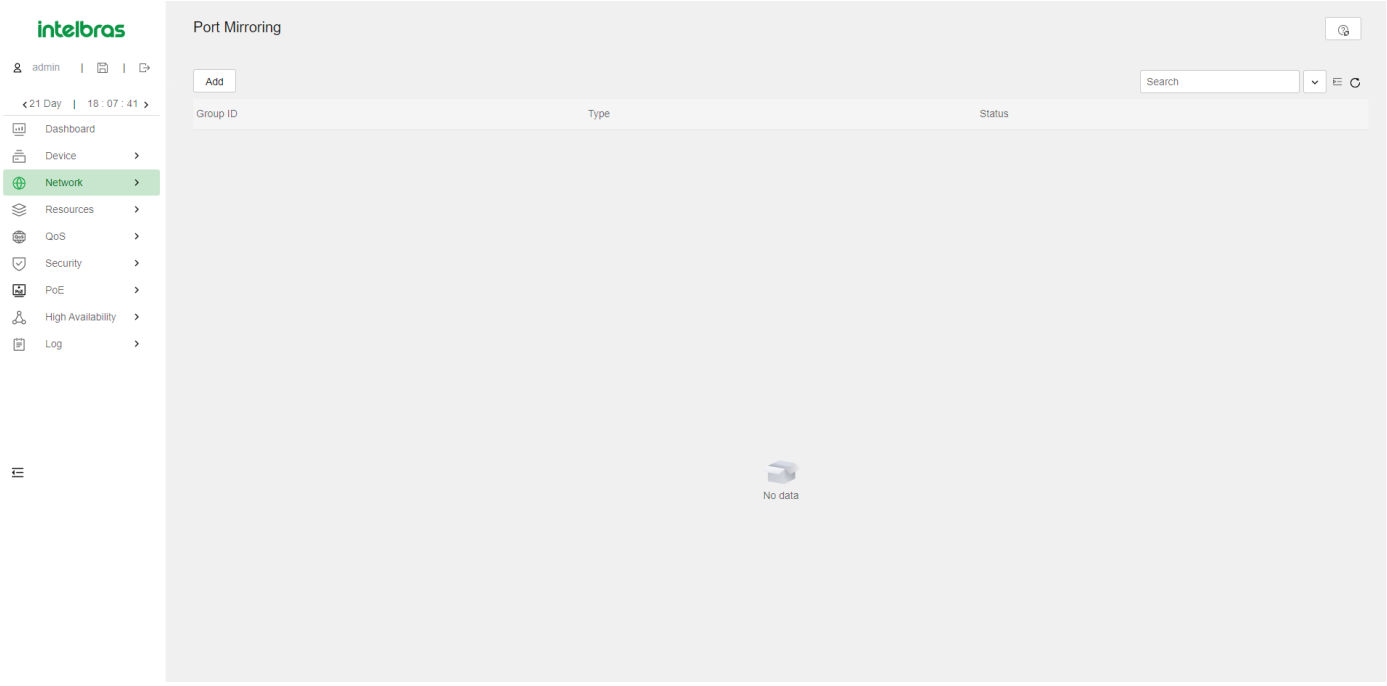
Port Mirroring

O port mirroring (espelhamento de porta) copia os pacotes que passam por uma porta para a porta de destino que se conecta a um dispositivo de monitoramento de dados para análise de pacotes. As cópias são chamadas de pacotes espelhados.

O espelhamento de porta possui os seguintes termos:

- **Porta de origem (Source port)** - Porta monitorada no dispositivo. Os pacotes da porta monitorada serão copiados e enviados para a porta de destino.
- **Dispositivo de origem (Source device)** - Dispositivo onde uma porta de origem reside.

- **Porta de destino (Destination port)** - Porta que se conecta ao dispositivo de monitoramento de dados. Os pacotes da porta de origem serão copiados e enviados para a porta de destino.
- **Dispositivo de destino (Destination device)** - Dispositivo onde a porta de destino reside.
- **Grupo de espelhamento (Mirroring group)** - Inclui o grupo de espelhamento local e o grupo de espelhamento remoto.
- **Grupo de espelhamento local (Local mirroring group)** - A porta de origem e a porta de destino estão no mesmo dispositivo. Um grupo de espelhamento local é um grupo de espelhamento que contém as portas de origem e a porta de destino no mesmo dispositivo.
- **Espelhamento de porta remota (Remote Port Mirroring)** - A porta de origem e a porta de destino estão em dispositivos diferentes. Um grupo de origem remota é um grupo de espelhamento que contém as portas de origem. Um grupo de destino remoto é um grupo de espelhamento que contém a porta de destino. No espelhamento de porta remota, os pacotes espelhados são transmitidos pela VLAN de sonda remota do dispositivo de origem para o dispositivo de destino.



Rotas Estáticas

Rotas estáticas são configuradas manualmente. Se a topologia de uma rede for simples, você só precisa configurar rotas estáticas para que a rede funcione corretamente.

Rotas estáticas não podem se adaptar a mudanças na topologia da rede. Se ocorrer uma falha ou uma mudança topológica na rede, o administrador de rede deve modificar as rotas estáticas manualmente.

Uma rota padrão é usada para encaminhar pacotes que não correspondem a nenhuma entrada de roteamento específica na tabela de roteamento. Você pode configurar uma rota IPv4 padrão com o endereço de destino 0.0.0.0/0 e configurar uma rota IPv6 padrão com o endereço de destino ::/0.

OSPF (Open Shortest Path First)

O Open Shortest Path First (OSPF) é um IGP (Protocolo de Gateway Interno) baseado em estado de link que encapsula seus dados diretamente em pacotes IP usando o número de protocolo 89. O OSPF se aplica a redes de vários tamanhos e pode suportar no máximo centenas de roteadores.

O OSPF oferece suporte aos modos de autenticação MD5/HMAC-MD5 e autenticação de interface simples para evitar vazamento de rotas e ataques.

BGP (Border Gateway Protocol)

O Protocolo de Gateway de Borda (BGP) é um protocolo de gateway externo (EGP). Ele é chamado de BGP interno (IBGP) quando é executado dentro de um Sistema Autônomo (AS) e chamado de BGP externo (EBGP) quando é executado entre ASs. Um AS refere-se a um grupo de roteadores que utilizam a mesma política de roteamento e operam sob a mesma administração.

Peer BGP

Um roteador executando o BGP é um BGP speaker. Um BGP speaker estabelece relacionamentos de par com outros BGP speakers para trocar informações de roteamento por meio de conexões TCP.

Os pares do BGP incluem os seguintes tipos:

Pares IBGP - Residem no mesmo AS que o roteador local.

Pares EBGP - Residem em ASs diferentes do roteador local.

Famílias de endereços BGP

Conforme mostrado na Tabela 19, o BGP define várias famílias de endereços para transmitir informações de roteamento diferentes.

Família de Endereços	Função
BGP IPv4 unicast	Transmite as rotas unicast IPv4 na rede pública.

BGP IPv4 multicast	O PIM usa rotas unicast estáticas e dinâmicas para realizar a verificação RPF antes de criar entradas de roteamento multicast. Quando as topologias multicast e unicast são diferentes, você pode usar o MP-BGP para anunciar as rotas para verificação RPF. O MP-BGP armazena as rotas na tabela de roteamento multicast BGP.
BGP IPv4 MDT	O MP-BGP anuncia informações MDT, incluindo o endereço PE e o grupo padrão, para que a VPN multicast possa criar um MDT padrão que usa o PE como raiz na rede pública.
BGP VPNv4	Transmite rotas VPNv4.
BGP IPv6 unicast	Transmite as rotas unicast IPv6 na rede pública.
BGP IPv6 multicast	O PIM usa rotas unicast estáticas e dinâmicas para realizar a verificação RPF antes de criar entradas de roteamento multicast. Quando as topologias multicast e unicast são diferentes, você pode usar o MP-BGP para anunciar as rotas para verificação RPF. O MP-BGP armazena as rotas na tabela de roteamento multicast BGP.
BGP VPNv6	Transmite rotas VPNv6.
BGP L2VPN	Transmite informações de bloco de rótulo L2VPN e informações de pares remotos.

Redistribuir rotas externas para o BGP

Os pares BGP podem trocar informações de roteamento. No entanto, o BGP não descobre ativamente informações de roteamento. Em vez disso, as rotas externas (por exemplo, rotas IGP) são redistribuídas na tabela de roteamento da família de endereços especificada e anunciadas para os pares.

Roteamento baseado em política

O roteamento baseado em política (PBR) utiliza políticas definidas pelo usuário para rotear pacotes. Uma política pode especificar próximos saltos para pacotes que atendem a critérios específicos, como ACLs.

Política

Uma política inclui critérios de correspondência e ações a serem executadas nos pacotes correspondentes. Uma política pode ter um ou vários nós, da seguinte forma:

Cada nó é identificado por um número de nó. Um número de nó menor tem uma prioridade mais alta. Um nó contém os seguintes elementos: **Critério de correspondência** - Usa uma ACL para corresponder a pacotes. **Ação** - Define um próximo salto para os pacotes permitidos. Você pode associar um próximo salto a uma entrada de rastreamento e especificar se o próximo salto está diretamente conectado. Um nó possui um modo de correspondência de **permitir** ou **negar**.

Uma política corresponde a nós por ordem de prioridade em relação aos pacotes. Se um pacote corresponde aos critérios em um nó, ele é processado pela ação no nó. Se o pacote não corresponder aos critérios no nó, ele passará para o próximo nó para uma correspondência. Se o pacote não corresponder aos critérios em nenhum nó, ele será encaminhado de acordo com a tabela de roteamento.

PBR e Track

O PBR pode trabalhar com o recurso Track para adaptar dinamicamente o status de uma ação ao status de disponibilidade de um próximo salto rastreado.

Quando a entrada de rastreamento muda para **Negativo**, a ação é inválida.

Quando a entrada de rastreamento muda para **Positivo** ou **Não Pronto**, a ação é válida.

Roteamento de Multicast

Para que outras funcionalidades de multicast de camada 3 (como IGMP e PIM) tenham efeito, primeiro é necessário habilitar o roteamento de multicast IPv4.

As tabelas a seguir estão envolvidas no roteamento de multicast IPv4 e encaminhamento:

- Tabela de roteamento de multicast IPv4 de cada protocolo de roteamento de multicast, como a tabela de roteamento PIM.
- Tabela geral de roteamento de multicast IPv4 que resume as informações de roteamento de multicast geradas por diferentes protocolos de roteamento de multicast.

Protocolo Independente de Multicast (PIM)

O Protocolo Independente de Multicast (PIM) fornece o encaminhamento de multicast IP aproveitando rotas estáticas de unicast ou tabelas de roteamento de unicast geradas por qualquer protocolo de roteamento de unicast. O PIM usa o roteamento de unicast subjacente para gerar uma tabela de roteamento de multicast sem depender de nenhum protocolo de roteamento de unicast específico.

Com base no mecanismo de implementação, o PIM inclui as seguintes categorias:

- Protocolo Independente de Multicast – Modo Denso (PIM-DM) – O PIM-DM é adequado para redes de pequeno porte com membros de multicast distribuídos densamente.
- Protocolo Independente de Multicast – Modo Esparsa (PIM-SM) – O PIM-SM é adequado para redes de médio e grande porte com membros de grupos de multicast distribuídos de forma esparsa e ampla.
- Protocolo Independente de Multicast – Multicast Específico de Fonte (PIM-SSM) – O PIM-SSM pode ser implementado aproveitando parte da técnica PIM-SM. Antes de configurar o PIM-SSM, você deve primeiro habilitar o PIM-SM.

  Se você habilitar o PIM-DM em uma interface, será usado o modo PIM-DM. Se você habilitou o PIM-SM em uma interface, o modo PIM na interface varia de acordo com o grupo de multicast para o qual um pacote de multicast é destinado.

- Se o grupo de multicast estiver na faixa de grupos SSM, será usado o modo PIM-SSM.
- Se o grupo de multicast não estiver na faixa de grupos SSM, será usado o modo PIM-SM.

Protocolo de Gerenciamento de Grupo da Internet (IGMP)

O Protocolo de Gerenciamento de Grupo da Internet (IGMP) estabelece e mantém as associações de grupos de multicast entre um dispositivo de multicast de Camada 3 e os hosts na sub-rede diretamente conectada.

O IGMP possui as seguintes versões:

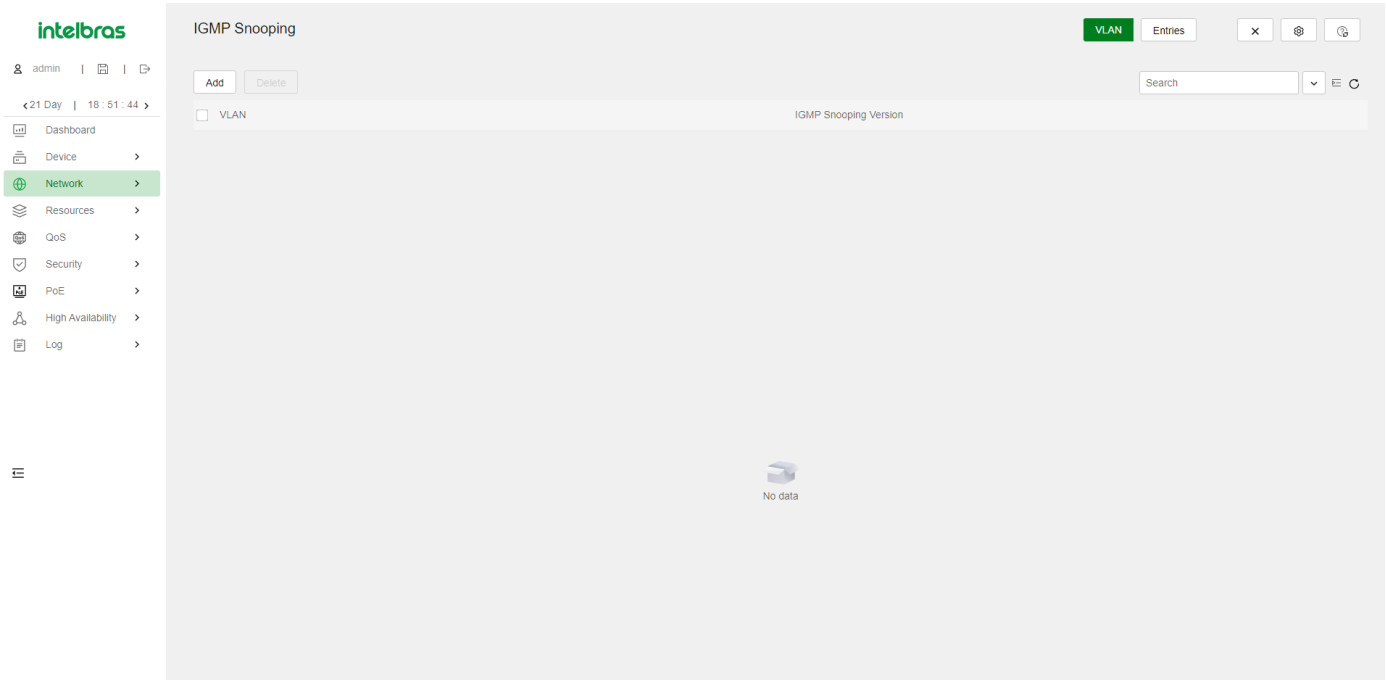
- **IGMPv1** - O IGMPv1 gerencia as associações de grupos de multicast com base no mecanismo de consulta e resposta.
- **IGMPv2** - Compatível com o IGMPv1, o IGMPv2 introduziu um mecanismo de eleição de consultor e um mecanismo de saída de grupo.
- **IGMPv3** - Com base e compatível com o IGMPv1 e o IGMPv2, o IGMPv3 aprimora as capacidades de controle dos hosts e as capacidades de consulta e relatório dos roteadores IGMP. O IGMPv3 introduziu dois modos de filtragem de fontes (Incluir e Excluir). Esses modos permitem que um host receba ou rejeite dados de multicast das fontes de multicast especificadas.

Após a ativação do IGMP em uma interface, a interface pode estabelecer e manter associações de grupos de multicast.

IGMP Snooping

O IGMP Snooping é executado em um dispositivo de Camada 2 como um mecanismo de restrição de multicast. Ele cria entradas de encaminhamento de multicast de Camada 2 a partir de pacotes IGMP trocados entre os hosts e o dispositivo de Camada 3.

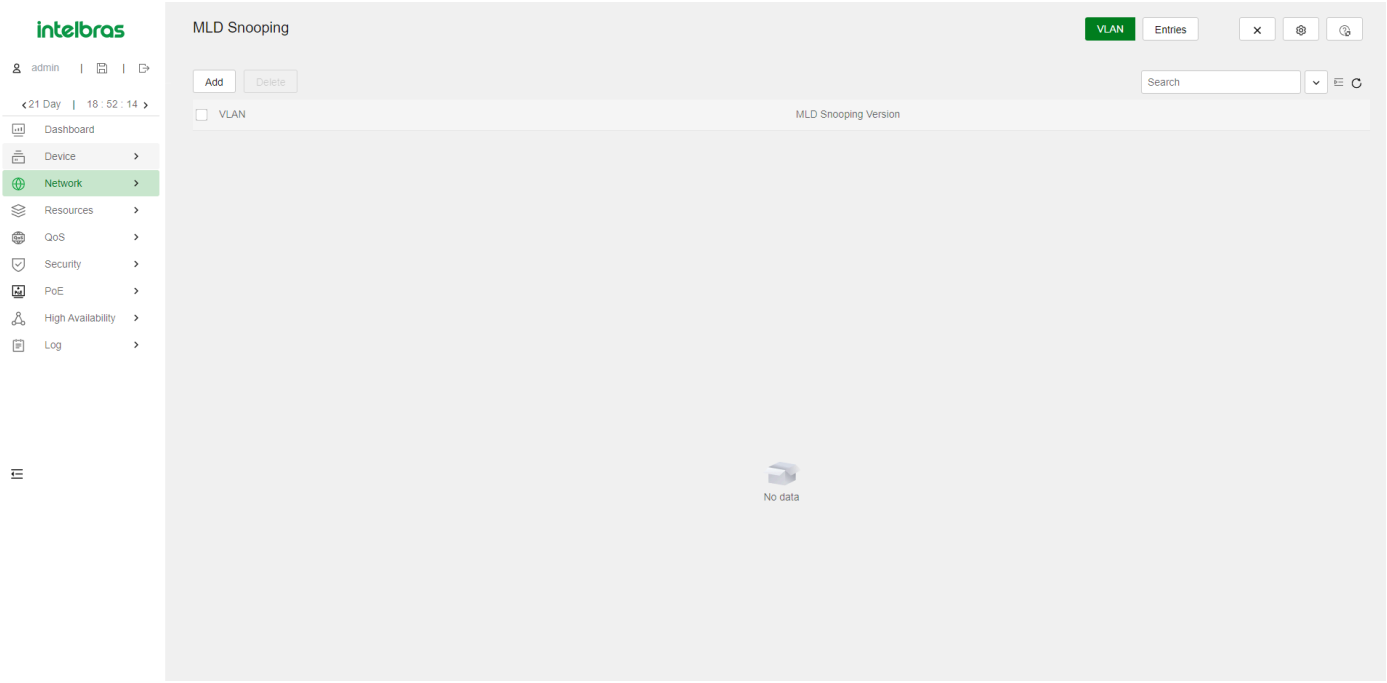
O dispositivo de Camada 2 encaminha dados de multicast com base nas entradas de encaminhamento de multicast de Camada 2. Uma entrada de encaminhamento de multicast de Camada 2 contém a VLAN, o endereço do grupo de multicast, o endereço da fonte de multicast e as portas de host. Uma porta de host é uma porta do lado receptor de multicast no dispositivo de multicast de Camada 2.



MLD Snooping

O MLD Snooping é executado em um dispositivo de Camada 2 como um mecanismo de restrição de multicast IPv6. Ele cria entradas de encaminhamento de multicast IPv6 de Camada 2 a partir de pacotes MLD trocados entre os hosts e o dispositivo de Camada 3.

O dispositivo de Camada 2 encaminha dados de multicast com base nas entradas de encaminhamento de multicast IPv6 de Camada 2. Uma entrada de encaminhamento de multicast IPv6 de Camada 2 contém a VLAN, o endereço do grupo de multicast IPv6, o endereço da fonte de multicast IPv6 e as portas de host. Uma porta de host é uma porta do lado receptor de multicast no dispositivo de multicast de Camada 2.



Protocolo de Configuração Dinâmica de Host (DHCP)

O Protocolo de Configuração Dinâmica de Host (DHCP) fornece uma estrutura para atribuir informações de configuração a dispositivos de rede.

Um cenário típico de aplicação do DHCP envolve um servidor DHCP e vários clientes DHCP implantados na mesma sub-rede. Os clientes DHCP também podem obter parâmetros de configuração de um servidor DHCP em outra sub-rede por meio de um agente de retransmissão DHCP.

Servidor DHCP

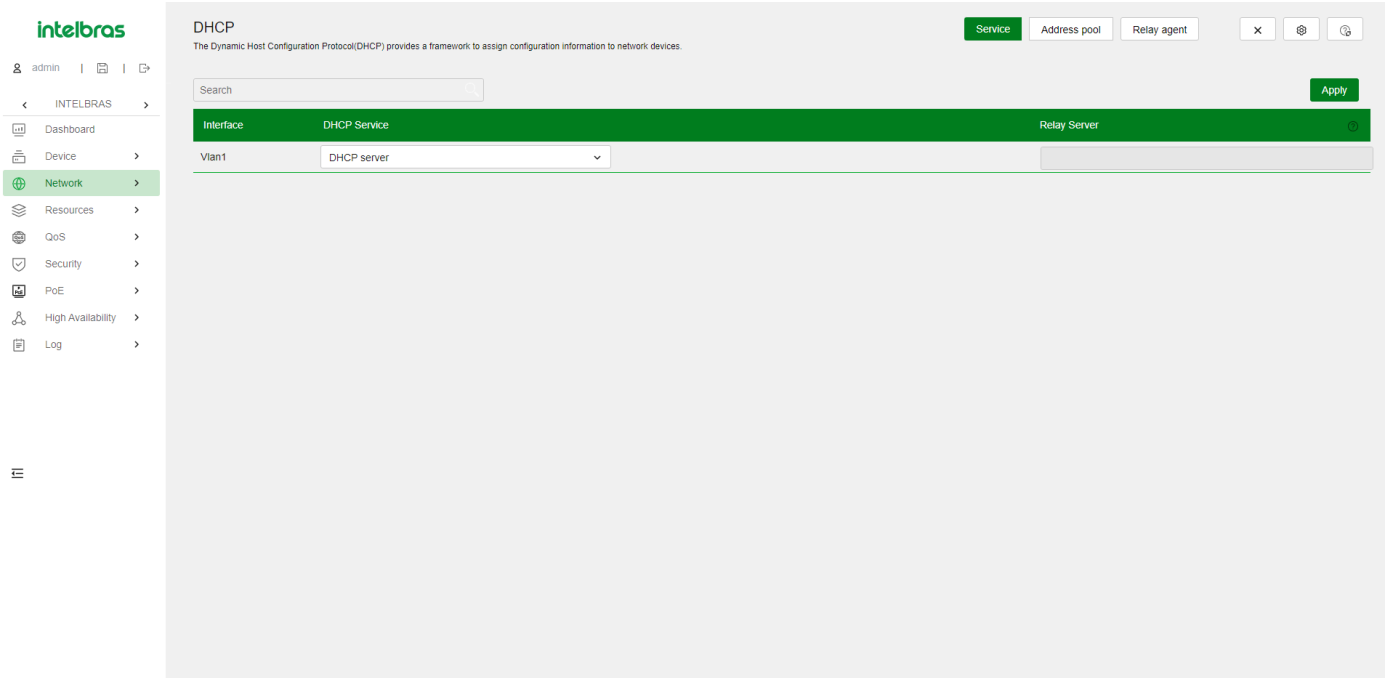
O servidor DHCP é adequado para redes onde:

- A configuração manual e a administração centralizada são difíceis de implementar.
- Os endereços IP são limitados. Por exemplo, um provedor de serviços de Internet limita o número de usuários online simultâneos, e os usuários devem adquirir endereços IP dinamicamente.
- A maioria dos hosts não precisa de endereços IP fixos.

  O servidor DHCP seleciona endereços IP e outros parâmetros a partir de um pool de endereços e os atribui aos clientes DHCP. Um pool de endereços DHCP contém os seguintes itens:

- Endereços IP atribuíveis.
- Duração do arrendamento.
- Endereços de gateway.
- Sufixo de nome de domínio.
- Endereços de servidores DNS.
- Endereços de servidores WINS.
- Tipo de nó NetBIOS.
- Opções DHCP.

Antes de atribuir um endereço IP, o servidor DHCP realiza a detecção de conflito de endereço IP para verificar se o endereço IP está em uso.



Pool de Endereços DHCP

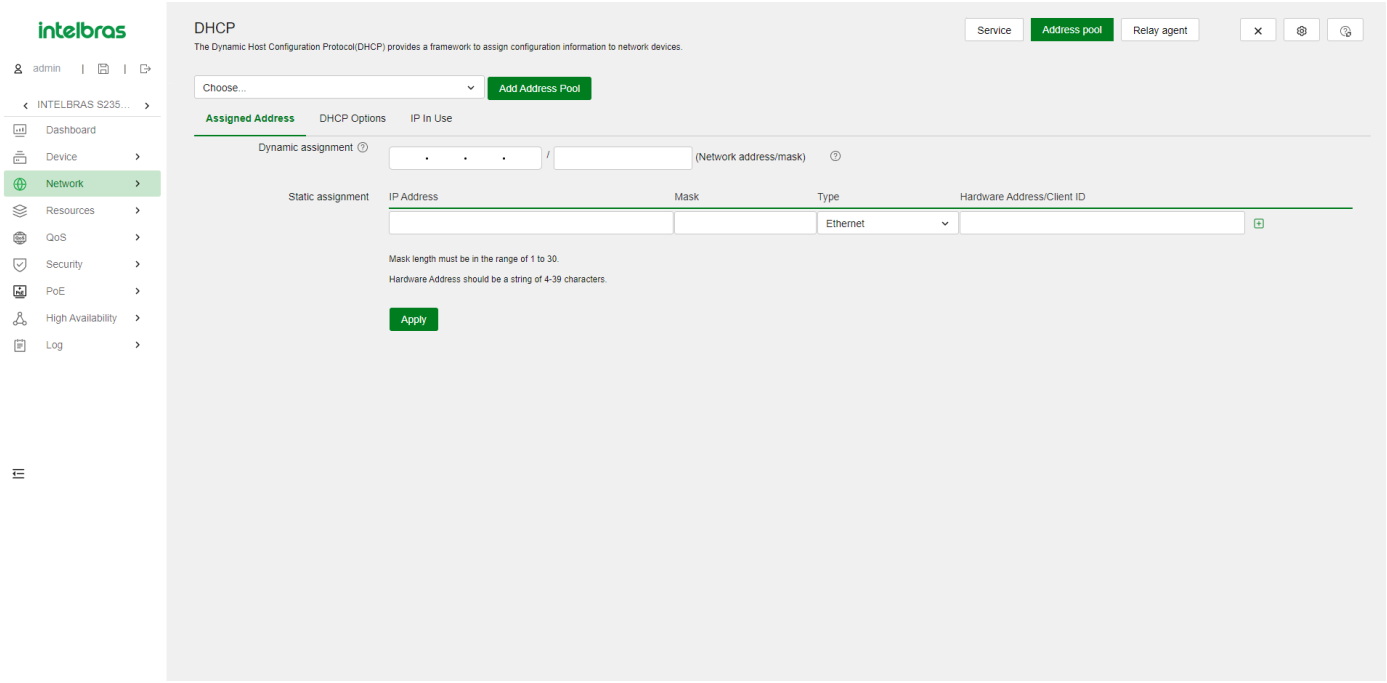
O servidor DHCP oferece suporte aos seguintes mecanismos de atribuição de endereços:

- **Alocação de endereço estático** - Associe manualmente o endereço MAC ou ID de um cliente a um endereço IP em um pool de endereços DHCP. Quando o cliente solicita um endereço IP, o servidor DHCP atribui o endereço IP na associação estática ao cliente.
- **Alocação de endereço dinâmico** - Especifique faixas de endereços IP em um pool de endereços DHCP. Ao receber uma solicitação DHCP, o servidor DHCP seleciona dinamicamente um endereço IP na faixa de endereços IP correspondente no pool.

  Você pode especificar a duração do arrendamento para endereços IP no pool de endereços DHCP.

  O servidor DHCP observa os seguintes princípios para selecionar um pool de endereços para um cliente:

- Se houver um pool de endereços onde um endereço IP está vinculado estaticamente ao endereço MAC ou ID do cliente, o servidor DHCP seleciona esse pool de endereços e atribui o endereço IP vinculado estaticamente e outros parâmetros de configuração ao cliente.
- Se nenhum pool de endereço estático estiver configurado, o servidor DHCP seleciona um pool de endereços com base na localização do cliente.
  - Cliente na mesma sub-rede que o servidor - O servidor DHCP compara o endereço IP da interface receptora com as sub-redes de todos os pools de endereços. Se houver correspondência, o servidor seleciona o pool de endereços com a sub-rede correspondente mais longa.
  - Cliente em uma sub-rede diferente da do servidor - O servidor DHCP compara o endereço IP no campo **giaddr** da solicitação DHCP com as sub-redes de todos os pools de endereços. Se houver correspondência, o servidor seleciona o pool de endereços com a sub-rede correspondente mais longa.



Sequência de Alocação de Endereço IP

O servidor DHCP seleciona um endereço IP para um cliente na seguinte sequência:

1. Endereço IP vinculado estaticamente ao MAC ou ID do cliente.
2. Endereço IP que já foi atribuído ao cliente anteriormente.
3. Endereço IP designado pelo campo Opção 50 na mensagem DHCP-DISCOVER enviada pelo cliente. A Opção 50 é a Opção de Endereço IP Solicitado. O cliente usa esta opção para especificar o endereço IP desejado em uma mensagem DHCP-DISCOVER. O conteúdo da Opção 50 é definido pelo usuário.
4. Primeiro endereço IP atribuível encontrado na escolha de um pool de endereços.
5. Endereço IP que estava em conflito ou que passou do prazo de arrendamento. Se nenhum endereço IP for atribuível, o servidor não responde.

Opções DHCP

O DHCP usa o campo de opções para transportar informações para alocação dinâmica de endereços e fornecer informações adicionais de configuração para clientes.

Você pode personalizar opções para os seguintes fins:

- Adicionar novas opções de DHCP lançadas.
- Adicionar opções para as quais o fornecedor define o conteúdo, por exemplo, Opção 43. Servidores e clientes DHCP podem usar opções específicas do fornecedor para trocar informações de configuração específicas do fornecedor.
- Adicionar opções para as quais a interface Web não fornece uma página de configuração dedicada. Por exemplo, você pode usar a Opção 4 para especificar o endereço do servidor de tempo 1.1.1.1 para clientes DHCP.
- Adicionar todos os valores das opções se o requisito real exceder o limite de uma página de configuração de opção dedicada. Por exemplo, na página de configuração do servidor DNS, você pode especificar até oito servidores DNS. Para especificar mais de oito servidores DNS, você pode usar a Opção 6 para especificar todos os servidores DNS.

A tabela a seguir mostra as opções de DHCP mais comumente usadas.

Número da Opção	Nome da Opção	Formato recomendado de preenchimento
3	Roteador	Endereço IP
6	Servidor de Nome de Domínio	Endereço IP

15	Nome de Domínio	String ASCII
44	Servidor de Nome NetBIOS sobre TCP/IP	Endereço IP
46	Tipo de Nó NetBIOS sobre TCP/IP	String hexadecimal
66	Nome do Servidor TFTP	String ASCII
67	Nome do Arquivo de Inicialização	String ASCII
43	Informações Específicas do Fornecedor	String hexadecimal

Deteção de Conflito de Endereço IP

Antes de atribuir um endereço IP, o servidor DHCP faz ping ao endereço IP.

Se o servidor receber uma resposta dentro do período especificado, ele seleciona e faz ping a outro endereço IP.

Se não receber nenhuma resposta, o servidor continua a fazer ping ao endereço IP até que um número específico de pacotes de ping seja enviado. Se ainda assim não receber nenhuma resposta, o servidor atribui o endereço IP ao cliente solicitante.

Agente de Retransmissão DHCP

O agente de retransmissão DHCP permite que os clientes obtenham endereços IP de um servidor DHCP em outra sub-rede. Essa função evita a implantação de um servidor DHCP para cada sub-rede, centralizando a administração e reduzindo o investimento.

Registro de Entradas de Retransmissão DHCP Dinâmicas

Essa função permite que o agente de retransmissão DHCP registre automaticamente as associações IP-MAC dos clientes (entradas de retransmissão) depois que eles obtêm endereços IP por meio do DHCP.

Algumas funções de segurança usam as entradas de retransmissão para verificar pacotes recebidos e bloquear pacotes que não correspondam a nenhuma entrada. Dessa forma, hosts ilegais não conseguem acessar redes externas por meio do agente de retransmissão. Exemplos de funções de segurança incluem verificação de endereço ARP, ARP autorizado e proteção de origem IP.

Atualização Periódica de Entradas de Retransmissão DHCP Dinâmicas

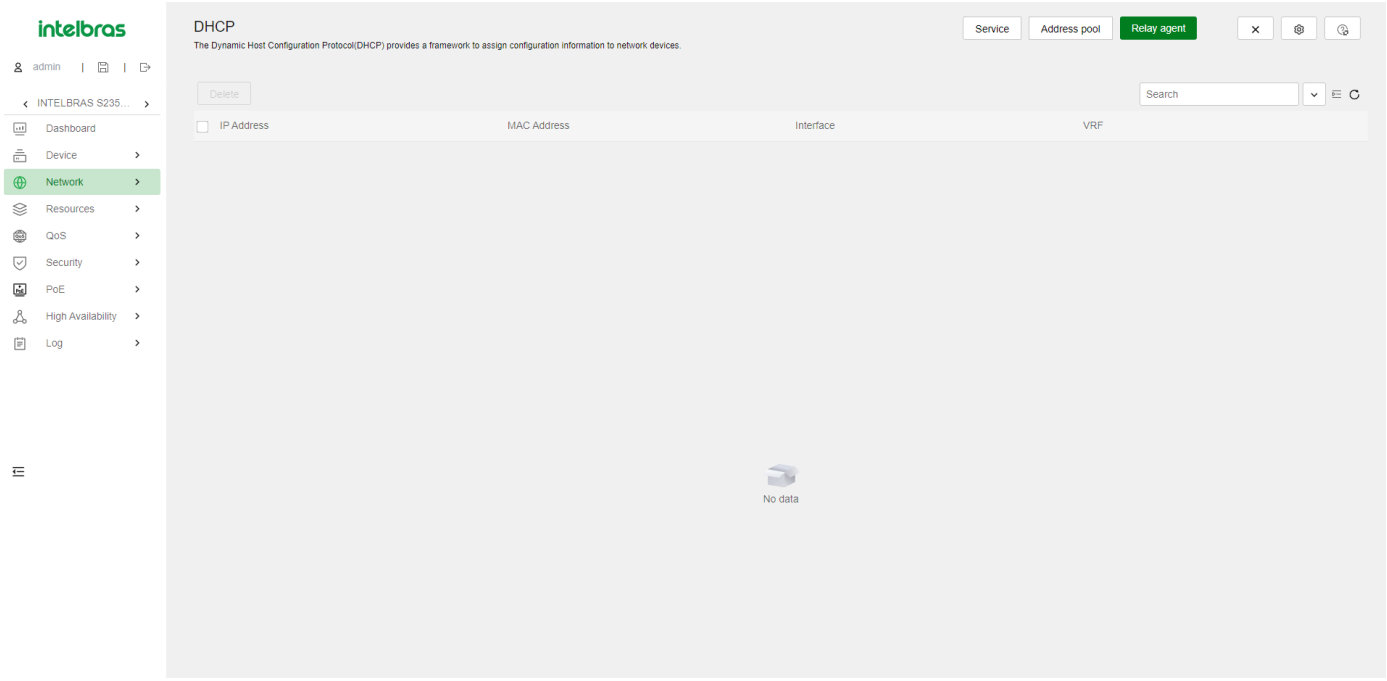
Um cliente DHCP envia uma mensagem DHCP-RELEASE ao servidor DHCP para liberar seu endereço IP. O agente de retransmissão DHCP transmite a mensagem para o servidor DHCP e não remove a entrada IP-MAC do cliente.

Com esse recurso, o agente de retransmissão DHCP usa as seguintes informações para enviar periodicamente uma mensagem DHCP-REQUEST ao servidor DHCP:

- O endereço IP de uma entrada de retransmissão.
- O endereço MAC da interface de retransmissão DHCP.

  O agente de retransmissão mantém as entradas de retransmissão com base no que recebe do servidor DHCP:

- Se o servidor retornar uma mensagem DHCP-ACK ou não retornar nenhuma mensagem dentro de um intervalo, o agente de retransmissão DHCP remove a entrada de retransmissão. Além disso, ao receber a mensagem DHCP-ACK, o agente de retransmissão envia uma mensagem DHCP-RELEASE para liberar o endereço IP.
- Se o servidor retornar uma mensagem DHCP-NAK, o agente de retransmissão mantém a entrada de retransmissão.



HTTP/HTTPS

O dispositivo oferece um servidor web embutido. Após habilitar o servidor web no dispositivo, os usuários podem fazer login na interface web para gerenciar e monitorar o dispositivo.

O servidor web embutido do dispositivo suporta tanto o Protocolo de Transferência de Hipertexto (HTTP) (versão 1) quanto o Protocolo de Transferência de Hipertexto Seguro (HTTPS). O HTTPS é mais seguro que o HTTP devido aos seguintes itens:

- O HTTPS usa SSL para garantir a integridade e segurança dos dados trocados entre o cliente e o servidor.
- O HTTPS permite definir uma política de controle de acesso baseada em atributos de certificado para permitir apenas clientes legais a acessar a interface web.

Você também pode especificar uma ACL básica para HTTP ou HTTPS para evitar o acesso web não autorizado.

Se você não especificar uma ACL para HTTP ou HTTPS, ou a ACL especificada não existir ou não tiver regras, o dispositivo permitirá todos os logins HTTP ou HTTPS.

Se a ACL especificada tiver regras, somente os usuários permitidos pela ACL poderão fazer login na interface web por HTTP ou HTTPS.

SSH

O Secure Shell (SSH) é um protocolo de segurança de rede. Usando criptografia e autenticação, o SSH pode implementar acesso remoto e transferência de arquivos seguros em uma rede insegura.

O SSH utiliza o modelo cliente-servidor típico para estabelecer um canal de transferência de dados seguro baseado no TCP.

O SSH inclui duas versões: SSH1.x e SSH2.0 (a seguir referido como SSH1 e SSH2), que não são compatíveis. O SSH2 é melhor que o SSH1 em desempenho e segurança.

O dispositivo pode atuar como um servidor SSH para fornecer as seguintes aplicações SSH para clientes SSH:

- Telnet Seguro - O Stelnet fornece serviços de acesso seguro e confiável ao terminal de rede. Através do Stelnet, um usuário pode fazer login com segurança em um servidor remoto. O Stelnet pode proteger dispositivos contra ataques, como spoofing de IP e interceptação de senhas em texto simples. O dispositivo pode atuar como um servidor Stelnet ou um cliente Stelnet.
- Protocolo de Transferência de Arquivos Seguro - Com base no SSH2, o SFTP usa conexões SSH para fornecer transferência de arquivos segura.
- Cópia Segura - Com base no SSH2, o SCP oferece um método seguro para copiar arquivos.

- Quando atua como servidor Stelnet, SFTP ou SCP, o dispositivo suporta tanto SSH2 quanto SSH1 no modo não FIPS e somente SSH2 no modo FIPS.

FTP

O Protocolo de Transferência de Arquivos (FTP) é um protocolo de camada de aplicação para transferir arquivos de um host para outro em uma rede IP. Ele usa a porta TCP 20 para transferir dados e a porta TCP 21 para transferir comandos de controle.

O dispositivo pode atuar como servidor FTP.

Telnet

O dispositivo pode atuar como um servidor Telnet para permitir login via Telnet. Após configurar o serviço Telnet no dispositivo, os usuários podem fazer login remotamente no dispositivo para gerenciar e monitorar o dispositivo.

Para evitar logins Telnet não autorizados, você pode usar ACLs para filtrar logins Telnet.

Se você não especificar uma ACL para o serviço Telnet, ou a ACL especificada não existir ou não tiver regras, o dispositivo permitirá todos os logins Telnet.

Se a ACL especificada tiver regras, somente os usuários permitidos pela ACL poderão usar o Telnet para acessar o dispositivo.

NTP

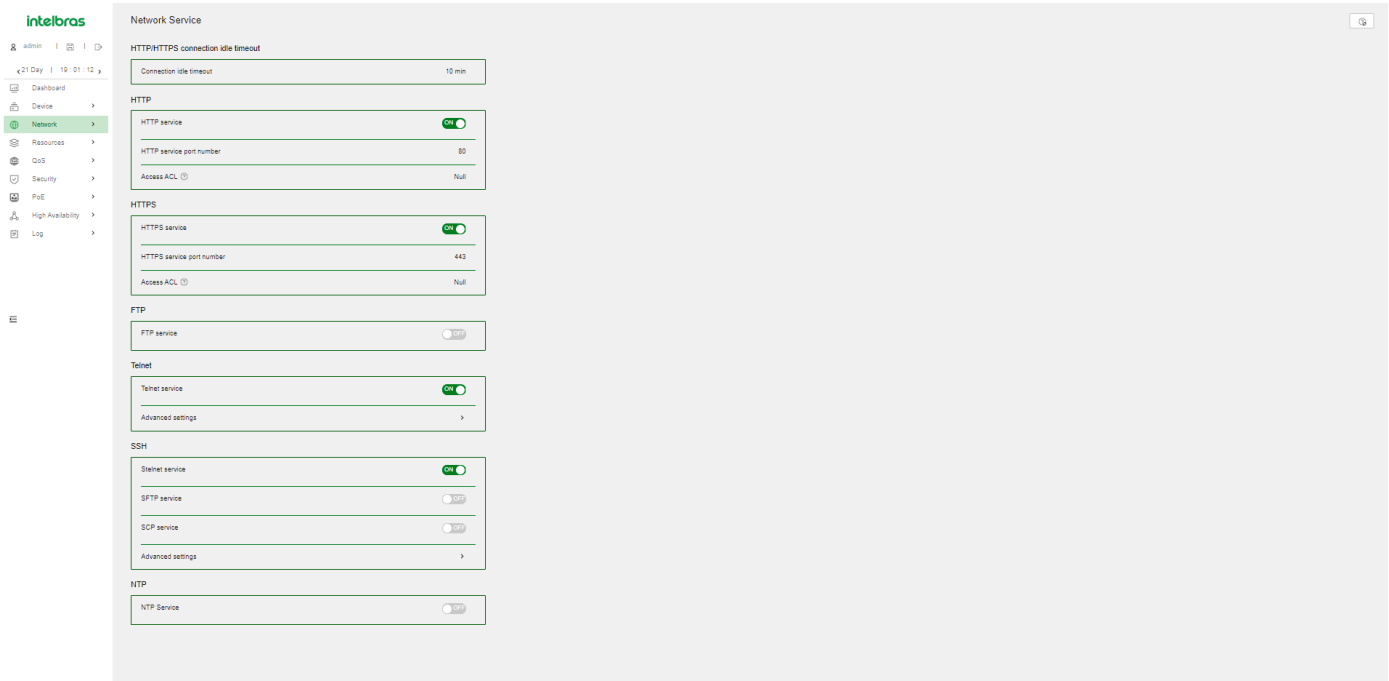
Sincronize o dispositivo com uma fonte de tempo confiável usando o Protocolo de Tempo de Rede (NTP) ou alterando a hora do sistema antes de executá-lo em uma rede ativa.

O NTP usa a estratificação para definir a precisão de cada servidor. O valor está na faixa de 1 a 15. Um valor menor representa uma maior precisão.

Se os dispositivos em uma rede não puderem sincronizar com uma fonte de tempo autoritária, você pode executar as seguintes tarefas:

- Selecione um dispositivo que tenha um relógio relativamente preciso na rede.
- Use o relógio local do dispositivo como relógio de referência para sincronizar outros dispositivos na rede.

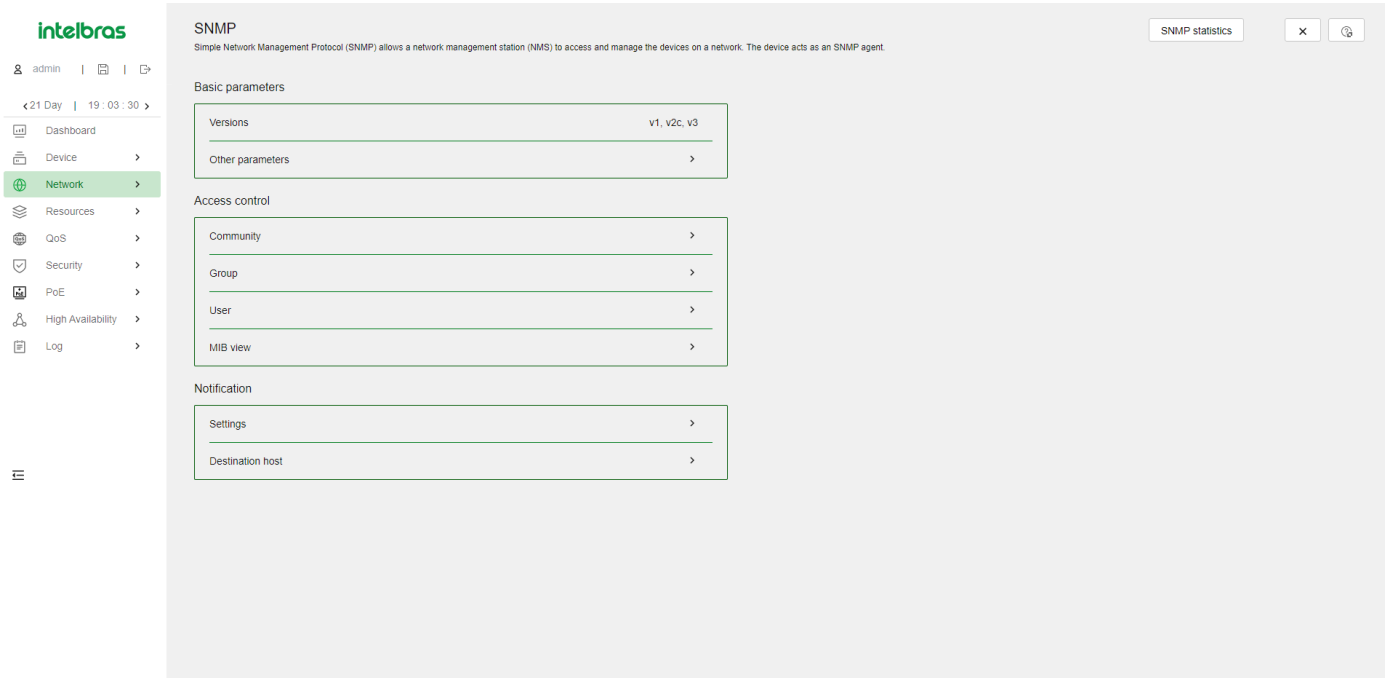
Você pode configurar o relógio local como um relógio de referência na interface web.



SNMP

O Protocolo Simples de Gerenciamento de Rede (SNMP) é um protocolo padrão da Internet amplamente usado para uma estação de gerenciamento de rede (NMS) acessar e gerenciar dispositivos (agentes) em uma rede. Após habilitar o SNMP no dispositivo, o dispositivo age como um agente SNMP.

O SNMP permite que um NMS leia e configure os valores das variáveis em um agente. O agente envia armadilhas para relatar eventos ao NMS.



MIB

A Base de Informações de Gerenciamento (MIB) é uma coleção de objetos. Ela define relações hierárquicas entre objetos e propriedades de objetos, incluindo nome do objeto, privilégio de acesso e tipo de dados.

Um NMS gerencia um dispositivo lendo e configurando os valores das variáveis (por exemplo, status da interface e uso da CPU) no dispositivo. Essas variáveis são objetos na MIB.

OID e subárvore: Uma MIB armazena variáveis chamadas "nós" ou "objetos" em uma hierarquia de árvore e identifica cada nó com um OID único. Um OID é uma sequência numérica pontuada que identifica de forma exclusiva o caminho do nó raiz a um nó folha. Por exemplo, o objeto internet é identificado de forma única pelo OID {1.3.6.1}.

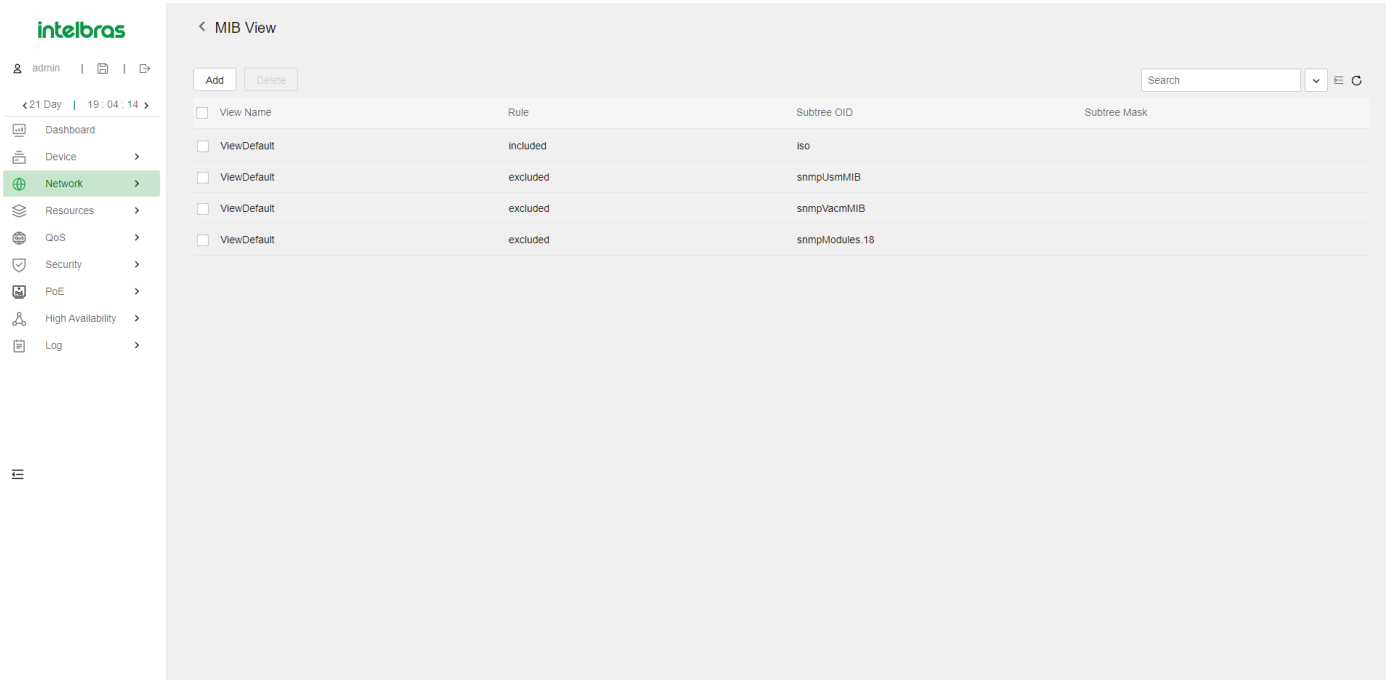
Uma subárvore é como um ramo na hierarquia da árvore. Ela contém um nó raiz e os nós de nível inferior do nó raiz. Uma subárvore é identificada pelo OID do nó raiz.

Visualização MIB: Uma visualização MIB é um subconjunto de uma MIB. Você pode controlar o acesso do NMS a objetos MIB especificando uma visualização MIB para o nome de usuário ou nome da comunidade que o NMS utiliza. Para uma subárvore incluída em uma visualização MIB, todos os nós na subárvore são acessíveis para o NMS. Para uma subárvore excluída de uma visualização MIB, todos os nós na subárvore são inacessíveis para o NMS.

Máscara de subárvore: Uma máscara de subárvore está no formato hexadecimal. Ela identifica uma visualização MIB coletivamente com o OID da subárvore. Para determinar se um objeto MIB está em uma visualização MIB, converta a máscara de subárvore em bits binários (0 e 1) e corresponda cada bit com cada número de nó do OID do objeto da esquerda para a direita. Se os números de nó correspondentes de 1-bit do

objeto OID forem iguais aos da subárvore OID, o objeto MIB está na visualização MIB. Os números de nó correspondentes de 0-bit podem ser diferentes dos da subárvore OID.

NOTA: Se o número de bits na máscara de subárvore for maior que o número de nós do OID, os bits excedentes da máscara de subárvore serão ignorados durante a correspondência máscara-OID da subárvore. Se o número de bits na máscara de subárvore for menor que o número de nós do OID, os bits curtos da máscara de subárvore serão definidos como 1 durante a correspondência máscara-OID da subárvore.



Versões SNMP

Você pode habilitar SNMPv1, SNMPv2c ou SNMPv3 em um dispositivo. Para que um NMS e um agente se comuniquem, eles devem executar a mesma versão do SNMP.

- SNMPv1 e SNMPv2c usam o nome da comunidade para autenticação. Um NMS pode acessar um dispositivo somente quando o NMS e o dispositivo usam o mesmo nome de comunidade.
- O SNMPv3 usa o nome de usuário para autenticação e permite que você configure uma chave de autenticação e uma chave de privacidade para aprimorar a segurança da comunicação. A chave de autenticação autentica a validade do remetente do pacote. A chave de privacidade é usada para criptografar os pacotes transmitidos entre o NMS e o dispositivo.

Controle de Acesso SNMP

Controle de acesso SNMPv1 e SNMPv2c

O SNMPv1 e o SNMPv2 usam o nome da comunidade para autenticação. Para controlar o acesso do NMS aos objetos MIB, configure uma ou ambas as seguintes configurações no nome da comunidade que o NMS utiliza:

- Especificar uma visualização MIB para a comunidade. Você pode especificar apenas uma visualização MIB para uma comunidade.
  - Se você conceder permissão de leitura apenas para a comunidade, o NMS só poderá ler os valores dos objetos na visualização MIB.
  - Se você conceder permissão de leitura e gravação para a comunidade, o NMS poderá ler e definir os valores dos objetos na visualização MIB.
- Especificar uma ACL IPv4 básica ou uma ACL IPv6 básica para a comunidade para filtrar NMSs ilegítimos para acessar o agente.
  - Apenas NMSs com o endereço IPv4/IPv6 permitido na ACL IPv4/IPv6 podem acessar o agente SNMP.
  - Se você não especificar uma ACL, ou a ACL especificada não existir, todos os NMSs na comunidade SNMP podem acessar o agente SNMP. Se a ACL especificada não tiver regras, nenhum NMS na comunidade SNMP poderá acessar o agente SNMP.

  Controle de acesso SNMPv3

O SNMPv3 usa o nome de usuário para autenticação. Para controlar o acesso do NMS aos objetos MIB, configure uma ou ambas as seguintes configurações no nome de usuário que o NMS utiliza:

- Crie um grupo SNMPv3 e atribua o nome de usuário ao grupo. O usuário tem o mesmo direito de acesso do grupo.
  - Quando você cria o grupo, especifique uma ou mais visualizações MIB para o grupo. As visualizações MIB incluem visualização MIB somente leitura, visualização MIB leitura/gravação ou visualização MIB de notificação. Você pode especificar apenas uma visualização MIB de um tipo para um grupo.
  - A visualização MIB somente leitura permite que o grupo leia apenas os valores dos objetos na visualização.
  - A visualização MIB leitura/gravação permite que o grupo leia e defina os valores do objeto na visualização.
  - A visualização MIB de notificação envia automaticamente uma notificação para o NMS quando o grupo acessa a visualização.
- Especifique uma ACL IPv4 básica ou uma ACL IPv6 básica tanto para o usuário quanto para o grupo para filtrar NMSs ilegítimos para acessar o agente.
  - Apenas os NMSs permitidos pelas ACLs especificadas tanto para o usuário quanto para o grupo podem acessar o agente.
  - Se você não especificar uma ACL, ou a ACL especificada não existir, todos os NMSs na comunidade SNMP podem acessar o agente SNMP. Se a ACL especificada não tiver regras, nenhum NMS na comunidade SNMP poderá acessar o agente SNMP.

Recursos

ACL (Lista de Controle de Acesso)

Os recursos de rede são recursos comuns que podem ser usados por várias funcionalidades. Por exemplo, você pode usar uma ACL tanto em um filtro de pacotes para filtrar o tráfego quanto em uma política de QoS para combinar o tráfego.

A interface da Web fornece acesso à página de criação de recursos para funcionalidades que podem usar esses recursos. Ao configurar essas funcionalidades, você pode criar um recurso sem precisar navegar até o menu de **Recursos**. No entanto, para modificar ou remover um recurso, é necessário acessar o menu de **Recursos**.

Uma lista de controle de acesso (ACL) é um conjunto de regras (ou declarações de permitir ou negar) para identificar o tráfego com base em critérios, como endereço IP de origem, endereço IP de destino e número da porta.

As ACLs são usadas principalmente para filtragem de pacotes. Você pode usar ACLs em módulos de QoS, segurança, roteamento e outros módulos de recursos para identificar o tráfego. As decisões de descarte ou encaminhamento de pacotes dependem dos módulos que usam as ACLs.

Tipos de ACL e Critérios de Correspondência

A Tabela 20 mostra os tipos de ACL disponíveis no switch e os campos que podem ser usados para filtrar ou corresponder ao tráfego.

Tabela 20 Tipos de ACL e Critérios de Correspondência

Tipo	Número da ACL	Versão IP	Critérios de Correspondência
ACLs Básicas	2000 a 2999	IPv4	Endereço IPv4 de Origem.
		IPv6	Endereço IPv6 de Origem.
ACLs Avançadas	3000 a 3999	IPv4	Endereço IPv4 de Origem. Endereço IPv4 de Destino. Prioridade do Pacote. Número do Protocolo. Outros campos de cabeçalho de Camada 3 e Camada 4.
		IPv6	Endereço IPv6 de Origem. Endereço IPv6 de Destino. Prioridade do Pacote. Número do Protocolo. Outros campos de cabeçalho de Camada 3 e Camada 4.

ACLs de Cabeçalho de Quadro Ethernet	4000 a 4999	IPv4 e IPv6	Campos de Cabeçalho de Camada 2, incluindo: Endereços MAC de Origem e Destino. Prioridade 802.1p. Tipo de Protocolo de Camada de Link.
ACLs Definidas pelo Usuário			ACLs definidas pelo usuário permitem que você personalize regras com base em informações nos cabeçalhos de protocolo. Você pode definir uma ACL definida pelo usuário para corresponder a pacotes. Um número específico de bytes após um deslocamento (relativo ao cabeçalho especificado) é comparado com um padrão de correspondência após ser aplicado a uma máscara de padrão de correspondência E.

Ordem de Correspondência

As regras em uma ACL são ordenadas em uma ordem específica. Quando um pacote corresponde a uma regra, o dispositivo interrompe o processo de correspondência e executa a ação definida na regra. Se uma ACL contém regras sobrepostas ou conflitantes, o resultado da correspondência e a ação a ser tomada dependem da ordem das regras.

As seguintes ordens de correspondência de ACL estão disponíveis:

config – Classifica as regras da ACL em ordem crescente do ID da regra. Uma regra com um ID menor é correspondida antes de uma regra com um ID maior. Se você usar esse método, verifique cuidadosamente as regras e sua ordem.

NOTA:

A ordem de correspondência das ACLs definidas pelo usuário só pode ser **config**.

auto – Classifica as regras da ACL em ordem de profundidade primeiro. A ordenação em profundidade garante que qualquer subconjunto de uma regra seja sempre correspondido antes da regra. A Tabela 21 lista a sequência de critérios que a ordenação em profundidade utiliza para classificar as regras para cada tipo de ACL.

Categoria de ACL	Sequência de Critérios
ACL Básica IPv4	1. Instância VPN. 2. Mais 0s no wildcard de endereço IPv4 de origem (mais 0s significam uma faixa de endereços IPv4 mais estreita). 3. Regra configurada anteriormente.
ACL Avançada IPv4	1. Instância VPN. 2. Número de protocolo específico. 3. Mais 0s na máscara de wildcard de endereço IPv4 de origem. 4. Mais 0s no wildcard de endereço IPv4 de destino. 5. Faixa de números de porta de serviço TCP/UDP mais estreita. 6. Regra configurada anteriormente.
ACL Básica IPv6	1. Instância VPN. 2. Prefixo mais longo para o endereço IPv6 de origem (um prefixo mais longo significa uma faixa de endereços IPv6 mais estreita). 3. Regra configurada anteriormente.
ACL Avançada IPv6	1. Instância VPN. 2. Número de protocolo específico. 3. Prefixo mais longo para o endereço IPv6 de origem. 4. Prefixo mais longo para o endereço IPv6 de destino. 5. Faixa de números de porta de serviço TCP/UDP mais estreita. 6. Regra configurada anteriormente.
ACL de Cabeçalho de Quadro Ethernet	1. Mais 1s na máscara de endereço MAC de origem (mais 1s significam um endereço MAC menor). 2. Mais 1s na máscara de endereço MAC de destino. 3. Regra configurada anteriormente.

NOTA:

Uma máscara de wildcard, também chamada de máscara inversa, é um número binário de 32 bits representado em notação decimal pontilhada. Ao contrário de uma máscara de rede, os bits 0 em uma máscara de wildcard representam bits "a considerar" e os bits 1 representam bits "não a considerar". Se os bits "a considerar" em um endereço IP forem idênticos aos bits "a considerar" em um critério de endereço IP, o endereço IP

corresponde ao critério. Todos os bits "não a considerar" são ignorados. Os 0s e 1s em uma máscara de wildcard podem ser não contíguos. Por exemplo, 0.255.0.255 é uma máscara de wildcard válida.

Numeramento de Regras

As regras da ACL podem ser numeradas manualmente ou numeradas automaticamente.

Passo de numeração de regra

Se você não atribuir um ID à regra que está criando, o sistema atribuirá automaticamente um ID à regra. O passo de numeração da regra define o incremento pelo qual o sistema numera automaticamente as regras. Por exemplo, o passo de numeração de regras da ACL padrão é 5. Se você não atribuir IDs às regras que está criando, elas serão numeradas automaticamente como 0, 5, 10, 15 e assim por diante. Quanto maior o passo de numeração, mais regras podem ser inseridas entre duas regras.

Introduzindo um espaço entre as regras, em vez de numerá-las de forma contígua, você tem a flexibilidade de inserir regras em uma ACL. Esse recurso é importante para uma ACL de ordem de configuração, onde as regras da ACL são correspondidas em ordem crescente do ID da regra.

Numeramento automático de regras e renúmeração

O ID atribuído automaticamente a uma regra da ACL leva o múltiplo mais próximo do passo de numeração ao ID da regra mais alto atual, começando em 0.

Por exemplo, se o passo de numeração for 5 (o padrão) e houver cinco regras da ACL numeradas 0, 5, 9, 10 e 12, a regra recém-definida será numerada como 15. Se a ACL não contiver nenhuma regra, a primeira regra será numerada como 0.

Sempre que o passo for alterado, as regras serão renumeradas, começando em 0. Por exemplo, se houver cinco regras numeradas 5, 10, 13, 15 e 20, a alteração do passo de 5 para 2 fará com que as regras sejam renumeradas como 0, 2, 4, 6 e 8.

Intervalo de Tempo

Você pode implementar um serviço baseado na hora do dia aplicando um intervalo de tempo a ele. Um serviço baseado no tempo só entra em vigor nos períodos de tempo especificados pelo intervalo de tempo. Por exemplo, você pode implementar regras de ACL baseadas no tempo aplicando um intervalo de tempo a elas. Se um intervalo de tempo não existir, o serviço baseado no intervalo de tempo não terá efeito.

Os seguintes tipos básicos de intervalos de tempo estão disponíveis:

Intervalo de tempo periódico – Recorre periodicamente em um dia ou dias da semana.

Intervalo de tempo absoluto – Representa apenas um período de tempo e não se repete.

Um intervalo de tempo é identificado exclusivamente pelo nome do intervalo de tempo. Um intervalo de tempo pode incluir várias declarações periódicas e declarações absolutas. O período ativo de um intervalo de tempo é calculado da seguinte maneira:

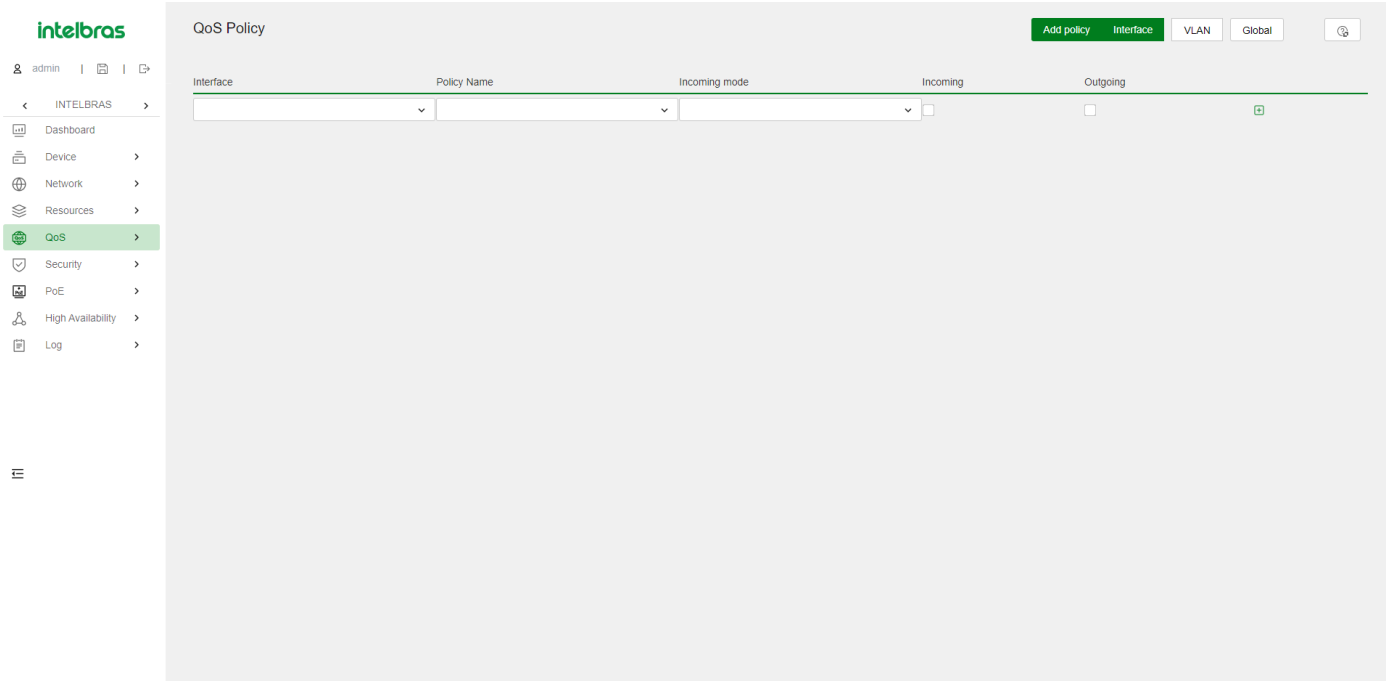
1. Combinando todas as declarações periódicas.
2. Combinando todas as declarações absolutas.
3. Tomando a interseção dos dois conjuntos de declarações como o período ativo do intervalo de tempo.

Recursos de QoS

Políticas de QoS

Nas comunicações de dados, a Qualidade de Serviço (QoS) fornece garantias de serviço diferenciadas para o tráfego diversificado em termos de largura de banda, atraso, variação de atraso e taxa de descarte, todos os quais podem afetar a QoS.

Ao associar um comportamento de tráfego com uma classe de tráfego em uma política de QoS, você aplica ações de QoS no comportamento de tráfego à classe de tráfego.



Classe de Tráfego

Uma classe de tráfego define um conjunto de critérios de correspondência para a classificação de tráfego.

Comportamento de Tráfego

Um comportamento de tráfego define um conjunto de ações de QoS a serem tomadas em pacotes.

Política de QoS

Uma política de QoS associa classes de tráfego a comportamentos de tráfego e executa as ações em cada comportamento em sua classe de tráfego associada.

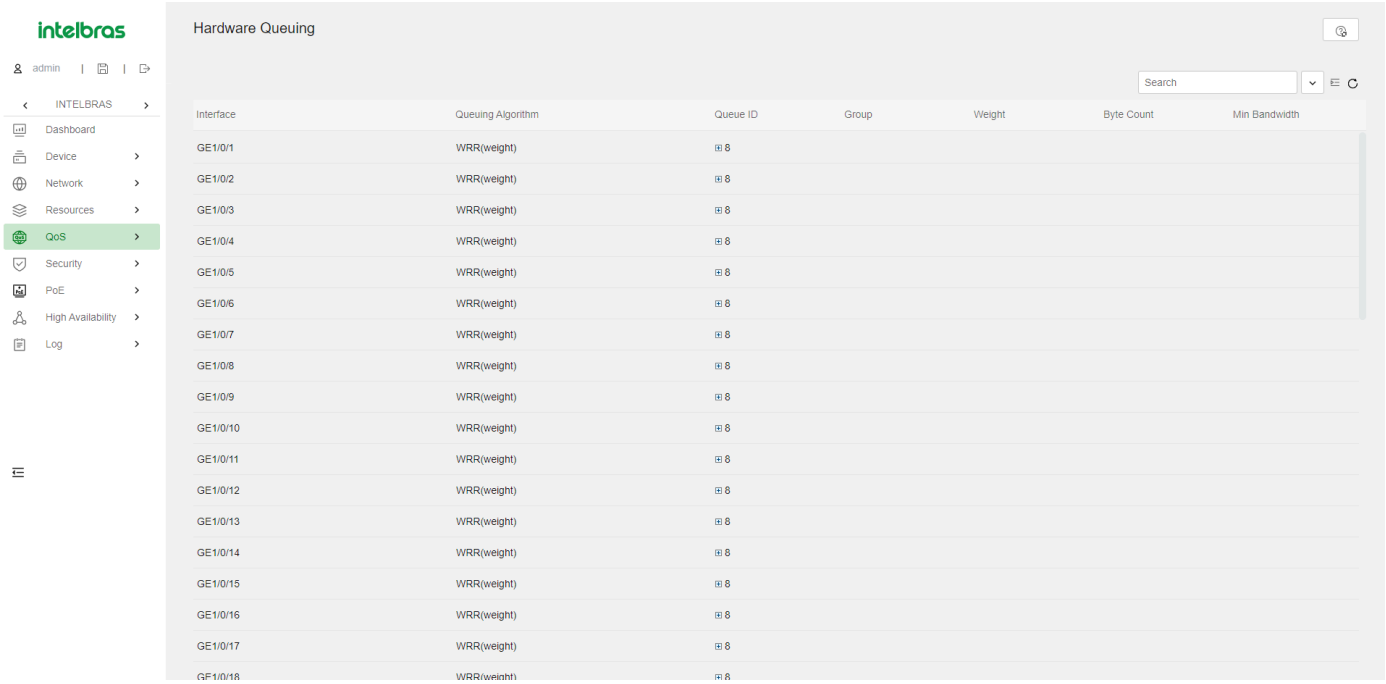
Aplicando uma Política de QoS

Você pode aplicar uma política de QoS aos seguintes destinos:

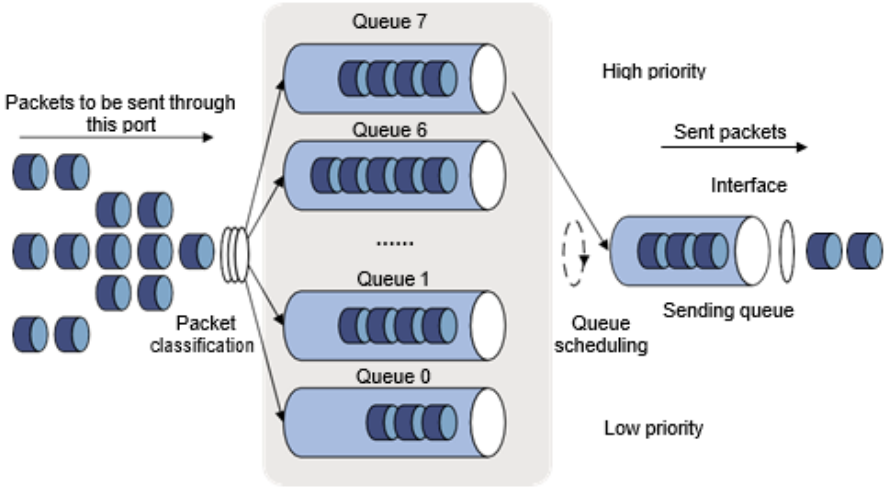
- **Interface** - A política de QoS entra em vigor no tráfego enviado ou recebido na interface. A política de QoS aplicada ao tráfego de saída em uma interface ou PVC não regula pacotes locais. Pacotes locais referem-se a pacotes de protocolos críticos enviados pelo sistema local para manutenção operacional. Os pacotes locais mais comuns incluem manutenção de link, LDP e pacotes SSH.
- **VLAN** - A política de QoS entra em vigor no tráfego enviado ou recebido em todas as portas na VLAN.
- **Globalmente** - A política de QoS entra em vigor no tráfego enviado ou recebido em todas as portas.

Enfileiramento de Hardware

A congestão ocorre em um link ou nó quando o tamanho do tráfego excede a capacidade de processamento do link ou nó. A congestão é inevitável em redes comutadas ou em ambientes de aplicativos multiusuários. Para melhorar o desempenho do serviço da sua rede, implemente políticas de gerenciamento de congestão. O enfileiramento é uma técnica comum de gerenciamento de congestão. SP, WRR e WFQ são métodos de enfileiramento comuns.



Enfileiramento SP

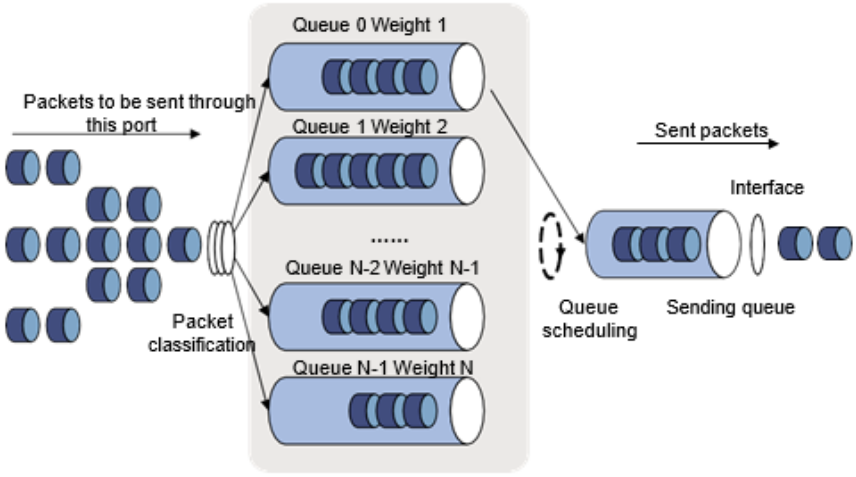


O enfileiramento SP é projetado para aplicativos críticos que exigem um serviço preferencial para reduzir o atraso de resposta quando ocorre congestão. O enfileiramento SP classifica oito filas em uma porta em oito classes, numeradas de 7 a 0 em ordem de prioridade decrescente.

O enfileiramento SP agenda as oito filas em ordem decrescente de prioridade. O enfileiramento SP envia pacotes na fila com a prioridade mais alta primeiro. Quando a fila com a maior prioridade estiver vazia, ele enviará pacotes na fila com a segunda maior prioridade e assim por diante. Você pode atribuir pacotes críticos para missões a uma fila de alta prioridade para garantir que eles sejam sempre atendidos primeiro. Pacotes de serviço comum podem ser atribuídos a filas de baixa prioridade para serem transmitidos quando as filas de alta prioridade estiverem vazias.

A desvantagem do enfileiramento SP é que os pacotes nas filas de prioridade mais baixa não podem ser transmitidos se houver pacotes nas filas de prioridade mais alta. No pior caso, o tráfego de menor prioridade pode nunca ser atendido.

Enfileiramento WRR



O enfileiramento WRR agenda todas as filas por vez para garantir que cada fila seja atendida por algum tempo. Suponha que uma porta forneça oito filas de saída. O WRR atribui a cada fila um valor de peso (representado por w7, w6, w5, w4, w3, w2, w1 ou w0). O valor de peso de uma fila decide a proporção de recursos atribuídos à fila. Em uma porta de 100 Mbps, você pode definir os valores de peso para 50, 30, 10, 10, 50, 30, 10 e 10 para w7 a w0. Dessa forma, a fila com a prioridade mais baixa pode obter um mínimo de 5 Mbps de largura de banda. O WRR resolve o problema de o enfileiramento SP não conseguir atender pacotes em filas de baixa prioridade por um longo tempo.

Outra vantagem do enfileiramento WRR é que, quando as filas são programadas por vez, o tempo de serviço de cada fila não é fixo. Se uma fila estiver vazia, a próxima fila será agendada imediatamente. Isso melhora a eficiência do uso de recursos de largura de banda.

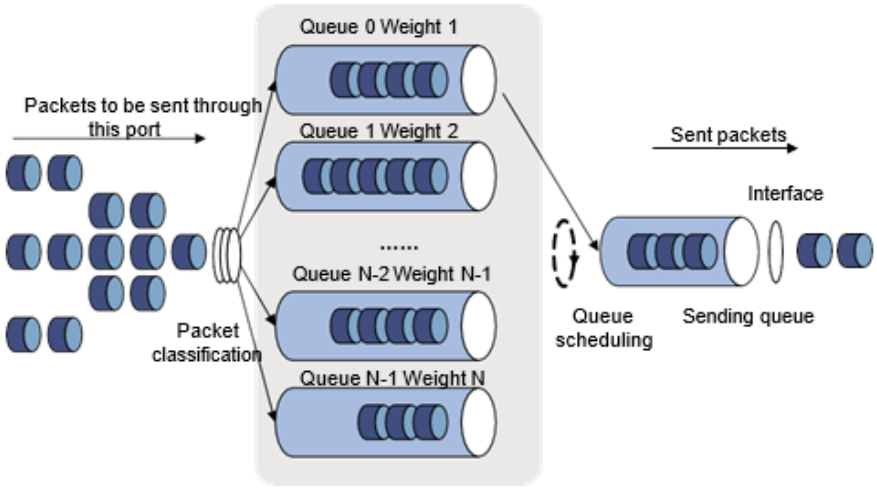
O enfileiramento WRR inclui os seguintes tipos:

- **Enfileiramento WRR Básico** - Contém várias filas. Você pode configurar o peso para cada fila, e o WRR programa essas filas com base nos parâmetros definidos pelo usuário de forma circular.
- **Enfileiramento WRR Baseado em Grupo** - Todas as filas são programadas pelo WRR. Você pode dividir as filas de saída para o grupo WRR 1 e o grupo WRR 2. A programação circular da fila é realizada primeiro para o grupo 1 do WRR. Quando o grupo 1 estiver vazio, a programação circular da fila será realizada para o grupo 2.

Em uma interface habilitada com enfileiramento WRR baseado em grupo, você pode atribuir filas ao grupo SP. As filas no grupo SP são programadas com SP. O grupo SP tem prioridade de programação mais alta do que os grupos WRR.

O grupo WRR 1 é suportado na versão de software atual.

Enfileiramento WFQ



O WFQ pode classificar automaticamente o tráfego de acordo com as informações de "sessão" do tráfego (tipo de protocolo, números de porta de origem/destino TCP ou UDP, endereços IP de origem/destino, bits de precedência IP no campo ToS, etc.). O WFQ fornece o máximo de filas possível para que cada fluxo de tráfego possa ser colocado em uma fila diferente para equilibrar o atraso de cada fluxo de tráfego como um todo. Ao retirar pacotes, o WFQ atribui a largura de banda da interface de saída a cada fluxo de tráfego por precedência. Quanto maior o valor de precedência de um fluxo de tráfego, maior será a largura de banda que ele recebe.

Suponha que existam cinco fluxos na interface atual com precedência 0, 1, 2, 3 e 4. A cota de largura de banda total é a soma de todos os (valor de precedência + 1), ou seja, 1 + 2 + 3 + 4 + 5 = 15. A porcentagem de largura de banda atribuída a cada fluxo é (valor de precedência do fluxo + 1)/cota de largura de banda total. As porcentagens de largura de banda para os fluxos são 1/15, 2/15, 3/15, 4/15 e 5/15.

O WFQ é semelhante ao WRR. Em uma interface com enfileiramento WFQ baseado em grupo habilitado, você pode atribuir filas ao grupo SP. As filas no grupo SP são programadas com SP. O grupo SP tem prioridade de programação mais alta do que os grupos WFQ. A diferença é que o WFQ permite definir a largura de banda garantida que uma fila do WFQ pode obter durante a congestão.

A configuração da fila do WFQ a partir da interface da Web não é suportada na versão de software atual.

Perfil de Programação de Filas

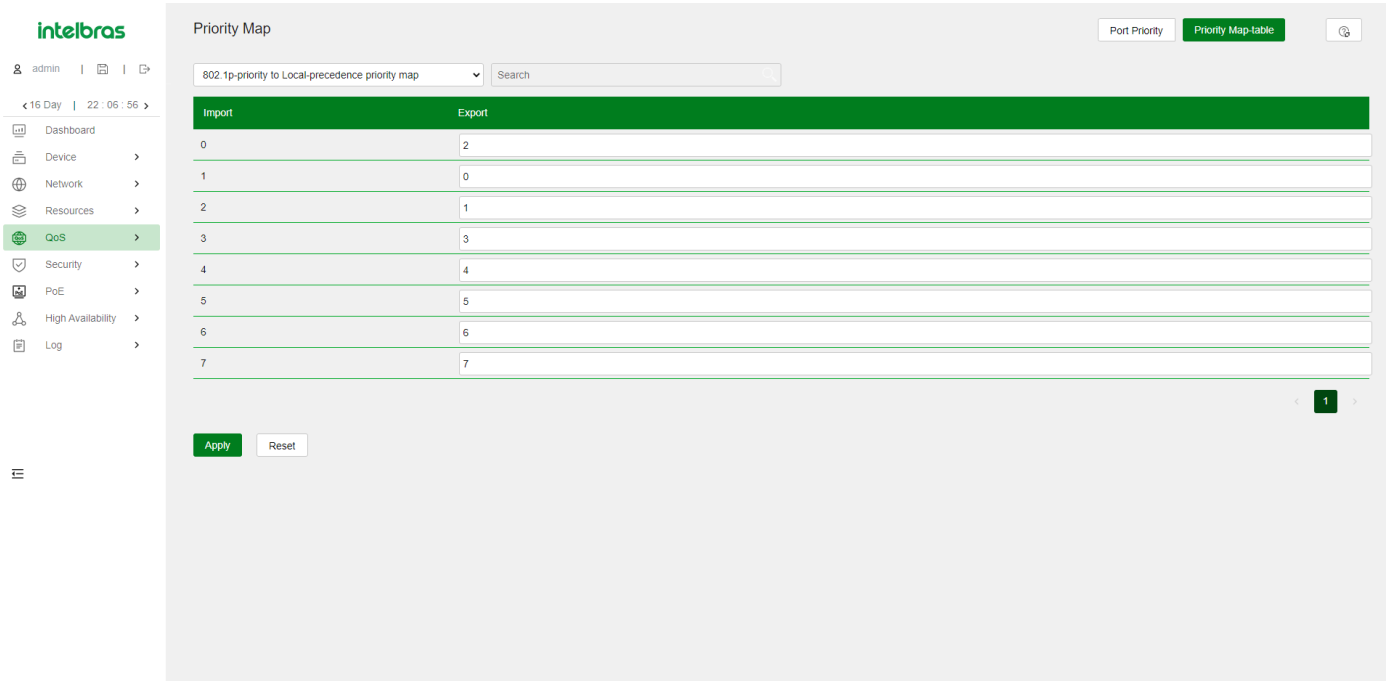
Os perfis de programação de filas oferecem dois algoritmos de programação de filas: SP e WRR. Em um perfil de programação de filas, você pode configurar SP + WRR. Quando os dois algoritmos de programação de filas estão configurados, as filas SP e os grupos WRR são programados em ordem decrescente do ID da fila. Em um grupo WRR, as filas são programadas com base em seus pesos. Quando SP e grupos WRR são configurados em um perfil de programação de filas, a figura a seguir mostra a ordem de programação.

- Q7 Q6 Q5 Q4 Q3 Q2 Q1 Q0
- Grupo SP
- Grupo WRR 1
- Grupo WRR 2
- A fila 7 tem a prioridade mais alta. Seus pacotes são enviados preferencialmente.
- A fila 6 tem a segunda maior prioridade. Os pacotes na fila 6 são enviados quando a fila 7 estiver vazia.
- As filas 3, 4 e 5 são programadas de acordo com seus pesos. Quando as filas 6 e 7 estiverem vazias, o grupo WRR 1 é programado.
- As filas 1 e 2 são programadas de acordo com seus pesos. O grupo WRR 2 é programado quando as filas 7, 6, 5, 4 e 3 estiverem todas vazias.
- A fila 0 tem a prioridade mais baixa e é programada quando todas as outras filas estiverem vazias.

Mapeamento de Prioridade

Quando um pacote chega, um dispositivo atribui valores de parâmetros de prioridade ao pacote com o objetivo de programação de filas e controle de congestão.

O mapeamento de prioridade permite modificar os valores de prioridade do pacote de acordo com as regras de mapeamento de prioridade. Os parâmetros de prioridade decidem a prioridade de programação e prioridade de encaminhamento do pacote.



Prioridade de Porta

Quando uma porta é configurada com um modo de confiança de prioridade, o dispositivo confia nas prioridades incluídas nos pacotes recebidos. O dispositivo pode resolver automaticamente as prioridades ou bits de sinalização incluídos nos pacotes. O dispositivo, em seguida, mapeia a prioridade confiada para os tipos e valores de prioridade alvo de acordo com os mapas de prioridade.

Quando uma porta não está configurada com um modo de confiança de prioridade e está configurada com uma prioridade de porta, o dispositivo não confia nas prioridades incluídas nos pacotes recebidos. O dispositivo usa sua prioridade de porta para procurar parâmetros de prioridade nos pacotes recebidos.

Configurando a Prioridade da Porta

Depois de configurar uma prioridade de porta para uma porta, o dispositivo usa sua prioridade de porta para procurar parâmetros de prioridade nos pacotes recebidos.

Configurando o Modo de Confiança de Prioridade

Depois de configurar um modo de confiança de prioridade para uma porta, o dispositivo mapeia a prioridade confiada nos pacotes recebidos para os tipos e valores de prioridade alvo de acordo com os mapas de prioridade.

Os modos de confiança de prioridade disponíveis incluem os seguintes tipos:

- **Não Confiança** - Não confia em nenhuma prioridade incluída nos pacotes.
- **802.1p** - Confia nas prioridades 802.1p incluídas nos pacotes.
- **DSCP** - Confia nas prioridades DSCP incluídas nos pacotes IP.

Mapa de Prioridade

O dispositivo fornece três mapas de prioridade: 802.1p-lp, DSCP-802.1p e DSCP-DSCP. Se um mapa de prioridade padrão não atender aos seus requisitos, você pode modificar o mapa de prioridade conforme necessário.

Limite de taxa

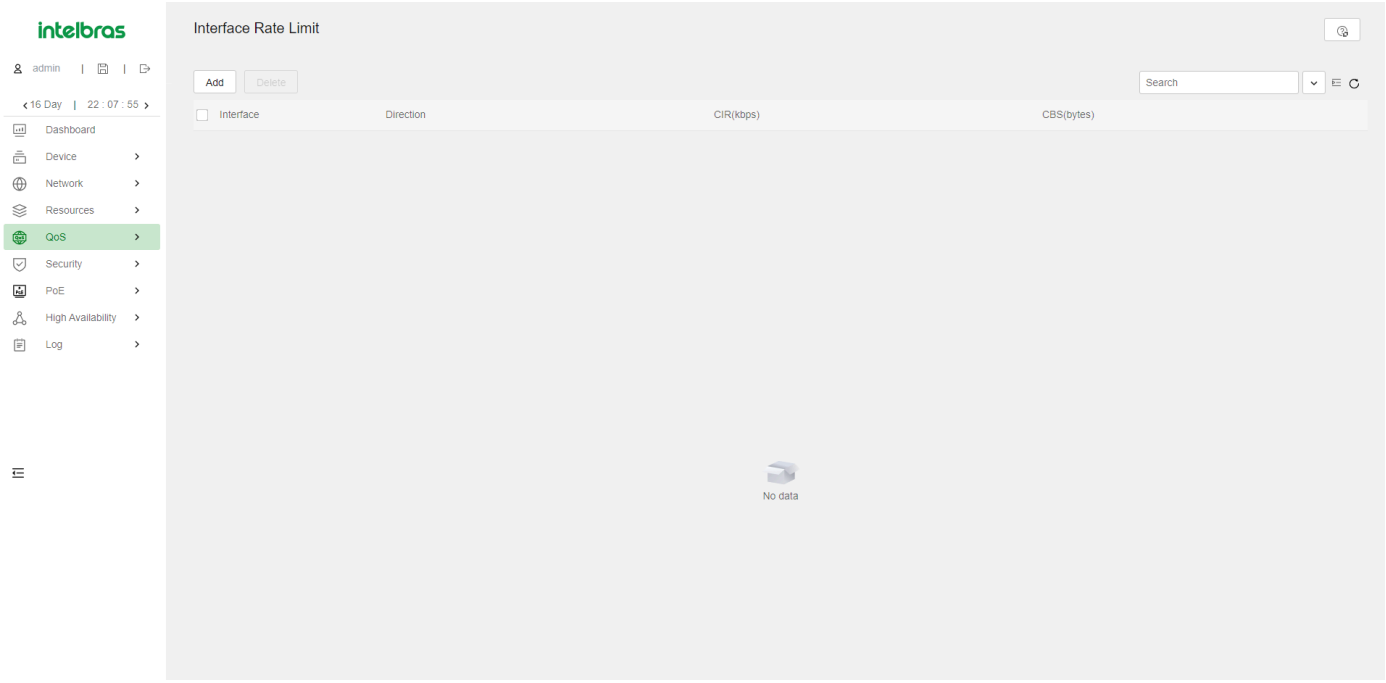
O limite de taxa utiliza baldes de tokens para o controle de tráfego. Se houver tokens no balde de tokens, é permitido o tráfego com rajadas. Caso contrário, os pacotes não são encaminhados até que novos tokens sejam gerados. Dessa forma, os pacotes são limitados à taxa de geração de tokens, enquanto o tráfego com rajadas é permitido.

Um balde de tokens possui os seguintes parâmetros configuráveis:

- Taxa média na qual os tokens são inseridos no balde, que é a taxa média permitida de tráfego. Geralmente, é definida como a taxa de informação comprometida (CIR).
- Tamanho da rajada ou capacidade do balde de tokens. É o tamanho máximo de tráfego permitido em cada rajada. Geralmente, é definido como o tamanho de rajada comprometida (CBS). O tamanho de rajada definido deve ser maior que o tamanho máximo de pacote.

Cada pacote que chega é avaliado. Em cada avaliação, se o número de tokens no balde for suficiente, o tráfego está em conformidade com a especificação e os tokens para encaminhar o pacote são retirados. Se o número de tokens no balde não for suficiente, o tráfego é excessivo.

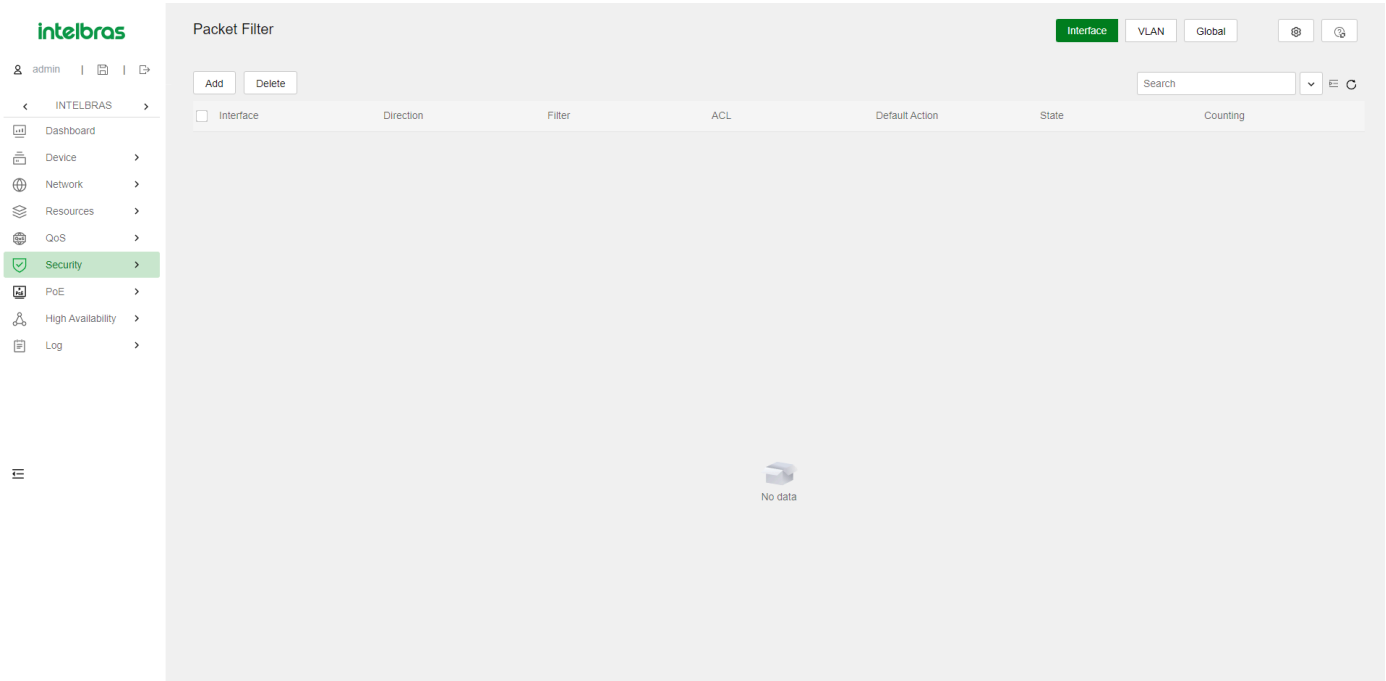
Quando o limite de taxa é configurado em uma interface, um balde de tokens lida com todos os pacotes a serem enviados por meio da interface para limitação de taxa. Se houver tokens suficientes no balde de tokens, os pacotes podem ser encaminhados. Caso contrário, os pacotes são colocados em filas de QoS para o gerenciamento de congestionamento. Dessa forma, o tráfego que passa pela interface é controlado.



Recursos de segurança

Filtro de pacotes

O filtro de pacotes utiliza listas de controle de acesso (ACLs) para filtrar pacotes de entrada ou saída em interfaces, VLANs ou globalmente. Uma interface permite que pacotes que correspondam às declarações "permitir" sejam encaminhados e nega pacotes que correspondam às declarações "negar". A ação padrão se aplica aos pacotes que não correspondem a nenhuma regra da ACL.



IP Source Guard

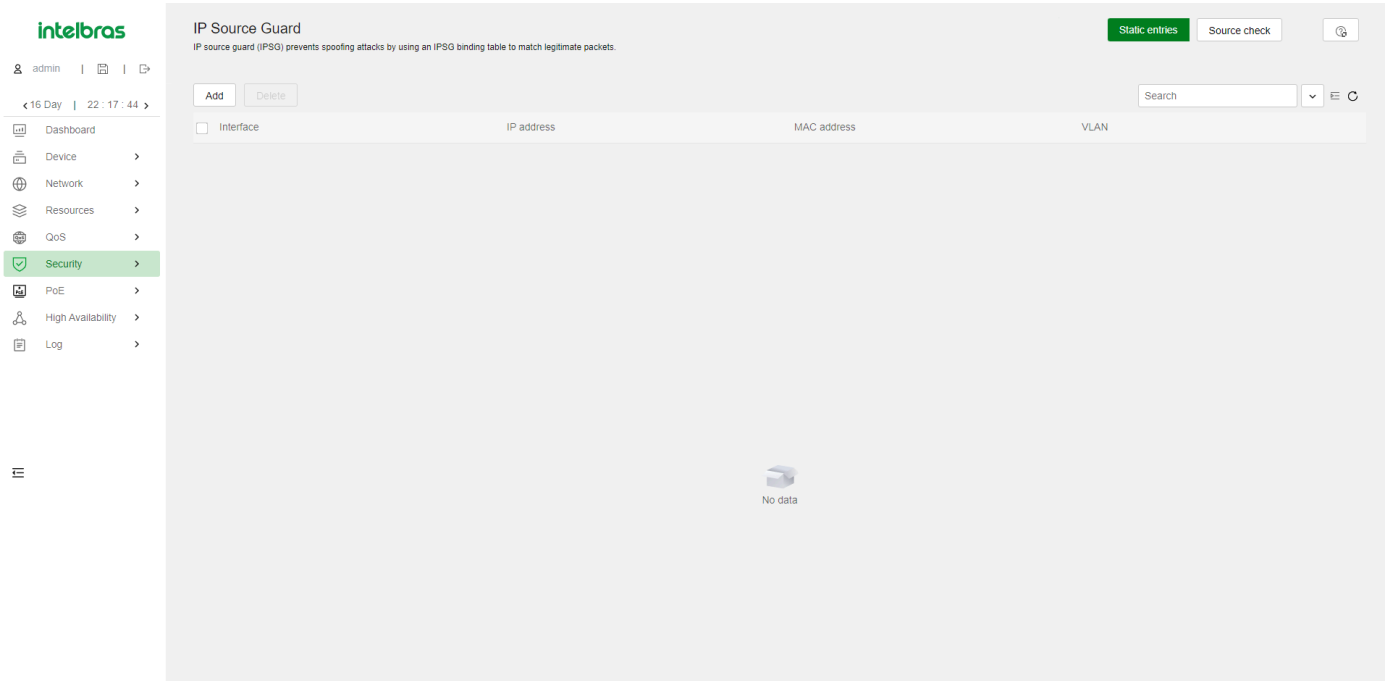
Visão geral

O IP Source Guard (IPSG) previne ataques de spoofing usando uma tabela de associação IPSG para corresponder a pacotes legítimos. Ele descarta todos os pacotes que não correspondem à tabela.

A tabela de associação IPSG pode incluir as seguintes associações:

- IP-interface.

- MAC-interface.
- IP-MAC-interface.
- IP-VLAN-interface.
- MAC-VLAN-interface.
- IP-MAC-VLAN-interface.



Associações estáticas específicas da interface para IPv4SG

Associações estáticas específicas da interface para IPv4SG são configuradas manualmente e têm efeito apenas na interface. Elas são adequadas para cenários em que existem alguns hosts em uma LAN e seus endereços IP são configurados manualmente. Por exemplo, você pode configurar uma associação estática IPv4SG em uma interface que se conecta a um servidor. Essa associação permite que a interface receba pacotes apenas do servidor.

Associações estáticas IPv4SG em uma interface implementam as seguintes funções:

- Filtram pacotes IPv4 de entrada na interface.
- Cooperam com a detecção ARP para verificar a validade do usuário.

Você pode configurar a mesma associação estática IPv4SG em diferentes interfaces.

802.1X

O 802.1X é um protocolo de controle de acesso à rede baseado em porta que controla o acesso à rede autenticando os dispositivos conectados às portas LAN habilitadas para 802.1X.

Arquitetura 802.1X

O 802.1X inclui as seguintes entidades:

- **Cliente** - Um terminal de usuário que busca acesso à LAN. O terminal deve ter software 802.1X para autenticar no dispositivo de acesso.
- **Dispositivo de acesso** - Autentica o cliente para controlar o acesso à LAN. Em um ambiente típico de 802.1X, o dispositivo de acesso usa um servidor de autenticação para realizar a autenticação.
- **Servidor de autenticação** - Fornece serviços de autenticação para o dispositivo de acesso. O servidor de autenticação autentica primeiro os clientes 802.1X usando os dados enviados pelo dispositivo de acesso. Em seguida, o servidor retorna os resultados da autenticação para o dispositivo de acesso para tomar decisões de acesso. O servidor de autenticação é tipicamente um servidor RADIUS. Em uma LAN pequena, você pode usar o dispositivo de acesso como servidor de autenticação.

Métodos de autenticação 802.1X

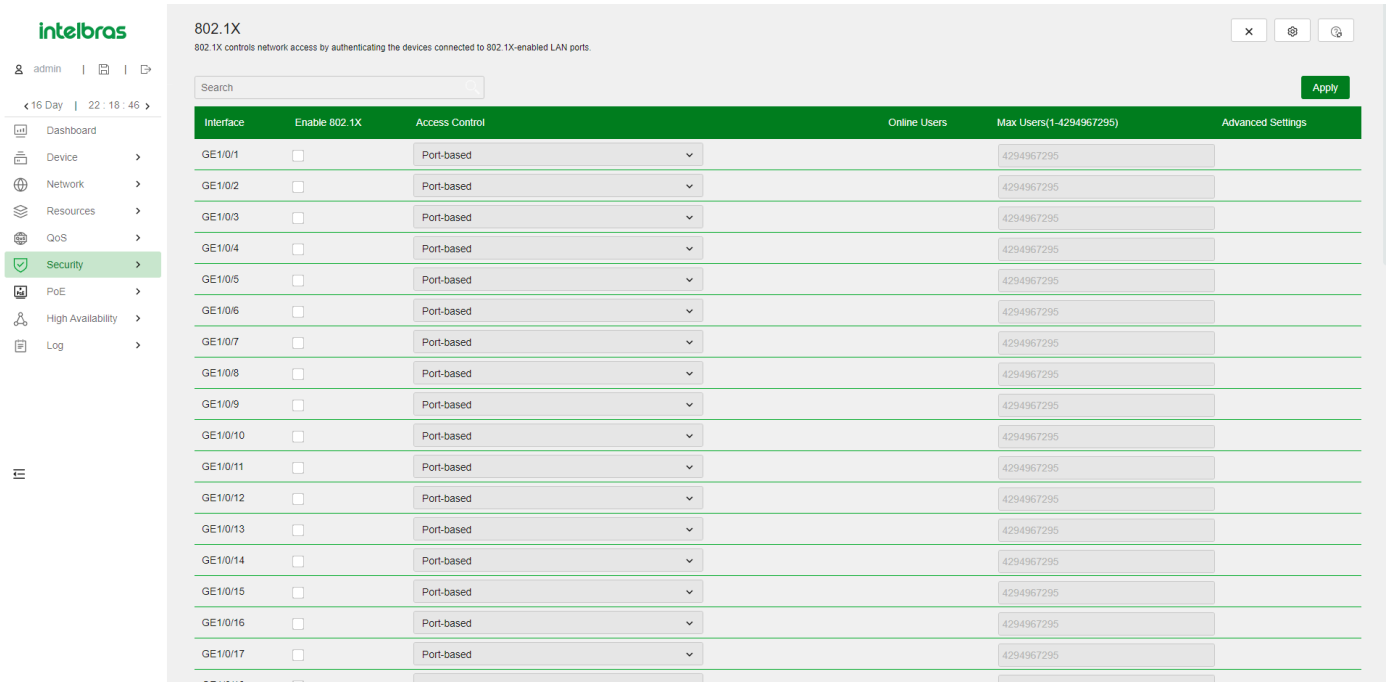
O dispositivo de acesso pode realizar relé EAP ou término EAP para se comunicar com o servidor RADIUS.

Término EAP - O dispositivo de acesso executa as seguintes operações no modo de término EAP:

- Encerra os pacotes EAP recebidos do cliente.
- Encapsula as informações de autenticação do cliente em pacotes RADIUS padrão.
- Usa PAP ou CHAP para autenticar no servidor RADIUS.

O CHAP não envia a senha em texto simples para o servidor RADIUS, e o PAP envia a senha em texto simples para o servidor RADIUS.

Relé EAP - O dispositivo de acesso usa pacotes EAPOR para enviar informações de autenticação ao servidor RADIUS.



Métodos de controle de acesso

O Comware implementa o controle de acesso baseado em porta conforme definido no protocolo 802.1X e estende o protocolo para suportar o controle de acesso baseado em MAC.

Controle de acesso baseado em porta - Uma vez que um usuário 802.1X passa na autenticação em uma porta, todos os usuários subsequentes podem acessar a rede através da porta sem autenticação. Quando o usuário autenticado faz logoff, todos os outros usuários também fazem logoff. **Controle de acesso baseado em MAC** - Cada usuário é autenticado separadamente em uma porta. Quando um usuário faz logoff, os outros usuários online não são afetados.

Estado de autorização de porta

O estado de autorização da porta determina se o cliente recebe acesso à rede. Você pode controlar o estado de autorização de uma porta usando as seguintes opções:

Autorizado - Coloca a porta no estado autorizado, permitindo que os usuários na porta acessem a rede sem autenticação. **Não autorizado** - Coloca a porta no estado não autorizado, negando todas as solicitações de acesso dos usuários na porta. **Automático** - Coloca inicialmente a porta no estado não autorizado para permitir apenas que os pacotes EAPOL passem. Após um usuário passar na autenticação, coloca a porta no estado autorizado para permitir o acesso à rede. Você pode usar essa opção na maioria dos cenários.

Reautenticação periódica do usuário online

A reautenticação periódica do usuário online acompanha o status de conexão dos usuários online e atualiza os atributos de autorização atribuídos pelo servidor. Os atributos incluem a ACL, VLAN e QoS baseados no perfil do usuário. O intervalo de reautenticação é configurável pelo usuário.

Handshake do usuário online

O recurso de handshake do usuário online verifica o status de conectividade dos usuários 802.1X online. O dispositivo de acesso envia mensagens de handshake para os usuários online no intervalo de handshake. Se o dispositivo não receber respostas de um usuário online após ter feito as tentativas máximas de handshake, ele coloca o usuário no estado offline.

Você também pode habilitar o recurso de segurança de handshake de usuário online para verificar as informações de autenticação nos pacotes de handshake dos clientes. Com esse recurso, o dispositivo impede que os usuários 802.1X que usam software de cliente ilegal contornem a verificação de segurança iNode, como a detecção de placas de interface de rede (NICs) duplas.

Desencadeamento de autenticação

O dispositivo de acesso inicia a autenticação se um cliente não pode enviar pacotes EAPOL-Start. Um exemplo é o cliente 802.1X disponível com o Windows XP.

O dispositivo de acesso suporta os seguintes modos:

Modo de desencadeamento unicast - Ao receber um quadro de um endereço MAC desconhecido, o dispositivo de acesso envia um pacote de EAP-Request de Identidade fora da porta de recebimento para o endereço MAC. O dispositivo retransmite o pacote se nenhuma resposta for recebida dentro do intervalo especificado. **Modo de desencadeamento multicast** - O dispositivo de acesso envia periodicamente pacotes de EAP-Request de Identidade (a cada 30 segundos, por padrão) para iniciar a autenticação 802.1X.

VLAN de falha de autenticação (Auth-Fail VLAN)

A VLAN de falha de autenticação 802.1X em uma porta acomoda usuários que falharam na autenticação 802.1X devido a não cumprimento da estratégia de segurança da organização. Por exemplo, a VLAN acomoda usuários que inseriram uma senha errada. A VLAN de falha de autenticação não acomoda usuários 802.1X que falharam na autenticação devido a timeouts de autenticação ou problemas de conexão de rede.

O dispositivo de acesso lida com VLANs em uma porta 802.1X com base no método de controle de acesso 802.1X.

Em uma porta que executa controle de acesso baseado em porta:

Status de autenticação

Manipulação de VLAN

Um usuário falha na autenticação 802.1X.

O dispositivo atribui a VLAN de falha de autenticação à porta como PVID. Todos os usuários 802.1X nesta porta podem acessar apenas os recursos na VLAN de falha de autenticação.

Um usuário na VLAN de falha de autenticação falha na reautenticação 802.1X.

A VLAN de falha de autenticação ainda é o PVID na porta, e todos os usuários 802.1X nesta porta estão nessa VLAN.

Um usuário passa na autenticação 802.1X.

O dispositivo atribui a VLAN de autorização do usuário à porta como PVID e remove a porta da VLAN de falha de autenticação. Após o usuário fazer logoff, a VLAN de convidado é atribuída à porta como PVID. Se nenhuma VLAN de convidado estiver configurada, o PVID inicial da porta é restaurado. Se o servidor de autenticação não autorizar uma VLAN, aplica-se o PVID inicial da porta. O usuário e todos os usuários 802.1X subsequentes são atribuídos ao PVID inicial. Após o usuário fazer logoff, o PVID da porta permanece inalterado. Em uma porta que executa controle de acesso baseado em MAC:

Status de autenticação

Manipulação de VLAN

Um usuário falha na autenticação 802.1X.

O dispositivo mapeia o endereço MAC do usuário para a VLAN de falha de autenticação 802.1X. O usuário pode acessar apenas recursos na VLAN de falha de autenticação.

Um usuário na VLAN de falha de autenticação 802.1X falha na reautenticação.

O usuário ainda está na VLAN de falha.

Um usuário na VLAN de falha de autenticação 802.1X passa na autenticação 802.1X.

O dispositivo remapeia o endereço MAC do usuário para a VLAN de autorização.

Se o servidor de autenticação (seja o dispositivo de acesso local ou um servidor RADIUS) não autorizar uma VLAN, o dispositivo remapeia o endereço MAC do usuário para o PVID inicial na porta.

Um usuário na VLAN de convidado falha na autenticação 802.1X.

O dispositivo mapeia o endereço MAC do usuário para a VLAN de falha de autenticação 802.1X. O usuário pode acessar apenas recursos na VLAN de falha de autenticação.

Um usuário na VLAN de falha de autenticação 802.1X falha na autenticação.

O usuário permanece na VLAN de falha de autenticação 802.1X.

VLAN de convidado

A VLAN de convidado 802.1X em uma porta acomoda usuários que não passaram na autenticação 802.1X. Uma vez que um usuário na VLAN de convidado passa na autenticação 802.1X, ele é removido da VLAN de convidado e pode acessar recursos de rede autorizados.

O dispositivo de acesso lida com VLANs em uma porta 802.1X com base no método de controle de acesso 802.1X. Em uma porta que executa controle de acesso baseado em porta:

Status de autenticação

Manipulação de VLAN

Um usuário não passou na autenticação 802.1X.

O dispositivo atribui a VLAN de convidado 802.1X à porta como PVID. Todos os usuários 802.1X nesta porta podem acessar apenas os recursos na VLAN de convidado.

Se nenhuma VLAN de convidado 802.1X estiver configurada, o dispositivo de acesso não executa nenhuma operação de VLAN.

Um usuário na VLAN de convidado 802.1X falha na autenticação 802.1X.

Se uma VLAN de falha de autenticação 802.1X estiver disponível, o dispositivo atribui a VLAN de falha de autenticação à porta como PVID. Todos os usuários nesta porta podem acessar apenas os recursos na VLAN de falha de autenticação. Se nenhuma VLAN de falha de autenticação estiver configurada, o PVID na porta ainda é a VLAN de convidado 802.1X. Todos os usuários na porta estão na VLAN de convidado.

Se uma VLAN de falha de autenticação 802.1X não estiver configurada, o PVID inicial da porta permanece inalterado.

Um usuário na VLAN de convidado 802.1X passa na autenticação 802.1X.

O dispositivo atribui a VLAN de autorização do usuário à porta como PVID e remove a porta da VLAN de convidado 802.1X. Após o usuário fazer logoff, o PVID inicial da porta é restaurado. Se nenhuma VLAN de convidado 802.1X estiver configurada, o PVID inicial da porta é restaurado. Se o servidor de autenticação (seja o dispositivo de acesso local ou um servidor RADIUS) não autorizar uma VLAN, o PVID inicial se aplica. O usuário e todos os usuários 802.1X subsequentes são atribuídos ao PVID da porta. Após o usuário fazer logoff, o PVID da porta permanece inalterado.

A VLAN de convidado 802.1X no dispositivo de acesso lida com VLANs em uma porta 802.1X com base no método de controle de acesso 802.1X.

Em uma porta que executa controle de acesso baseado em MAC:

Status de autenticação

Manipulação de VLAN

Um usuário não passou na autenticação 802.1X e está no processo de autenticação.

O dispositivo cria um mapeamento entre o endereço MAC do usuário e a VLAN de convidado 802.1X. O usuário pode acessar apenas recursos na VLAN de convidado.

Um usuário na VLAN de convidado 802.1X falha na reautenticação.

Se uma VLAN de falha de autenticação 802.1X estiver configurada, o dispositivo remapeia o endereço MAC do usuário para o ID da VLAN de falha de autenticação. O usuário pode acessar apenas os recursos na VLAN de falha de autenticação.

Se nenhuma VLAN de falha de autenticação 802.1X estiver configurada, o dispositivo remapeia o endereço MAC do usuário para a VLAN de convidado 802.1X. O usuário pode acessar apenas recursos na VLAN de convidado.

Se uma VLAN de falha de autenticação 802.1X não estiver configurada, o dispositivo remapeia o endereço MAC do usuário para a VLAN de convidado 802.1X. O usuário pode acessar apenas recursos na VLAN de convidado 802.1X.

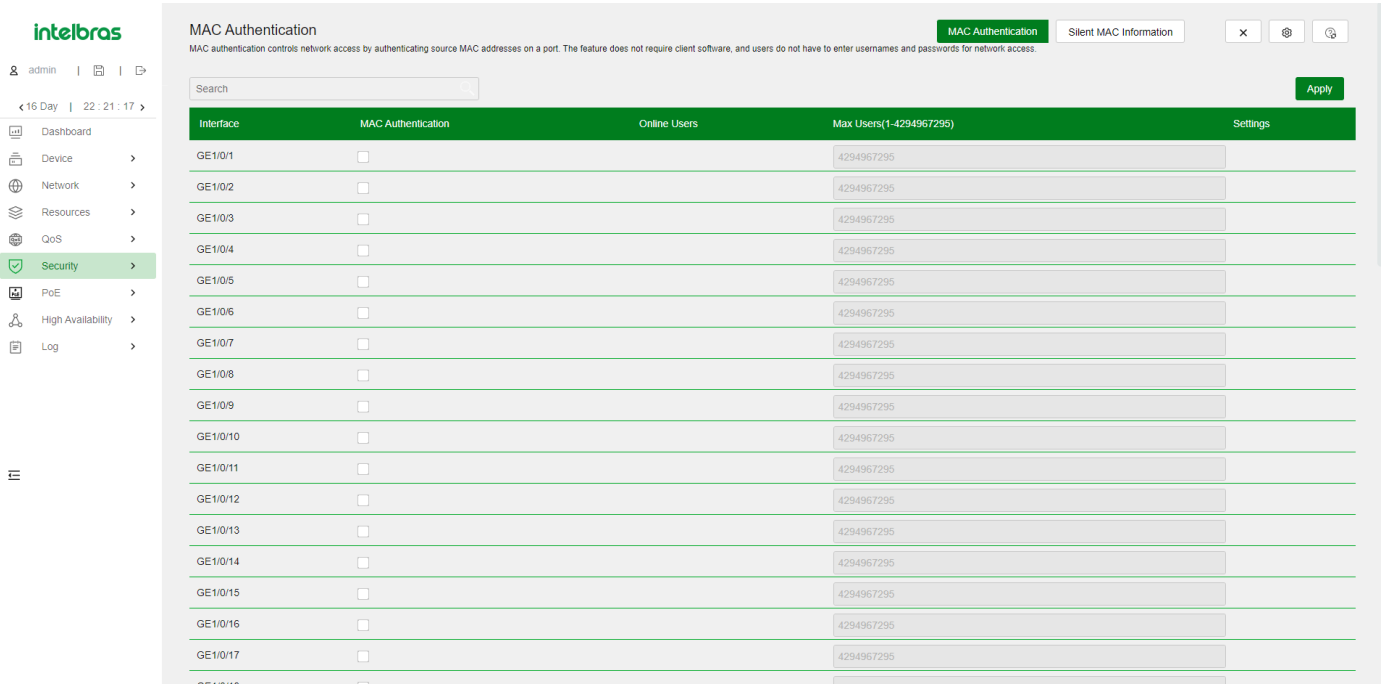
Um usuário na VLAN de convidado 802.1X passa na autenticação.

O dispositivo cria um mapeamento entre o endereço MAC do usuário e a VLAN de autorização. O usuário pode acessar apenas recursos na VLAN de autorização. Se o servidor de autenticação não autorizar uma VLAN, o dispositivo cria um mapeamento entre o endereço MAC do usuário e o PVID inicial na porta. O usuário pode acessar apenas recursos na VLAN inicial.

Se o usuário falhar na autenticação 802.1X e na reautenticação em um dos seguintes casos, o dispositivo remove o mapeamento entre o endereço MAC do usuário e a VLAN de convidado 802.1X: Quando o usuário faz logoff. Quando o dispositivo de acesso local fica inativo. Quando um usuário falha na autenticação ou na reautenticação 802.1X.

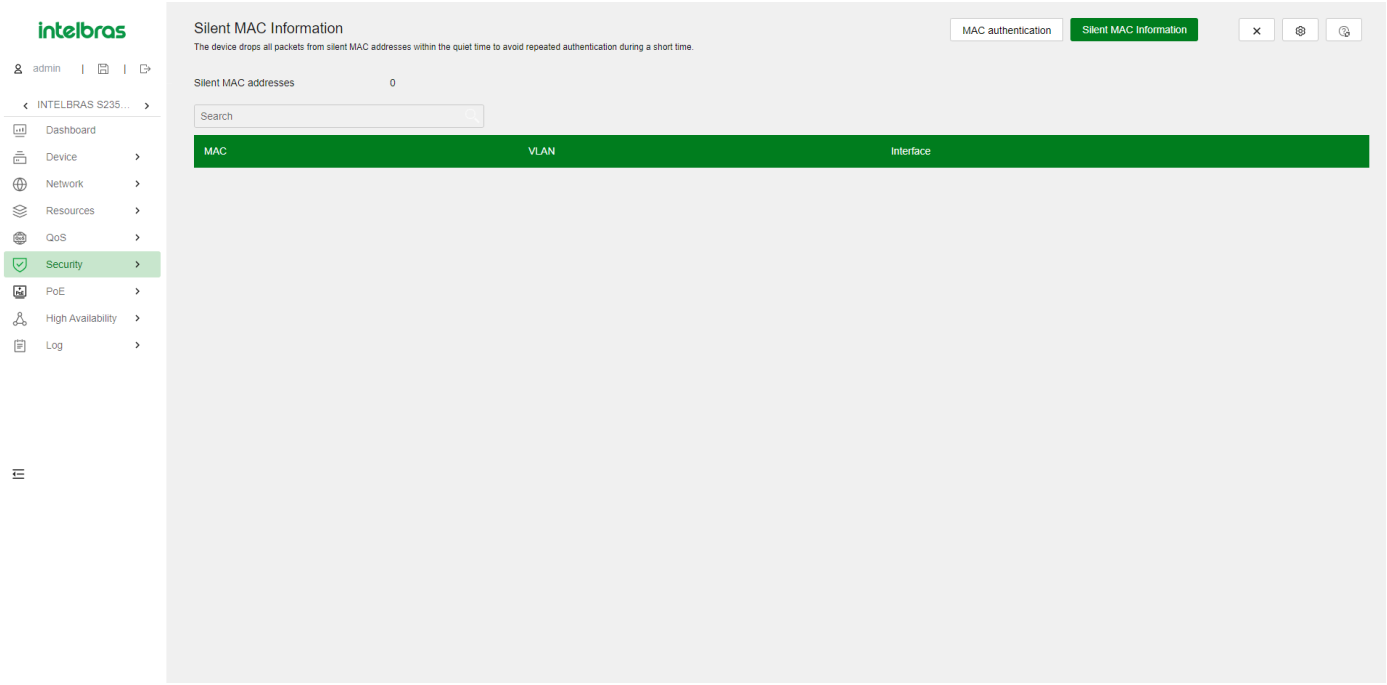
Autenticação MAC

O controle de autenticação MAC controla o acesso à rede autenticando os endereços MAC de origem em uma porta. Esse recurso não requer software do cliente, e os usuários não precisam inserir nomes de usuário e senhas para acessar a rede. O dispositivo inicia um processo de autenticação MAC quando detecta um endereço MAC de origem desconhecido em uma porta habilitada para autenticação MAC.



Informações de Endereço MAC Silencioso

Quando um usuário falha na autenticação MAC, o dispositivo marca o endereço MAC do usuário como um endereço MAC silencioso, descarta o pacote e inicia um temporizador silencioso. O dispositivo descarta todos os pacotes subsequentes do endereço MAC silencioso dentro do tempo silencioso. O mecanismo silencioso evita a autenticação repetida durante um curto período de tempo.



Formato de Nome de Usuário

A autenticação MAC suporta os seguintes formatos de nome de usuário:

- Endereço MAC individual - O dispositivo usa o endereço MAC de cada usuário como nome de usuário e senha para a autenticação MAC. Este formato é adequado para um ambiente não seguro.
- Nome de usuário compartilhado - Você especifica um nome de usuário e senha, que não necessariamente é um endereço MAC, para todos os usuários de autenticação MAC no dispositivo. Este formato é adequado para um ambiente seguro.

Domínio de Autenticação MAC

Por padrão, os usuários de autenticação MAC estão no domínio de autenticação padrão do sistema. Para implementar políticas de acesso diferentes para os usuários, você pode usar um dos seguintes métodos para especificar domínios de autenticação para os usuários de autenticação MAC:

- Especificar um domínio de autenticação global. Essa configuração de domínio se aplica a todas as portas habilitadas com autenticação MAC.
- Especificar um domínio de autenticação para uma porta individual.

A autenticação MAC escolhe um domínio de autenticação para os usuários em uma porta na seguinte ordem: domínio específico da porta, domínio global e domínio padrão.

Temporizador de Detecção Offline

Esse temporizador define o intervalo em que o dispositivo aguarda o tráfego de um usuário antes de considerá-lo inativo. Se uma conexão do usuário estiver inativa dentro do intervalo, o dispositivo encerra a sessão do usuário e para de contabilizar o uso do usuário.

Temporizador Silencioso

Esse temporizador define o intervalo em que o dispositivo deve aguardar antes de realizar a autenticação MAC para um usuário que falhou na autenticação MAC. Todos os pacotes do endereço MAC são descartados durante o tempo silencioso.

Temporizador de Tempo Limite do Servidor

Esse temporizador define o intervalo em que o dispositivo aguarda uma resposta de um servidor RADIUS antes de considerar o servidor RADIUS indisponível. Se o temporizador expirar durante a autenticação MAC, o usuário não poderá acessar a rede.

Configuração de Autenticação MAC em uma Porta

Para que a autenticação MAC tenha efeito em uma porta, você deve habilitar o recurso globalmente e na porta.

VLAN de Visitantes de Autenticação MAC

Uma VLAN de visitantes de autenticação MAC em uma porta acomoda usuários que falharam na autenticação MAC na porta. Os usuários na VLAN de visitantes de autenticação MAC podem acessar um conjunto limitado de recursos de rede, como um servidor de software, para baixar software e patches do sistema. Se nenhuma VLAN de visitantes de autenticação MAC estiver configurada, os usuários que falharam na autenticação MAC não podem acessar nenhum recurso de rede.

A Tabela 22 mostra como o dispositivo de acesso à rede lida com as VLANs de visitantes para usuários de autenticação MAC.

Status de Autenticação	Manipulação da VLAN
Um usuário na VLAN de convidado de autenticação MAC falha na autenticação MAC por qualquer motivo que não seja a inacessibilidade do servidor.	O usuário permanece na VLAN de convidado de autenticação MAC.
Um usuário na VLAN de convidado de autenticação MAC passa na autenticação MAC.	O dispositivo remapeia o endereço MAC do usuário para a VLAN de autorização atribuída pelo servidor de autenticação. Se nenhuma VLAN de autorização estiver configurada para o usuário no servidor de autenticação, o dispositivo remapeia o endereço MAC do usuário para a VLAN inicial.

VLAN Crítica de Autenticação MAC

Uma VLAN crítica de autenticação MAC em uma porta acomoda usuários que falharam na autenticação MAC porque nenhum servidor de autenticação RADIUS está acessível. Os usuários em uma VLAN crítica de autenticação MAC só podem acessar recursos de rede na VLAN crítica.

A funcionalidade da VLAN crítica é ativada quando a autenticação MAC é realizada apenas por meio de servidores RADIUS. Se um usuário de autenticação MAC falhar na autenticação local após a autenticação RADIUS, o usuário não é atribuído à VLAN crítica.

Atraso de Autenticação MAC

Quando a autenticação 802.1X e a autenticação MAC estão habilitadas em uma porta, você pode atrasar a autenticação MAC para que a autenticação 802.1X seja acionada preferencialmente.

Se nenhuma autenticação 802.1X for acionada ou a autenticação 802.1X falhar dentro do período de atraso, a porta continua a processar a autenticação MAC.

Não defina o modo de segurança da porta como macAddressElseUserLoginSecure ou macAddressElseUserLoginSecureExt quando usar o atraso de autenticação MAC. O atraso não tem efeito em uma porta em nenhum dos dois modos.

Modo de Múltiplas VLANs de Autenticação MAC

O modo de múltiplas VLANs de autenticação MAC impede que um usuário online autenticado sofra interrupções no serviço devido a alterações de VLAN em uma porta. Quando a porta recebe um pacote originado pelo usuário em uma VLAN que não corresponde à mapeação MAC-VLAN existente, o dispositivo não desconecta o usuário nem o reautentica. O dispositivo cria uma nova mapeação MAC-VLAN para o usuário e a transmissão de tráfego não é interrompida. A mapeação MAC-VLAN original para o usuário permanece no dispositivo até que expire dinamicamente.

Esse recurso melhora a transmissão de dados vulneráveis a atrasos e interferências. Normalmente, é aplicável a usuários de telefones IP.

Reautenticação MAC Periódica

A reautenticação MAC periódica rastreia o status da conexão de usuários online e atualiza os atributos de autorização atribuídos pelo servidor RADIUS. Os atributos incluem ACL, VLAN e QoS com base no perfil do usuário.

O dispositivo reautentica um usuário online de autenticação MAC periodicamente somente após receber a ação de término Radius-request do servidor de autenticação para esse usuário. O atributo Session-Timeout (período de tempo de sessão) atribuído pelo servidor é o intervalo de reautenticação. O suporte para a configuração do servidor e a atribuição de atributos Session-Timeout e Termination-Action dependem do modelo do servidor.

Quando nenhum servidor é alcançável para a reautenticação MAC, o dispositivo mantém os usuários de autenticação MAC online ou desconecta os usuários, dependendo da configuração do recurso de manter online no dispositivo.

Manter Usuários Online

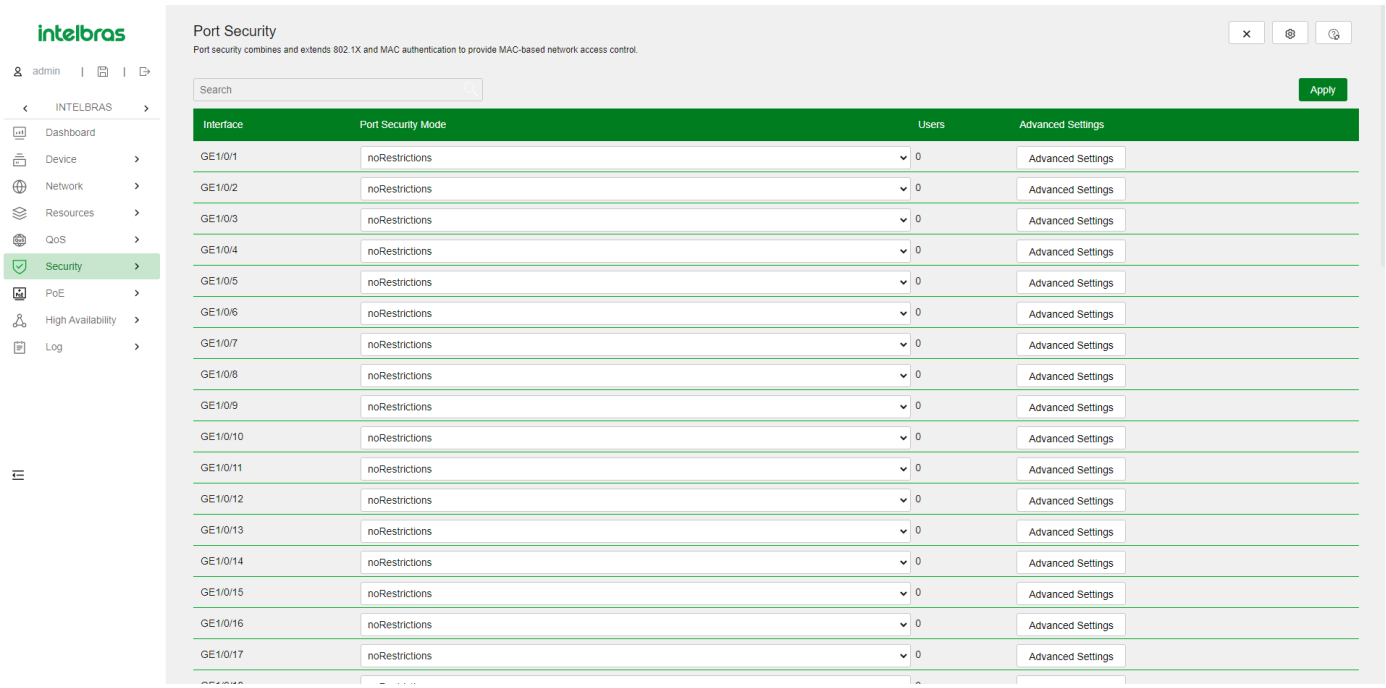
Por padrão, o dispositivo desconecta os usuários online de autenticação MAC se nenhum servidor for alcançável para a reautenticação MAC. O recurso de manter online mantém os usuários autenticados de autenticação MAC online quando nenhum servidor é alcançável para a reautenticação MAC.

Em uma rede de recuperação rápida, você pode usar o recurso de manter online para evitar que os usuários de autenticação MAC entrem online e offline frequentemente.

Segurança de Porta

A segurança de porta combina e estende a autenticação 802.1X e MAC para fornecer controle de acesso à rede baseado em MAC. A segurança de porta oferece as seguintes funções:

- Previne o acesso não autorizado à rede verificando os endereços MAC de origem do tráfego de entrada.
- Impede o acesso de dispositivos ou hosts não autorizados verificando os endereços MAC de destino do tráfego de saída.
- Controla a aprendizagem de endereços MAC e autenticação em uma porta para garantir que a porta aprenda apenas endereços MAC de origem confiáveis.



Um quadro é ilegal se o seu endereço MAC de origem não puder ser aprendido em um modo de segurança de porta ou se for de um cliente que falhou na autenticação 802.1X ou MAC. A função de segurança de porta toma automaticamente uma ação predefinida em quadros ilegais. Esse mecanismo automático aprimora a segurança da rede e reduz a intervenção humana.

Authorization-fail-offline

O recurso authorization-fail-offline desconecta os usuários de segurança de porta que falham na autorização de ACL ou perfil de usuário.

Um usuário falha na autorização de ACL ou perfil de usuário nas seguintes situações:

- O dispositivo falha em autorizar o ACL ou perfil de usuário especificado para o usuário.
- O servidor atribui um ACL ou perfil de usuário inexistente ao usuário.

Quando esse recurso está desativado, o dispositivo não desconecta os usuários que falham na autorização de ACL ou perfil de usuário.

Tempo de envelhecimento para endereços MAC seguros

Quando os endereços MAC seguros envelhecem, eles são removidos da tabela de endereços MAC seguros.

Este temporizador se aplica a todos os endereços MAC seguros pegajosos configurados e aqueles aprendidos automaticamente por uma porta. Para desativar o temporizador de envelhecimento, defina o tempo como 0.

Período de silêncio

Este período define a duração durante a qual uma porta permanece desativada quando recebe quadros ilegais. A ação de proteção contra intrusões na porta deve ser "Desativar temporariamente a porta".

Autenticação OUI

O valor OUI configurado entra em vigor apenas quando o modo de autenticação da porta é "userLoginWithOUI".

No modo "userLoginWithOUI", a porta permite que os seguintes usuários passem:

- Um usuário que passa na autenticação 802.1X.
- Um usuário cujo endereço MAC contém o mesmo OUI que o OUI configurado no dispositivo.

Configurações de segurança de porta

Modos de segurança de porta

A segurança de porta oferece suporte às seguintes categorias de modos de segurança:

- Controle de aprendizagem MAC - Inclui dois modos: autoLearn e secure. A aprendizagem de endereços MAC é permitida em uma porta no modo autoLearn e desativada no modo secure.
- Autenticação - Os modos de segurança nesta categoria implementam a autenticação MAC, a autenticação 802.1X ou uma combinação desses dois métodos de autenticação.

  Ao receber um quadro, a porta em um modo de segurança pesquisa a tabela de endereços MAC em busca do endereço MAC de origem. Se houver correspondência, a porta encaminha o quadro. Se nenhuma correspondência for encontrada, a porta aprende o endereço MAC ou realiza a autenticação, dependendo do modo de segurança. Se o quadro for ilegal, a porta toma a ação predefinida de NTK ou proteção contra intrusões. Quadros de saída não são restritos pela ação NTK da segurança de porta, a menos que acionem o recurso NTK.

- Controlar o Aprendizado de Endereços MAC:
  - autoLearn.

    Uma porta neste modo pode aprender endereços MAC. Os endereços MAC aprendidos automaticamente não são adicionados à tabela de endereços MAC como endereços MAC dinâmicos. Em vez disso, esses endereços MAC são adicionados à tabela de endereços MAC seguros como endereços MAC seguros. Você também pode adicionar manualmente endereços MAC seguros. Uma porta no modo autoLearn permite que os quadros provenientes dos seguintes endereços MAC passem:

    - Endereços MAC seguros.
    - Endereços MAC estáticos e dinâmicos configurados manualmente.

      Quando o número de endereços MAC seguros atinge o limite máximo, a porta entra no modo seguro.

  - secure.

    O aprendizado de endereços MAC é desativado em uma porta no modo seguro. Uma porta no modo seguro permite apenas que quadros provenientes dos seguintes endereços MAC passem:

    - Endereços MAC seguros.
    - Endereços MAC estáticos e dinâmicos configurados manualmente.

- Realizar autenticação 802.1X:
  - userLogin.

    Uma porta neste modo realiza a autenticação 802.1X e implementa o controle de acesso baseado em porta. A porta pode atender a vários usuários 802.1X. Uma vez que um usuário 802.1X passa pela autenticação na porta, qualquer usuário subsequente 802.1X pode acessar a rede pela porta sem autenticação.

  - userLoginSecure.

    Uma porta neste modo realiza a autenticação 802.1X e implementa o controle de acesso baseado em MAC. A porta atende apenas a um usuário que passa pela autenticação 802.1X.

  - userLoginSecureExt.

    Este modo é semelhante ao modo userLoginSecure, exceto que este modo suporta vários usuários 802.1X online.

  - userLoginWithOUI.

    Este modo é semelhante ao modo userLoginSecure. A diferença é que uma porta neste modo também permite quadros de um usuário cujo endereço MAC contém um OUI específico. Neste modo, a porta realiza primeiro a verificação de OUI. Se a verificação de OUI falhar, a porta realiza a autenticação 802.1X. A porta permite quadros que passam na verificação de OUI ou na autenticação 802.1X.

- Realizar autenticação MAC:
  - macAddressWithRadius:

    Uma porta neste modo realiza a autenticação MAC e atende a vários usuários.

- Realizar uma combinação de autenticação MAC e autenticação 802.1X:
  - macAddressOrUserLoginSecure.

    Este modo é a combinação dos modos macAddressWithRadius e userLoginSecure. O modo permite um usuário de autenticação 802.1X e vários usuários de autenticação MAC se conectarem. Neste modo, a porta realiza primeiro a autenticação 802.1X. Se a autenticação 802.1X falhar, a autenticação MAC é realizada.

- macAddressOrUserLoginSecureExt.
  Este modo é semelhante ao modo macAddressOrUserLoginSecure, exceto que este modo suporta vários usuários de autenticação 802.1X e MAC.
- macAddressElseUserLoginSecure.
  Este modo é a combinação dos modos macAddressWithRadius e userLoginSecure, com a autenticação MAC tendo prioridade mais alta, como implica a palavra-chave "Else". O modo permite um usuário de autenticação 802.1X e vários usuários de autenticação MAC se conectarem. Neste modo, a porta realiza a autenticação MAC ao receber quadros que não são 802.1X. Ao receber quadros 802.1X, a porta realiza a autenticação MAC e, em seguida, se a autenticação falhar, a autenticação 802.1X.
- macAddressElseUserLoginSecureExt.
  Este modo é semelhante ao modo macAddressElseUserLoginSecure, exceto que este modo suporta vários usuários de autenticação 802.1X e MAC, como a palavra-chave "Ext" implica.

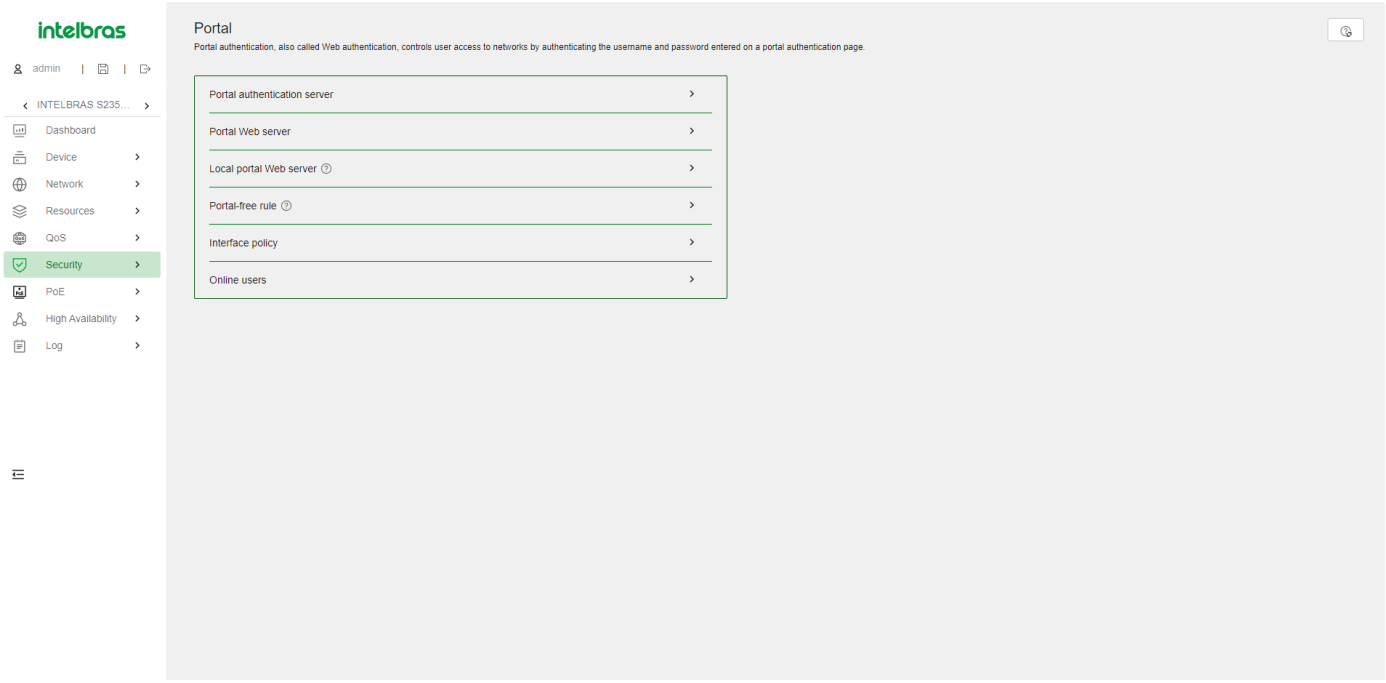
Portal

O portal de autenticação controla o acesso de usuários às redes. Ele autentica um usuário pelo nome de usuário e senha inseridos em uma página de autenticação. Portanto, a autenticação de portal é também conhecida como autenticação web.

O portal de autenticação impõe de forma flexível o controle de acesso na camada de acesso e entradas de dados vitais. Ele possui as seguintes vantagens:

- Permite que os usuários realizem a autenticação por meio de um navegador da web sem instalar software cliente.
- Fornece às ISPs opções de gerenciamento diversificadas e funções estendidas. Por exemplo, as ISPs podem exibir anúncios, oferecer serviços comunitários e publicar informações na página de autenticação.
- Suporta vários modos de autenticação. Por exemplo, a autenticação re-DHCP implementa um esquema flexível de atribuição de endereços e economiza endereços IP públicos. A autenticação entre sub-redes pode autenticar usuários que residem em uma sub-rede diferente do dispositivo de acesso.

- Cliente de autenticação - Um navegador da web que executa HTTP/HTTPS ou um host de usuário que executa um aplicativo de cliente de portal.
- Dispositivo de acesso - Dispositivo de acesso de banda larga, como um switch ou um roteador.
- Servidor de autenticação de portal - Recebe solicitações de autenticação dos clientes de autenticação e interage com informações de autenticação de usuário no dispositivo de acesso.
- Servidor da web de portal - Envia a página de autenticação web para os clientes de autenticação e encaminha as informações de autenticação do usuário (nome de usuário e senha) para o servidor de autenticação de portal.



Servidor de Autenticação AAA

O servidor AAA interage com o dispositivo de acesso para implementar autenticação, autorização e contabilidade para usuários de portal.

Servidor de Autenticação de Portal

O servidor de autenticação de portal recebe solicitações de autenticação dos clientes de autenticação e interage com informações de autenticação de usuário no dispositivo de acesso.

Deteção do Servidor de Autenticação de Portal

Durante a autenticação de portal, se a comunicação entre o dispositivo de acesso e o servidor de autenticação de portal for interrompida, ocorrem as seguintes situações:

- Os novos usuários do portal não conseguem fazer login.
- Os usuários online no portal não conseguem fazer logout normalmente.

Para resolver esse problema, o dispositivo de acesso precisa ser capaz de detectar as mudanças na acessibilidade do servidor de portal rapidamente e tomar ações correspondentes para lidar com as mudanças.

Sincronização de Usuários do Portal

Uma vez que o dispositivo de acesso perde a comunicação com um servidor de autenticação de portal, as informações dos usuários do portal no dispositivo de acesso e no servidor podem ficar inconsistentes após a retomada da comunicação. Para resolver esse problema, o dispositivo oferece o recurso de sincronização de usuário do portal.

Isso é implementado por meio do envio e da detecção de pacotes de sincronização do portal. Quando o servidor de autenticação de portal envia o pacote de informações de usuário online ao dispositivo de acesso em um intervalo de pulso do usuário, o dispositivo de acesso compara os usuários incluídos no pacote com sua própria lista de usuários e realiza as seguintes operações:

- Se um usuário contido no pacote não existir no dispositivo de acesso, o dispositivo de acesso notifica o servidor de autenticação de portal para excluir o usuário.
- Se o usuário não aparecer em nenhum pacote de sincronização dentro de um intervalo de detecção de sincronização, o dispositivo de acesso considera que o usuário não existe no servidor e faz logout do usuário.

Servidor Web de Portal

O servidor web de portal envia a página de autenticação web para os clientes de autenticação e encaminha as informações de autenticação do usuário (nome de usuário e senha) para o servidor de autenticação de portal.

Parâmetros de URL de Redirecionamento

Este recurso configura os parâmetros a serem incluídos na URL de redirecionamento. Os parâmetros comuns exigidos incluem o endereço IP do usuário, o endereço MAC do usuário e a URL originalmente visitada pelo usuário.

Após configurar os parâmetros de URL, o dispositivo de acesso envia a URL do servidor web de portal com esses parâmetros para os usuários do portal. Suponha que a URL de um servidor web de portal seja http://www.test.com/portal, a URL originalmente visitada pelo usuário, cujo endereço IP é 1.1.1.1, seja http://www/abc.com/welcome, e você configura os parâmetros de endereço IP do usuário e URL original. Nesse caso, o dispositivo de acesso envia para o usuário com endereço IP 1.1.1.1 a URL http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome.

Deteção do Servidor Web de Portal

Um processo de autenticação de portal não pode ser concluído se a comunicação entre o dispositivo de acesso e o servidor web de portal for interrompida. Para resolver esse problema, você pode habilitar a detecção do servidor web de portal no dispositivo de acesso.

Com o recurso de detecção do servidor web de portal, o dispositivo de acesso simula um processo de acesso web para iniciar uma conexão TCP com o servidor web de portal. Se a conexão TCP puder ser estabelecida com sucesso, o dispositivo de acesso considera a detecção bem-sucedida e o servidor web de portal é acessível. Caso contrário, considera a detecção como falha. O status da autenticação do portal nas interfaces do dispositivo de acesso não afeta o recurso de detecção do servidor web de portal.

Você pode configurar os seguintes parâmetros de detecção:

- Intervalo de detecção - Intervalo em que o dispositivo detecta a acessibilidade do servidor.
- Número máximo de falhas consecutivas - Se o número de falhas consecutivas de detecção atingir esse valor, o dispositivo de acesso considera que o servidor web de portal não está acessível.

Servidor de Portal Web Local

Usando este recurso, o dispositivo de acesso também atua como servidor web de portal e servidor de autenticação de portal para realizar autenticação local de portal para usuários do portal. Nesse caso, o sistema de portal consiste apenas em três componentes: cliente de autenticação, dispositivo de acesso e servidor AAA.

Protocolos de Interação Cliente e Servidor de Portal Local

O HTTP e o HTTPS podem ser usados para a interação entre um cliente de autenticação e um servidor de portal local. Se o HTTP for usado, existem problemas de segurança potenciais, porque os pacotes HTTP são transferidos em texto simples. Se o HTTPS for usado, a transmissão segura de dados é garantida porque os pacotes HTTP são protegidos pelo SSL.

Customização de Páginas de Portal

Para realizar a autenticação local de portal, você deve personalizar um conjunto de páginas de autenticação que o dispositivo enviará aos usuários. Você pode personalizar vários conjuntos de páginas de autenticação, compactar cada conjunto de páginas em um arquivo .zip e fazer o upload dos arquivos compactados para o meio de armazenamento do dispositivo. No dispositivo, você deve especificar um dos arquivos como o arquivo de página de autenticação padrão.

As páginas de autenticação são arquivos HTML. A autenticação local de portal requer as seguintes páginas de autenticação:

- Página de login
- Página de sucesso de login
- Página de falha de login
- Página online

- Página de sistema ocupado
- Página de sucesso de logout

Você deve personalizar as páginas de autenticação, incluindo os elementos da página que as páginas de autenticação usarão, por exemplo, back.jpg para a página de autenticação Logon.htm.

Regras de Nomenclatura de Arquivos

Os nomes dos principais arquivos de página de autenticação são fixos (consulte a Tabela 24). Você pode definir os nomes dos arquivos que não sejam os principais arquivos de página de autenticação. Os nomes de arquivos e nomes de diretório não fazem distinção entre maiúsculas e minúsculas.

Tabela 24 Nomes de arquivos principais de página de autenticação

Página de Autenticação Principal	Nome do Arquivo
Página de login	logon.htm
Página de sucesso de login	logonSuccess.htm
Página de falha de login	logonFail.htm
Página online	online.htm
Página de sistema ocupado	busy.htm
Página de sucesso de logout	logoffSuccess.htm

Regras de Solicitação de Página

O servidor web de portal local suporta apenas solicitações Get e Post.

- Solicitações Get - Usadas para obter arquivos estáticos nas páginas de autenticação e não permitem recursão. Por exemplo, se o arquivo Logon.htm inclui conteúdo que executa a ação Get no arquivo ca.htm, o arquivo ca.htm não pode fazer referência ao arquivo Logon.htm.
- Solicitações Post - Usadas quando os usuários enviam pares de nome de usuário e senha, fazem login e logout.

Regras de Atributos de Solicitação Post

1. Observe as seguintes exigências ao editar um formulário de uma página de autenticação:
   - Uma página de autenticação pode ter vários formulários, mas deve haver um e apenas um formulário cuja ação seja logon.cgi. Caso contrário, as informações do usuário não podem ser enviadas para o servidor web de portal local.
   - O atributo de nome de usuário é fixado como PtUser. O atributo de senha é fixado como PtPwd.
   - O valor do atributo PtButton é Logon ou Logoff, o que indica a ação solicitada pelo usuário.
   - Uma solicitação Post de login deve conter os atributos PtUser, PtPwd e PtButton.
   - Uma solicitação Post de logout deve conter o atributo PtButton.
2. As páginas de autenticação Logon.htm e LogonFail.htm devem conter a solicitação Post de login.
3. As páginas de autenticação LogonSuccess.htm e Online.htm devem conter a solicitação Post de logout.

Regras de Compressão e Salvamento de Arquivos de Página

Você deve compactar as páginas de autenticação e seus elementos de página em um arquivo zip padrão.

- O nome de um arquivo zip pode conter apenas letras, números e sublinhados.
- As páginas de autenticação devem ser colocadas no diretório raiz do arquivo zip.
- Arquivos zip podem ser transferidos para o dispositivo via FTP ou TFTP e devem ser salvos no diretório raiz do dispositivo.

Exemplos de arquivos zip no dispositivo:

```
<Sysname> dir Directory of flash:
0       -rw-    1405    Feb     28      2008    15:53:31        ssid2.zip
1       -rw-    1405    Feb     28      2008    15:53:20        ssid1.zip
2       -rw-    1405    Feb     28      2008    15:53:39        ssid3.zip
3       -rw-    1405    Feb     28      2008    15:53:44        ssid4.zip
2540 KB total (1319 KB free)
```

Redirecionamento de Usuários Autenticados para uma Página Específica

Para fazer com que o dispositivo redirecione automaticamente os usuários autenticados para uma página específica, siga as etapas a seguir em Logon.htm e LogonSuccess.htm:

1. Em Logon.htm, defina o atributo target do Form como _blank. Veja o conteúdo em cinza:

   ```
   <form method="post" action="logon.cgi" target="_blank">
   ```

2. Adicione a função para o carregamento da página pt_init() em LogonSuccess.htm. Veja o conteúdo em cinza:

   ```
   <html>
   <head>
   <title>LogonSuccessed</title>
       <script type="text/javascript" language="javascript" src="pt_private.js"></script>
   </head>
   <body onload="pt_init();" onbeforeunload="return pt_unload();">
   ... ...
   </body>
   </html>
   ```

Regras de Portal Livre

Uma regra de portal livre permite que usuários especificados acessem sites externos especificados sem autenticação de portal.

- Regras de portal livre baseadas em IP - Os itens correspondentes para uma regra de portal livre baseada em IP incluem o endereço IP e a porta TCP/UDP.
- Regras de portal livre baseadas em origem - Os itens correspondentes para uma regra de portal livre baseada em origem incluem o endereço MAC de origem, a interface de acesso e a VLAN.

  Pacotes correspondentes a uma regra de portal livre não acionarão a autenticação do portal, portanto, os usuários que enviam os pacotes podem acessar diretamente os sites externos especificados.

Política de Interface

Uma política de interface é um conjunto de recursos de portal configurados em uma interface.

Recurso de Falha de Portal

Este recurso permite que os usuários em uma interface tenham acesso à rede sem autenticação de portal quando o dispositivo de acesso detecta que o servidor de autenticação de portal ou o servidor web de portal não está acessível.

Se você habilitar o fail-permit para ambos um servidor de autenticação de portal e um servidor web de portal em uma interface, a interface executará as seguintes operações:

- Desativa a autenticação de portal quando um dos servidores não está acessível.
- Restaura a autenticação de portal quando ambos os servidores estão acessíveis.

Após a restauração da autenticação de portal, os usuários não autenticados devem passar pela autenticação de portal para acessar a rede. Os usuários que passaram pela autenticação de portal antes do evento fail-permit podem continuar acessando a rede.

Atributo BAS-IP

Este recurso permite que você configure o atributo BAS-IP ou BAS-IPv6 em uma interface habilitada para portal. O dispositivo utiliza o endereço BAS-IP ou BAS-IPv6 configurado como o endereço IP de origem das notificações de portal enviadas da interface para o servidor de autenticação de portal.

Se você não configurar este recurso, o atributo BAS-IP/BAS-IPv6 de um pacote de notificação de portal enviado para o servidor de autenticação de portal será o endereço IPv4/IPv6 da interface de saída do pacote. O atributo BAS-IP/BAS-IPv6 de um pacote de resposta do portal é o endereço IPv4/IPv6 de origem do pacote.

Deteção de Usuário

Este recurso implementa a detecção rápida de saídas anormais de usuários de portal. Ele oferece suporte à detecção ARP ou ICMP para usuários de portal IPv4 e ND ou ICMPv6 para usuários de portal IPv6.

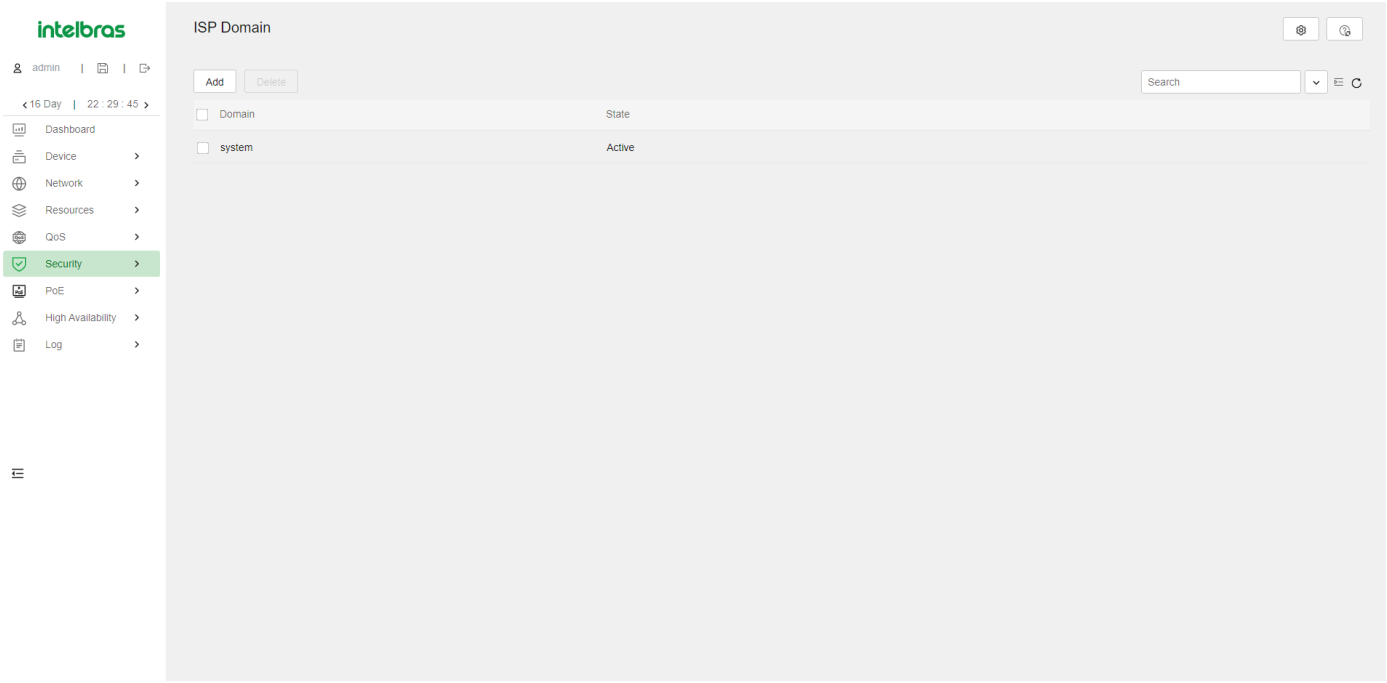
As detecções ARP e ND se aplicam apenas à autenticação de portal direta e re-DHCP. A detecção ICMP se aplica a todos os modos de autenticação de portal.

Se o dispositivo não receber pacotes de um usuário de portal dentro do tempo ocioso, ele detecta o status online do usuário da seguinte maneira:

- Deteção ICMP ou ICMPv6 - Envia solicitações ICMP ou ICMPv6 para o usuário em intervalos configuráveis para detectar o status do usuário.
- Se o dispositivo receber uma resposta dentro do número máximo de tentativas de detecção, ele determina que o usuário está online e interrompe o envio de pacotes de detecção. Em seguida, o dispositivo redefine o temporizador de ociosidade e repete o processo de detecção quando o temporizador expira.
- Se o dispositivo não receber resposta após o número máximo de tentativas de detecção, o dispositivo faz logout do usuário.
- Deteção ARP ou ND - Envia solicitações ARP ou ND para o usuário e detecta o status da entrada ARP ou ND do usuário em intervalos configuráveis.
- Se a entrada ARP ou ND do usuário for atualizada dentro do número máximo de tentativas de detecção, o dispositivo considera que o usuário está online e interrompe a detecção. Em seguida, o dispositivo redefine o temporizador de ociosidade e repete o processo de detecção quando o temporizador expira.
- Se a entrada ARP ou ND do usuário não for atualizada após o número máximo de tentativas de detecção, o dispositivo faz logout do usuário.

Domínios ISP

O dispositivo gerencia os usuários com base em domínios ISP. Um ISP domain inclui métodos de autenticação, autorização e contabilidade para usuários. O dispositivo determina o domínio ISP e o tipo de acesso de um usuário. Ele também usa os métodos configurados para o tipo de acesso no domínio para controlar o acesso do usuário.



Métodos de Autenticação

- Sem autenticação: Este método confia em todos os usuários e não realiza autenticação. Por motivos de segurança, não utilize este método.
- Autenticação Local: O dispositivo autentica os usuários com base nas informações do usuário configuradas localmente, incluindo nomes de usuário, senhas e atributos. A autenticação local permite alta velocidade e baixo custo, mas a quantidade de informações que pode ser armazenada é limitada pelo espaço de armazenamento.
- Autenticação Remota: O dispositivo trabalha com um servidor RADIUS remoto ou servidor TACACS para autenticar usuários. O servidor gerencia as informações do usuário de maneira centralizada. A autenticação remota fornece serviços de autenticação de alta capacidade, confiáveis e centralizados para vários dispositivos. Você pode configurar métodos de backup a serem usados quando o servidor remoto não estiver disponível.

Métodos de Autorização

- Sem autorização: O dispositivo não realiza troca de autorização. As seguintes informações padrão de autorização se aplicam após os usuários passarem pela autenticação:
  - Usuários não logados podem acessar a rede.
  - Usuários FTP, SFTP e SCP têm o diretório raiz do dispositivo definido como o diretório de trabalho. No entanto, os usuários não têm permissão para acessar o diretório raiz.
  - Outros usuários logados obtêm a função de usuário padrão.
- Autorização Local: O dispositivo realiza a autorização de acordo com os atributos do usuário configurados localmente.
- Autorização Remota: O dispositivo trabalha com um servidor RADIUS remoto ou servidor TACACS para autorizar usuários. A autorização RADIUS está vinculada à autenticação RADIUS. A autorização RADIUS só pode funcionar depois que a autenticação RADIUS for bem-sucedida, e as informações de autorização estão incluídas no pacote Access-Accept. A autorização TACACS é independente da autenticação TACACS, e as informações de autorização estão incluídas na resposta.

Métodos de Contabilidade

- Sem contabilidade: O dispositivo não realiza contabilidade para os usuários.
- Contabilidade Local: A contabilidade local é implementada no dispositivo. Ela conta e controla o número de usuários simultâneos que usam a mesma conta de usuário local, mas não fornece estatísticas para cobrança.

- Contabilidade Remota: O dispositivo trabalha com um servidor RADIUS remoto ou servidor TACACS para contabilidade. Você pode configurar métodos de backup a serem usados quando o servidor remoto não estiver disponível.

Tipo de Acesso dos Usuários

No dispositivo, cada usuário pertence a um domínio ISP. O dispositivo determina o domínio ISP a que um usuário pertence com base no nome de usuário inserido pelo usuário no momento do login. O AAA gerencia os usuários no mesmo domínio ISP com base nos tipos de acesso dos usuários. O dispositivo suporta os seguintes tipos de acesso do usuário:

- LAN: Os usuários da LAN devem passar pela autenticação 802.1X para se conectar online.
- Login: Os usuários de login incluem Telnet, FTP e usuários de terminal que fazem login no dispositivo. Os usuários de terminal podem acessar através de uma porta de console.
- Portal: Usuários de portal.

  Em um cenário de rede com vários ISPs, o dispositivo pode se conectar a usuários de diferentes ISPs. O dispositivo suporta vários domínios ISP, incluindo um domínio ISP definido pelo sistema chamado "system". Um dos domínios ISP é o domínio padrão. Se um usuário não fornecer um nome de domínio ISP para autenticação, o dispositivo considera que o usuário pertence ao domínio ISP padrão.

  O dispositivo escolhe um domínio de autenticação para cada usuário na seguinte ordem:

1. O domínio de autenticação especificado para o módulo de acesso (por exemplo, 802.1X).
2. O domínio ISP no nome de usuário.
3. O domínio ISP padrão do dispositivo.

RADIUS

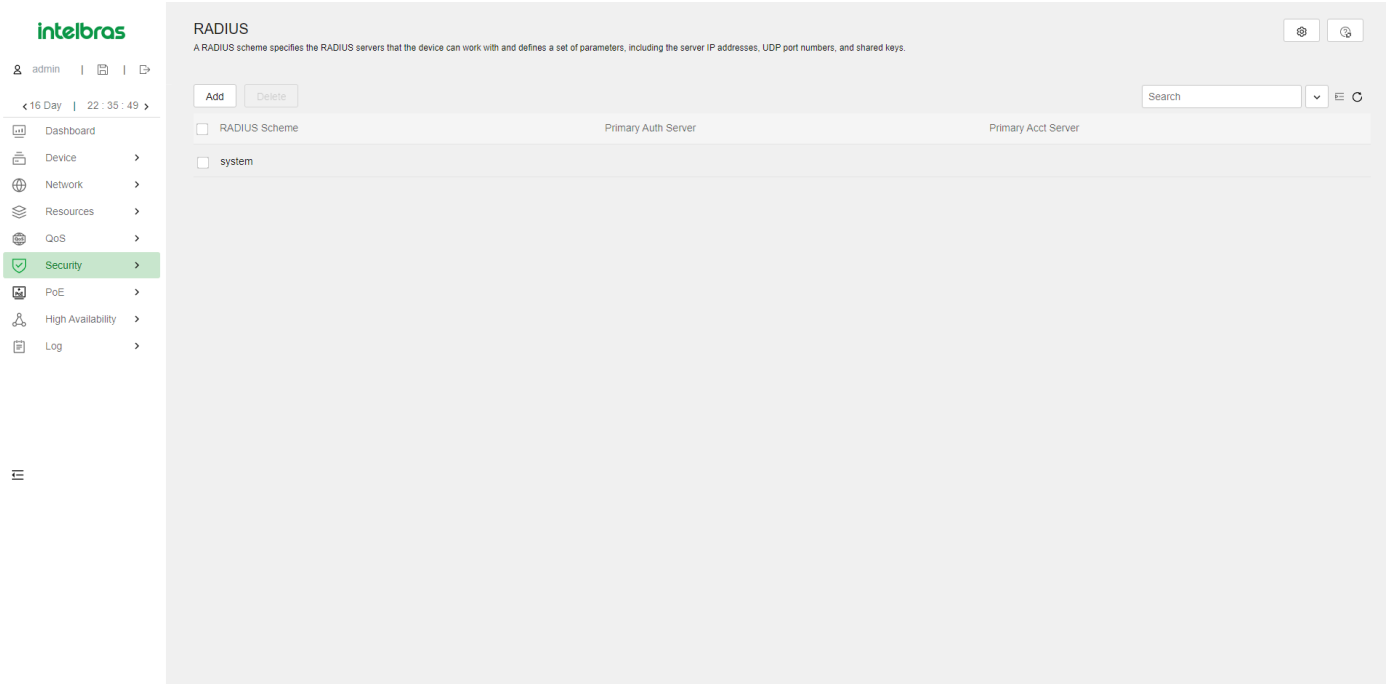
O protocolo RADIUS (Remote Authentication Dial-In User Service) é um protocolo de interação de informações distribuídas que utiliza um modelo cliente/servidor. Esse protocolo pode proteger redes contra acessos não autorizados e é frequentemente usado em ambientes de rede que exigem alta segurança e acesso de usuários remotos.

O cliente RADIUS é executado nos NASs (Network Access Servers) localizados em toda a rede. Ele envia informações do usuário para os servidores RADIUS e age com base nas respostas, por exemplo, para rejeitar ou aceitar solicitações de acesso do usuário.

O servidor RADIUS é executado no computador ou estação de trabalho no centro da rede e mantém informações relacionadas à autenticação do usuário e ao acesso aos serviços de rede.

O RADIUS utiliza o protocolo UDP para transmitir pacotes. O cliente e o servidor RADIUS trocam informações com a ajuda de chaves compartilhadas.

Quando o AAA é implementado por um servidor RADIUS remoto, configure as configurações do servidor RADIUS no dispositivo que atua como NAS para os usuários.



Recursos Avançados do RADIUS

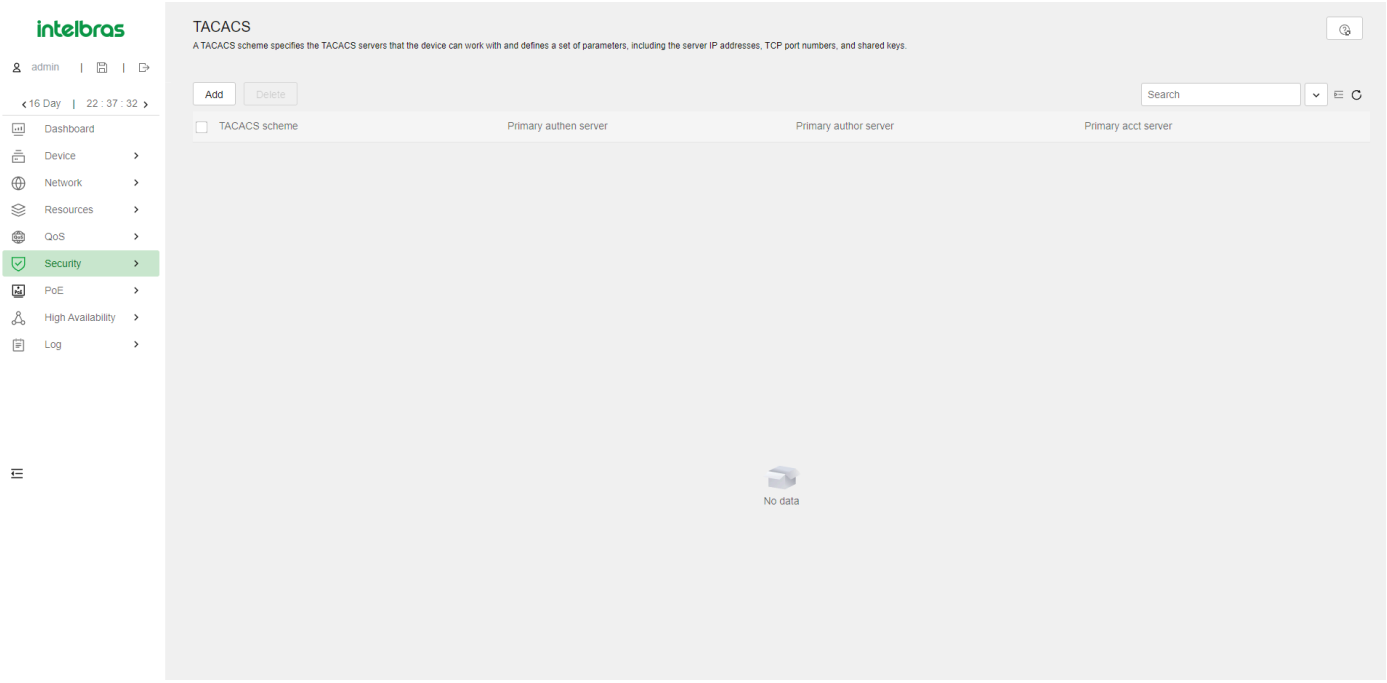
- Accounting-on: Esse recurso permite que o dispositivo envie automaticamente um pacote "accounting-on" para o servidor RADIUS após uma reinicialização. Após receber o pacote "accounting-on", o servidor RADIUS desconecta todos os usuários online para que possam fazer login novamente por meio do dispositivo. Sem esse recurso, os usuários não podem fazer login novamente após a reinicialização, porque o servidor RADIUS os considera como "online". É possível configurar o intervalo no qual o dispositivo aguarda para reenviar o pacote "accounting-on" e o número máximo de tentativas. O servidor RADIUS deve ser executado no IMC para desconectar corretamente os usuários quando um cartão é reiniciado no dispositivo distribuído ao qual os usuários estão conectados.
- Controle de Sessão: Um servidor RADIUS em execução no IMC pode usar pacotes de controle de sessão para informar solicitações de desconexão ou alteração de autorização dinâmica. Ative o controle de sessão no dispositivo para receber pacotes de controle de sessão RADIUS na porta UDP 1812.

TACACS

O TACACS (Terminal Access Controller Access Control System) é definido no RFC 1492 e é um protocolo de segurança aprimorado. O TACACS é semelhante ao RADIUS e usa um modelo cliente/servidor para a troca de informações entre o NAS e o servidor TACACS.

O TACACS normalmente fornece serviços AAA para PPP, VPDN e usuários de terminal. Em um cenário típico de TACACS, os usuários de terminal precisam fazer login no NAS. Atuando como cliente TACACS, o NAS envia os nomes de usuário e senhas dos usuários para o servidor TACACS para autenticação. Após passar pela autenticação e obter direitos autorizados, um usuário faz login no dispositivo e executa operações. O servidor TACACS registra as operações que cada usuário realiza.

Para atuar como cliente TACACS, você deve configurar os parâmetros do servidor TACACS no dispositivo.



Usuários Locais

O dispositivo realiza autenticação, autorização e contabilidade locais com base nas informações do usuário configuradas localmente, incluindo nome de usuário, senha e atributos de autorização. Cada usuário local é identificado pelo nome de usuário.

Grupos de usuários simplificam a configuração e gerenciamento de usuários locais. Um grupo de usuários contém um conjunto de usuários locais e possui um conjunto de atributos de usuário local. Os atributos de usuário do grupo se aplicam a todos os usuários desse grupo.

Power over Ethernet (PoE)

O Power over Ethernet (PoE) é uma tecnologia que permite transmitir energia elétrica através de cabos Ethernet, permitindo alimentar dispositivos de rede.

Equipamento de Fonte de Energia (PSE)

- O Equipamento de Fonte de Energia (PSE) fornece energia elétrica a Dispositivos de Alimentação (PDs) por meio da tecnologia PoE.

Potência Garantida Restante

- A potência garantida restante é a máxima potência do PSE menos a potência para PIs críticos em PoE.

Potência Máxima

- A potência máxima do PSE é a máxima que ele pode fornecer a todos os PDs.

Power Injector (PI)

- O Power Injector (PI) fornece energia a dispositivos não-PoE em uma rede.

Potência Máxima do PI

- A potência máxima do PI é o máximo que ele pode fornecer a todos os PDs. Quando atingida, o PI não fornece mais energia.

Prioridade de Fornecimento de Energia

- O gerenciamento de energia do PI permite ao PSE realizar o gerenciamento de energia baseado na prioridade do PI.

Operações de PSE para Novos PDs

Dependendo da prioridade de um novo PD, o PSE pode realizar várias operações.

Prioridade do Novo PD	Operações do PSE
Low	O PSE não fornece energia a um novo PD.
High	Se PDs de baixa prioridade existirem, o PSE interrompe o fornecimento de energia aos PDs de baixa prioridade existentes e fornece energia ao novo PD. Se nenhum PD de baixa prioridade existir, o PSE não fornece energia ao novo PD.
Critical	Se PDs de baixa ou alta prioridade existirem, o PSE interrompe o fornecimento de energia aos PDs de baixa ou alta prioridade existentes e fornece energia ao novo PD. Se nenhum PD de baixa ou alta prioridade existir, o PSE não fornece energia ao novo PD.

Observação: A configuração para PIs cuja energia é preemptada permanece inalterada.

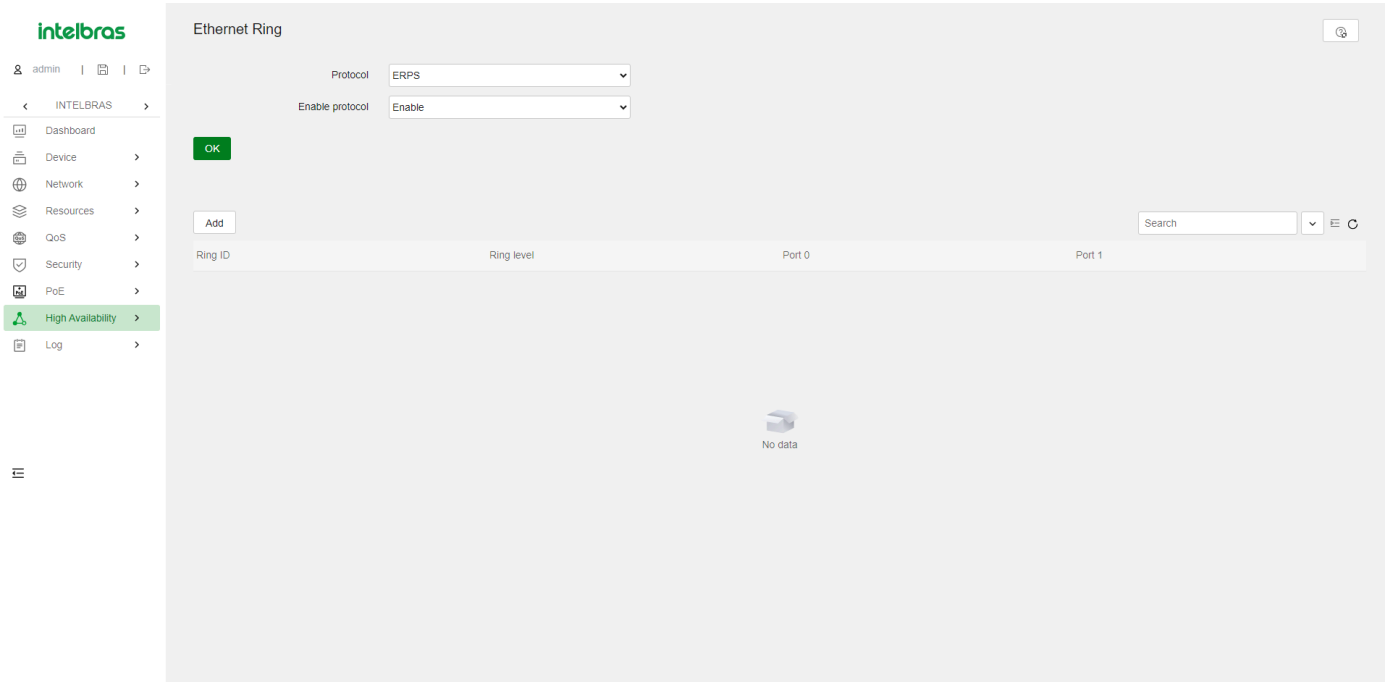
Se vários novos PDs precisarem de fornecimento de energia, o PSE fornece energia aos PDs em ordem de prioridade decrescente. Para PDs com a mesma prioridade, aquele com o menor ID de PD tem precedência.

Se vários PDs existentes precisarem ser interrompidos com fornecimento de energia, o PSE interrompe o fornecimento de energia aos PDs em ordem de prioridade crescente. Para PDs com a mesma prioridade, aquele com o maior ID tem precedência.

O PSE garante energia ininterrupta para seus PIs críticos, reservando potência garantida. Se você deseja que um PI seja alocado com energia ininterrupta, configure o PI com prioridade crítica. Caso contrário, configure o PI com alta ou baixa prioridade para garantir que outros PIs possam ser alimentados com energia.

High Availability Ethernet Ring ERPS

O Ethernet Ring Protection Switching (ERPS) é um protocolo robusto de camada de link que garante uma topologia sem loops e implementa uma recuperação rápida de links.



Aneis

Os anéis ERPS podem ser divididos em anéis principais e subanéis. Por padrão, um anel é considerado um anel principal. É possível configurar manualmente um anel como um subanel. Um domínio ERPS contém um ou vários anéis ERPS, sendo um deles o anel principal e os outros servindo como subanéis.

RPL (Ring Protection Link)

Alguns nós utilizam links de proteção de anel (RPLs) para evitar loops no anel ERPS.

Nós ERPS

Os nós ERPS incluem nós proprietários, nós vizinhos, nós de interconexão e nós normais.

- Os nós proprietários e nós vizinhos bloqueiam e desbloqueiam portas no RPL para evitar loops e comutar tráfego.
- Um RPL conecta um nó proprietário a um nó vizinho.
- Os nós de interconexão conectam diferentes anéis. Eles residem em subanéis e encaminham pacotes de serviço, mas não pacotes de protocolo.
- Os nós normais encaminham tanto pacotes de serviço quanto pacotes de protocolo.

Portas de Membro do Anel ERPS

Cada nó consiste em duas portas de membro de anel ERPS: Porta 0 e Porta 1. As portas de membro do anel ERPS têm os seguintes tipos:

- Porta RPL - Porta em um link RPL.
- Porta de Interconexão - Porta que conecta um subanel a um anel principal.
- Porta Normal - Tipo padrão de porta que encaminha tanto pacotes de serviço quanto pacotes de protocolo.

Instâncias

Um anel ERPS suporta várias instâncias ERPS. Uma instância ERPS é um anel lógico para processar pacotes de serviço e de protocolo. Cada instância ERPS tem seu próprio nó proprietário e mantém seu próprio estado e dados.

VLAN de Controle e VLAN Protegida

O ERPS utiliza os seguintes tipos de VLAN:

- VLAN de Controle - Transporta pacotes de protocolo ERPS. Cada instância ERPS tem sua própria VLAN de controle.
- VLAN Protegida - Transporta pacotes de dados. Cada instância ERPS tem sua própria VLAN protegida.

Rapid Ring Protection Protocol (RRPP)

O Rapid Ring Protection Protocol (RRPP) é um protocolo de camada de link projetado para anéis Ethernet. O RRPP pode evitar tempestades de broadcast causadas por loops de dados quando um anel Ethernet está saudável. O RRPP também pode restaurar rapidamente os caminhos de comunicação entre os nós quando um link é desconectado no anel.

Comparado com o protocolo de árvore de abrangência, o tempo de convergência do RRPP é rápido e independente do número de nós no anel Ethernet. O RRPP é aplicável a redes de grande diâmetro.

Domínio RRPP

Um domínio RRPP é identificado de forma exclusiva por um ID de domínio. Os dispositivos interconectados com o mesmo ID de domínio e VLANs de controle constituem um domínio RRPP. Um domínio RRPP contém os seguintes elementos:

- Anel principal e subanel.
- VLAN de controle.
- Nó mestre, nó de trânsito, nó de borda e nó de borda assistente.
- Porta principal, porta secundária, porta comum e porta de borda.

Aneis RRPP

Uma topologia em forma de anel Ethernet é chamada de anel RRPP. Os anéis RRPP incluem anéis principais e subanéis. Um domínio RRPP contém um ou vários anéis RRPP, sendo um deles o anel principal e os outros servindo como subanéis.

VLAN de Controle e VLAN Protegida

VLAN de Controle

Em um domínio RRPP, uma VLAN de controle é dedicada à transferência de pacotes RRPPDU. Em um dispositivo, as portas de acesso a um anel RRPP pertencem às VLANs de controle do anel e somente essas portas podem participar das VLANs de controle.

Um domínio RRPP é configurado com as seguintes VLANs de controle:

- Uma VLAN de controle principal, que é a VLAN de controle para o anel principal.
- Uma VLAN de controle secundária, que é a VLAN de controle para subanéis.

Após especificar uma VLAN como VLAN de controle principal, o sistema configura automaticamente a VLAN de controle secundária. O ID da VLAN é o ID da VLAN de controle principal mais um. Todos os subanéis no mesmo domínio RRPP compartilham a mesma VLAN de controle secundária. A configuração de endereço IP é proibida nas interfaces de VLAN de controle.

VLAN Protegida

Uma VLAN protegida é dedicada à transferência de pacotes de dados. Tanto portas RRPP quanto portas não-RRPP podem ser atribuídas a uma VLAN protegida.

Função dos Nós

Cada dispositivo em um anel RRPP é um nó. A função de um nó é configurável e o RRPP tem as seguintes funções de nó:

- Nó mestre - Cada anel tem apenas um nó mestre. O nó mestre inicia o mecanismo de pesquisa e determina as operações a serem realizadas após uma mudança de topologia.
- Nó de trânsito - No anel principal, os nós de trânsito se referem a todos os nós, exceto o nó mestre. No subanel, os nós de trânsito se referem a todos os nós, exceto o nó mestre e os nós onde o anel principal se interconecta com o subanel. Um nó de trânsito monitora o estado de suas conexões diretas do RRPP e notifica o nó mestre das mudanças de estado da conexão, se houver. Com base nas mudanças de estado da conexão, o nód mestre determina as operações a serem realizadas.
- Nó de borda - Um nó especial que reside tanto no anel principal quanto em um subanel ao mesmo tempo. Um nó de borda age como nó mestre ou nó de trânsito no anel principal e como nó de borda no subanel.
- Nó de borda assistente - Um nó especial que reside tanto no anel principal quanto em um subanel ao mesmo tempo. Um nó de borda assistente age como nó mestre ou nó de trânsito no anel principal e como nó de borda assistente no subanel. Esse nó trabalha em conjunto com o nó de borda para detectar a integridade do anel principal e executar a proteção contra loops.

Função das Portas

Porta Principal e Porta Secundária

Cada nó mestre ou nó de trânsito possui duas portas conectadas a um anel RRPP, uma porta principal e uma porta secundária. Você pode determinar a função de uma porta.

Em termos de funcionalidade, a porta principal e a porta secundária de um nó mestre têm as seguintes diferenças:

- A porta principal e a porta secundária são projetadas para desempenhar o papel de envio e recebimento de pacotes Hello, respectivamente.
- Quando um anel RRPP está no estado de Saúde, a porta secundária nega logicamente as VLANs protegidas e permite apenas os pacotes das VLANs de controle.
- Quando um anel RRPP está no estado de Desconexão, a porta secundária encaminha os pacotes das VLANs protegidas.

Em termos de funcionalidade, a porta principal e a porta secundária de um nó de trânsito são iguais. Ambas são projetadas para transferir pacotes de protocolo e pacotes de dados por meio de um anel RRPP.

Porta Comum e Porta de Borda

As portas que conectam o nó de borda e o nó de borda assistente ao anel principal são portas comuns. As portas que conectam o nó de borda e o nó de borda assistente apenas aos subanéis são portas de borda. Você pode determinar a função de uma porta.

VRRP (Virtual Router Redundancy Protocol)

O VRRP adiciona um grupo de gateways de rede a um grupo VRRP chamado de roteador virtual. Um grupo VRRP contém um mestre e vários backups. Quando o mestre em um grupo VRRP em uma LAN multicast ou broadcast (por exemplo, uma rede Ethernet) falha, outro roteador no grupo VRRP assume o controle. A troca é concluída sem causar recálculo de rotas dinâmicas, redescoberta de rotas, reconfiguração de gateway nos hosts ou interrupção do tráfego. O VRRP evita pontos únicos de falha.

Restrições e Diretrizes

Ao configurar um grupo VRRP, siga estas restrições e diretrizes:

- O IPv4 VRRPv3 e o IPv6 VRRPv3 não suportam autenticação de pacotes VRRP. O modo de autenticação especificado ao adicionar o grupo VRRP não tem efeito. Por padrão, o dispositivo suporta o VRRPv3.
- Você pode configurar diferentes modos de autenticação e chaves de autenticação para grupos VRRP em uma interface. No entanto, os membros do mesmo grupo VRRP devem usar o mesmo modo de autenticação e chave de autenticação.

Endereço IP Virtual de um Grupo VRRP

O endereço IP virtual do roteador virtual pode ser um dos seguintes tipos de endereços IP:

- Endereço IP não utilizado na sub-rede onde o grupo VRRP reside.
- Endereço IP de uma interface em um roteador no grupo VRRP. Nesse caso, o roteador é chamado de proprietário do endereço IP. Um grupo VRRP pode ter apenas um proprietário de endereço IP.

Prioridade do Roteador em um Grupo VRRP

O VRRP determina a função (mestre ou backup) de cada roteador em um grupo VRRP com base na prioridade. Um roteador com prioridade mais alta tem mais chances de se tornar o mestre.

As prioridades do VRRP variam de 0 a 255, e um número maior representa uma prioridade mais alta. As prioridades de 1 a 254 são configuráveis. A prioridade 0 é reservada para usos especiais, e a prioridade 255 é para o proprietário do endereço IP. O proprietário do endereço IP em um grupo VRRP sempre tem uma prioridade em execução de 255 e age como mestre enquanto estiver operando corretamente.

Preempção (Preempção)

Um roteador em um grupo VRRP opera no modo não preemptivo ou preemptivo.

- Modo não preemptivo - O roteador mestre age como mestre enquanto estiver operando corretamente, mesmo se um roteador de backup receber posteriormente uma prioridade mais alta. O modo não preemptivo ajuda a evitar trocas frequentes entre os roteadores mestre e de backup.
- Modo preemptivo - Um backup inicia uma nova eleição de mestre e assume o controle como mestre quando detecta que tem uma prioridade mais alta que o mestre atual. O modo preemptivo garante que o roteador com a maior prioridade em um grupo VRRP sempre atue como mestre.

  Você pode configurar o temporizador de atraso de preempção do VRRP para os seguintes fins:

- Avoid trocas frequentes de estado entre membros em um grupo VRRP.
- Fornecer aos backups tempo suficiente para coletar informações (como informações de roteamento).

No modo preemptivo, um backup não se torna imediatamente o mestre após receber um anúncio com prioridade inferior à prioridade local. Em vez disso, ele aguarda por um período de tempo (tempo de atraso de preempção + tempo de inclinação) antes de assumir como mestre.

Método de Autenticação

Para evitar ataques de usuários não autorizados, os roteadores membros do VRRP adicionam chaves de autenticação em pacotes VRRP para autenticar uns aos outros. O VRRP fornece os seguintes métodos de autenticação:

- Autenticação simples: O remetente preenche uma chave de autenticação no pacote VRRP, e o receptor compara a chave de autenticação recebida com sua chave de autenticação local. Se as duas chaves de autenticação coincidirem, o pacote VRRP recebido é legítimo. Caso contrário, o pacote recebido é ilegítimo e é descartado.
- Autenticação MD5: O remetente calcula um resumo para o pacote VRRP usando a chave de autenticação e o algoritmo MD5, e salva o resultado no pacote. O receptor realiza a mesma operação com a chave de autenticação e o algoritmo MD5 e compara o resultado com o conteúdo no cabeçalho de autenticação. Se os resultados coincidirem, o pacote VRRP recebido é legítimo. Caso contrário, o pacote recebido é ilegítimo e é descartado.
- Em uma rede segura, você pode optar por não autenticar pacotes VRRP.

Intervalo de Anúncio VRRP

O mestre em um grupo VRRP envia periodicamente anúncios VRRP para declarar sua presença. Você pode configurar o intervalo em que o mestre envia os anúncios VRRP.

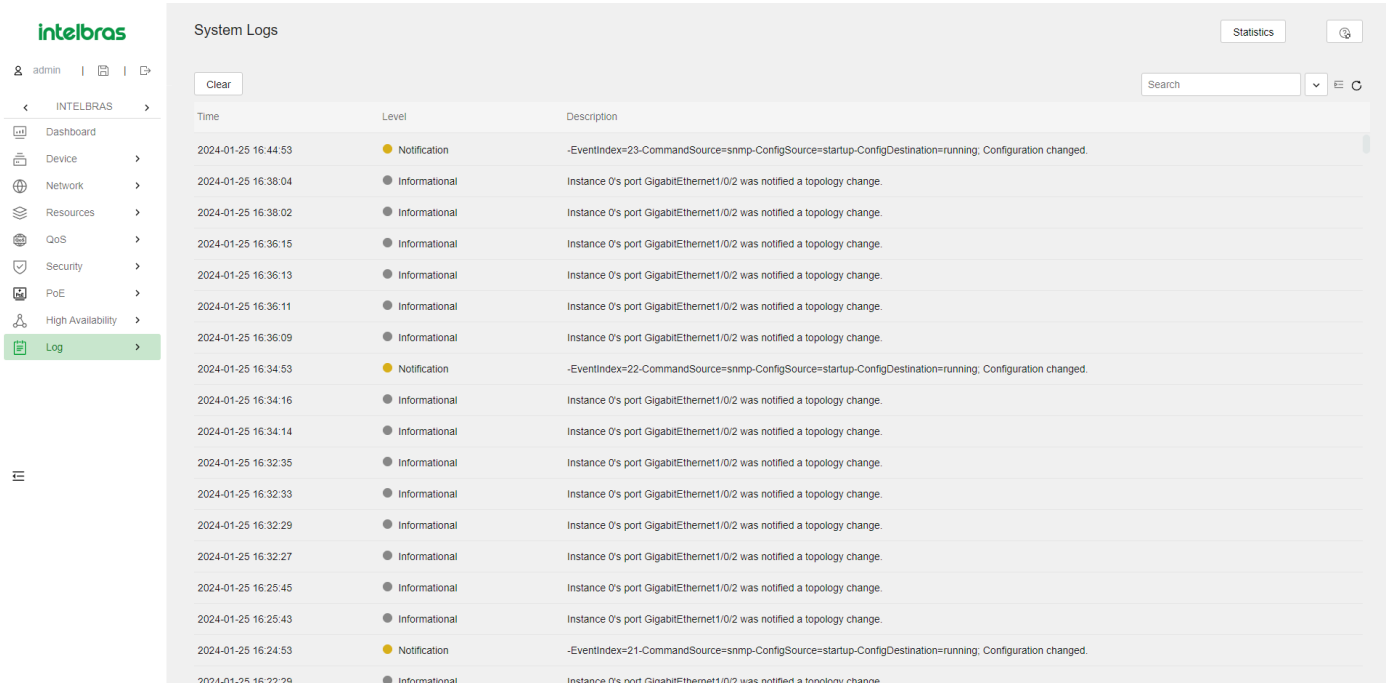
A Intelbras recomenda que você defina o intervalo de anúncio VRRP para ser maior que 100 centésimos de segundo para manter a estabilidade do sistema.

No VRRPv2, todos os roteadores em um grupo VRRP IPv4 devem ter o mesmo intervalo para enviar anúncios VRRP.

No VRRPv3, os roteadores em um grupo VRRP IPv4 podem ter intervalos diferentes para enviar anúncios VRRP. O mestre no grupo VRRP envia anúncios VRRP no intervalo especificado e carrega o atributo de intervalo nos anúncios. Após um backup receber o anúncio, ele registra o intervalo no anúncio. Se o backup não receber nenhum anúncio VRRP quando o temporizador (3 * intervalo registrado + tempo de inclinação) expirar, ele considera o mestre como falho e assume o controle.

Se existir um grande tráfego de rede, um backup pode falhar em receber anúncios VRRP do mestre dentro do tempo especificado. Como resultado, ocorre uma troca inesperada de mestre. Para resolver esse problema, você pode configurar um intervalo maior.

Recursos de Registro



Níveis de Registro

Os registros são classificados em oito níveis de gravidade de 0 a 7 em ordem decrescente.

Valor de Gravidade	Nível	Descrição
0	Emergência	O sistema está inutilizável. Por exemplo, a autorização do sistema expirou.
1	Alerta	Ação deve ser tomada imediatamente. Por exemplo, o tráfego em uma interface excede o limite superior.
2	Crítico	Condição crítica. Por exemplo, a temperatura do dispositivo excede o limite superior, o módulo de energia falha ou a bandeja do ventilador falha.
3	Erro	Condição de erro. Por exemplo, o estado da conexão muda ou um cartão de armazenamento é desconectado.
4	Aviso	Condição de aviso. Por exemplo, uma interface está desconectada ou os recursos de memória estão esgotados.

5	Notificação	Condição normal, mas significativa. Por exemplo, um terminal faz login no dispositivo ou o dispositivo é reiniciado.
6	Informativo	Mensagem informativa. Por exemplo, um comando ou uma operação de ping é executado.
7	Depuração	Mensagem de depuração.

Destinos de Registro

O sistema envia registros para destinos, como o buffer de registros e o host de registros. Os destinos de saída de registros são independentes e podem ser configurados na interface web.

Exemplos de Configuração

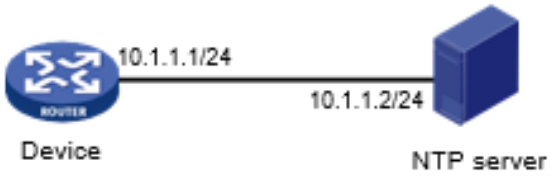
Exemplos de manutenção do dispositivo Exemplo de configuração de horário do sistema

Requisitos de Rede

Conforme mostrado na Figura 11:

Configure o dispositivo para obter o horário UTC a partir do servidor NTP.

Configure a autenticação NTP tanto no dispositivo quanto no servidor NTP.



Procedimento de Configuração

Configurar o cliente NTP:

No painel de navegação, selecione **Dispositivo** > **Manutenção** > **Configurações**. Clique no link **Data e Hora**.

Na página de configurações de data e hora, execute as seguintes tarefas:

Selecione autenticação do servidor NTP.

Insira o ID da chave de autenticação, o método de autenticação e o valor da chave.

Insira o endereço IP do servidor NTP, selecione o modo de servidor unicast e insira o ID da chave de autenticação.

Configurar o servidor NTP:

No servidor NTP, ative o serviço NTP e configure a autenticação NTP no servidor NTP. Para obter mais informações sobre o procedimento de configuração, consulte a documentação do servidor NTP. (Detalhes não mostrados.)

Verificação da Configuração

Verifique se o relógio do sistema está em estado sincronizado e se o dispositivo está sincronizado com o servidor NTP.

Exemplo de Configuração para Administradores

Requisitos de Rede

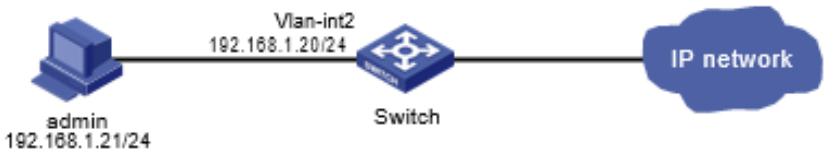
Conforme mostrado na Figura 12, configure uma conta de administrador para atender aos seguintes requisitos:

Permita que o usuário use a conta para fazer login no switch através de HTTP.

Realize autenticação local para o usuário que usa a conta de administrador para fazer login no switch.

Atribua a função de usuário network-admin ao usuário autenticado.

Figura 12 Diagrama de Rede



Procedimento de Configuração

Configure a VLAN e a interface de VLAN:

A partir da Menu de navegação, selecione **Rede** > **Links** > **VLAN**.

Crie a VLAN **2**.

Acesse a página de detalhes da VLAN 2 para realizar as seguintes tarefas:

Adicione a interface que se conecta ao PC do administrador à lista de portas marcadas.

Crie a VLAN-interface **2**.

Atribua o endereço IP **192.168.1.20/24** à VLAN-interface 2.

Configure uma conta de administrador:

A partir da Menu de navegação, selecione **Dispositivo** > **Maintenance** > **Administradores**.

Crie uma conta de administrador:

Defina o nome de usuário e a senha.

Selecione a função de usuário network-admin.

Selecione HTTP como o tipo de acesso permitido.

Ative os serviços HTTP e HTTPS:

A partir da Menu de navegação, selecione **Network** > **Service** > **HTTP/HTTPS**.

Ative o serviço HTTP.

Ative o serviço HTTPS.

Verificação da Configuração

Verifique que a conta de administrador foi adicionada com sucesso.

Insira **http://192.168.1.20 (http://192.168.1.20)** na barra de endereços para verificar os seguintes itens:

Você pode usar a conta de administrador para fazer login na interface da Web.

Após o login, você pode configurar o dispositivo.

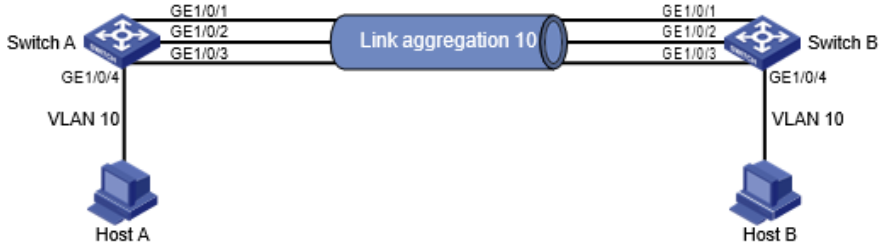
Exemplos de Configuração de Serviços de Rede

Exemplo de Configuração de Agregação de Link Ethernet

Requisitos de Rede

Conforme mostrado na Figura 14, configure a agregação estática de links de camada 2 no Switch A e Switch B para melhorar a confiabilidade da conexão.

Figura 14 Diagrama de Rede



Procedimento de Configuração

1. Configure a agregação de link Ethernet no Switch A:

a. A partir da Menu de navegação, selecione **Rede** > **Interfaces** > **Agregação de Link**.

b. Configure um grupo de agregação de camada 2 no Switch A da seguinte forma:

- Configure o modo de agregação como estático.
- Atribua portas ao grupo de agregação.

2. Configure a VLAN no Switch A:

a. A partir da Menu de navegação, selecione **Rede** > **Links** > **VLAN**.

b. Crie a VLAN 10.

c. Acesse a página de detalhes da VLAN 10 para realizar as seguintes tarefas:

- Adicione a porta que se conecta ao Host A à lista de portas sem marcação.
- Adicione as portas GigabitEthernet 1/0/1 a GigabitEthernet 1/0/3 à lista de portas marcadas.
- Configure o Switch B da mesma forma que o Switch A está configurado. (Detalhes não mostrados.)

Verificando a Configuração

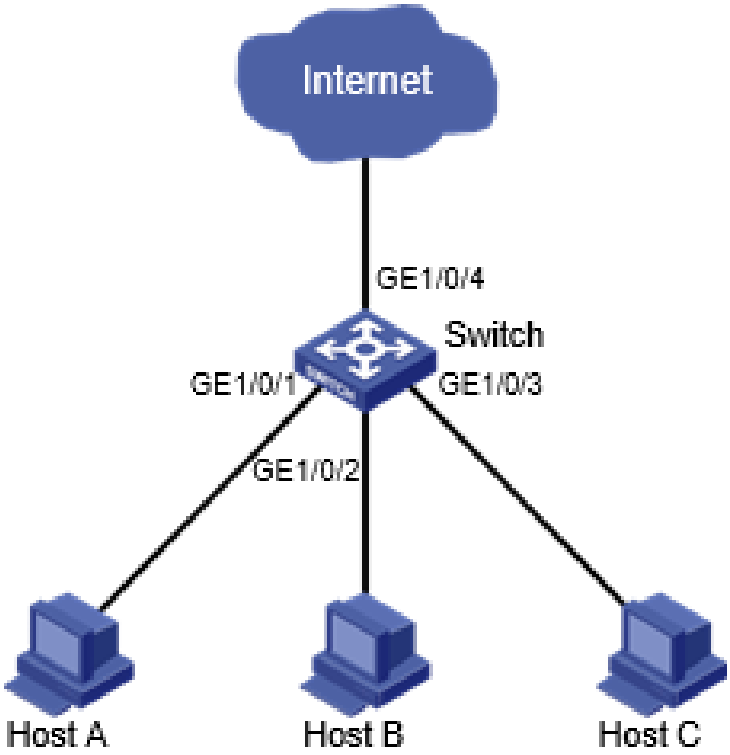
1. Acesse a página de agregação de links e verifique se as portas GigabitEthernet 1/0/1 a GigabitEthernet 1/0/3 foram atribuídas ao grupo de agregação de links.
2. Verifique se o Host A consegue fazer ping no Host B.
3. Verifique se o Host A ainda consegue fazer ping no Host B após uma falha na ligação entre o Switch A e o Switch B.

Exemplo de Configuração de Isolamento de Porta

Requisitos de Rede

Conforme mostrado na Figura 15, configure o switch para fornecer acesso à Internet para todos os hosts e isolá-los uns dos outros.

Figura 15 Diagrama de Rede



Host A Host B Host C

Procedimento de Configuração

1. A partir da Menu de navegação, selecione **Rede** > **Interfaces** > **Isolamento de Porta**.
2. Crie um grupo de isolamento.
3. Acesse a página de detalhes do grupo de isolamento.
4. Atribua as portas GigabitEthernet 1/0/1 a GigabitEthernet 1/0/3 ao grupo de isolamento.

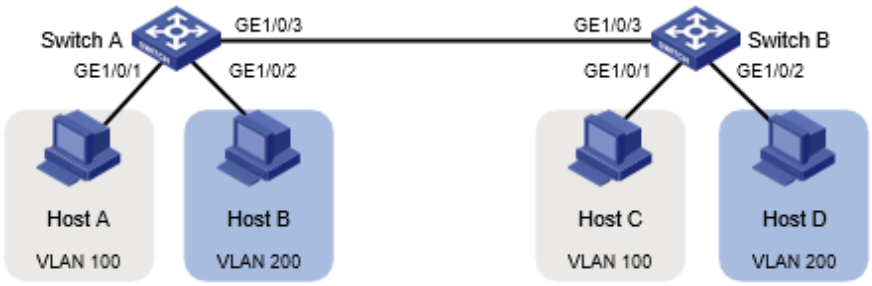
Verificando a Configuração

Verifique se Host A, Host B e Host C não conseguem fazer ping uns aos outros.

Exemplo de Configuração de VLAN

Requisitos de Rede

Conforme mostrado na Figura 16:



- Host A e Host C pertencem ao Departamento A. A VLAN 100 é atribuída ao Departamento A.
- Host B e Host D pertencem ao Departamento B. A VLAN 200 é atribuída ao Departamento B.
- No Switch A e Switch B, o tipo de link da GigabitEthernet 1/0/1 é acesso, o tipo de link da GigabitEthernet 1/0/2 é híbrido, e o tipo de link da GigabitEthernet 1/0/3 é trunk.

Configure VLANs para que apenas os hosts no mesmo departamento possam se comunicar entre si.

Figura 16 Diagrama de Rede

Procedimento de Configuração

1. Configure o Switch A:

   # Configure as configurações de tipo de link para as portas:

1. A partir da Menu de navegação, selecione **Rede** > **Interfaces** > **Interfaces**.
2. Acesse a página de detalhes da GigabitEthernet 1/0/1 e defina o tipo de link da porta como acesso na área de VLAN.
3. Acesse a página de detalhes da GigabitEthernet 1/0/2 e defina o tipo de link da porta como híbrido e defina o PVID como 200 na área de VLAN.
4. Acesse a página de detalhes da GigabitEthernet 1/0/3 e defina o tipo de link da porta como trunk na área de VLAN.

   # Configure as configurações de VLAN para as portas:

1. A partir da Menu de navegação, selecione **Rede** > **Links** > **VLAN**.
2. Crie a VLAN 100 e a VLAN 200 no Switch A.
3. Acesse a página de detalhes da VLAN 100 para realizar as seguintes tarefas:

   Adicione a GigabitEthernet 1/0/1 à lista de portas sem marcação (Host A não pode reconhecer tags VLAN).

   Adicione a GigabitEthernet 1/0/3 à lista de portas marcadas (Switch B precisa identificar as tags VLAN dos pacotes).

- Acesse a página de detalhes da VLAN 200 para realizar as seguintes tarefas:

  Adicione a GigabitEthernet 1/0/2 à lista de portas sem marcação (Host B não pode reconhecer tags VLAN).

  Adicione a GigabitEthernet 1/0/3 à lista de portas marcadas (Switch B precisa identificar as tags VLAN dos pacotes).

- Configure o Switch B da mesma forma que o Switch A está configurado. (Detalhes não mostrados.)

Verificando a Configuração

1. Verifique se Host A e Host C conseguem fazer ping um no outro, mas nenhum deles pode fazer ping em Host B ou Host D.
2. Verifique se Host B e Host D podem fazer ping um no outro, mas nenhum deles pode fazer ping em Host A ou Host C.

Exemplo de Configuração de Voice VLAN

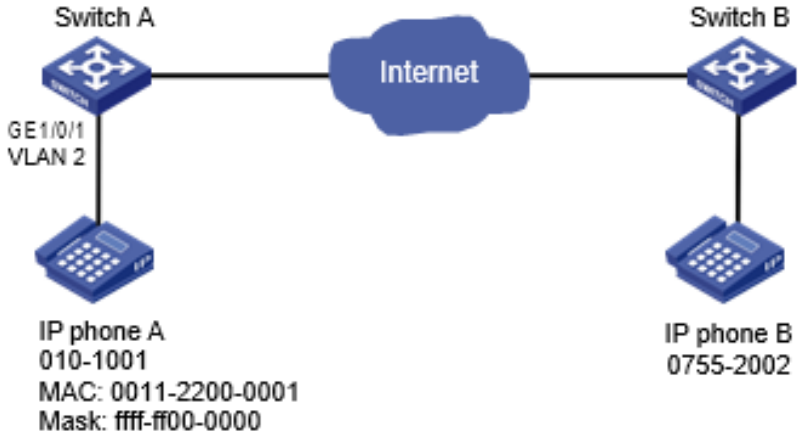
Requisitos de Rede

Conforme mostrado na Figura 17, o telefone IP A envia e reconhece apenas pacotes de voz não marcados.

Para permitir que a GigabitEthernet 1/0/1 transmita apenas pacotes de voz, execute as seguintes tarefas no Switch A:

- Crie a VLAN 2. Esta VLAN será usada como uma Voice Vlan.
- Adicione a GigabitEthernet 1/0/1 à VLAN 2.
- Adicione o endereço OUI do telefone IP A à lista OUI do Switch A.

Figura 17 Diagrama de Rede



Procedimento de Configuração

1. A partir da Menu de navegação, selecione **Rede** > **Interfaces**.
2. Defina o PVID da GigabitEthernet 1/0/1 como 2.
3. A partir da Menu de navegação, selecione **Rede** > **Links** > **VLAN**.
1. Crie a VLAN 2.
2. Acesse a página de detalhes da VLAN 2 e adicione a GigabitEthernet 1/0/1 à lista de portas não marcadas.
4. A partir da Menu de navegação, selecione **Rede** > **Links** > **Voice Vlan**.
1. Acesse a página para selecionar portas, atribua a GigabitEthernet 1/0/1 à VLAN 2 e defina o modo da porta como manual.
2. Acesse a página de configurações avançadas e defina o modo como segurança.
3. Acesse a página para adicionar um endereço OUI e adicione o endereço OUI 0011-2200-0000, a máscara ffff-ff00-0000 e a descrição Endereço OUI do telefone IP A.

Verificando a Configuração

1. Veja o resumo de OUI para verificar se o endereço OUI 0011-2200-0000 foi adicionado.
2. Veja o resumo da porta para verificar se a GigabitEthernet 1/0/1 foi atribuída à Voice Vlan 2.

Exemplo de Configuração de Entrada de Endereço MAC

Requisitos de Rede

Conforme mostrado na Figura 18:

- Host A com endereço MAC 000f-e235-dc71 está conectado à GigabitEthernet 1/0/1 do switch e pertence à VLAN 1.
- Host B com endereço MAC 000f-e235-abcd, que se comportou de forma suspeita na rede, também pertence à VLAN 1.
- Configure a tabela de endereços MAC no switch da seguinte forma:

Para evitar a falsificação de endereços MAC, adicione uma entrada estática para Host A.

Para descartar todos os quadros destinados a Host B, adicione uma entrada de endereço MAC blackhole para Host B.

Defina o temporizador de envelhecimento como 500 segundos para entradas de endereços MAC dinâmicos.

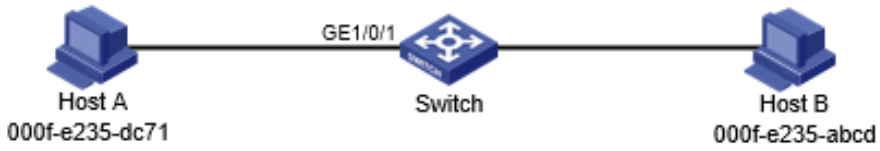


Figura 18 Diagrama de Rede

Procedimento de Configuração

1. A partir da Menu de navegação, selecione **Rede** > **Links** > **MAC**.
1. Adicione uma entrada de endereço MAC estático para o endereço MAC 000f-e235-dc71. A interface de saída é GigabitEthernet 1/0/1 e a VLAN é 1.
2. Adicione uma entrada de endereço MAC blackhole para o endereço MAC 000f-e235-abcd. A VLAN é 1.
3. Acesse a página de configurações avançadas de MAC e defina o temporizador de envelhecimento de MAC como 500 segundos.

Verificando a Configuração

1. Verifique se as entradas de endereços MAC criadas existem na tabela de endereços MAC e se o Host B não pode fazer ping em Host A.

Exemplo de Configuração MSTP

Requisitos de Rede

Conforme mostrado na Figura 19, todos os dispositivos na rede estão na mesma região MST. O Switch A e o Switch B funcionam na camada de agregação. O Switch C e o Switch D funcionam na camada de acesso.

Configure o MSTP para que os pacotes de VLANs diferentes sejam encaminhados ao longo de diferentes árvores de abrangência.

Pacotes da VLAN 10 são encaminhados ao longo de MSTI 1.

Pacotes da VLAN 30 são encaminhados ao longo de MSTI 2.

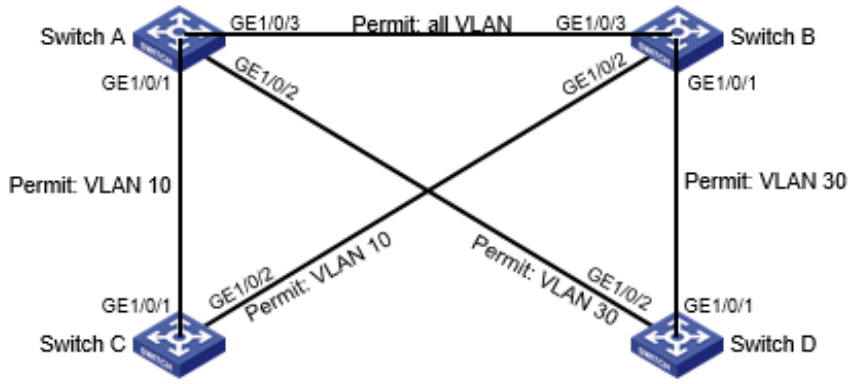


Figura 19 Diagrama de Rede

Procedimento de Configuração

1. Configure VLANs:

a. Configure VLANs no Switch A:

1. A partir da Menu de navegação, selecione **Rede** > **Links** > **VLAN**.
2. Crie VLAN 10 e VLAN 30.
3. Acesse a página de detalhes da VLAN 10. Adicione as portas GigabitEthernet 1/0/1 e GigabitEthernet 1/0/3 à lista de portas marcadas.
4. Acesse a página de detalhes da VLAN 30. Adicione as portas GigabitEthernet 1/0/2 e GigabitEthernet 1/0/3 à lista de portas marcadas.

b. Configure VLANs no Switch B:

1. A partir da Menu de navegação, selecione **Rede** > **Links** > **VLAN**.
2. Crie VLAN 10 e VLAN 30.
3. Acesse a página de detalhes da VLAN 10. Adicione as portas GigabitEthernet 1/0/2 e GigabitEthernet 1/0/3 à lista de portas marcadas.
4. Acesse a página de detalhes da VLAN 30. Adicione as portas GigabitEthernet 1/0/1 e GigabitEthernet 1/0/3 à lista de portas marcadas.

c. Configure VLANs no Switch C:

1. A partir da Menu de navegação, selecione **Rede** > **Links** > **VLAN**.
2. Crie VLAN 10.
3. Acesse a página de detalhes da VLAN 10. Adicione as portas GigabitEthernet 1/0/1 e GigabitEthernet 1/0/2 à lista de portas marcadas.

d. Configure VLANs no Switch D:

1. A partir da Menu de navegação, selecione **Rede** > **Links** > **VLAN**.
2. Crie VLAN 30.
3. Acesse a página de detalhes da VLAN 30. Adicione as portas GigabitEthernet 1/0/1 e GigabitEthernet 1/0/2 à lista de portas marcadas.

2. Configure o MSTP no Switch A através do Switch D:

a. A partir da Menu de navegação, selecione **Rede** > **Links** > **STP**.

b. Habilite o STP e configure o modo de operação como MSTP.

c. Acesse a página de configuração da região MST para realizar as seguintes tarefas:

1. Configure o nome da região MST como Web.
2. Mapeie a VLAN 10 e a VLAN 30 para MSTI 1 e MSTI 2, respectivamente.
3. Defina o nível de revisão do MSTP como 0.

Verificando a Configuração

Verifique se os papéis das portas e os estados das portas no status da árvore de abrangência estão conforme o esperado.

Procedimento de Configuração

1. Configure o Dispositivo A (servidor NTP):

   Em Rede > Serviço > NTP:

a. Habilite o serviço NTP.

a. Especifique o endereço IP do relógio local como 127.127.1.0.

a. Configure o nível de estrato do relógio local como 2.

- Configure o Dispositivo B:

Em Dispositivo > Manutenção > Configurações:

a. Acesse a página de data e hora para selecionar a sincronização automática com uma fonte de tempo confiável e, em seguida, selecione o NTP como o protocolo de tempo.

a. Especifique o endereço IP do Dispositivo A como 1.0.1.11 e configure o Dispositivo B para operar no modo servidor.

Verificando a Configuração

Verifique se o Dispositivo B sincronizou com o Dispositivo A e se o nível de estrato do relógio é 3 no Dispositivo B e 2 no Dispositivo A.

Exemplo de Configuração do SNMP

Requisitos de Rede

Conforme mostrado na Figura 38, o NMS (1.1.1.2/24) usa SNMPv2c para gerenciar o agente SNMP (1.1.1.1/24), e o agente envia automaticamente notificações para relatar eventos ao NMS.

Figura 38 Diagrama de Rede

Procedimento de Configuração

1. Configure o dispositivo:

   Em Rede > Serviço > SNMP:

a. Clique em Habilitar SNMP para ativar o serviço SNMP.

a. Especifique SNMPv2c.

a. Crie uma comunidade de leitura e escrita chamada "readandwrite", que pode acessar todos os nós na visualização MIB padrão. Configure uma ACL básica IPv4 para permitir apenas que o NMS SNMPv2c em 1.1.1.2/24 use o nome da comunidade "readandwrite" para acessar o dispositivo.

a. Habilite armadilhas e defina o host de destino como 1.1.1.2, com a string de segurança "readandwrite" e o modelo de segurança v2c.

- Configure o NMS SNMP:

Especifique SNMPv2c.

a. Crie a comunidade de leitura e escrita "readandwrite".

- Para obter informações sobre a configuração do NMS, consulte o manual do NMS.

Verificando a Configuração

Verifique se o NMS pode obter o valor do nó sysName e se pode receber notificações de linkDown quando uma interface no dispositivo é desativada.

Exemplo de Configuração de QoS

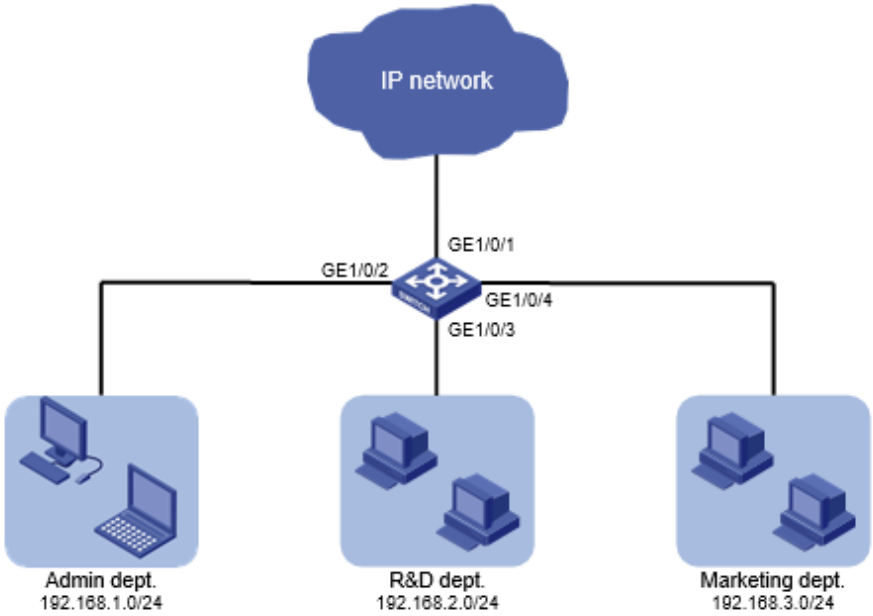
Requisitos de Rede

Conforme mostrado na Figura 39, configure o QoS para atender aos seguintes requisitos:

O tráfego do departamento de administração, departamento de P&D e departamento de marketing é agendado na proporção de 2:1:1.

A taxa de tráfego para acessar a Internet é limitada a 15 Mbps.

Figura 39 Diagrama de Rede



Procedimento de Configuração

1. Configure políticas de QoS:

   Em QoS > QoS > Política de QoS:

a. Aplique uma política de QoS ao tráfego de entrada de GigabitEthernet 1/0/2.

a. Acesse a página de detalhes da política de QoS para modificar a política de QoS aplicada da seguinte forma:

a. Crie uma ACL IPv4 2000 e adicione uma regra para permitir pacotes com endereço IP de origem 192.168.1.0 e máscara 0.0.0.255.

a. Configure a ACL como critério de correspondência de uma classe e especifique o comportamento associado para marcar os pacotes correspondentes com prioridade 802.1p 0.

a. Aplique uma política de QoS ao tráfego de entrada de GigabitEthernet 1/0/3.

a. Acesse a página de detalhes da política de QoS para modificar a política de QoS aplicada da seguinte forma:

a. Crie uma ACL IPv4 2002 e adicione uma regra para permitir pacotes com endereço IP de origem 192.168.2.0 e máscara 0.0.0.255.

a. Configure a ACL como critério de correspondência de uma classe e especifique o comportamento associado para marcar os pacotes correspondentes com prioridade 802.1p 1.

a. Aplique uma política de QoS ao tráfego de entrada de GigabitEthernet 1/0/4.

a. Acesse a página de detalhes da política de QoS para modificar a política de QoS aplicada da seguinte forma:

a. Crie uma ACL IPv4 2003 e adicione uma regra para permitir pacotes com endereço IP de origem 192.168.1.0 e máscara 0.0.0.255.

a. Configure a ACL como critério de correspondência de uma classe e especifique o comportamento associado para marcar os pacotes correspondentes com prioridade 802.1p 2.

- Configure mapeamento de prioridade:

Em QoS > QoS > Mapeamento de Prioridade:

a. Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3 e GigabitEthernet 1/0/4 para confiar na prioridade 802.1p.

a. Configure o mapa de prioridade 802.1p para mapear os valores de prioridade 802.1p 0, 1 e 2 para valores de precedência local 0, 1 e 2, respectivamente.

- Configure o escalonamento de hardware:

Em QoS > QoS > Escalonamento de Hardware:

a. Acesse a página de detalhes de GigabitEthernet 1/0/1 para realizar as seguintes tarefas:

a. Configure o algoritmo de escalonamento como WRR (contagem de bytes).

a. Modifique as contagens de bytes das filas 0, 1 e 2 para 2, 1 e 1, respectivamente.

- Configure o limite de taxa:

Em QoS > QoS > Limite de Taxa:

a. Defina o CIR para 15360 kbps para o tráfego de entrada de GigabitEthernet 1/0/1.

Verificando a Configuração

Verifique se o status de aplicação de QoS na página de política de QoS e a configuração de escalonamento na página de escalonamento de hardware estão conforme o esperado.

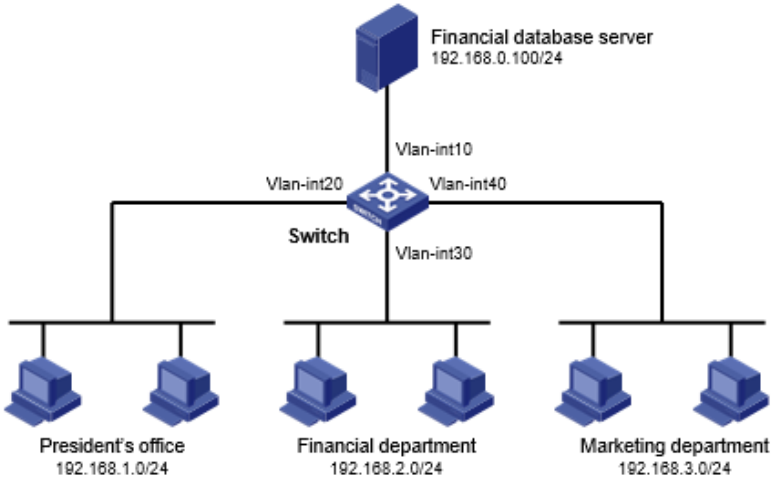
Exemplo de Configuração de Filtro de Pacotes baseado em ACL

Requisitos de Rede

Como mostrado na Figura 40, uma empresa interconecta seus departamentos por meio do switch. Configure o filtro de pacotes para atender aos seguintes requisitos:

- Permitir o acesso do escritório da Presidência a qualquer momento ao servidor de banco de dados financeiro.
- Permitir o acesso do departamento Financeiro ao servidor de banco de dados apenas durante o horário de trabalho (das 8:00 às 18:00) nos dias úteis.
- Negar o acesso de qualquer outro departamento ao servidor de banco de dados.

Diagrama de Rede



Procedimento de Configuração

1. Na Menu de navegação, selecione Segurança > Filtro de Pacotes > Filtro de Pacotes.
2. Crie uma política de filtro de pacotes:
   - Selecione a VLAN-interface 10.
   - Selecione a direção da aplicação de saída.
   - Selecione o tipo de ACL IPv4 para o filtro de pacotes.
3. Crie uma ACL IPv4 avançada e configure as seguintes regras na ordem em que são descritas:

Ação	Tipo de Protocolo	IP/Máscara curinga	Intervalo de Tempo
Permitir	256	Origem: 192.168.1.0/0.0.0.255 Destino: 192.168.0.100/0	N/A
Permitir	256	Origem: 192.168.2.0/0.0.0.255 Destino: 192.168.0.100/0	Criar um intervalo de tempo chamado trabalho: • Especificar o horário de início como 08:00. • Especificar o horário de término como 18:00. • Selecionar de segunda a sexta-feira.
Negar	256	Destino: 192.168.0.100/0	N/A

4. Ativar a Contagem de Correspondências para a ACL

Verificação da Configuração

1. Realize um ping no servidor de banco de dados a partir de diferentes departamentos para verificar os seguintes itens:
   - Você pode acessar o servidor a partir do escritório da Presidência a qualquer momento.
   - Você pode acessar o servidor a partir do departamento Financeiro durante o horário de trabalho.
   - Você não pode acessar o servidor a partir do departamento de Marketing a qualquer momento.
2. Acesse a interface da web das regras da ACL e verifique se as regras da ACL estão ativas.

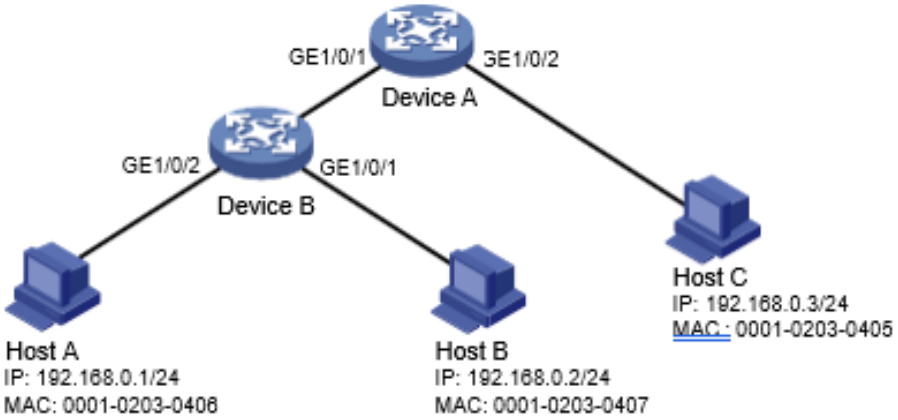
Configuração de Proteção de Origem IPv4 Estática

Requisitos de Rede

Como mostrado na Figura 41, todos os hosts usam endereços IP estáticos.

Configure as entradas de proteção de origem IPv4 estática nos dispositivos A e B para atender aos seguintes requisitos:

- A GigabitEthernet 1/0/2 do dispositivo A permite apenas pacotes IP do Host C.
- A GigabitEthernet 1/0/1 do dispositivo A permite apenas pacotes IP do Host A.
- A GigabitEthernet 1/0/2 do dispositivo B permite apenas pacotes IP do Host A.
- A GigabitEthernet 1/0/1 do dispositivo B permite apenas pacotes IP do Host B.



Procedimento de Configuração

1. Configure o dispositivo A:

   1. Configure os endereços IP para as interfaces. (Detalhes não mostrados.)
   2. No painel de navegação, selecione Segurança > Filtro de Pacotes > Proteção de Origem IP.
   3. Adicione uma entrada de proteção de origem IP para o Host A.

      A entrada contém a interface GigabitEthernet 1/0/1, o endereço IP 192.168.0.1 e o endereço MAC 00-01-02-03-04-06.
   4. Adicione uma entrada de proteção de origem IP para o Host C.

      A entrada contém a interface GigabitEthernet 1/0/2, o endereço IP 192.168.0.3 e o endereço MAC 00-01-02-03-04-05.

2. Configure o dispositivo B:

   1. Configure os endereços IP para as interfaces. (Detalhes não mostrados.)
   2. No painel de navegação, selecione Segurança > Filtro de Pacotes > Proteção de Origem IP.
   3. Adicione uma entrada de proteção de origem IP para o Host B.

      A entrada contém a interface GigabitEthernet 1/0/1, o endereço IP 192.168.0.2 e o endereço MAC 00-01-02-03-04-07.
   4. Adicione uma entrada de proteção de origem IP para o Host A.

      A entrada contém a interface GigabitEthernet 1/0/2, o endereço IP 192.168.0.1 e o endereço MAC 00-01-02-03-04-06.

Verificação da Configuração

1. No painel de navegação, selecione Segurança > Filtro de Pacotes > Proteção de Origem IP no dispositivo A.

2. Verifique se as entradas de proteção de origem IPv4 estática estão configuradas com sucesso na página de configuração de proteção de origem IP.

3. Repita o passo 1 e 2 no dispositivo B para verificar se as entradas de proteção de origem IPv4 estática estão configuradas com sucesso.

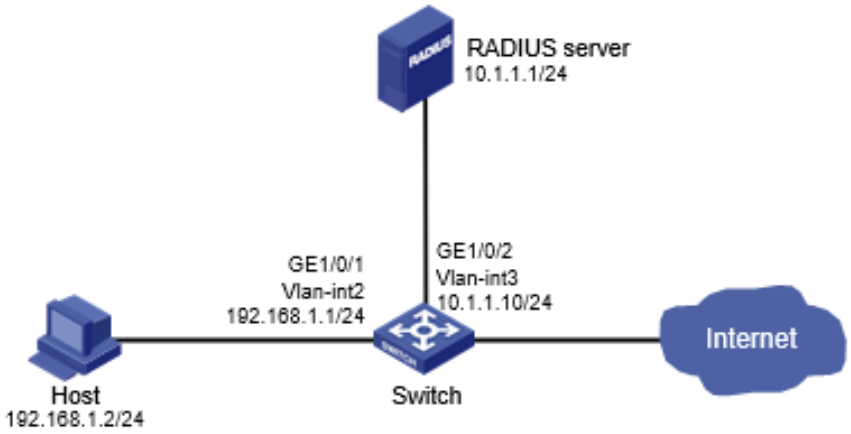
Configuração de Autenticação RADIUS 802.1X

Requisitos de Rede

Como mostrado na Figura 42, configure o switch para atender aos seguintes requisitos:

- Use o servidor RADIUS para realizar autenticação, autorização e contabilidade para os usuários 802.1X.
- Autentique todos os usuários 802.1X que acessam o switch através de GigabitEthernet 1/0/1 no domínio ISP dm1X.
- Use controle de acesso baseado em MAC na GigabitEthernet 1/0/1 para autenticar separadamente todos os usuários 802.1X na porta.
- Exclua nomes de domínio dos nomes de usuário enviados para o servidor RADIUS.

- Use "name" como as chaves de autenticação e contabilidade para comunicação segura entre o switch e o servidor RADIUS.
- Use as portas 1812 e 1813 para autenticação e contabilidade, respectivamente.



Procedimento de Configuração

1. Configure os endereços IP para as interfaces, conforme mostrado na Figura 42. (Detalhes não mostrados.)

2. Configure um esquema RADIUS no switch:

1. No painel de navegação, selecione Segurança > Autenticação > RADIUS.

2. Adicione o esquema RADIUS 802.1X.

3. Configure o servidor de autenticação primário:

- Defina o endereço IP como 10.1.1.1.
- Defina a porta de autenticação como 1812.
- Defina a chave compartilhada como "name".
- Defina o estado do servidor como Ativo.

4. Configure o servidor de contabilidade primário:

- Defina o endereço IP como 10.1.1.1.
- Defina a porta de contabilidade como 1813.
- Defina a chave compartilhada como "name".
- Defina o estado do servidor como Ativo.

5. Configure o switch para não incluir nomes de domínio nos nomes de usuário enviados para o servidor RADIUS.

3. Configure um domínio ISP no switch:

1. No painel de navegação, selecione Segurança > Autenticação > Domínios ISP.

2. Adicione o domínio ISP dm1X e defina o estado do domínio como Ativo.

3. Defina o serviço de acesso como acesso LAN.

4. Configure o domínio ISP para usar o esquema RADIUS 802.1X para autenticação, autorização e contabilidade de usuários LAN.

4. Configure o 802.1X no switch:

1. No painel de navegação, selecione Segurança > Controle de Acesso > 802.1X.

2. Habilite o 802.1X globalmente.

3. Habilite o 802.1X na GigabitEthernet 1/0/1 e defina o método de controle de acesso como baseado em MAC.

4. Na página de configurações avançadas para a GigabitEthernet 1/0/1, defina o estado de autorização de porta como Automático e defina o domínio ISP obrigatório como dm1X.

5. Configure o servidor RADIUS:

1. Adicione uma conta de usuário no servidor. (Detalhes não mostrados.)

2. Configure as configurações de autenticação, autorização e contabilidade. (Detalhes não mostrados.)

Verificação da Configuração

1. No painel de navegação, selecione Segurança > Autenticação > RADIUS.

2. Verifique a configuração do esquema RADIUS 802.1X.

3. No painel de navegação, selecione Segurança > Autenticação > Domínios ISP.

4. Verifique a configuração do domínio ISP dm1X.

5. Use a conta de usuário configurada para passar na autenticação.

6. No painel de navegação, selecione Segurança > Controle de Acesso > 802.1X.

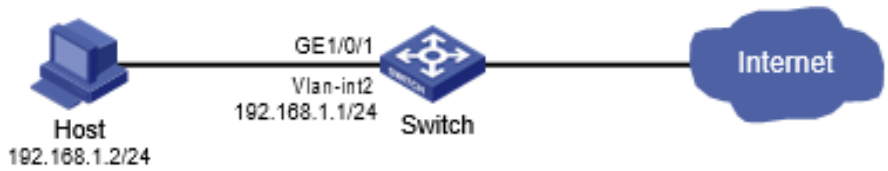
7. Verifique que o número de usuários online não é 0 na GigabitEthernet 1/0/1.

Exemplo de Configuração de Autenticação 802.1X Local

Requisitos de Rede

Como mostrado na Figura 43, adicione uma conta de usuário com nome de usuário "dotuser" e senha "12345" no switch. Configure o switch para atender aos seguintes requisitos:

- Realizar autenticação 802.1X local para controlar o acesso à rede dos usuários na GigabitEthernet 1/0/1.
- Autenticar os usuários no domínio ISP "abc".
- Especificar controle de acesso baseado em porta na GigabitEthernet 1/0/1. Após um usuário passar na autenticação na porta, todos os usuários subsequentes podem acessar a rede sem autenticação.



Procedimento de Configuração

1. 1. Configure os endereços IP para as interfaces, conforme mostrado na Figura 43. (Detalhes não mostrados.)

2. 2. Configure a conta de usuário local:

1. No painel de navegação, selecione Segurança > Autenticação > Usuários Locais.

2. Adicione a conta de usuário "dotuser" e defina a senha como "12345".

3. Defina o tipo de serviço como acesso LAN.

3. 3. Configure o domínio ISP:

1. No painel de navegação, selecione Segurança > Autenticação > Domínios ISP.

2. Adicione o domínio ISP "abc" e defina o estado como Ativo.

3. Defina o serviço de acesso como acesso LAN.

4. Configure o domínio ISP para usar o método local para autenticação e autorização de usuários LAN, e não realizar contabilidade para usuários LAN.
4. 4. Configure o 802.1X:

1. No painel de navegação, selecione Segurança > Controle de Acesso > 802.1X.
2. Habilite o 802.1X globalmente.
3. Habilite o 802.1X na GigabitEthernet 1/0/1 e defina o método de controle de acesso como baseado em porta.
4. Na página de configurações avançadas para GigabitEthernet 1/0/1, defina o estado de autorização da porta como Automático e defina o domínio ISP obrigatório como "abc".

Verificação da Configuração

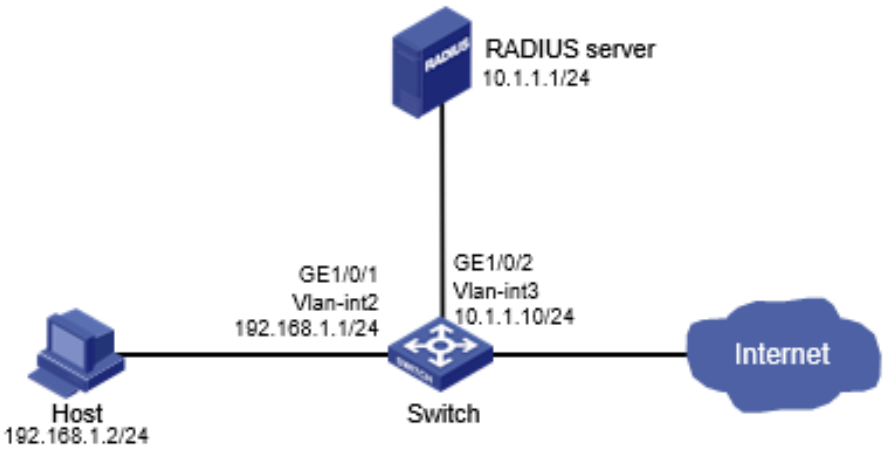
1. No painel de navegação, selecione Segurança > Autenticação > Usuários Locais.
2. Verifique a configuração do usuário local "dotuser".
3. No painel de navegação, selecione Segurança > Autenticação > Domínios ISP.
4. Verifique a configuração do domínio ISP "abc".
5. Use a conta de usuário "dotuser" e a senha "12345" para passar na autenticação.
6. No painel de navegação, selecione Segurança > Controle de Acesso > 802.1X.

Exemplo de Configuração de Autenticação MAC Baseada em RADIUS

Requisitos de Rede

Como mostrado na Figura 44, o switch usa autenticação MAC para controlar o acesso à Internet de usuários na GigabitEthernet 1/0/1. Configure o switch para atender aos seguintes requisitos:

- Use o servidor RADIUS para realizar autenticação, autorização e contabilidade para todos os usuários.
- Autentique todos os usuários no domínio ISP "macauth".
- Use uma conta com nome de usuário "aaa" e senha "qaz123wdc" para identificar todos os usuários.
- Exclua os nomes de domínio dos nomes de usuário enviados para o servidor RADIUS.
- Use "name" como as chaves compartilhadas de autenticação e contabilidade para comunicação segura RADIUS entre o switch e o servidor RADIUS.
- Use as portas 1812 e 1813 para autenticação e contabilidade, respectivamente.



Procedimento de Configuração

1. Configure os endereços IP para as interfaces, conforme mostrado na Figura 44. (Detalhes não mostrados.)

2. Configure um esquema RADIUS no switch:

1. No painel de navegação, selecione Segurança > Autenticação > RADIUS.

2. Adicione o esquema RADIUS "macauth".

3. Configure o servidor de autenticação primário:

- Defina o endereço IP como 10.1.1.1.
- Defina o número da porta de autenticação como 1812.
- Defina a chave compartilhada como "name".
- Defina o estado do servidor como Ativo.

4. Configure o servidor de contabilidade primário:

- Defina o endereço IP como 10.1.1.1.
- Defina o número da porta de contabilidade como 1813.
- Defina a chave compartilhada como "name".
- Defina o estado do servidor como Ativo.

5. Configure o switch para não incluir os nomes de domínio nos nomes de usuário enviados para o servidor RADIUS.

3. Configure um domínio ISP no switch:

1. No painel de navegação, selecione Segurança > Autenticação > Domínios ISP.

2. Adicione o domínio ISP "macauth" e defina o estado do domínio como Ativo.

3. Defina o serviço de acesso como acesso LAN.

4. Configure o domínio ISP para usar o esquema RADIUS "macauth" para autenticação, autorização e contabilidade de usuários LAN.

4. Configure a autenticação MAC no switch:

1. No painel de navegação, selecione Segurança > Controle de Acesso > Autenticação MAC.

2. Habilite a autenticação MAC globalmente.

3. Habilite a autenticação MAC na GigabitEthernet 1/0/1.

4. Na página de configurações avançadas, configure os seguintes parâmetros:

- Defina que todos os usuários usem o mesmo nome de usuário e senha.
- Configure o nome de usuário como "aaa" e a senha como "qaz123wdc".
- Especifique o domínio de autenticação como "macauth".

Verificação da Configuração

1. No painel de navegação, selecione Segurança > Autenticação > RADIUS.

2. Verifique a configuração do esquema RADIUS "macauth".

3. No painel de navegação, selecione Segurança > Autenticação > Domínios ISP.

4. Verifique a configuração do domínio ISP "macauth".

5. Use a conta de usuário "aaa" e a senha "qaz123wdc" para passar na autenticação MAC.

6. No painel de navegação, selecione Segurança > Controle de Acesso > Autenticação MAC.

7. Verifique que o número de usuários online não é 0 na GigabitEthernet 1/0/1.

Exemplo de Configuração de Segurança de Porta com Base em RADIUS

Requisitos de Rede

Conforme mostrado na Figura 45, a porta GigabitEthernet 1/0/1 opera no modo userLoginWithOUI para controlar o acesso à Internet dos usuários.

Configure o switch para atender aos seguintes requisitos:

- Use o servidor RADIUS para autenticação, autorização e contabilidade de usuários.
- Use "name" como as chaves compartilhadas de autenticação e contabilidade para comunicação RADIUS segura entre o switch e o servidor RADIUS.
- Use as portas 1812 e 1813 para autenticação e contabilidade, respectivamente.
- Autentique todos os usuários 802.1X no domínio ISP "portsec" e exclua os nomes de domínio dos nomes de usuário enviados ao servidor RADIUS.
- Permita que apenas um usuário 802.1X e um usuário cujo OUI corresponde a um dos seguintes OUIs se conectem na porta GigabitEthernet 1/0/1:
  - 1234-0100-1111
  - 1234-0200-1111
  - 1234-0300-1111
  - 1234-0400-1111
  - 1234-0500-1111

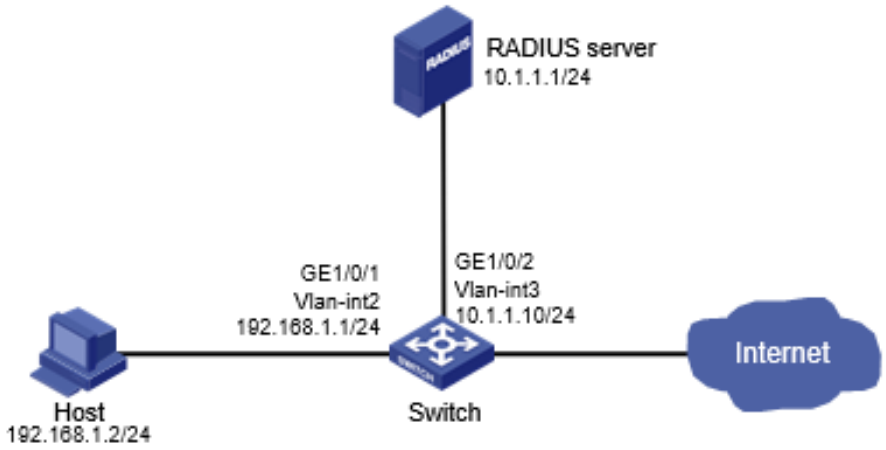


Figura 45 - Diagrama de Rede

Procedimento de Configuração

1. Configure os endereços de IP para as interfaces, conforme mostrado na Figura 45. (Detalhes não mostrados.)
2. Configure um esquema RADIUS no switch:

a. A partir da Menu de navegação, selecione Segurança > Autenticação > RADIUS.

b. Adicione o esquema RADIUS "portsec".

c. Configure o servidor de autenticação primário:

- Defina o endereço IP como 10.1.1.1.
- Defina a porta de autenticação como 1812.
- Defina a chave compartilhada como "name".
- Defina o estado do servidor como Ativo.

d. Configure o servidor de contabilidade primário:

- Defina o endereço IP como 10.1.1.1.
- Defina a porta de contabilidade como 1813.
- Defina a chave compartilhada como "name".
- Defina o estado do servidor como Ativo.

e. Configure o switch para não incluir nomes de domínio nos nomes de usuário enviados ao servidor RADIUS.

3. Configure um domínio ISP no switch:

a. A partir da Menu de navegação, selecione Segurança > Autenticação > Domínios ISP.

b. Adicione o domínio ISP "portsec" e defina o estado do domínio como Ativo.

c. Defina o serviço de acesso como acesso LAN.

d. Configure o domínio ISP para usar o esquema RADIUS "portsec" para autenticação, autorização e contabilidade de usuários LAN.

4. Configure a segurança da porta no switch:

a. A partir da Menu de navegação, selecione Segurança > Controle de Acesso > Segurança de Porta.

b. Habilite a segurança da porta.

c. Defina o modo de segurança da porta como "userLoginWithOUI" para GigabitEthernet 1/0/1.

d. Na guia 802.1X das configurações avançadas para GigabitEthernet 1/0/1, defina o domínio obrigatório 802.1X como "portsec".

e. Nas configurações avançadas de segurança de porta, adicione cinco valores de OUI à lista de OUI. Os valores de OUI incluem 1234-0100-1111, 1234-0200-1111, 1234-0300-1111, 1234-0400-1111 e 1234-0500-1111.

5. Configure o servidor RADIUS:

a. Adicione uma conta de usuário no servidor. (Detalhes não mostrados.)

b. Configure as configurações de autenticação, autorização e contabilidade. (Detalhes não mostrados.)

Verificando a Configuração

1. A partir da Menu de navegação, selecione Segurança > Autenticação > RADIUS.
2. Verifique a configuração do esquema RADIUS "portsec".
3. A partir da Menu de navegação, selecione Segurança > Autenticação > Domínios ISP.
4. Verifique a configuração do domínio ISP "portsec".
5. Use a conta de usuário configurada para passar pela autenticação.
6. A partir da Menu de navegação, selecione Segurança > Controle de Acesso > Segurança de Porta.
7. Verifique que o número de usuários online não é 0 na GigabitEthernet 1/0/1.

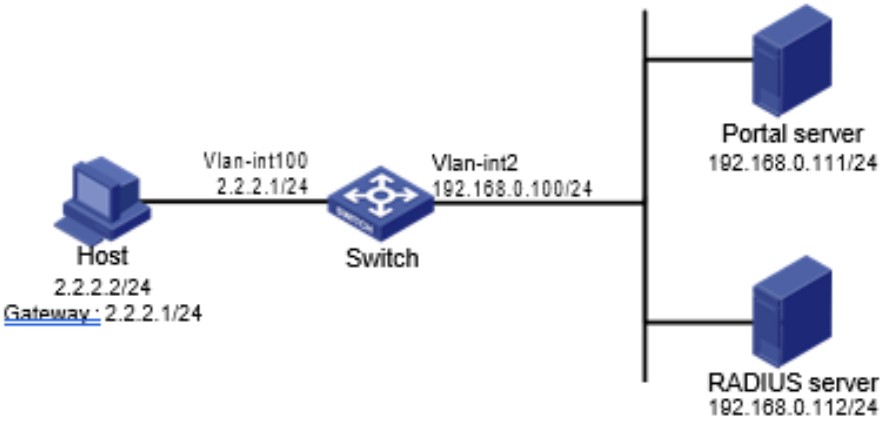
Exemplo de Configuração de Autenticação de Portal Direto

Requisitos de Rede

Conforme mostrado na Figura 46, o host está diretamente conectado ao switch (o dispositivo de acesso). O host é atribuído um endereço IP público manualmente ou através do DHCP. Um servidor de portal atua como servidor de autenticação de portal e servidor Web de portal. Um servidor RADIUS atua como servidor de autenticação/contabilidade.

Configure a autenticação de portal direto para que o host possa acessar apenas o servidor de portal antes de passar pela autenticação e acessar outros recursos de rede após a autenticação.

Figura 46 - Diagrama de Rede



Procedimento de Configuração

1. Configure o servidor de portal. (Detalhes não mostrados.)
2. Configure um esquema RADIUS no switch:

a. A partir da Menu de navegação, selecione Segurança > Autenticação > RADIUS.

b. Adicione o esquema RADIUS "rs1".

c. Configure o servidor de autenticação primário:

- Defina o endereço IP como 192.168.0.112.
- Defina a porta de autenticação como 1812.
- Defina a chave compartilhada como "radius".
- Defina o estado do servidor como Ativo.

d. Configure o servidor de contabilidade primário:

- Defina o endereço IP como 192.168.0.112.
- Defina a porta de contabilidade como 1813.

- Defina a chave compartilhada como "radius".
- Defina o estado do servidor como Ativo.

e. Configure o switch para não incluir nomes de domínio nos nomes de usuário enviados ao servidor RADIUS.

f. Clique no ícone de configurações avançadas na página RADIUS.

g. Habilite o recurso de controle de sessão.

3. Configure um domínio ISP no switch:

a. A partir da Menu de navegação, selecione Segurança > Autenticação > Domínios ISP.

b. Adicione o domínio ISP "dm1" e defina o estado do domínio como Ativo.

c. Defina o serviço de acesso como Portal.

d. Configure o domínio ISP para usar o esquema RADIUS "rs1" para autenticação, autorização e contabilidade de usuários de portal.

e. Clique no ícone de configurações avançadas na página de Domínio ISP.

f. Especifique "dm1" como o domínio ISP padrão. Se um usuário inserir o nome de usuário sem o nome de domínio ISP no login, os métodos de autenticação e contabilidade do domínio padrão são usados para o usuário.

4. Configure a VLAN e a interface de VLAN:

a. A partir da Menu de navegação, selecione Rede > Links > VLAN.

b. Crie a VLAN 100.

c. Abra a página de detalhes para a VLAN 100.

d. Crie a interface de VLAN 100 e atribua o endereço IP 2.2.2.1 a ela.

5. Configure a autenticação de portal no switch:

a. A partir da Menu de navegação, selecione Segurança > Controle de Acesso > Portal.

b. Adicione um servidor de autenticação de portal:

- Especifique o nome do servidor como "newpt".
- Especifique o endereço IP como 192.168.0.111.
- Especifique a chave compartilhada como "portal".
- Defina a porta de escuta do servidor como 50100.

c. Adicione um servidor Web de portal:

- Especifique o nome do servidor como "newpt".
- Especifique a URL.
- A URL deve ser a mesma que a URL do servidor Web de portal usada na rede. Neste exemplo, utilizamos http://192.168.0.111:8080/portal.

d. Adicione uma política de interface:

- Selecione a interface VLAN-interface 100.
- Na área de configuração IPv4, habilite a autenticação de portal e selecione o método Direto.
- Selecione o servidor Web de portal "newpt".
- Configure o endereço BAS-IP como 2.2.2.1.

6. Configure o servidor RADIUS:

a. Adicione uma conta de usuário no servidor. (Detalhes não mostrados.)

b. Configure as configurações de autenticação, autorização e contabilidade. (Detalhes não mostrados.)

Verificando a Configuração

1. A partir da Menu de navegação, selecione Segurança > Autenticação > RADIUS.
2. Verifique a configuração do esquema RADIUS "rs1".
3. A partir da Menu de navegação, selecione Segurança > Autenticação > Domínios ISP.
4. Verifique a configuração do domínio ISP "dm1".
5. Use a conta de usuário configurada para passar pela autenticação de portal.
6. A partir da Menu de navegação, selecione Segurança > Controle de Acesso > Portal.
7. Verifique que o número de usuários online não é 0 na VLAN-interface 100.

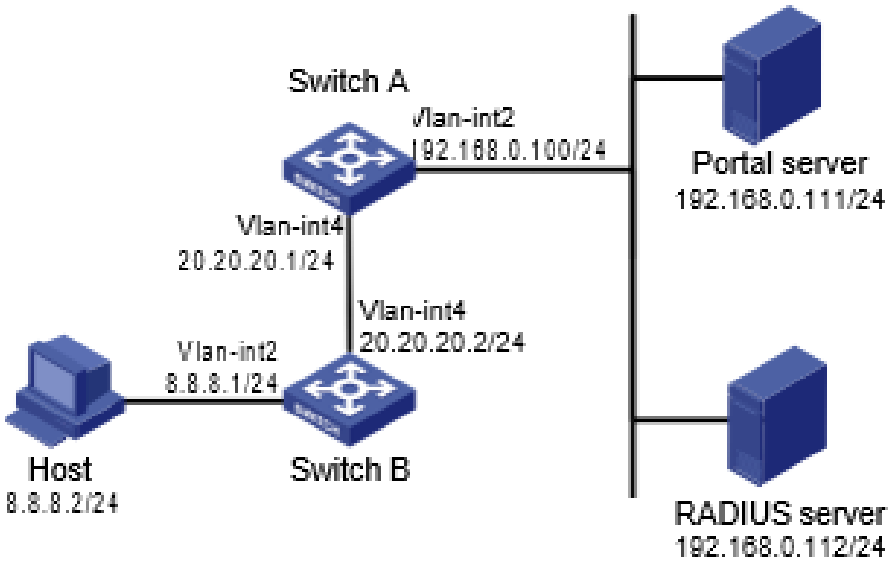
Exemplo de Configuração de Autenticação de Portal em Sub-redes Cruzadas

Requisitos de Rede

Conforme mostrado na Figura 47, o Switch A suporta autenticação de portal. O host acessa o Switch A através do Switch B. Um servidor de portal atua como servidor de autenticação de portal e servidor Web de portal. Um servidor RADIUS atua como servidor de autenticação/contabilidade.

Configure o Switch A para autenticação de portal em sub-redes cruzadas. Antes de passar pela autenticação, o host pode acessar apenas o servidor Web de portal. Após passar pela autenticação, o usuário pode acessar outros recursos de rede.

Figura 47 - Diagrama de Rede



Switch A
Vlan-int4 20.20.20.1/24
Vlan-int2 192.168.0.100/24

Vlan-int2 8.8.8.1/24	Vlan-int4 20.20.20.2/24

Procedimento de Configuração

1. Configure o servidor de portal. (Detalhes não mostrados.)
2. Configure um esquema RADIUS no Switch A:

a. A partir da Menu de navegação, selecione Segurança > Autenticação > RADIUS.

b. Adicione o esquema RADIUS "rs1".

c. Configure o servidor de autenticação primário:

- Defina o endereço IP como 192.168.0.112.

- Defina a porta de autenticação como 1812.
- Defina a chave compartilhada como "radius".
- Defina o estado do servidor como Ativo.

d. Configure o servidor de contabilidade primário:

- Defina o endereço IP como 192.168.0.112.
- Defina a porta de contabilidade como 1813.
- Defina a chave compartilhada como "radius".
- Defina o estado do servidor como Ativo.

e. Configure o switch para não incluir nomes de domínio nos nomes de usuário enviados ao servidor RADIUS.

f. Clique no ícone de configurações avançadas na página RADIUS.

g. Habilite o recurso de controle de sessão.

3. Configure um domínio ISP no Switch A:

a. A partir da Menu de navegação, selecione Segurança > Autenticação > Domínios ISP.

b. Adicione o domínio ISP "dm1" e defina o estado do domínio como Ativo.

c. Defina o serviço de acesso como Portal.

d. Configure o domínio ISP para usar o esquema RADIUS "rs1" para autenticação, autorização e contabilidade de usuários de portal.

e. Clique no ícone de configurações avançadas na página de Domínio ISP.

f. Especifique "dm1" como o domínio ISP padrão. Se um usuário inserir o nome de usuário sem o nome de domínio ISP no login, os métodos de autenticação e contabilidade do domínio padrão são usados para o usuário.

4. Configure a VLAN e a interface de VLAN no Switch A:

a. A partir da Menu de navegação, selecione Rede > Links > VLAN.

b. Crie a VLAN 4.

c. Abra a página de detalhes para a VLAN 4.

d. Crie a interface de VLAN 4 e atribua o endereço IP 20.20.20.1 a ela.

5. Configure a autenticação de portal no Switch A:

a. A partir da Menu de navegação, selecione Segurança > Controle de Acesso > Portal.

b. Adicione um servidor de autenticação de portal:

- Especifique o nome do servidor como "newpt".
- Especifique o endereço IP como 192.168.0.111.
- Especifique a chave compartilhada como "portal".
- Defina a porta de escuta do servidor como 50100.

c. Adicione um servidor Web de portal:

- Especifique o nome do servidor como "newpt".
- Especifique a URL.
- A URL deve ser a mesma que a URL do servidor Web de portal usada na rede. Neste exemplo, utilizamos http://192.168.0.111:8080/portal.

d. Adicione uma política de interface:

- Selecione a interface VLAN-interface 4.
- Na área de configuração IPv4, habilite a autenticação de portal e selecione o método de Camada 3.
- Selecione o servidor Web de portal "newpt".
- Configure o endereço BAS-IP como 20.20.20.1.

6. Configure o servidor RADIUS:

a. Adicione uma conta de usuário no servidor. (Detalhes não mostrados.)

b. Configure as configurações de autenticação, autorização e contabilidade. (Detalhes não mostrados.)

Verificando a Configuração

1. A partir da Menu de navegação, selecione Segurança > Autenticação > RADIUS.
2. Verifique a configuração do esquema RADIUS "rs1".

3. A partir da Menu de navegação, selecione Segurança > Autenticação > Domínios ISP.
4. Verifique a configuração do domínio ISP "dm1".
5. Use a conta de usuário configurada para passar pela autenticação de portal.
6. A partir da Menu de navegação, selecione Segurança > Controle de Acesso > Portal.
7. Verifique que o número de usuários online não é 0 na VLAN-interface 4.

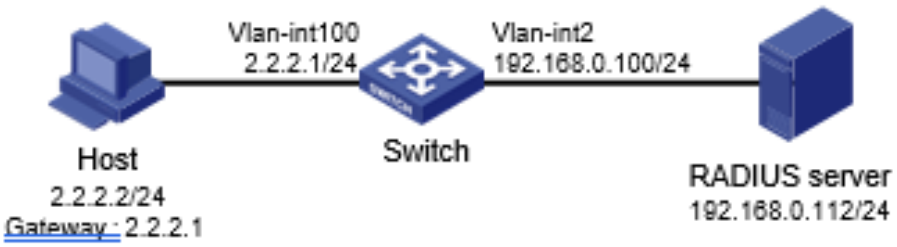
Exemplo de Configuração de Autenticação Direta de Portal Usando um Servidor Web de Portal Local

Requisitos de Rede

Conforme mostrado na Figura 48, o host está diretamente conectado ao switch (o dispositivo de acesso). O host é atribuído um endereço IP público manualmente ou através do DHCP. O switch atua como servidor de autenticação de portal e servidor Web de portal. Um servidor RADIUS atua como servidor de autenticação/contabilidade.

Configure a autenticação direta de portal no switch. Antes que um usuário passe pela autenticação de portal, o usuário só pode acessar o servidor Web de portal local. Após passar pela autenticação de portal, o usuário pode acessar outros recursos de rede.

Figura 48 - Diagrama de Rede



Host	
2.2.2.2/24	Gateway: 2.2.2.1
Switch	

Procedimento de Configuração

1. Configure um esquema RADIUS no switch:

a. A partir da Menu de navegação, selecione Segurança > Autenticação > RADIUS.

b. Adicione o esquema RADIUS "rs1".

c. Configure o servidor de autenticação primário:

- Defina o endereço IP como 192.168.0.112.
- Defina a porta de autenticação como 1812.
- Defina a chave compartilhada como "radius".
- Defina o estado do servidor como Ativo.

d. Configure o servidor de contabilidade primário:

- Defina o endereço IP como 192.168.0.112.
- Defina a porta de contabilidade como 1813.
- Defina a chave compartilhada como "radius".
- Defina o estado do servidor como Ativo.

e. Configure o switch para não incluir nomes de domínio nos nomes de usuário enviados ao servidor RADIUS.

f. Clique no ícone de configurações avançadas na página RADIUS.

g. Habilite o recurso de controle de sessão.

2. Configure um domínio ISP no switch:

a. A partir da Menu de navegação, selecione Segurança > Autenticação > Domínios ISP.

b. Adicione o domínio ISP "dm1" e defina o estado do domínio como Ativo.

c. Defina o serviço de acesso como Portal.

d. Configure o domínio ISP para usar o esquema RADIUS "rs1" para autenticação, autorização e contabilidade de usuários de portal.

e. Clique no ícone de configurações avançadas na página de Domínio ISP.

f. Especifique "dm1" como o domínio ISP padrão. Se um usuário inserir o nome de usuário sem o nome de domínio ISP no login, os métodos de autenticação e contabilidade do domínio padrão são usados para o usuário.

3. Configure a VLAN e a interface de VLAN no Switch A:

a. A partir da Menu de navegação, selecione Rede > Links > VLAN.

b. Crie a VLAN 100.

c. Abra a página de detalhes para a VLAN 100.

d. Crie a interface de VLAN 100 e atribua o endereço IP 2.2.2.1 a ela.

4. Configure a autenticação de portal no switch:

a. A partir da Menu de navegação, selecione Segurança > Controle de Acesso > Portal.

b. Adicione um servidor Web de portal:

- Especifique o nome do servidor como "newpt".
- Especifique a URL como http://2.2.2.1:2331/portal.
- A URL pode ser o endereço IP da interface habilitada com autenticação de portal ou o endereço de uma interface de loopback diferente de 127.0.0.1.

c. Adicione um servidor Web de portal local:

- Selecione HTTP.
- Selecione a página de logon padrão abc.zip.
- O arquivo de página de logon padrão deve existir no diretório raiz do meio de armazenamento do switch.
- Defina a porta TCP como 2331.

d. Adicione uma política de interface:

- Selecione a interface VLAN-interface 100.
- Na área de configuração IPv4, habilite a autenticação de portal e selecione o método Direto.
- Selecione o servidor Web de portal "newpt".

5. Configure o servidor RADIUS:

a. Adicione uma conta de usuário no servidor. (Detalhes não mostrados.)

b. Configure as configurações de autenticação, autorização e contabilidade. (Detalhes não mostrados.)

Verificando a Configuração

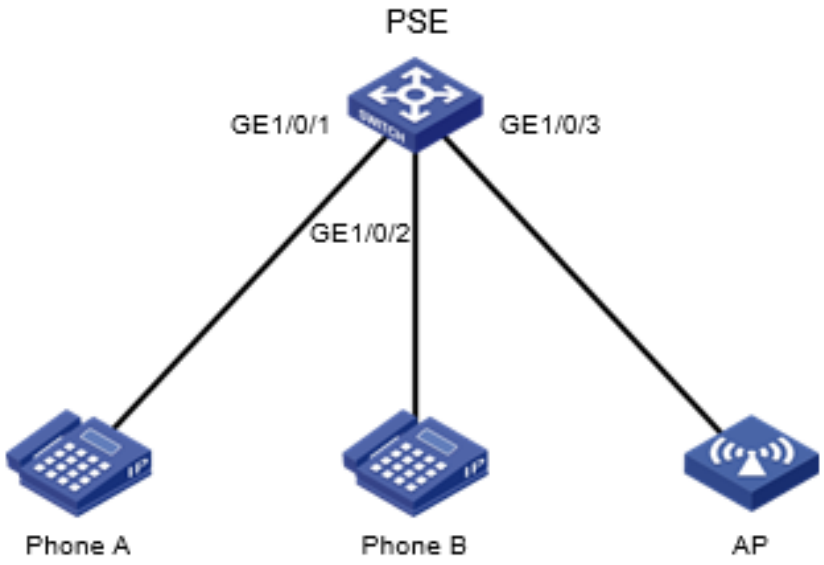
1. A partir da Menu de navegação, selecione Segurança > Autenticação > RADIUS.
2. Verifique a configuração do esquema RADIUS "rs1".
3. A partir da Menu de navegação, selecione Segurança > Autenticação > Domínios ISP.
4. Verifique a configuração do domínio ISP "dm1".
5. Use a conta de usuário configurada para passar pela autenticação de portal.
6. A partir da Menu de navegação, selecione Segurança > Controle de Acesso > Portal.
7. Verifique que o número de usuários online não é 0 na VLAN-interface 100.

Exemplo de Configuração de PoE (Power over Ethernet)

Requisitos de Rede

Conforme mostrado na Figura 50, configure o PoE para atender aos seguintes requisitos:

- Habilitar o dispositivo para fornecer energia a telefones IP e ao AP (Access Point).
- Habilitar o dispositivo para fornecer energia a telefones IP em primeiro lugar quando ocorrer sobrecarga.
- Alocar ao AP uma potência máxima de 9000 miliwatts.



PSE (Equipment Supplying Power)	Telefone A	Telefone B	AP (Access Point)

Procedimento de Configuração

1. A partir da Menu de navegação, selecione PoE > PoE.
2. Habilite o PoE para GigabitEthernet 1/0/1 e GigabitEthernet 1/0/2, defina a prioridade de fornecimento de energia como crítica.
3. Habilite o PoE para GigabitEthernet 1/0/3 e defina a potência máxima de PoE para a interface como 9000 miliwatts.

Cuidados e Diretrizes para Configuração Baseada na Web

Este guia contém informações importantes que, se não forem compreendidas ou seguidas, podem resultar em situações indesejáveis, incluindo:

- Desligamento inesperado ou reinicialização de dispositivos ou placas.
- Anomalias ou interrupção de serviços.
- Perda de dados, configurações ou arquivos importantes.
- Falha no login de usuários ou logoff inesperado.

Apenas pessoal treinado e qualificado está autorizado a realizar as tarefas de configuração descritas neste guia.

Antes de configurar o seu dispositivo, leia atentamente as informações contidas neste documento.

Manutenção de Dispositivos

Excluindo uma Conta de Administrador

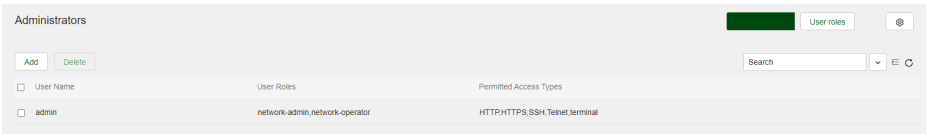
Consequências

Após a exclusão de uma conta de administrador, os usuários não poderão mais fazer login no dispositivo com essa conta de usuário.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Administradores.
2. Exclua uma conta de administrador.

Figura 57 - Excluindo uma conta de administrador



Modificando a Senha de uma Conta de Usuário

Consequências

Se você modificar a senha de uma conta de usuário, os usuários que não conheçam a nova senha não poderão fazer login no dispositivo com a conta de usuário.

Recomendação

Após modificar a senha de uma conta de usuário, registre a nova senha e notifique os usuários que utilizam a conta da nova senha.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Administradores.
2. Clique no ícone de Detalhes para uma conta de usuário.
3. Informe uma senha e confirme a senha.

Figura 58 - Modificando a senha de uma conta de usuário

Desativando uma Conta de Usuário Permanentemente Após o Número Máximo de Tentativas de Login Consecutivas

Consequências

Com o controle de senha habilitado, esta operação impede que um usuário use seu endereço IP para acessar o dispositivo após atingir o número máximo de tentativas de login consecutivas.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Administradores.
2. Clique no ícone de Controle de Senha no canto superior direito da página.
3. Clique em Ativar Controle de Senha.

4. Selecione "Desativa permanentemente a conta de usuário" na área de Login de Usuário.

Figura 59 - Desativando uma conta de usuário permanentemente

Salvando a Configuração Atual

Consequências

Salvar a configuração atual pode sobrescrever as configurações em um arquivo de configuração existente.

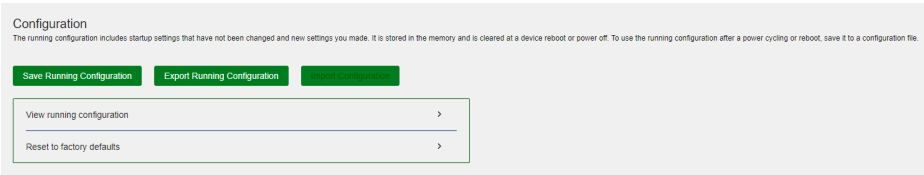
Recomendação

Realize esta operação de acordo com o prompt do sistema.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Configuração.
2. Clique em Salvar Configuração Atual.

Figura 60 - Salvando a configuração atual



Importando Configuração

Consequências

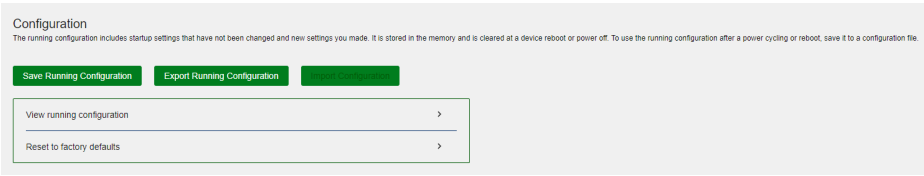
Esta operação restaura a configuração em execução para a configuração no arquivo de configuração especificado. A configuração anterior à restauração é perdida.

Esta operação pode causar interrupção do serviço.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Configuração.
2. Clique em Importar Configuração.

Figura 61 - Importando configuração



Restaurando as Configurações Padrão de Fábrica

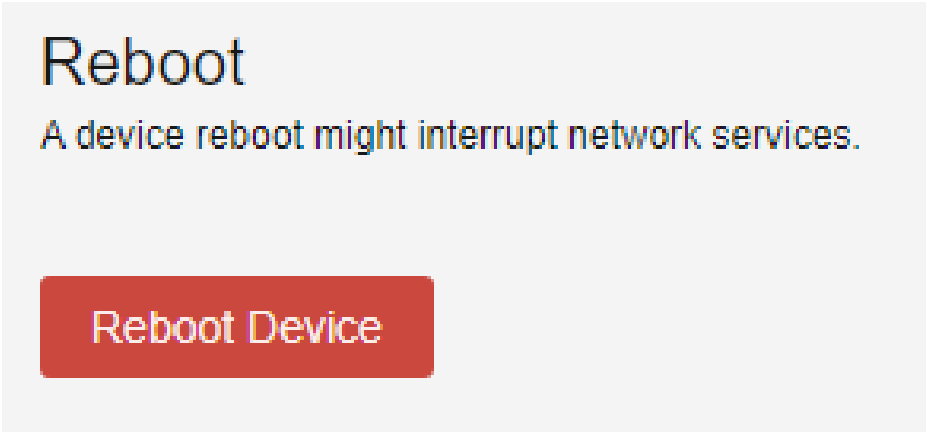
Consequências

Esta operação exclui arquivos de configuração a serem usados na próxima inicialização do dispositivo e restaura as configurações do dispositivo para os padrões de fábrica.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Configuração.
2. Clique no ícone de ao lado de "Redefinir para as configurações padrão de fábrica".
3. Clique em Redefinir.

Figura 62 - Restaurando as configurações padrão de fábrica



Excluindo um Arquivo ou Pasta de Arquivos

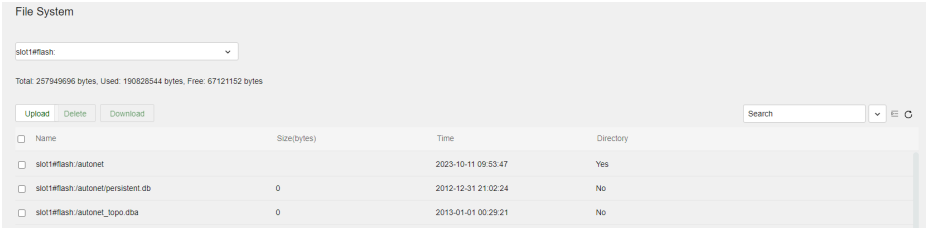
Consequências

Arquivos e pastas excluídos não podem ser recuperados.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Sistema de Arquivos.
2. Exclua um arquivo ou pasta de arquivos.

Figura 63 - Excluindo um arquivo ou pasta de arquivos



Atualizando as Imagens de Software de Inicialização

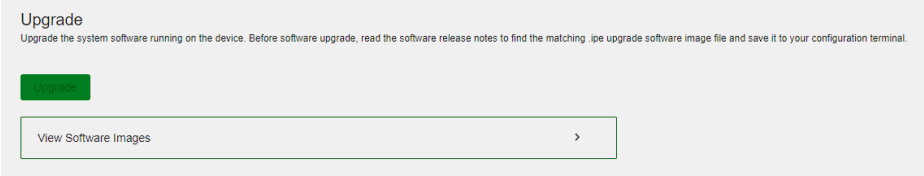
Consequências

Esta operação pode causar interrupção do serviço.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Atualização.
2. Atualize as imagens de software de inicialização.

Figura 64 - Atualizando as imagens de software de inicialização



Reinicializando o Dispositivo

Consequências

Esta operação pode causar interrupção do serviço.

Procedimento

1. A partir do painel de navegação, selecione Dispositivo > Manutenção > Reiniciar.
2. Reinicie o dispositivo.

Figura 65 - Reinicializando o dispositivo

Restaurando as Configurações Padrão de uma Interface

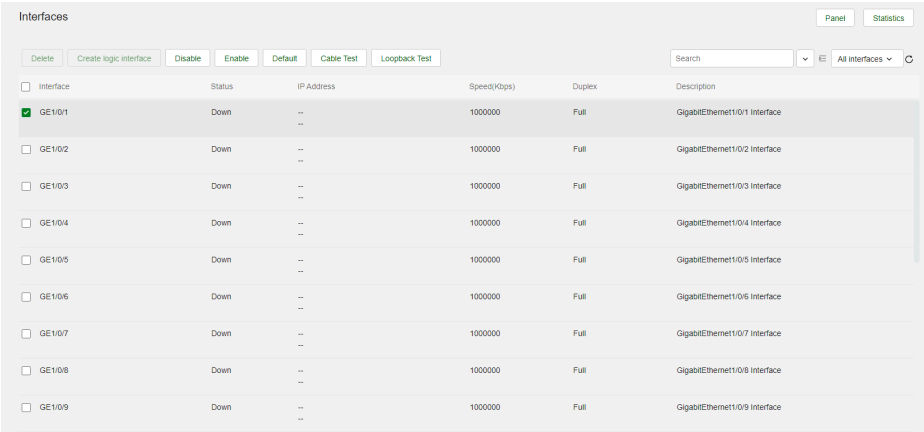
Consequências

Esta operação pode interromper os serviços de rede em andamento. Certifique-se de estar plenamente ciente do impacto dessa operação ao executá-la em uma rede em funcionamento.

Procedimento

1. A partir do painel de navegação, selecione Rede > Interfaces > Interfaces.
2. Selecione uma ou várias interfaces e clique em Padrão na parte inferior da página.

Figura 70 - Restaurando as Configurações Padrão de uma Interface



Desativando uma Interface

Consequências

Desativar uma interface desconecta os links conectados a ela e pode causar interrupção na comunicação.

Procedimento

1. A partir do painel de navegação, selecione Rede > Interfaces > Interfaces.
2. Clique no ícone Detalhes para uma interface.

3. Desative a interface.

Figura 71 - Desativando uma Interface

Excluindo Todas as Entradas ARP Dinâmicas

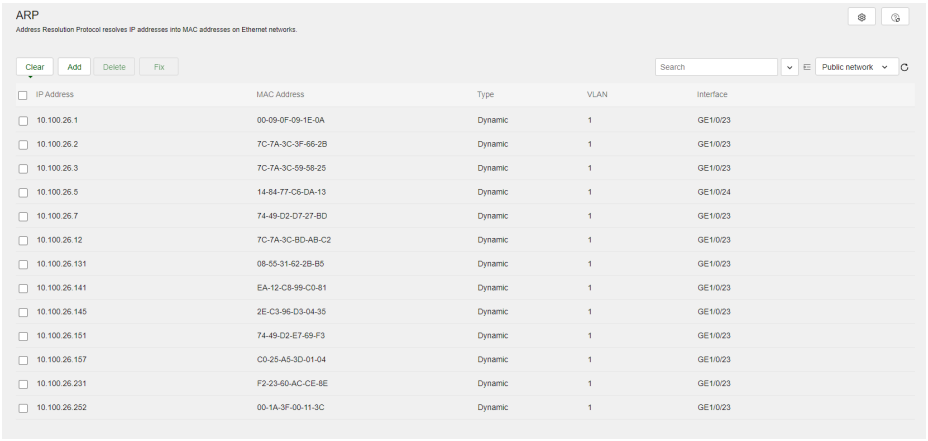
Consequências

Esta operação limpa todas as entradas ARP dinâmicas no dispositivo. Nesta situação, o dispositivo pode deixar de encaminhar o tráfego externo para os usuários internos.

Procedimento

1. A partir do painel de navegação, selecione Rede > IP > ARP.
2. Exclua todas as entradas dinâmicas do dispositivo.

Figura 72 - Excluindo Todas as Entradas ARP Dinâmicas



Excluindo Todas as Rotas Estáticas IPv4

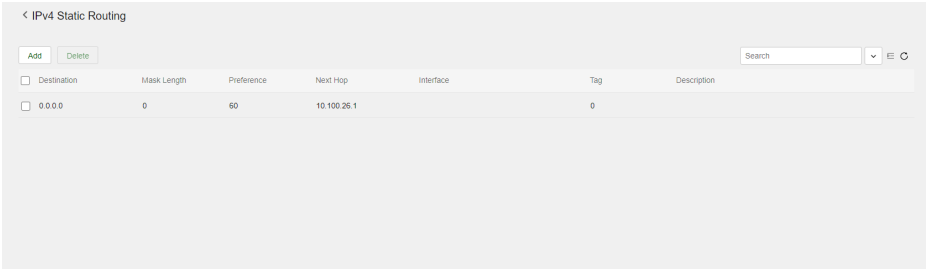
Consequências

A exclusão de todas as rotas estáticas IPv4 pode causar problemas de alcance de rede e falhas no encaminhamento de pacotes.

Procedimento

1. A partir do painel de navegação, selecione Rede > Roteamento > Roteamento Estático.
2. Clique no ícone próximo ao roteamento estático IPv4.
3. Exclua todas as rotas estáticas IPv4.

Figura 73 - Excluindo Todas as Rotas Estáticas IPv4



Excluindo Todas as Rotas Estáticas IPv6

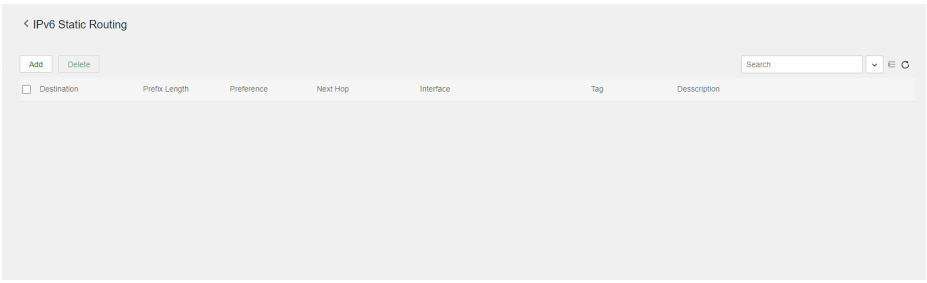
Consequências

A exclusão de todas as rotas estáticas IPv6 pode causar problemas de alcance de rede e falhas no encaminhamento de pacotes.

Procedimento

1. A partir do painel de navegação, selecione Rede > Roteamento > Roteamento Estático.
2. Clique no ícone próximo ao roteamento estático IPv6.
3. Exclua todas as rotas estáticas IPv6.

Figura 74 - Excluindo Todas as Rotas Estáticas IPv6



Serviços de Rede - Desabilitar o Serviço HTTP ou HTTPS

Consequências: Se o serviço HTTP ou HTTPS for desabilitado, os usuários não poderão acessar o dispositivo por meio da interface da web.

Procedimento

1. A partir do painel de navegação, selecione Rede > Serviço > HTTP/HTTPS.
2. Altere o estado do serviço HTTP ou HTTPS de ON para OFF. Veja a Figura 75 abaixo para desabilitar o serviço HTTP ou HTTPS.

Network Service

HTTP/HTTPS connection idle timeout

Connection idle timeout	10 min

HTTP

HTTP service	ON
HTTP service port number	80
Access ACL	Null

HTTPS

HTTPS service	ON
HTTPS service port number	443
Access ACL	Null

Termo de garantia

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

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 3 (três) meses 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 gratuita de partes, peças e componentes que apresentarem vício de fabricação, incluindo as despesas com a mão de obra utilizada nesse reparo. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.

2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.

3. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fa- bricante – 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, de- verá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as des- pesas 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 hipó- teses 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, eletro- magnética, 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 equipa- mento 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 so- mos

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.

Produto beneficiado pela Legislação de Informática.

Suporte a clientes: (48) 2106 0006

Fórum: forum.intelbras.com.br (http://forum.intelbras.com.br)

Suporte via chat: intelbras.com.br/suporte-tecnico (http://www.intelbras.com.br/suporte-tecnico)

Suporte via e-mail: suporte@intelbras.com.br

SAC: 0800 7042767

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 (http://www.intelbras.com.br)

Indústria Brasileira