Manual do usuário

RW 6305W
RW 6302
RW 6181
RW 6302X
RW 6302 MAX

intelbras

RW 6305W / RW 6302 / RW 6181 / RW 6302X / RW 6302 MAX

Roteador empresarial

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

O RW 6305W / RW 6302 / RW 6181 / RW 6302X / RW 6302 MAX é membro da família de roteadores empresariais desenvolvidos para aplicações em ambientes corporativos, como empresas, hotéis e eventos.

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

A senha do produto deverá ter no mínimo 8 e no máximo 63 caracteres. Procure cadastrar uma senha forte que contenha ao menos uma letra maiúscula, uma letra minúscula, um número e um caractere especial.

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados. O número de homologação se encontra na etiqueta do produto, para consultas acesse o site : *https://www.gov.br/anatel/pt-br.*

Este manual é baseado na Web do modo Cloud dos Access Points da série RW descreve as funções da Web dos Access Points da Intelbras, como início rápido, visão geral da Web, configuração do serviço sem fio, configurações relacionadas à segurança e autenticação, configuração de QoS e configurações avançadas.

Este prefácio inclui os seguintes tópicos sobre a documentação:

- Público
- Convenções

Público

Esta documentação se destina a:

- Planejadores de rede.
- Suporte técnico de campo e engenheiros de manutenção.
- Administradores de rede que trabalham com os Access Points da Intelbras.

Convenções

As informações a seguir descrevem as convenções usadas na documentação.

Convenções de comando

Convenção	Descrição
Em negrito	O texto em negrito representa comandos e palavras-chave que você digita literalmente como mostrado.
Itálico	O texto em itálico representa argumentos que você substitui por valores reais.
[ ]	Os colchetes incluem opções de sintaxe (palavras-chave ou argumentos) que são opcionais.
{ x | y | ... }	Os colchetes contêm um conjunto de opções de sintaxe obrigatórias separadas por barras verticais, das quais você seleciona uma.
[x | y | ...]	Os colchetes incluem um conjunto de opções opcionais de sintaxe separadas por barras verticais, das quais você seleciona uma ou nenhuma.
{ x | y | ... } *	As chaves marcadas com asterisco incluem um conjunto de opções de sintaxe obrigatórias separadas por barras verticais, das quais você seleciona um mínimo de uma.
[x | y | ...] *	Os colchetes marcados com asterisco incluem opções de sintaxe opcionais separadas por barras verticais, das quais você seleciona uma opção, várias opções ou nenhuma.
&<1-n>	O argumento ou a combinação de palavra-chave e argumento antes do sinal de E comercial (&) pode ser inserido de 1 a n vezes.
#	Uma linha que começa com um sinal de libra (#) é um comentário.

Convenções da GUI

Convenção	Descrição
Em negrito	Nomes de janelas, nomes de botões, nomes de campos e itens de menu estão em negrito. Por exemplo, a janela Novo usuário é aberta; clique em O*K*.
>	Os menus de vários níveis são separados por colchetes angulares. Por exemplo, *File* > *Create* > *Folder.*

Símbolos

Convenção	Descrição
	**Aviso!** Um alerta que chama a atenção para informações importantes que, se não forem compreendidas ou seguidas, podem resultar em lesões pessoais.
	**Cuidado!** Um alerta que chama a atenção para informações importantes que, se não forem compreendidas ou seguidas, podem resultar em perda de dados, corrupção de dados ou danos ao hardware ou ao software.
	**Importante:** um alerta que chama a atenção para informações essenciais.
	**Dica!** Um alerta que fornece informações úteis.

Ícones de topologia de rede

Convenção	Descrição
	Representa um dispositivo de rede genérico, como um roteador, um switch ou um firewall.
	Representa um dispositivo com capacidade de roteamento, como um roteador ou um switch de camada 3.
	Representa um switch genérico, como um switch de Camada 2 ou Camada 3, ou um roteador que suporta encaminhamento de Camada 2 e outros recursos de Camada 2.
	Representa um controlador de acesso, um módulo de Wired-WLAN unificado ou o mecanismo do controlador de acesso em um switch de Wired-WLAN unificado.
	Representa um Access Point.
	Representa uma unidade terminadora Wireless.
	Representa um terminador Wireless.
	Representa um ponto de acesso em malha.
	Representa sinais omnidirecionais.
	Representa sinais direcionais.
	Representa um produto de segurança, como um firewall, UTM, gateway de segurança multisserviço ou dispositivo de balanceamento de carga.
	Representa um módulo de segurança, como um firewall, balanceamento de carga, NetStream, SSL VPN, IPS ou módulo ACG.

Exemplos fornecidos neste documento

Os exemplos neste documento podem usar dispositivos que diferem de seu dispositivo em termos de modelo de hardware, configuração ou versão de software. É normal que os números de porta, a saída de amostra, as capturas de tela e outras informações nos exemplos sejam diferentes das que você tem no seu dispositivo.

LGPD - Lei Geral de Proteção de Dados Pessoais

Este produto faz tratamento de dados pessoais, porém a Intelbras não possui acesso aos dados a partir deste produto.

LGPD - Segurança do produto no tratamento de dados

Este produto possui criptografia na transmissão dos dados pessoais.

Índice

1. Fazer login na interface Web

Faça login na interface da Web por HTTP ou HTTPS.

1.1. Restrições e diretrizes

Para garantir um login bem-sucedido, verifique se o sistema operacional e o navegador da Web atendem aos requisitos e siga as diretrizes desta seção.

1.1.1. Requisitos do navegador da Web

Como prática recomendada, use os seguintes navegadores da Web:

- Internet Explorer 10 ou superior.
- Mozilla Firefox 30.0.0.5269 ou superior
- Google Chrome 35.0.1916.114 ou superior.
- Safari 6.0 ou superior.

Para acessar a interface da Web, é necessário usar as seguintes configurações do navegador:

- Aceite os cookies primários (cookies do site que você está acessando).
- Para garantir a exibição correta do conteúdo da página da Web após a atualização ou downgrade do software, limpe os dados armazenados em cache pelo navegador antes de fazer login.
- Ative o script ativo ou o JavaScript, dependendo do navegador da Web.
- Se você estiver usando o navegador Microsoft Internet Explorer, deverá ativar as seguintes configurações de segurança:
  - Execute controles ActiveX e plug-ins.
  - Controles ActiveX de script marcados como seguros para scripting.

Certifique-se de que a resolução da tela do PC, laptop ou tablet que você usa para acessar a interface da Web seja de 1024× 768 ou superior.

1.1.2. Configurações de login padrão

Use as configurações em para o primeiro login.

Item	Configuração
Nome de usuário	admin
Senha	Intelbras@AP
Função do usuário	administrador de rede

1.2. Efetuando login na interface da Web pela primeira vez

Você pode fazer login no dispositivo por HTTP ou HTTPS. Por padrão, o HTTP e o HTTPS estão ativados.

Para fazer login na interface da Web pela primeira vez:

- Conecte ao Access Point pelo IP recebido do seu roteador ou então ponto a ponto com a interface do seu switch pelo endereço ip de loopback 10.0.0.1. O endereço loopback só será setado no RW caso não haja um DHCP server na rede.
- Acesse *http://10.0.0.1* por meio de um navegador.
- Na página de login, digite o nome de usuário padrão *(admin)* e a senha padrão *(Intelbras@AP)*.
- Clique em *Login.*
- Você pode alterar a senha de login conforme solicitado para aumentar a segurança.

1.3. Fazer logout da interface da Web

Importante:

» Por motivos de segurança, faça logout da interface da Web imediatamente após concluir suas tarefas.

» O dispositivo não salva automaticamente a configuração quando você se desconecta da interface da Web. Para evitar a perda de configuração quando o dispositivo for reinicializado, você deve salvar a configuração.

1.3.1. Para fazer logout da interface da Web

Use um dos métodos a seguir para salvar a configuração atual:

» **Método 1:** clique no ícone *Salvar* no canto superior direito da interface da Web.

» **Método 2:** no painel de navegação, selecione *System* > *Management* > *Configuration.*
Clique em *Save Running Configuration (Salvar configuração em execução).*

Clique no ícone de *administrador* no canto superior direito da página e, em seguida, clique em *Logout.*

2. Usando a interface da Web

Conforme mostrado em , a interface da Web contém as seguintes áreas:

Área	Descrição
(1) Banner e área auxiliar	Contém os seguintes itens: » O logotipo da Intelbras. » Modelo do dispositivo. » Ícone para salvar as configurações atuais. » Ícone para exibir o roadmap. » Ícone de administrador admin - Clique nesse ícone para selecionar um idioma, alterar a senha de login, fazer logout ou usar o recurso de digitalização para acompanhamento.
(2) Árvore de navegação	Organiza os menus de recursos em uma árvore na visualização do sistema ou na visualização da rede.
(3) Painel de conteúdo	Exibe informações e fornece uma área para você configurar recursos. Dependendo do conteúdo desse painel, as páginas da Web incluem os seguintes tipos: » **Página de recursos:** contém funções ou recursos que um módulo de recursos pode fornecer (consulte *Uso de uma página de recurso).* » **Página de tabela:** exibe entradas em uma tabela (consulte *Uso de uma página de tabela).* » **Página de configuração:** contém parâmetros para você configurar um recurso ou função (consulte *Usando uma página de configuração).*

2.1. 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 obter mais informações sobre como usar os ícones e botões nas páginas, consulte o item *2.2. Ícones e botões.*

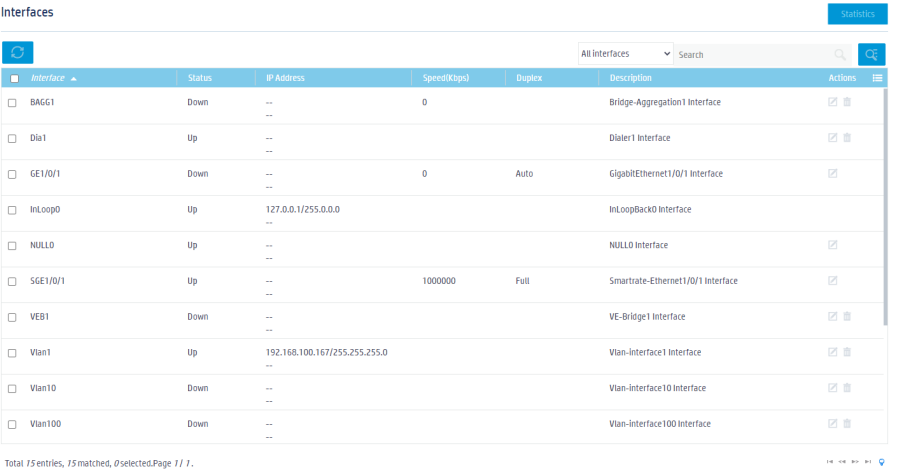
2.1.1. Uso de uma página de recurso

Conforme mostrado em , uma página de recurso contém informações sobre um módulo de recurso, inclusive estatísticas de entrada de tabela, recursos e funções. Em uma página de recurso, você pode configurar os recursos fornecidos por um módulo de recurso.

Exemplo de página de recurso

2.1.2. Uso de uma página de tabela

Conforme mostrado em , uma página de tabela exibe entradas em uma tabela. Para classificar as entradas por um campo em ordem crescente ou decrescente, clique no campo. Por exemplo, clique em *Interface* para classificar as entradas por interfaces.

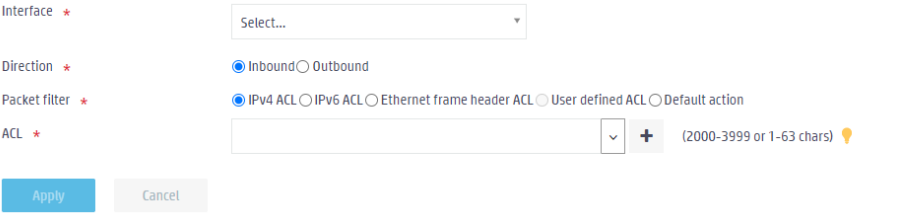


Exemplo de página de tabela

2.1.3. Usando uma página de configuração

Conforme mostrado em , uma página de configuração contém todos os parâmetros de uma tarefa de configuração. Se um parâmetro precisar ser configurado em outra página, a página de configuração normalmente fornece um link. Não é necessário navegar até a página de destino.

Por exemplo, você deve usar uma ACL ao configurar um filtro de pacotes. Se não houver ACLs disponíveis quando você executar a tarefa, poderá clicar no ícone *Add (Adicionar)*  para criar uma ACL. Nessa situação, não é necessário navegar até a página de gerenciamento de ACL.



Exemplo de configuração page

2.2. Ícones e botões

Descreve os ícones e botões que você pode usar para configurar e gerenciar o dispositivo.

Ícone/botão	Nome do ícone/botão	Tarefa
Ícones gerais		
	Atualizar	Atualizar estatísticas ou informações manualmente.
	Mais informações	Exibir mais conteúdo.
	Adicionar	Adicionar uma nova entrada de configuração.
	Filtro	Filtrar estatísticas ou informações por um campo específico.
Ícones de ajuda		
	Dica	Obter informações de ajuda para uma função ou parâmetro.
	Observação	Exibir notas para uma função ou serviço.
Ícone do contador		
	Índices	Identifique o número total de entradas da tabela.
Ícone de navegação		
	Próximo	Acesse a página de nível inferior para exibir informações ou definir configurações.
Ícone de controle de status		
	Controle de status	Controle o status de ativação do recurso. Se ON for exibido, o recurso está ativado. Para desativar o recurso, clique no botão. Se OFF for exibido, o recurso está desativado. Para ativar o recurso, clique no botão.
Ícones de pesquisa		
	Pesquisa	Digite uma expressão de pesquisa na caixa de pesquisa e, em seguida, clique nesse ícone para realizar uma pesquisa básica.
	Pesquisa avançada	Clique nesse ícone e insira uma combinação de critérios para realizar uma pesquisa avançada.
Ícones de gerenciamento de entrada		
	Atualizar	Atualizar manualmente as entradas da tabela.
	Adicionar	Adicionar uma nova entrada. Confirme a adição de uma entrada e continue a adicionar uma entrada adicional.
	Exportação	Exportar uma entrada.
	Excluir	Excluir uma entrada. Esse ícone aparece no final de uma entrada quando você passa o cursor do mouse sobre a entrada.
	Modificar	Modificar uma entrada. Esse ícone aparece no final de uma entrada quando você passa o cursor do mouse sobre a entrada.
	Excluir em massa	Excluir todas as entradas.
	Detalhes	Exibir informações detalhadas de um registro. Esse ícone aparece no final de uma entrada quando você passa o cursor do mouse sobre a entrada.
	Seletor de campo	Selecione os campos a serem exibidos.

Ícone/botão	Nome do ícone/botão	Tarefa
	Ícone de configurações avançadas	
	Configurações avançadas	Acesse a página de configuração avançada.
	Ícone de configuração rápida	
	Configuração rápida	Orientá-lo na configuração rápida de um serviço.

2.3. Realização de tarefas básicas

Esta seção descreve as tarefas básicas que devem ser executadas com frequência quando você configura ou gerencia o dispositivo.

2.3.1. Salvando a configuração

Para evitar a perda de configurações, salve manualmente a configuração em tempo hábil. Para salvar manualmente a configuração, use um dos seguintes métodos:

- Clique em *Save (Salvar)* no canto superior direito.
- Execute as seguintes tarefas para acessar a página de gerenciamento de configuração:
  - Na árvore de navegação, selecione *Sistema>Gerenciamento>Configuração.*
  - Clique em *Save Running Configuration (Salvar configuração em execução).*

2.3.2. Exibição de configurações de uma entrada de tabela

- Passe o cursor do mouse sobre a entrada.
- Clique no ícone *Detail (Detalhes)*  no final da entrada.

2.3.3. Reinicialização do dispositivo

A reinicialização é necessária para que algumas configurações tenham efeito.

Para reiniciar o dispositivo:

- Salve a configuração.
- Na árvore de navegação, selecione *Sistema>Gerenciamento>Reiniciar.*
- Clique em *Reboot Device (Reiniciar dispositivo).*

3. Navegador de recursos

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 exibir informações. Para configurar recursos, é necessário ter a função de usuário *network-admin.* Este capítulo descreve todos os menus disponíveis para a função de usuário *administrador da rede.*

4. Tabelas do navegador de menus

Para cada menu superior, exceto o menu do painel, é fornecida uma tabela de navegação. Use as tabelas de navegação para navegar até as páginas das tarefas que você deseja executar. Nas tabelas de navegação, um menu está em negrito se tiver submenus.

4.1. Menu do painel

O menu do painel fornece uma visão geral do sistema e seu status de execução, incluindo as seguintes informações:

- Registros de eventos.
- Estatísticas de serviços Wireless.
- Estatísticas de clientes.
- Estatísticas de tráfego Wireless.

Esse menu não contém submenus.

4.2. Menu de monitoramento

Use para navegar até as tarefas que você pode executar no menu *Monitoring (Monitoramento).*

Menus	Tarefas
Clientes	
Informações sobre os clientes	Exibir informações de estatísticas do cliente.
Quadros de categorias de acesso	Exibir informações de estatísticas de pacotes de clientes por quadro ou byte.
Categoria de acesso Bytes	
Total de quadros	
Total de bytes	
Redes Wireless	
Serviços Wireless	Veja os serviços sem fio.
Estatísticas de serviços Wireless	Visualize as informações de estatísticas do serviço Wireless.
Segurança Wireless	
WIPS	Exibir informações de estatísticas do WIPS.
Monitoramento de aplicativos	
Otimização de multicast	Exibir informações de estatísticas de multicast IPv4/IPv6.
Sensor de proximidade do cliente	Exibir informações do usuário.

4.3. Menu de início rápido

Use para navegar até as tarefas que você pode executar no menu *Quick Start (Início rápido).*

Navegador de menu de início rápido

Menus	Tarefas
Adicionar serviços Wireless	Configure os serviços Wireless. Configurar a autenticação da camada de link. Ativar ou desativar a autorização e a detecção de intrusão. Gerenciar chaves. Vincular APs. Configure o controle de acesso.
Adicionar usuário	Adicionar um novo usuário.

4.4. Menu de configuração Wireless

Use para navegar até as tarefas que podem ser executadas no menu *Wireless Configuration (Configuração Wireless).*

Navegador de menu de configuração Wireless

Menus	Tarefas
Serviços Wireless	
Configuração de serviços Wireless	Exibir serviços sem fio. Adicione, exclua ou modifique serviços Wireless. Configurar a autenticação da camada de link. Ativar ou desativar a autorização e a detecção de intrusão. Gerenciar chaves. Vincular APs. Configure o controle de acesso.
Gerenciamento de AP	
Serviço Bind Wireless	Vincule serviços Wireless a rádios.
Configurações básicas	Configurar os códigos de região do AP. Ativar ou desativar o bloqueio de código de região. Altere o modo de iluminação do LED. Configure o modo de operação do AP.

Menus	Tarefas
QoS sem fio	
Limite da tarifa do cliente	Exibir informações detalhadas sobre o limite de taxa do cliente. Configurar o limite de taxa do cliente com base no tipo de cliente. Configurar o limite de taxa do cliente baseado em serviço.
Garantia de largura de banda	Exibir detalhes da garantia de largura de banda. Defina a largura de banda máxima do rádio. Configurar a garantia de largura de banda baseada em AP.
Multimídia Wi-Fi	Exibir ou configurar o status e as informações de QoS sem fio. Exibir ou configurar os parâmetros EDCA do rádio. Exibir ou configurar parâmetros de negociação de rádio e cliente. Exibir estatísticas WMM para clientes. Exibir informações sobre o fluxo de transporte.
Gerenciamento de rádio	
Configuração de rádio	Exibir ou modificar informações do rádio.
Navegação da banda	Ativar ou desativar a navegação global por banda. Configurar os parâmetros de navegação da banda.
Segurança Wireless	
WIPS	Exibir informações detalhadas sobre o WIPS. Ativar WIPS. Configurar VSDs. Configurar políticas de classificação. Configurar políticas de detecção de ataques. Configurar políticas de assinatura. Configurar políticas de contramedidas. Configurar as regras de classificação do AP. Configurar assinaturas. Adicionar endereços MAC à lista de dispositivos ignorados por alarme.
Allowlist e denylist	Configurar listas de permissões. Configurar listas de negação estáticas e dinâmicas.
Aplicativos	
Serviços de malha	Configurar serviços de malha.
Otimização de multicast	Configurar e exibir as definições de otimização de multicast IPv4. Configurar e exibir as definições de otimização de multicast IPv6.
Sensor de proximidade do cliente	Ativar e desativar a sondagem de clientes. Exibir informações de sondagem do cliente.

4.5. Menu de configuração da rede

Use para navegar até as tarefas que podem ser executadas no menu *Network Configuration (Configuração da rede)*.

Menus	Tarefas
Interfaces de rede	
Interfaces	Exibir interfaces e seus atributos, inclusive: Status da interface. Endereço IP. Velocidade e modo duplex. Descrição da interface. Excluir interfaces lógicas. Modificar interfaces. Restaurar a configuração padrão.
Agregação de links	Criar, modificar ou excluir grupos de agregação da Camada 2.
PPPoE	Adicionar, excluir ou modificar clientes PPPoE.
Link	
VLAN	Configurar VLANs baseadas em portas. Criar interfaces de VLAN. Modificar ou excluir VLANs.
MAC	Excluir ou criar entradas MAC estáticas, entradas MAC dinâmicas e entradas MAC blackhole. Exibir entradas MAC existentes.

Menus	Tarefas
STP	Ativar ou desativar o STP globalmente. Ativar ou desativar o STP nas interfaces. Configure o modo de operação do STP como STP, RSTP, PVST ou MSTP. Configurar prioridades de instância. Configurar regiões MST. Ativar ou desativar o TC snooping.
Roteamento de rede	
Tabela de roteamento	Exibir informações da tabela de roteamento IPv4 e IPv6, incluindo informações breves da tabela de roteamento e estatísticas de rota.
Roteamento estático	Exibir entradas de roteamento estático IPv4 e IPv6. Criar, modificar ou excluir entradas de roteamento estático IPv4 e IPv6.
IP	
NAT	Configurar NAT dinâmico e estático, servidores internos e NAT444 dinâmico e estático. Configure grupos de endereços NAT, grupos de endereços NAT444, grupos de blocos de portas e grupos de servidores. Configure o modo PAT, os mapeamentos de DNS e o hairpin NAT. Ativar NAT ALG. Exibir registros de NAT.
IP	Configure o método para obter um endereço IP (DHCP ou estático). Configurar o endereço IP ou o MTU de uma interface. Crie uma interface de loopback.
ARP	Adicionar entradas ARP estáticas. Excluir entradas dinâmicas de ARP e entradas estáticas de ARP. Configure o proxy ARP. Configure o ARP gratuito. Configure a proteção contra ataques ARP. Configurar a persistência da entrada ARP.
DNS IPv4	Configurar a resolução de nome de domínio estático IPv4. Configurar a resolução dinâmica de nomes de domínio IPv4. Configure o proxy DNS. Configurar sufixos de nomes de domínio IPv4. Exibir os nomes de domínio resolvidos.
IPv6	
IPv6	Configure o método para obter um endereço IPv6 (atribuição manual, atribuição dinâmica ou geração automática). Configurar o endereço IPv6 de uma interface. Crie uma interface de loopback.
ND	Adicionar entradas estáticas de ND. Excluir entradas de ND dinâmicas e entradas de ND estáticas. Configure o tempo de envelhecimento para entradas ND obsoletas. Ativar ou desativar a minimização da entrada de ND local do link. Configurar o limite de salto. Configurar os atributos do prefixo RA, inclusive: Prefixo do endereço. Comprimento do prefixo. Vida útil válida. Vida útil preferida. Configurar as definições de RA para uma interface, inclusive: Supressão de mensagens RA. Intervalos máximo e mínimo para o envio de mensagens RA. Bandeira M. Opção MTU. Limite de salto. O-flag. Vida útil do roteador. Intervalo de retransmissão da mensagem NS. Preferência do roteador. Tempo de alcance do vizinho. Habilite o proxy ND comum e local em uma interface. Configurar regras de ND para a interface, inclusive: Número máximo de entradas de vizinhos dinâmicos. Número máximo de tentativas de DAD.

Menus	Tarefas
DNS IPv6	Configurar a resolução estática e dinâmica de nomes de domínio IPv6. Configure o proxy DNS IPv6. Configurar sufixos de nomes de domínio IPv6. Exibir os nomes de domínio resolvidos.
Protocolos de gerenciamento	
DHCP	Configurar as funções do servidor DHCP. Configurar serviços DHCP. Configure a interface para operar no modo de servidor DHCP. Configurar pools de endereços DHCP. Configurar a detecção de conflitos de endereços IP. Configurar as funções do agente de retransmissão DHCP. Configurar serviços DHCP. Configure o modo de agente de retransmissão DHCP e configure o endereço IP do servidor DHCP. Configure as definições para a entrada de retransmissão DHCP, incluindo: Registro de entradas de retransmissão DHCP. Atualização periódica das entradas de retransmissão DHCP. Intervalo para atualização das entradas de retransmissão DHCP.
HTTP/HTTPS	Ativar ou desativar o serviço HTTP. Ativar ou desativar o serviço HTTPS. Defina o tempo limite da conexão com a Web. Defina o número da porta do serviço HTTP. Defina o número da porta do serviço HTTPS. Especifique as ACLs de controle de acesso à Web.
Telnet	Ativar ou desativar o serviço Telnet. Defina os valores DSCP que o dispositivo usará para os pacotes IPv4 ou IPv6 Telnet de saída. Especifique as ACLs de controle de acesso Telnet.
SSH	Ativar ou desativar os serviços Stelnet, SFTP e SCP. Configurar parâmetros de SSH.
NTP	Ativar ou desativar o serviço NTP. Configure o endereço IP e o nível de estrato do relógio local. Definir uma chave de autenticação NTP.
LLDP	Ativar ou desativar o LLDP. Ativar ou desativar a compatibilidade com CDP. Configurar parâmetros LLDP. Exibir o status da interface. Configurar o status da interface. Exibir vizinhos LLDP. Configure o LLDP para anunciar os TLVs especificados.

4.6. Menu de segurança da rede

Use para navegar até as tarefas que podem ser executadas no menu *Segurança da rede.*

Menus	Tarefas
	Política de tráfego
Filtro de pacotes	Criar, modificar ou excluir um filtro de pacotes para uma interface. Configure a ação padrão para o filtro de pacotes.
Mapeamento de prioridades	Consultar ou configurar a prioridade da porta. Configurar o modo de confiança de prioridade para uma porta. Consultar ou modificar a tabela de mapeamento de prioridades.
Controle de acesso	
ACL IPv4 ACL IPv6 Layer 2 ACL	Criar ACLs IPv4, IPv6 e de camada 2. Modificar e excluir ACLs criadas na página atual e nas páginas de outros módulos de serviço, como filtro de pacotes.
Autenticação	
Autenticação MAC	Configurar a autenticação de endereço MAC.
802.1X	Ativar ou desativar o 802.1X. Configure o 802.1X em uma interface. Configure o método de controle de acesso à porta. Configure o número máximo de usuários 802.1X simultâneos na porta. Configurar recursos 802.1X avançados.
Portal	Configurar a autenticação do portal.

Menus	Tarefas
Segurança portuária	Configurar a segurança da porta.
AAA	
Domínios ISP	Configurar domínios ISP.
RADIUS	Configurar esquemas RADIUS.
Gerenciamento de usuários	
Usuários locais	Adicionar, modificar ou excluir usuários locais. Adicione, modifique ou exclua grupos de usuários locais.

4.7. Menu do sistema

Use para navegar até as tarefas que você pode executar no menu *System (Sistema).*

Menus	Tarefas
Registro	
Registros de eventos	Consultar, coletar ou excluir informações de registro.
Configurações de registro	Exportar os logs do sistema para a partição de cache de log ou para o host de log.
Recursos	
Intervalo de tempo	Crie, modifique ou exclua um intervalo de tempo.
Plataforma Cloud	
Plataforma Cloud	Configure o nome de domínio da plataforma Cloud.
QuickNet	
Gerenciamento do QuickNet	Ativar ou desativar o gerenciamento do QuickNet.
Gerenciamento de arquivos	
Gerenciamento de arquivos	Faça upload, download ou exclua arquivos.
Desvincular dispositivo	Desvincule os dispositivos do servidor da plataforma Cloud.
Gerenciamento	
Administradores	Criar, modificar ou excluir funções. Criar, modificar ou excluir administradores. Configurar a função dos administradores. Controle a autoridade de acesso do administrador. Gerenciar senhas. Controle os logins de usuários.
Configurações	Defina o nome do dispositivo. Defina a hora do sistema.
Configuração	Salvar ou exportar a configuração em execução. Importar configuração. Exibir a configuração em execução. Restaurar as configurações para os padrões de fábrica.
Atualização	Atualizar o software do sistema. Exibir listas de software do sistema, incluindo: Lista de softwares ativados na inicialização atual do sistema. Lista do software principal a ser ativado na próxima inicialização do sistema.
Reinicialização	Reinicie o dispositivo.
Sobre	Exibir informações básicas do dispositivo, incluindo nome do dispositivo, número de série, modelo, descrição, versão, etiqueta eletrônica e declaração.

4.8. Menu Ferramentas

Use para navegar até as tarefas que você pode executar no menu *Tools (Ferramentas).*

Menus	Tarefas
Depurar	
Diagnóstico	Coletar informações de diagnóstico para localizar problemas.
Registros do sistema	Exporte os registros do sistema para localizar problemas.

5. Configuração Wireless

5.1. Serviços sem fio

5.1.1. Acesso à WLAN

O acesso à WLAN fornece acesso a WLANs para clientes Wireless.

5.1.1.1. Serviço Wireless

Um serviço wireless define um conjunto de atributos de serviço wireless, como SSID e método de autenticação.

5.1.1.2. SSID

Um identificador de conjunto de serviços é o nome de uma WLAN.

5.1.1.3. VLAN padrão

Um cliente é atribuído à VLAN padrão depois de acessar a WLAN.

5.1.1.4. Ocultação de SSID

Os APs anunciam SSIDs em quadros de beacon. Se o número de clientes em um BSS exceder o limite ou se o BSS não estiver disponível, você poderá ativar a ocultação de SSID para impedir que os clientes descubram o BSS. Quando a ocultação de SSID está ativada, o BSS oculta seu SSID nos quadros de beacon e não responde às solicitações de sonda de difusão. Um cliente deve enviar solicitações de sondagem com o SSID especificado para acessar a WLAN. Esse recurso pode proteger a WLAN contra ataques

5.1.1.5. Isolamento de usuário baseado em SSID

O isolamento de usuário baseado em SSID é aplicável tanto ao modo de encaminhamento local quanto ao modo de encaminhamento centralizado.

Quando o isolamento de usuário baseado em SSID está ativado para um serviço, o dispositivo isola todos os usuários Wireless que acessam a rede por meio do serviço na mesma VLAN.

5.1.1.6. Modo de autenticação

Obs.: *para obter informações sobre autenticação MAC e autenticação de portal, consulte* Autenticação de acesso.

Autenticação de sistema aberto

A autenticação de sistema aberto é o método de autenticação padrão e o algoritmo de autenticação mais simples, o que significa que não há autenticação. Se o tipo de autenticação for definido como autenticação de sistema aberto, qualquer cliente poderá ser aprovado na autenticação.

Autenticação de sistema aberto aprimorada

A autenticação de sistema aberto aprimorada é um serviço de autenticação aberta aprimorada que fornece criptografia de dados para clientes sem fio que suportam o protocolo OWE (Opportunistic Wireless Encryption) em redes de acesso sem fio abertas. Com esse serviço, os clientes que suportam o protocolo OWE podem se conectar à rede sem digitar uma senha. O dispositivo e o cliente negociarão automaticamente uma chave usando o protocolo OWE para criptografar os pacotes de dados.

Autenticação PSK

A autenticação PSK requer que o mesmo PSK seja configurado tanto para um AP quanto para um cliente. A integridade do PSK é verificada durante o Handshake de quatro vias. Se a negociação do PSK for bem-sucedida, o cliente será aprovado na autenticação.

Autenticação 802.1X

O autenticador usa o relé EAP ou a terminação EAP para se comunicar com o servidor RADIUS. O autenticador pode ser o AC ou o AP.

- **Handshake de usuário on-line:** o recurso de handshake de usuário on-line examina o status de conectividade dos clientes 802.1X on-line. O dispositivo envia periodicamente mensagens de handshake aos clientes on-line. Se o dispositivo não receber nenhuma resposta de um cliente on-line depois de ter feito o máximo de tentativas de handshake, o dispositivo colocará o cliente no estado off-line.
- **Segurança de handshake do usuário on-line:** o recurso de segurança de handshake do usuário on-line adiciona informações de autenticação nas mensagens de handshake. Esse recurso pode impedir que clientes ilegais forjem clientes 802.1X legais para trocar mensagens de handshake com o dispositivo. Com esse recurso, o dispositivo compara as informações de autenticação na mensagem de resposta do handshake de um cliente com as informações atribuídas pelo servidor de autenticação. Se não for encontrada nenhuma correspondência, o dispositivo fará o logoff do cliente.
- **Reautenticação periódica do usuário on-line:** a reautenticação periódica do usuário on-line rastreia o status da conexão dos clientes on-line e atualiza os atributos de autorização atribuídos pelo servidor. Os atributos incluem a ACL, a VLAN e a QoS baseada no perfil do usuário

5.1.1.7. Mecanismo WEP dinâmico

O IEEE 802.11 fornece o mecanismo WEP dinâmico para garantir que cada usuário use uma chave WEP privada. Para comunicações unicast, o mecanismo usa a chave WEP negociada pelo cliente e pelo servidor durante a autenticação 802.1X. Para comunicações multicast e broadcast, o mecanismo usa a chave WEP configurada. Se você não configurar uma chave WEP, o AP gerará aleatoriamente uma chave WEP para comunicações de difusão e multicast.

Depois que o cliente passa pela autenticação 802.1X, o AP envia ao cliente um pacote RC4-EAPOL que contém a ID da chave WEP unicast e a ID da chave WEP multicast e broadcast. A ID da chave WEP unicast é 4.

5.1.1.8. Associação rápida

A ativação do balanceamento de carga ou da navegação de banda pode afetar a eficiência da associação do cliente. Para serviços sensíveis a atrasos ou em um ambiente em que o balanceamento de carga e a navegação em banda não são necessários, é possível ativar a associação rápida para um modelo de serviço.

A associação rápida desativa o balanceamento de carga ou a navegação de banda em clientes associados ao modelo de serviço. O dispositivo não equilibrará o tráfego nem executará a navegação em banda, mesmo que esses dois recursos estejam ativados na WLAN.

5.1.1.9. Vinculação de serviços Wireless

Se você associar um serviço wireless a um rádio, o AP criará um BSS que poderá fornecer os serviços wireless definidos no serviço wireless.

É possível executar as seguintes tarefas ao vincular um serviço Wireless a um rádio:

- Vincule um grupo de VLAN ao rádio para que os clientes associados ao BSS sejam atribuídos uniformemente a todas as VLANs no grupo de VLAN.
- Vincule a ID da porta do NAS ou a ID do NAS ao rádio para identificar o servidor de acesso à rede.
- Habilite o AP a ocultar SSIDs em quadros de beacon.

5.1.2. Autenticação de camada de link e gerenciamento de chaves

O IEEE 802.11 original é um mecanismo de Associação de Rede de Segurança Pré-Robusta (Pre-RSNA). Esse mecanismo é vulnerável a ataques de segurança, como exposição de chaves, interceptação de tráfego e adulteração. Para aumentar a segurança da WLAN, foi introduzido o IEEE 802.11i (o mecanismo RSNA). Você pode selecionar o Pre-RSNA ou o RSNA conforme necessário para proteger sua WLAN.

O IEEE 802.11i criptografa apenas o tráfego de dados da WLAN. Os quadros de gerenciamento de WLAN não criptografados estão abertos a ataques de sigilo, autenticidade e integridade. O IEEE 802.11w oferece proteção de quadros de gerenciamento com base na estrutura do 802.11i para evitar ataques, como quadros falsos de desautenticação e desassociação.

5.1.2.1. Mecanismo pré-RSNA

O mecanismo pré-RSNA usa o sistema aberto e os algoritmos de chave compartilhada para autenticação e usa o WEP para criptografia de dados. O WEP usa a cifra de fluxo RC4 para confidencialidade e suporta tamanhos de chave de 40 bits (WEP40), 104 bits (WEP104) e 128 bits (WEP128)

5.1.2.2. Mecanismo RSNA

O mecanismo RSNA inclui os modos de segurança WPA e RSN. O RSNA oferece os seguintes recursos:

- Gerenciamento de chaves e autenticação 802.1X e PSK (AKM) para autenticar a integridade do usuário e gerar e atualizar chaves dinamicamente
  - **802.1X-802.1X:** realiza a autenticação do usuário e gera a chave mestra par a par (PMK) durante a autenticação. O cliente e o AP usam a PMK para gerar a chave transitória em pares (PTK).
  - **PSK privado:** o endereço MAC do cliente é usado como PSK para gerar o PMK. O cliente e o AP usam o PMK para gerar o PTK.
  - **PSK:** o PSK é usado para gerar o PMK. O cliente e o AP usam o PMK para gerar o PTK.
- Mecanismos TKIP (Temporal Key Integrity Protocol) e CCMP (Counter Mode CBC-MAC Protocol) para criptografia de dados.

Principais tipos de

O 802.11i usa a PTK e a chave temporária de grupo (GTK). A PTK é usada em unicast e a GTK é usada em multicast e broadcast.

Negociação de chave WPA

O WPA usa pacotes EAPOL-Key no four-way handshake para negociar o PTK e no two-way handshake para negociar o GTK.

Negociação de chaves RSN

A RSN usa pacotes EAPOL-Key no four-way handshake para negociar o PTK e o GTK.

Principais atualizações

As principais atualizações aumentam a segurança da WLAN. As principais atualizações incluem as do PTK e do GTK.

- **Atualizações de PTK:** atualizações das chaves unicast usando a negociação de handshake de quatro vias.
- **Atualizações GTK:** atualizações para as chaves multicast usando a negociação de handshake bidirecional.

Suítes de cifras

- Tanto o TKIP-TKIP quanto o WEP usam o algoritmo RC4. É possível alterar o pacote de cifras de WEP para TKIP atualizando o software sem alterar o hardware. O TKIP tem as seguintes vantagens sobre o WEP:
  - O TKIP fornece vetores de inicialização (IVs) mais longos para aumentar a segurança da criptografia. Em comparação com a criptografia WEP, a criptografia TKIP usa o algoritmo de criptografia RC4 de 128 bits e aumenta o comprimento dos IVs de 24 bits para 48 bits.
  - O TKIP permite a negociação de chaves dinâmicas para evitar a configuração de chaves estáticas. As chaves dinâmicas do TKIP não podem ser facilmente decifradas.
  - O TKIP oferece MIC e contramedidas. Se um pacote tiver sido adulterado, ele falhará no MIC. Se dois pacotes falharem no MIC em um período, o AP tomará contramedidas automaticamente, parando de fornecer serviços em um período para evitar ataques.
- O CCMP-CCMP é baseado no CCM (Counter-Mode/CBC-MAC) do algoritmo de criptografia AES (Advanced Encryption Standard).

  O CCMP contém um método dinâmico de negociação e gerenciamento de chaves. Cada cliente pode negociar dinamicamente um conjunto de chaves, que pode ser atualizado periodicamente para aumentar ainda mais a segurança do conjunto de cifras do CCMP. Durante o processo de criptografia, o CCMP usa um número de pacote (PN) de 48 bits para garantir que cada pacote criptografado use um PN diferente. Isso aumenta a segurança da WLAN.

5.1.3. Autorização

Você pode configurar o dispositivo para ignorar as informações de autorização recebidas do servidor RADIUS ou do dispositivo local depois que um cliente for aprovado na autenticação. As informações de autorização incluem VLAN, ACL e perfil de usuário.

5.1.3.1. Proteção contra intrusões

Quando o autenticador detecta uma solicitação de associação de um cliente que falha na autenticação, a proteção contra intrusão é acionada. O recurso executa uma das seguintes ações predefinidas no BSS em que a solicitação é recebida:

» Adiciona o endereço MAC de origem da solicitação à lista de endereços MAC bloqueados e descarta o pacote de solicitação. O cliente em um endereço MAC bloqueado não pode estabelecer conexões com o AP dentro de um período de bloqueio configurável pelo usuário.
» Interrompe o BSS em que a solicitação é recebida até que o BSS seja ativado manualmente na interface de rádio.
» Interrompe o BSS em que a solicitação é recebida por um período de interrupção configurável pelo usuário.

5.1.4. Controle de acesso baseado em ACL

Esse recurso controla o acesso do cliente usando regras de ACL vinculadas a um AP ou a um modelo de serviço.

Ao receber uma solicitação de associação de um cliente, o dispositivo executa as seguintes ações:

» Permite que o cliente acesse a WLAN se for encontrada uma correspondência e a ação da regra for permissão.
» Nega o acesso do cliente à WLAN se nenhuma correspondência for encontrada ou se a regra correspondente tiver uma instrução deny.

5.2. Gerenciamento de AP

5.2.1. Configuração do serviço Wireless

Se você vincular um serviço wireless a um rádio em um AP, o AP criará um BSS com base nos atributos dos serviços wireless. Os clientes no mesmo BSS acessam a rede por meio do mesmo SSID.

5.2.2. Código da região

Um código de região determina características como frequências disponíveis, canais disponíveis e nível de potência de transmissão. Defina um código de região válido antes de configurar um AP.

Para evitar a violação da regulamentação causada pela modificação do código de região, bloqueie o código de região.

5.2.3. LED modo de iluminação

Você pode configurar os LEDs em um AP para piscar nos seguintes modos:

» **Silencioso:** todos os LEDs estão apagados.
» **Desperto:** todos os LEDs piscam uma vez a cada minuto. O suporte a esse modo depende do modelo do AP.
» **Always-on: t**odos os LEDs ficam . O suporte a esse modo depende do modelo do AP.
» **Normal:** a forma como os LEDs piscam nesse modo varia de acordo com o modelo do AP. Esse modo pode identificar o status de execução de um AP.

5.2.4. Modo de operação do AP

O dispositivo suporta a mudança do AP atual para o modo de operação especificado. Depois que o modo de operação é alternado, o AP começa a usar os padrões de fábrica ou a configuração salva quando foi alternado pela última vez para esse modo. Quando um AP operando no modo Cloud precisa mudar para o modo Fit, você pode configurar o endereço IP do AC que estabelecerá um túnel CAPWAP com o AP com base nos requisitos reais de serviço.

5.3. QoS sem fio

5.3.1. Limitação da taxa do cliente

A limitação da taxa de clientes impede o uso agressivo da largura de banda por um cliente e garante o uso justo da largura de banda entre os clientes associados ao mesmo AP.

5.3.1.1. Cliente modo de limite de taxa

Os seguintes modos estão disponíveis para limitação da taxa de clientes:

» **Modo dinâmico:** define a largura de banda total compartilhada por todos os clientes. O limite de taxa para cada cliente é a taxa total dividida pelo número de clientes on-line. Por isso, se a taxa total for de 10 Mbps e cinco clientes estiverem on-line, o limite de taxa para cada cliente será de 2 Mbps.
» **Modo estático:** define a largura de banda que pode ser usada por cada cliente. Quando o limite de taxa multiplicado pelo número de clientes associados excede a largura de banda disponível fornecida pelo AP, os clientes podem não obter a largura de banda definida.

Você pode configurar o modo de limite de taxa de cliente somente para limitação de taxa de cliente baseada em serviço.

5.3.1.2. Métodos de limite de taxa de cliente

Você pode usar os seguintes métodos para limitar a taxa de tráfego:

- **Limitação da taxa de clientes com base no tipo de cliente:** a configuração entra em vigor em todos os clientes. A taxa de tráfego de cada tipo de cliente não pode exceder a configuração correspondente.
- **Limitação de taxa de cliente baseada em serviço:** a configuração entra em vigor em todos os clientes associados ao mesmo serviço Wireless.

Se mais de um método e modo forem configurados, todas as configurações terão efeito. A taxa para um cliente será limitada ao valor mínimo entre todas as configurações de limitação de taxa do cliente.

5.3.2. Recursos de garantia de largura de banda

A garantia de largura de banda oferece as seguintes funções:

- Garante que o tráfego de todos os BSSs possa passar livremente quando a rede não estiver congestionada.
- Assegura que cada BSS possa obter a largura de banda garantida quando a rede estiver congestionada.

Esse recurso melhora a eficiência da largura de banda e mantém o uso justo da largura de banda entre os serviços de WLAN. Por exemplo, você atribui ao SSID1, SSID2 e SSID3 25%, 25% e 50% da largura de banda total. Quando a rede não está , o SSID1 pode usar toda a largura de banda ociosa, além de sua largura de banda garantida. Quando a rede está , o SSID1 tem garantia de 25% da largura de banda.

Esse recurso se aplica apenas ao tráfego AP-para-cliente.

5.3.3. Recursos do WMM

Uma rede 802.11 fornece acesso wireless baseado em contenção. Para fornecer aos aplicativos serviços de QoS, o IEEE desenvolveu o 802.11e para WLANs baseadas em 802.11.

Enquanto o IEEE 802.11e estava sendo padronizado, a Wi-Fi Alliance definiu o padrão Wi-Fi Multimedia (WMM) para permitir a interoperação de dispositivos de fornecimento de QoS de diferentes fornecedores. O WMM permite que uma WLAN forneça serviços de QoS, de modo que os aplicativos de áudio e vídeo possam ter melhor desempenho nas WLANs.

5.3.3.1. Status do WMM

Você pode visualizar o status de ativação do WMM para cada AP conectado ao AC.

5.3.3.2. Configurações do WMM

Você pode configurar o número máximo de mapeamentos SVP, políticas CAC e clientes permitidos.

O mapeamento SVP atribui pacotes que têm o ID de protocolo 119 no cabeçalho IP à fila AC-VI ou AC-VO para fornecer pacotes SVP com a prioridade especificada. Quando o mapeamento de SVP está desativado, os pacotes SVP são atribuídos à fila AC-BE.

O Connect Admission Control (CAC) limita o número de clientes que podem usar ACs de alta prioridade (AC-VO e AC-VI) para garantir que haja largura de banda suficiente para esses clientes. Se for necessário um AC de alta prioridade (AC-VO ou AC-VI), o cliente deverá enviar uma solicitação ao AP. O AP retorna uma resposta positiva ou negativa com base na política de admissão baseada no uso do canal ou na política de admissão baseada no cliente. Se a solicitação for rejeitada, o AP atribui AC-BE aos clientes.

5.3.3.3. Parâmetros EDCA e políticas ACK

Você pode visualizar e modificar os parâmetros EDCA e as políticas ACK.

O EDCA é um mecanismo de contenção de canal definido pelo WMM para transmitir preferencialmente pacotes com alta prioridade e alocar mais largura de banda para esses pacotes

O WMM define os seguintes parâmetros EDCA:

- **Número de espaçamento entre quadros de arbitragem:** na WLAN baseada em 802.11, cada cliente tem a mesma duração de inatividade (DIFS), mas o WMM define uma duração de inatividade para cada AC. A duração da inatividade aumenta à medida que o AIFSN aumenta.
- **A forma de expoente de CWmin/forma de expoente de CWmax-ECWmin/ECWmax:** determina os slots de backoff, que aumentam à medida que os dois valores aumentam.
- **Limite de oportunidade de transmissão:** o limite de TXOP especifica o tempo máximo que um cliente pode manter o canal após uma contenção bem-sucedida. Um valor maior representa um tempo maior. Se o valor for 0, um cliente poderá enviar apenas um pacote cada vez que mantiver o canal.

O WMM define as seguintes políticas de ACK:

- **Normal ACK:** o destinatário reconhece cada pacote unicast recebido.
- **No ACK:** o destinatário não reconhece os pacotes recebidos durante a troca de pacotes sem fio. Essa política melhora a eficiência da transmissão em um ambiente em que a qualidade da comunicação é forte e a interferência é fraca. Se a qualidade da comunicação se deteriorar, essa política poderá aumentar a taxa de perda de pacotes.

5.3.3.4. Parâmetros EDCA das filas AC para clientes

Você pode visualizar e modificar os parâmetros do EDCA e ativar ou desativar uma política CAC.

5.3.3.5. Cliente Estatísticas de WMM

Você pode visualizar as seguintes informações:

- As informações básicas do dispositivo, como SSID.
- Estatísticas de tráfego de dados.
- Atributo APSD para uma fila AC.

O U-APSD é um método de economia de energia definido pelo WMM para economizar energia do cliente. O U-APSD permite que os clientes em modo de suspensão sejam ativados e recebam o número especificado de pacotes somente depois de receberem um pacote de acionamento. O U-APSD aprimora o mecanismo de economia de energia do 802.11 APSD.

O U-APSD é ativado automaticamente depois que você ativa o WMM.

5.3.3.6. Estatísticas de tráfego

Você pode visualizar as seguintes informações:

- Prioridade do usuário para pacotes de redes com fio.
- Identificador de tráfego.
- Direção do tráfego.
- Permissão de largura de banda excedente.

5.4. Gerenciamento de rádio

A radiofrequência (RF) é uma taxa de oscilação elétrica na faixa de 300 kHz a 300 GHz. A WLAN usa as radiofrequências da banda de 2,4 GHz e da banda de 5 GHz como mídia de transmissão. A banda de 2,4 GHz inclui frequências de rádio de 2,4 GHz a 2,4835 GHz. A banda de 5 GHz inclui frequências de rádio de 5,150 GHz a 5,350 GHz e de 5,725 GHz a 5,850 GHz.

O termo *radiofrequência* ou sua abreviação RF também é usado como sinônimo de "rádio" na comunicação Wireless.

5.4.1. Modo de rádio

Cuidado!

A alteração do modo de um rádio ativado faz o logoff de todos os clientes associados.

O IEEE define os modos de rádio 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax. fornece uma comparação desses modos de rádio.

Padrão IEEE	Banda de frequência	Taxa máxima
802.11a	5 GHz	54 Mbps
802.11b	2,4 GHz	11 Mbps
802.11g	2,4 GHz	54 Mbps
802.11n	2,4 GHz ou 5 GHz	600 Mbps
802.11ac	5 GHz	6900 Mbps
802.11ax	5 GHz	9600 Mbps
802.11gax	2,4 GHz	6900 Mbps

Obs.: *»* *A menos que estipulado de outra forma, o 802.11ax neste documento inclui o 802.11gax.*

- *O IEEE define 802.1ax como tecnologias em bandas de 5 GHz. A Intelbras suporta a aplicação do 802.11ax a bandas de 2,4 GHz, o que é chamado de 802.11gax.*

Modos de rádio diferentes suportam canais e potências de transmissão diferentes. Quando você edita o modo de rádio, o AP seleciona automaticamente um canal ou uma potência de transmissão se o novo modo de rádio não for compatível com o canal ou a potência de transmissão original.

As funções de rádio disponíveis variam de acordo com o modo de rádio:

- Para rádios 802.11a, 802.11b e 802.11g, você pode configurar funções básicas de rádio. Para obter mais informações sobre as funções básicas de rádio, consulte *Funções básicas do rádio.*
- Para rádios 802.11n, você pode configurar funções básicas de rádio e funções 802.11n. Para obter mais informações sobre as funções 802.11n, consulte *Funções 802.11n .*
- Para rádios 802.11ac, você pode configurar funções básicas de rádio, funções 802.11n e funções 802.11ac. Para obter mais informações sobre as funções 802.11ac, consulte *Funções 802.11ac.*
- Para rádios 802.11ax, você pode configurar funções básicas de rádio, funções 802.11n, funções 802.11ac e funções 802.11ax. Para obter mais informações sobre as funções 802.11ax, consulte *802.11ax funções.*

Obs.: *802.11g, 802.11n, 802.11ac e 802.11ax são compatíveis com versões anteriores.*

5.4.3. Canal

Um canal é um intervalo de frequências com uma largura de banda específica

A banda de 2,4 GHz tem 14 canais. A largura de banda de cada canal é de 20 MHz e cada dois canais têm um espaçamento de 5 MHz. Entre os 14 canais, existem quatro grupos de canais não sobrepostos e o mais comumente usado contém os canais 1, 6 e 11.

A banda de 5 GHz pode fornecer taxas mais altas e é mais imune a interferências. Há 24 canais não sobrepostos designados para a banda de 5 GHz. Os canais são espaçados em 20 MHz com uma largura de banda de 20 MHz. Os canais disponíveis variam de acordo com o país.

5.4.4. Potência de transmissão

A potência de transmissão reflete a força do sinal de um dispositivo Wireless. Uma potência de transmissão mais alta permite que um rádio cubra uma área maior, mas traz mais interferência aos dispositivos adjacentes. A intensidade do sinal diminui à medida que a distância de transmissão aumenta.

5.4.5. Taxa de transmissão

A taxa de transmissão refere-se à velocidade com que os dispositivos Wireless transmitem o tráfego. Ela varia de acordo com o modo de rádio e os esquemas de espalhamento, codificação e modulação. Veja a seguir as taxas suportadas por diferentes tipos de rádios:

- 802.11a-6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps.
- 802.11b-1 Mbps, 2 Mbps, 5,5 Mbps e 11 Mbps.
- 802.11g-1 Mbps, 2 Mbps, 5,5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps.
- 802.11n - As taxas dos rádios 802.11n variam de acordo com a largura de banda do canal. Para obter mais informações, consulte *MCS.*
- 802.11ac - As taxas dos rádios 802.11ac variam de acordo com a largura de banda do canal e o número de fluxos espaciais (NSS). Para obter mais informações, consulte *VHT-MCSVHT-MCS.*
- 802.11ax - As taxas dos rádios 802.11ax variam de acordo com a largura de banda do canal e o número de fluxos espaciais (NSS). Para obter mais informações, consulte *HE-MCS .*

5.4.6. MCS

O MCS (Modulation and Coding Scheme, esquema de modulação e codificação) definido no IEEE 802.11n-2009 determina a modulação, a codificação e o número de fluxos espaciais. Um MCS é identificado por um índice MCS, que é representado por um número inteiro no intervalo de 0 a 76. Um índice MCS é o mapeamento do MCS para uma taxa de dados e mostram exemplos de parâmetros MCS para 20 MHz e 40 MHz.

Quando o modo de largura de banda é de 20 MHz, os índices MCS de 0 a 15 são obrigatórios para APs, e os índices MCS de 0 a 7 são obrigatórios para clientes.

5.4.6.1. Parâmetros MCS para 20 MHz

			Taxa de dados (Mbps)	
Índice MCS	**Número de fluxos espaciais**	**Modulação**	**800ns GI**	**400ns GI**
0	1	BPSK	6.5	7.2
1	1	QPSK	13.0	14.4
2	1	QPSK	19.5	21.7
3	1	16-QAM	26.0	28.9
4	1	16-QAM	39.0	43.3

Índice MCS	Número de fluxos espaciais	Modulação	Taxa de dados (Mbps)	
			800ns GI	400ns GI
5	1	64-QAM	52.0	57.8
6	1	64-QAM	58.5	65.0
7	1	64-QAM	65.0	72.2
8	2	BPSK	13.0	14.4
9	2	QPSK	26.0	28.9
10	2	QPSK	39.0	43.3
11	2	16-QAM	52.0	57.8
12	2	16-QAM	78.0	86.7
13	2	64-QAM	104.0	115.6
14	2	64-QAM	117.0	130.0
15	2	64-QAM	130.0	144.4

5.4.6.2. Parâmetros MCS para 40 MHz

Índice MCS	Número de fluxos espaciais	Modulação	Taxa de dados (Mbps)	
			800ns GI	400ns GI
0	1	BPSK	13.5	15.0
1	1	QPSK	27.0	30.0
2	1	QPSK	40.5	45.0
3	1	16-QAM	54.0	60.0
4	1	16-QAM	81.0	90.0
5	1	64-QAM	108.0	120.0
6	1	64-QAM	121.5	135.0
7	1	64-QAM	135.0	150.0
8	2	BPSK	27.0	30.0
9	2	QPSK	54.0	60.0
10	2	QPSK	81.0	90.0
11	2	16-QAM	108.0	120.0
12	2	16-QAM	162.0	180.0
13	2	64-QAM	216.0	240.0
14	2	64-QAM	243.0	270.0
15	2	64-QAM	270.0	300.0

Os índices MCS são classificados nos seguintes tipos:

- **Índices MCS obrigatórios:** índices MCS obrigatórios para um AP. Para associar-se a um AP 802.11n, um cliente deve suportar os índices MCS obrigatórios para o AP.
- **Índices MCS suportados:** índices MCS suportados por um AP, exceto os índices MCS obrigatórios. Se um cliente for compatível com os índices MCS obrigatórios e compatíveis, ele poderá usar uma taxa compatível para se comunicar com o AP.
- **Índice MCS multicast:** índice MCS para a taxa na qual um AP transmite quadros multicast.

***Obs.:** para obter todas as tabelas de taxa de dados MCS, consulte IEEE 802.11n-2009.*

5.4.7. VHT-MCS

O 802.11 ac usa índices VHT-MCS (Very High Throughput Modulation and Coding Scheme) para indicar as taxas de dados sem fio. Um VHT-MCS é identificado por um índice VHT-MCS, que é representado por um número inteiro no intervalo de 0 a 9. Um índice VHT-MCS é o mapeamento do VHT-MCS para uma taxa de dados.

O 802.11ac é compatível com os modos de largura de banda de 20 MHz, 40 MHz, 80 MHz e 160 MHz e com um máximo de oito fluxos espaciaisa mostram os parâmetros do VHT-MCS que são suportados por um AP.

5.4.7.1. Parâmetros do VHT-MCS (20 MHz, NSS=1)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	6.5	7.2
1	QPSK	13.0	14.4
2	QPSK	19.5	21.7
3	16-QAM	26.0	28.9
4	16-QAM	39.0	43.3
5	64-QAM	52.0	57.8
6	64-QAM	58.5	65.0
7	64-QAM	65.0	72.2
8	256-QAM	78.0	86.7
9		Não válido	

5.4.7.2. Parâmetros do VHT-MCS (20 MHz, NSS=2)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	13.0	14.4
1	QPSK	26.0	28.9
2	QPSK	39.0	43.3
3	16-QAM	52.0	57.8
4	16-QAM	78.0	86.7
5	64-QAM	104.0	115.6
6	64-QAM	117.0	130.0
7	64-QAM	130.0	144.4
8	256-QAM	156.0	173.3
9		Não válido	

5.4.7.3. Parâmetros do VHT-MCS (20 MHz, NSS=3)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	19.5	21.7
1	QPSK	39.0	43.3
2	QPSK	58.5	65.0
3	16-QAM	78.0	86.7
4	16-QAM	117.0	130.0
5	64-QAM	156.0	173.3
6	64-QAM	175.5	195.0
7	64-QAM	195.0	216.7
8	256-QAM	234.0	260.0
9	256-QAM	260.0	288.9

5.4.7.4. Parâmetros do VHT-MCS (20 MHz, NSS=4)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	26.0	28.9
1	QPSK	52.0	57.8
2	QPSK	78.0	86.7
3	16-QAM	104.0	115.6
4	16-QAM	156.0	173.3
5	64-QAM	208.0	231.1
6	64-QAM	234.0	260.0
7	64-QAM	260.0	288.9
8	256-QAM	312.0	346.7
9		Não válido	

5.4.7.5. Parâmetros do VHT-MCS (40 MHz, NSS=1)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	13.5	15.0
1	QPSK	27.0	30.0
2	QPSK	40.5	45.0
3	16-QAM	54.0	60.0
4	16-QAM	81.0	90.0
5	64-QAM	108.0	120.0
6	64-QAM	121.5	135.0
7	64-QAM	135.0	150.0
8	256-QAM	162.0	180.0
9	256-QAM	180.0	200.0

5.4.7.6. Parâmetros do VHT-MCS (40 MHz, NSS=2)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	27.0	30.0
1	QPSK	54.0	60.0
2	QPSK	81.0	90.0
3	16-QAM	108.0	120.0
4	16-QAM	162.0	180.0
5	64-QAM	216.0	240.0
6	64-QAM	243.0	270.0
7	64-QAM	270.0	300.0
8	256-QAM	324.0	360.0
9	256-QAM	360.0	400.0

5.4.7.7. Parâmetros do VHT-MCS (40 MHz, NSS=3)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	40.5	45.0
1	QPSK	81.0	90.0
2	QPSK	121.5	135.0
3	16-QAM	162.0	180.0
4	16-QAM	243.0	270.0
5	64-QAM	324.0	360.0
6	64-QAM	364.5	405.0
7	64-QAM	405.0	450.0
8	256-QAM	486.0	540.0
9	256-QAM	540.0	600.0

5.4.7.8. Parâmetros do VHT-MCS (40 MHz, NSS=4)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	54.0	60.0
1	QPSK	108.0	120.0
2	QPSK	162.0	180.0
3	16-QAM	216.0	240.0
4	16-QAM	324.0	360.0
5	64-QAM	432.0	480.0
6	64-QAM	486.0	540.0
7	64-QAM	540.0	600.0
8	256-QAM	648.0	720.0
9	256-QAM	720.0	800.0

5.4.7.9. Parâmetros do VHT-MCS (80 MHz, NSS=1)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	29.3	32.5
1	QPSK	58.5	65.0
2	QPSK	87.8	97.5
3	16-QAM	117.0	130.0
4	16-QAM	175.5	195.0
5	64-QAM	234.0	260.0
6	64-QAM	263.0	292.5
7	64-QAM	292.5	325.0
8	256-QAM	351.0	390.0
9	256-QAM	390.0	433.3

5.4.7.10. Parâmetros do VHT-MCS (80 MHz, NSS=2)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	58.5	65.0
1	QPSK	117.0	130.0
2	QPSK	175.5	195.0
3	16-QAM	234.0	260.0
4	16-QAM	351.0	390.0
5	64-QAM	468.0	520.0
6	64-QAM	526.5	585.0
7	64-QAM	585.0	650.0
8	256-QAM	702.0	780.0
9	256-QAM	780.0	866.7

5.4.7.11. Parâmetros do VHT-MCS (80 MHz, NSS=3)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	87.8	97.5
1	QPSK	175.5	195.0
2	QPSK	263.3	292.5
3	16-QAM	351.0	390.0
4	16-QAM	526.5	585.0
5	64-QAM	702.0	780.0
6		Não válido	
7	64-QAM	877.5	975.0
8	256-QAM	1053.0	1170.0
9	256-QAM	1170.0	1300.0

Parâmetros do VHT-MCS (80 MHz, NSS=4)

Índice VHT-MCS	Modulação	Taxa de dados (Mbps)	
		800ns GI	400ns GI
0	BPSK	117.0	130.0
1	QPSK	234.0	260.0
2	QPSK	351.0	390.0
3	16-QAM	468.0	520.0
4	16-QAM	702.0	780.0
5	64-QAM	936.0	1040.0
6	64-QAM	1053.0	1170.0
7	64-QAM	1170.0	1300.0
8	256-QAM	1404.0	1560.0
9	256-QAM	1560.0	1733.3

Os NSSs 802.11ac são classificados nos seguintes tipos:

- **NSSs obrigatórios:** NSSs obrigatórios para um AP. Para associar-se a um AP 802.11ac, um cliente deve oferecer suporte aos NSSs obrigatórios do AP.
- **NSSs suportados:** NSSs suportados por um AP, exceto os NSSs obrigatórios. Se um cliente for compatível com os NSSs obrigatórios e compatíveis, ele poderá usar uma taxa compatível para se comunicar com o AP.
- **NSS multicast:** um AP usa uma taxa na tabela de taxas de dados VHT-MCS para que o NSS transmita quadros multicast.

Obs.: *para obter todas as tabelas de taxa de dados do VHT-MCS, consulte IEEE 802.11ac-2013.*

5.4.8. HE-MCS

5.4.8.1. Tipos de HE-MCS

Os HE-MCSs 802.11ax são classificados nos seguintes tipos:

- **HE-MCSs obrigatórios:** HE-MCSs obrigatórios para um AP. Para associar-se a um AP 802.11ax, um cliente deve suportar os HE-MCSs obrigatórios para o AP.
- **HE-MCSs suportados:** HE-MCSs suportados por um AP além dos HE-MCSs obrigatórios. Se um cliente for compatível com os HE-MCSs obrigatórios e compatíveis, ele poderá usar uma taxa compatível para se comunicar com o AP.
- **Multicast:** HE-MCS-HE-MCS para a taxa na qual um AP transmite quadros multicast.

5.4.8.2. Parâmetros do HE-MCS

O HE-MCS (High Efficiency Modulation and Coding Scheme, esquema de modulação e codificação de alta eficiência) definido no IEEE 802.11ax determina as taxas de dados sem fio.

Um HE-MCS é identificado por um índice HE-MCS, que é representado por um número inteiro no intervalo de 0 a 11. Um índice HE-MCS é o mapeamento do HE-MCS para uma taxa de dados.

O 802.11ax é compatível com os modos de largura de banda de 20 MHz, 40 MHz, 80 MHz e 160 MHz (80+80 MHz) e com um máximo de oito fluxos espaciais. a mostram os parâmetros HE-MCS suportados por um AP.

5.4.8.3. Parâmetros do HE-MCS (20 MHz, NSS=1)

		Taxa de dados (Mbps)	
Índice HE-MCS	**Modulação**	**1600ns GI**	**800ns GI**
0	BPSK	8	8.6
1	QPSK	16	17.2
2	QPSK	24	25.8
3	16-QAM	33	34.4
4	16-QAM	49	51.6
5	64-QAM	65	68.8
6	64-QAM	73	77.4
7	64-QAM	81	86
8	256-QAM	98	103.2
9	256-QAM	108	114.7
10	1024-QAM	122	129
11	1024-QAM	135	143.4

5.4.8.4. Parâmetros do HE-MCS (20 MHz, NSS=2)

		Taxa de dados (Mbps)	
Índice HE-MCS	**Modulação**	**1600ns GI**	**800ns GI**
0	BPSK	16	17.2
1	QPSK	32	34.4
2	QPSK	48	51.6
3	16-QAM	66	68.8
4	16-QAM	98	103.2
5	64-QAM	130	137.6
6	64-QAM	146	154.8
7	64-QAM	162	172
8	256-QAM	196	206.4
9	256-QAM	216	229.4
10	1024-QAM	244	258
11	1024-QAM	270	286.8

5.4.8.5. Parâmetros do HE-MCS (20 MHz, NSS=3)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	24	25.8
1	QPSK	48	51.6
2	QPSK	72	77.4
3	16-QAM	99	103.2
4	16-QAM	147	154.8
5	64-QAM	195	206.4
6	64-QAM	219	232.2
7	64-QAM	243	258
8	256-QAM	294	309.6
9	256-QAM	324	344.1
10	1024-QAM	366	387
11	1024-QAM	405	430.2

5.4.8.6. Parâmetros do HE-MCS (20 MHz, NSS=4)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	32	34.4
1	QPSK	64	68.8
2	QPSK	96	103.2
3	16-QAM	132	137.6
4	16-QAM	196	206.4
5	64-QAM	260	275.2
6	64-QAM	292	309.6
7	64-QAM	324	344
8	256-QAM	392	412.8
9	256-QAM	432	458.8
10	1024-QAM	488	516
11	1024-QAM	540	573.6

5.4.8.7. Parâmetros do HE-MCS (40 MHz, NSS=1)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	16	17.2
1	QPSK	33	34.4
2	QPSK	49	51.6
3	16-QAM	65	68.8
4	16-QAM	98	103.2
5	64-QAM	130	137.6
6	64-QAM	146	154.9
7	64-QAM	163	172.1
8	256-QAM	195	206.5
9	256-QAM	217	229.4
10	1024-QAM	244	258.1
11	1024-QAM	271	286.8

5.4.8.8. Parâmetros do HE-MCS (40 MHz, NSS=2)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	32	34.4
1	QPSK	66	68.8
2	QPSK	98	103.2
3	16-QAM	130	137.6
4	16-QAM	196	206.4
5	64-QAM	260	275.2
6	64-QAM	292	309.8
7	64-QAM	326	344.2
8	256-QAM	390	413
9	256-QAM	434	458.8
10	1024-QAM	488	516.2
11	1024-QAM	542	573.6

5.4.8.9. Parâmetros do HE-MCS (40 MHz, NSS=3)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	48	51.6
1	QPSK	99	103.2
2	QPSK	147	154.8
3	16-QAM	195	206.4
4	16-QAM	294	309.6
5	64-QAM	390	412.8
6	64-QAM	438	464.7
7	64-QAM	489	516.3
8	256-QAM	585	619.5
9	256-QAM	651	688.2
10	1024-QAM	732	774.3
11	1024-QAM	813	860.4

5.4.8.10. Parâmetros do HE-MCS (40 MHz, NSS=4)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	64	68.8
1	QPSK	132	137.6
2	QPSK	196	206.4
3	16-QAM	260	275.2
4	16-QAM	392	412.8
5	64-QAM	520	550.4
6	64-QAM	584	619.6
7	64-QAM	652	688.4
8	256-QAM	780	826
9	256-QAM	868	917.6
10	1024-QAM	976	1032.4
11	1024-QAM	1084	1147.2

5.4.8.11. Parâmetros do HE-MCS (80 MHz, NSS=1)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	34	36
1	QPSK	68	72.1
2	QPSK	102	108.1
3	16-QAM	136	144.1
4	16-QAM	204	216.2
5	64-QAM	272	288.2
6	64-QAM	306	324.4
7	64-QAM	340	360.3
8	256-QAM	408	432.4
9	256-QAM	453	480.4
10	1024-QAM	510	540.4
11	1024-QAM	567	600.5

5.4.8.12. Parâmetros do HE-MCS (80 MHz, NSS=2)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	68	72
1	QPSK	136	144.2
2	QPSK	204	216.2
3	16-QAM	272	288.2
4	16-QAM	408	432.4
5	64-QAM	544	576.4
6	64-QAM	612	648.8
7	64-QAM	680	720.6
8	256-QAM	816	864.8
9	256-QAM	906	960.8
10	1024-QAM	1020	1080.8
11	1024-QAM	1134	1201

5.4.8.13. Parâmetros do HE-MCS (80 MHz, NSS=3)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	102	108
1	QPSK	204	216.3
2	QPSK	306	324.3
3	16-QAM	408	432.3
4	16-QAM	612	648.6
5	64-QAM	816	864.6
6	64-QAM	918	973.2
7	64-QAM	1020	1080.9
8	256-QAM	1224	1297.2
9	256-QAM	1359	1441.2
10	1024-QAM	1530	1621.2
11	1024-QAM	1701	1801.5

Parâmetros do HE-MCS (80 MHz, NSS=4)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	136	144
1	QPSK	272	288.4
2	QPSK	408	432.4
3	16-QAM	544	576.4
4	16-QAM	816	864.8
5	64-QAM	1088	1152.8
6	64-QAM	1224	1297.6
7	64-QAM	1360	1441.2
8	256-QAM	1632	1729.6
9	256-QAM	1812	1921.6
10	1024-QAM	2040	2161.6
11	1024-QAM	2268	2402

5.4.8.14. Parâmetros HE-MCS (160MHz/80MHz+80MHz, NSS=1)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	68	72.1
1	QPSK	136	144.1
2	QPSK	204	216.2
3	16-QAM	272	288.2
4	16-QAM	408	432.4
5	64-QAM	544	576.5
6	64-QAM	612	648.5
7	64-QAM	681	720.6
8	256-QAM	817	864.7
9	256-QAM	907	960.7
10	1024-QAM	1021	1080.9
11	1024-QAM	1134	1201

5.4.8.15. Parâmetros HE-MCS (160MHz/80MHz+80MHz, NSS=2)

Índice HE-MCS	Modulação	Taxa de dados (Mbps)	
		1600ns GI	800ns GI
0	BPSK	136	144.1
1	QPSK	272	288.2
2	QPSK	408	432.4
3	16-QAM	544	576.5
4	16-QAM	817	864.7
5	64-QAM	1089	1152.9
6	64-QAM	1225	1297.1
7	64-QAM	1361	1441.2
8	256-QAM	1633	1729.4
9	256-QAM	1815	1921.5
10	1024-QAM	2042	2161.8
11	1024-QAM	2269	2401.9

5.4.8.16. Parâmetros HE-MCS (160MHz/80MHz+80MHz, NSS=3)

		Taxa de dados (Mbps)	
Índice HE-MCS	**Modulação**	**1600ns GI**	**800ns GI**
0	BPSK	204	216.2
1	QPSK	408	432.4
2	QPSK	613	648.5
3	16-QAM	817	864.7
4	16-QAM	1225	1297.1
5	64-QAM	1633	1729.4
6	64-QAM	1838	1945.6
7	64-QAM	2042	2161.8
8	256-QAM	2450	2594.1
9	256-QAM	2722	2882.4
10	1024-QAM	3062	3242.6
11	1024-QAM	3403	3602.9

Parâmetros HE-MCS (160MHz/80MHz+80MHz, NSS=4)

		Taxa de dados (Mbps)	
Índice HE-MCS	**Modulação**	**1600ns GI**	**800ns GI**
0	BPSK	272	288.2
1	QPSK	544	576.5
2	QPSK	817	864.7
3	16-QAM	1089	1152.9
4	16-QAM	1633	1729.4
5	64-QAM	2178	2305.9
6	64-QAM	2450	2594.1
7	64-QAM	2722	2882.4
8	256-QAM	3267	3458.8
9	256-QAM	3630	3843.1
10	1024-QAM	4083	4323.5
11	1024-QAM	4537	4803.9

Obs.: *»* *Para obter todas as tabelas de taxa de dados HE-MCS, consulte o protocolo IEEE 802.11ax.*

- *» O suporte aos índices HE-MCS depende do modelo do AP.*
- *» O 802.11gax suporta apenas os modos de largura de banda de 20 MHz e 40 MHz.*

5.4.9. Funções básicas do rádio

5.4.9.1. Canal de trabalho

Especifique um canal de trabalho para reduzir a interferência de dispositivos sem fio e sem fio.

Você pode especificar manualmente um canal ou configurar o sistema para selecionar automaticamente um canal para um rádio.

Quando os sinais de radar são detectados no canal de trabalho de um rádio, ocorre um dos seguintes eventos:

- » Se o canal for um canal especificado manualmente, o rádio mudará imediatamente de canal e voltará ao canal especificado após 30 minutos e, em seguida, iniciará o temporizador de silêncio. Se nenhum sinal de radar for detectado dentro do tempo de silêncio, o rádio começará a usar o canal. Se forem detectados sinais de radar dentro do tempo de silêncio, o rádio mudará de canal.
- » Se o canal for um canal atribuído automaticamente, o sistema selecionará automaticamente um novo canal para o rádio e o rádio mudará imediatamente de canal.

5.4.9.2. Potência máxima de transmissão

O intervalo de potência de transmissão suportado por um rádio varia de acordo com o código do país, o canal, o modelo do AP, o modo de rádio, o tipo de antena e o modo de largura de banda. Se você alterar esses atributos de um rádio depois de definir a potência máxima de transmissão, a potência máxima de transmissão configurada poderá estar fora do intervalo de potência de transmissão suportado. Se isso acontecer, o sistema ajustará automaticamente a potência máxima de transmissão para um valor válido.

5.4.9.3. Bloqueio de energia

Se você ativar o TPC e, em seguida, ativar o bloqueio de energia, a energia selecionada mais recentemente será bloqueada para os APs. Depois que o CA for reiniciado, a energia bloqueada ainda terá efeito. Se um rádio ativado com bloqueio de energia mudar para um novo canal que forneça uma energia menor do que a energia bloqueada, a energia máxima suportada pelo novo canal entrará em vigor.

Para que o TPC funcione, certifique-se de que a energia não esteja bloqueada antes de ativar o TPC. Para obter mais informações sobre o TPC, consulte a página *Wireless Configuration> Radio Management> RRM.*

5.4.9.4. Taxas de transmissão

As taxas de transmissão são classificadas nos seguintes tipos:

- **Tarifas proibidas:** tarifas que não podem ser usadas por um AP.
- **Taxas obrigatórias:** taxas que os clientes devem suportar para se associar a um AP.
- **Taxa suportada:** as taxas suportadas por um AP. Depois que um cliente se associa a um AP, ele pode selecionar uma taxa mais alta dentre as taxas suportadas para se comunicar com o AP. O AP diminui automaticamente a taxa de transmissão quando os sinais de interferência aumentam e aumenta a taxa de transmissão quando os sinais de interferência diminuem.
- **Taxa de multicast:** taxa na qual um AP transmite multicasts. A taxa de multicast deve ser selecionada entre as taxas obrigatórias.

5.4.9.5. Tipo de preâmbulo

Importante: esse recurso é aplicável somente a rádios de banda de 2,4 GHz.

Um preâmbulo é um conjunto de bits em um cabeçalho de pacote para sincronizar os sinais de transmissão entre o remetente e o receptor. Um preâmbulo curto melhora o desempenho da rede e um preâmbulo longo garante a compatibilidade com todos os dispositivos Wireless dos primeiros modelos.

5.4.9.7. Distância de transmissão

A intensidade dos sinais Wireless diminui gradualmente à medida que a distância de transmissão aumenta. A distância máxima de transmissão dos sinais sem fio depende do ambiente ao redor e do uso ou não de uma antena externa.

- **Sem uma antena externa:** cerca de 300 metros (984,25 pés).
- **Com uma antena externa:** 30 km (18,64 milhas) a 50 km (31,07 milhas).
- **Em uma área com obstáculos:** 35 m (114,83 pés) a 50 m (164,04 pés).

5.4.9.8. Intervalo do sinalizador

Um AP transmite quadros de beacon em um intervalo especificado para permitir que ele mesmo seja detectado pelos clientes. Um intervalo curto de beacon permite que os clientes detectem facilmente o AP, mas consome mais recursos do sistema.

5.4.9.9. Serviços de acesso para clientes 802.11b

Para evitar que clientes 802.11b de baixa velocidade diminuam o desempenho da transmissão de dados sem fio, é possível ativar um rádio 802.11g ou 802.11gn para desativar os serviços de acesso para clientes 802.11b.

5.4.9.10. RTS threshold

O 802.11 permite que os dispositivos Wireless enviem pacotes Request to Send (RTS) ou Clear to Send (CTS) para evitar colisões. Entretanto, o excesso de pacotes RTS e CTS custa recursos do sistema e reduz a eficiência da transmissão. Você pode configurar um limite de RTS para resolver esse problema. O sistema executa a prevenção de colisões somente para pacotes maiores que o limite RTS.

Em uma WLAN de baixa densidade, aumente o limite de RTS para melhorar a taxa de transferência e a eficiência da rede. Em uma WLAN de alta densidade, diminua o limite de RTS para reduzir as colisões na rede.

5.4.9.11. 802.11g protection

Esse recurso é aplicável somente aos rádios 802.11g e 802.11n (2,4 GHz).

Quando existem clientes 802.11b e 802.11g em uma WLAN, pode ocorrer colisão de transmissão porque eles usam modos de modulação diferentes. A proteção 802.11g pode evitar isso. Ela permite que os dispositivos 802.11g ou 802.11n enviem pacotes RTS/CTS ou CTS-to-self para informar aos clientes 802.11b que devem adiar o acesso ao meio.

Os dispositivos 802.11g ou 802.11n enviam pacotes RTS/CTS ou CTS-to-self antes de enviar dados somente quando sinais 802.11b são detectados no canal.

A proteção 802.11g entra em vigor automaticamente quando clientes 802.11b se associam a um AP 802.11g ou 802.11n (2,4 GHz).

5.4.9.12. Limite de fragmentos

Os quadros maiores que o limite de fragmentação são fragmentados antes da transmissão. Os quadros menores que o limite de fragmentação são transmitidos sem fragmentação.

Quando um fragmento não é recebido, apenas esse fragmento, e não o quadro inteiro, é retransmitido. Em uma WLAN com grande interferência, diminua o limite de fragmentos para melhorar a taxa de transferência e a eficiência da rede.

5.4.10. Funções 802.11n

Importante: ao configurar funções 802.11n para um AP, sua configuração falhará se outro usuário estiver configurando funções 802.11n para o mesmo AP.

O IEEE 802.11n fornece serviços wireless de alta qualidade e permite que uma WLAN tenha o mesmo desempenho de rede que a Ethernet. O 802.11n melhora o rendimento e a taxa de transmissão da WLAN otimizando a camada física e a camada MAC.

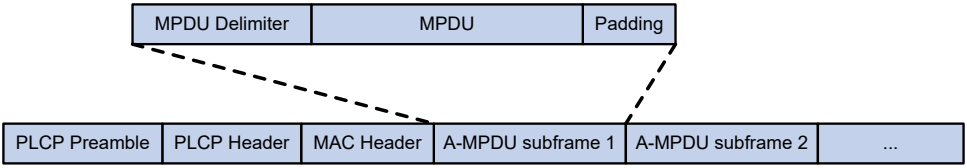
A camada física do 802.11n é baseada em OFDM. Essa camada permite alta taxa de transferência usando MIMO (Multiple Input, Multiple Output), largura de banda de 40 MHz, GI (Guard Interval) curto, STBC (Space-Time Block Coding) e LDPC (Low-Density Parity Check)

A camada MAC permite alta eficiência de transmissão usando A-MPDU, A-MSDU e Block Acknowledgment (BA).

5.4.10.1. Agregação de MPDU

Uma MPDU (MAC Protocol Data Unit, unidade de dados do protocolo MAC) é um quadro de dados no formato 802.11. A agregação de MPDU agrega várias MPDUs em uma MPDU agregada (A-MPDU) para reduzir informações adicionais, quadros ACK e sobrecarga de cabeçalho do procedimento de convergência da camada física (PLCP). Isso melhora a taxa de transferência da rede e a eficiência do canal.

Todas as MPDUs em uma A-MPDU devem ter a mesma prioridade de QoS, endereço de origem e endereço de destino.



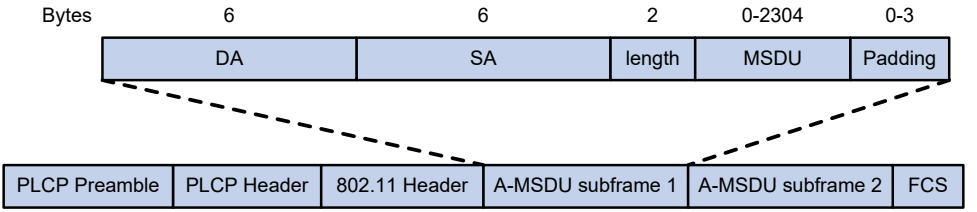
A-MPDU format

5.4.10.2. Agregação de MSDU

Um AP ou cliente encapsula uma unidade de dados de serviço MAC (MSDU) com um cabeçalho Ethernet e, em seguida, converte o quadro no formato 802.11 para encaminhamento.

A agregação de MSDU agrega várias MSDUs em uma única MSDU agregada (A-MSDU) para reduzir o preâmbulo do PLCP, o cabeçalho do PLCP e os excessos de cabeçalho do MAC. Isso melhora o rendimento da rede e a eficiência do encaminhamento de quadros.

Todas as MSDUs em uma A-MSDU devem ter a mesma prioridade de QoS, endereço de origem e endereço de destino. Quando um dispositivo recebe uma A-MSDU, ele restaura a A-MSDU em várias MSDUs para processamento.



Formato A-MSDU

5.4.10.3. GI curto

http://en.wikipedia.org/wiki/802.11 OFDM fragmenta quadros em blocos de dados para transmissão. Ele usa o GI para garantir que as transmissões de blocos de dados não interfiram umas nas outras e sejam imunes a atrasos na transmissão.

O IG usado pelo 802.11a/g é de 800 ns. O site http://en.wikipedia.org/wiki/802.11n suporta um IG curto de 400 ns, o que proporciona um aumento de 10% na taxa de dados.

Os modos de largura de banda de 20 MHz e 40 MHz suportam GI curto.

5.4.10.4. LDPC

O 802.11n introduz o mecanismo LDPC (Low-Density Parity Check, verificação de paridade de baixa densidade) para aumentar a relação sinal-ruído e melhorar a qualidade da transmissão. O LDPC entra em vigor somente quando ambas as extremidades suportam o LDPC.

5.4.10.5. STBC

O mecanismo STBC (Space-Time Block Coding) aumenta a confiabilidade da transmissão de dados e não exige que os clientes tenham altas taxas de transmissão.

5.4.10.6. Índices MSC

Os clientes 802.11n usam a taxa correspondente ao índice MCS para enviar quadros unicast. Os clientes não 802.11n usam a taxa 802.11a/b/g para enviar quadros unicast.

5.4.10.7. O recurso dot11n-only do cliente

O recurso cliente dot11n-only permite que um AP aceite apenas clientes 802.11n e 802.11ac. Use esse recurso para evitar que clientes 802.11a/b/g de baixa velocidade diminuam o desempenho da transmissão de dados sem fio.

5.4.10.8. Modo de largura de banda 802.11n

O 802.11n usa a estrutura de canal do 802.11a/b/g, mas aumenta o número de subcanais de dados em cada canal de 20 MHz para 52. Isso melhora a taxa de transmissão de dados.

O 802.11n une dois canais adjacentes de 20 MHz para formar um canal de 40 MHz (um canal primário e um canal secundário). Isso proporciona uma maneira simples de dobrar a taxa de dados.

A largura de banda de um rádio varia de acordo com a configuração do modo de largura de banda e a capacidade do chip.

5.4.10.9. Modos MIMO

O MIMO (Multiple-input and multiple-output) permite que um rádio envie e receba sinais Wireless por meio de vários fluxos espaciais. Isso melhora a capacidade do sistema e o uso do espectro sem exigir maior largura de banda.

Um rádio pode operar em um dos seguintes modos MIMO:

- 1×1 - envia e recebe sinais Wireless por meio de um fluxo espacial.
- 2×2 - Envia e recebe sinais Wireless por meio de dois fluxos espaciais.
- 3×3 - envia e recebe sinais Wireless por meio de três fluxos espaciais.
- 4×4 - envia e recebe sinais Wireless por meio de quatro fluxos espaciais.
- 5×5 - envia e recebe sinais Wireless por meio de cinco fluxos espaciais.
- 6×6 - envia e recebe sinais Wireless por meio de seis fluxos espaciais.
- 7×7 - envia e recebe sinais Wireless por meio de sete fluxos espaciais.
- 8×8 - envia e recebe sinais Wireless por meio de oito fluxos espaciais.

O número de fluxos espaciais suportados por um rádio varia de acordo com o modelo do dispositivo.

5.4.10.10. Economia de energia

O recurso de economia de energia permite que um AP altere automaticamente o modo MIMO de um rádio para 1×1 se nenhum cliente se associar ao rádio.

5.4.10.11. 802.11n protection

Quando existem clientes 802.11n e não 802.11n em uma WLAN, pode ocorrer colisão de transmissão porque eles usam modos de modulação diferentes. A proteção 802.11n pode evitar isso. Ela permite que os dispositivos 802.11n enviem pacotes RTS/CTS ou CTS-to-self para informar aos clientes não 802.11n que devem adiar o acesso ao meio.

Os dispositivos 802.11n enviam pacotes RTS/CTS ou CTS-to-self antes de enviar dados somente quando sinais não 802.11n são detectados no canal.

A proteção 802.11n entra em vigor automaticamente quando clientes não 802.11n se associam a um AP 802.11n, 802.11ac ou 802.11ax.

Obs.: *os dispositivos 802.11n referem-se aos dispositivos 802.11n, 802.11ac e 802.11ax.*

5.4.10.12. O recurso de antena inteligente

Importante: o suporte a esse recurso depende do modelo do AP. Esse recurso é aplicável somente aos rádios 802.11n e 802.11ac.

O recurso de antena inteligente permite que um AP ajuste automaticamente os parâmetros da antena com base na localização do cliente e nas informações do canal para melhorar a qualidade e a estabilidade do sinal.

Você pode configurar um rádio para operar em um dos seguintes modos de antena inteligente:

- **Automático:** usa o modo de alta disponibilidade para pacotes de áudio e vídeo e usa o modo de alta taxa de transferência para outros pacotes.
- **Alta disponibilidade:** aplicável a WLANs que exigem largura de banda estável, esse modo reduz os impactos de ruído e interferência e fornece largura de banda garantida para os clientes.
- **High-throughput:** aplicável a WLANs que exigem alto desempenho, esse modo aumenta a intensidade do sinal e a capacidade de associação.

5.4.11. Funções 802.11ac

Importante: ao configurar funções 802.11ac para um AP, sua configuração falhará se outro usuário estiver configurando funções 802.11ac para o mesmo AP.

Baseado no 802.11n, o 802.11ac aumenta ainda mais a taxa de transmissão de dados e melhora o desempenho da rede, fornecendo maior largura de banda, mais fluxos espaciais e esquemas de modulação mais avançados.

5.4.12.1. NSSs

Se o AP for compatível com um NSS, ele será compatível com todos os índices VHT-MCS para o NSS.

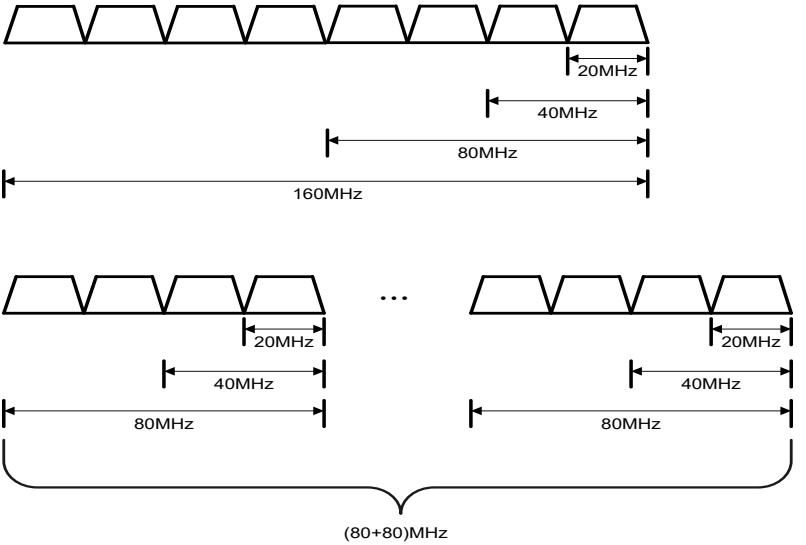
Os clientes 802.11ac usam a taxa correspondente ao índice VHT-MCS para que o NSS envie quadros unicast. Os clientes não 802.11ac usam a taxa 802.11a/b/g/n para enviar quadros unicast.

5.4.12.2. Cliente dot11ac-only

Para evitar que clientes 802.11a/b/g/n de baixa velocidade diminuam o desempenho da transmissão de dados sem fio, é possível ativar o recurso client dot11ac-only para que um AP aceite apenas clientes 802.11ac.

5.4.12.3. Modo de largura de banda 802.11ac

O 802.11ac usa a estrutura de canais do 802.11n e aumenta a largura de banda máxima de 40 MHz para 80 MHz/160 MHz. O 802.11ac pode vincular dois canais adjacentes de 20 MHz para formar um canal de 40 MHz, vincular dois canais adjacentes de 40 MHz para formar um canal de 80 MHz e vincular dois canais adjacentes de 80 MHz para formar um canal de 160 MHz.



Modos de largura de banda 802.11ac

5.4.13. 802.11ax funções

Importante!

- Ao configurar as funções 802.11ax para um AP, sua configuração falhará se outro usuário estiver configurando funções 802.11ax para o mesmo AP.
- Algumas NICs sem fio da Intel podem não conseguir detectar os sinais sem fio enviados pelos rádios 802.11ax. Nesse caso, atualize o driver da placa de rede.

5.4.14.1. NSS

Os clientes não 802.11ax usam a taxa 802.11a/b/g/n/ac para enviar quadros unicast.

Se um AP for compatível com um NSS, ele será compatível com todos os índices HE-MCS para o NSS. Clientes 802.11ax que usam a taxa correspondente ao índice HE-MCS para o NSS para enviar quadros unicast.

Se você não definir um NSS multicast, os clientes 802.11ax e o AP usarão a taxa multicast 802.11a/b/g/n/ac para enviar quadros multicast. Se você definir um NSS multicast e especificar um índice HE-MCS, ocorrerão as seguintes situações:

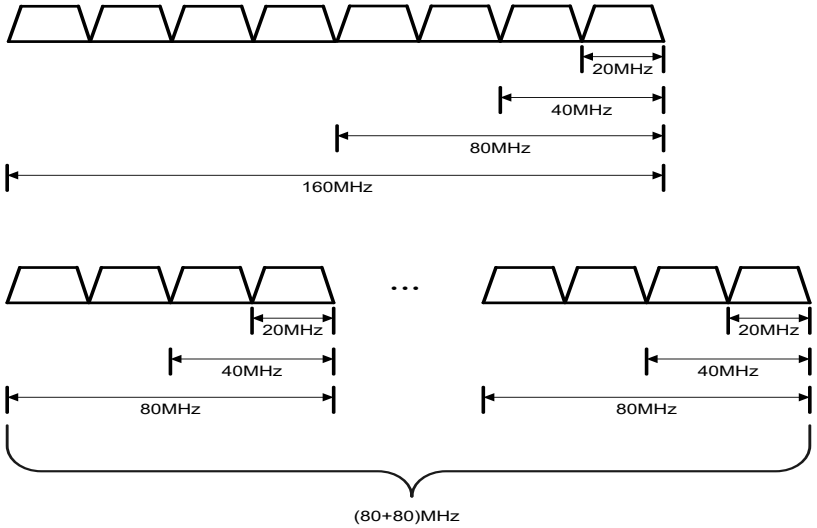
- O AP e os clientes usam a taxa correspondente ao índice HE-MCS para enviar quadros multicast se todos os clientes forem clientes 802.11ax.
- O AP e os clientes usam a taxa multicast 802.11a/b/g/n/ac para enviar quadros multicast se houver clientes não 802.11ax.

O NSS máximo suportado não pode ser menor que o NSS máximo obrigatório e o NSS multicast não pode ser maior que o NSS máximo obrigatório.

O NSS obrigatório máximo ou o NSS compatível determina um intervalo de taxas 802.11. Por exemplo, se o NSS máximo obrigatório for 5, as taxas correspondentes aos índices HE-MCS dos NSSs 1 a 5 serão taxas obrigatórias 802.11ax.

5.4.14.2. 802.11ax modo de largura de banda

O 802.11ax usa a estrutura de canal do 802.11n e aumenta a largura de banda máxima de 40 MHz para 160 MHz. O 802.11ax pode unir dois canais adjacentes de 20/40/80 MHz para formar um canal de 40/80/160 MHz. O 802.11gax suporta apenas 20 MHz e 40 MHz.

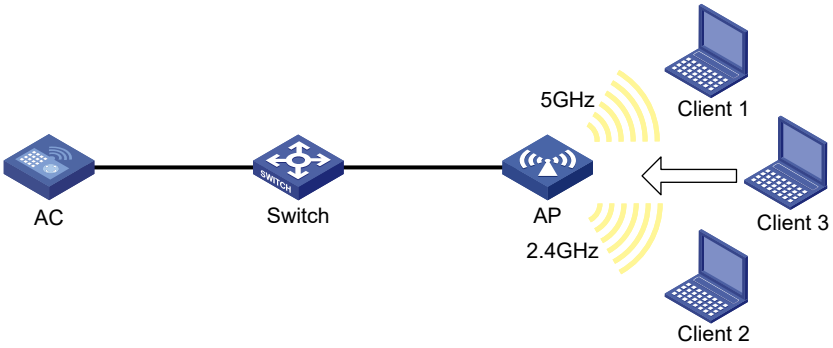


Modos de largura de banda 802.11ax

5.4.15. Navegação da banda

A navegação em banda permite que um AP direcione clientes de banda dupla (2,4 GHz e 5 GHz) para o rádio de 5 GHz sempre que possível para evitar o congestionamento típico na banda de 2,4 GHz. Isso pode equilibrar a carga dos rádios e melhorar o desempenho da rede.

Conforme mostrado em , a navegação em banda está ativada na WLAN. O Cliente 1 está associado ao rádio de 5 GHz e o Cliente 2 está associado ao rádio de 2,4 GHz. Quando o cliente de banda dupla Cliente 3 solicita a associação com o rádio de 2,4 GHz, o AP rejeita o Cliente 3 e o direciona para o rádio de 5 GHz.



Navegação da banda

5.5. Segurança Wireless

5.5.1. WIPS

O WIPS (Wireless Intrusion Prevention System) ajuda a monitorar a WLAN, detectar ataques e dispositivos não autorizados e tomar contramedidas. O WIPS oferece uma solução completa para a segurança da WLAN.

O WIPS contém o módulo de gerenciamento de rede, o AC e os sensores (APs habilitados com o WIPS). Eles oferecem as seguintes funções:

- Os sensores monitoram a WLAN, coletam informações sobre o canal e relatam as informações ao AC para análise posterior
- O AC determina ataques e dispositivos não autorizados, toma contramedidas e aciona alarmes
- O módulo de gerenciamento de rede permite que você configure o WIPS na interface da Web. Ele fornece funções de gerenciamento de configuração, geração de relatórios e gerenciamento de alarmes.

O WIPS oferece os seguintes recursos:

- **Detecção de ataques:** o WIPS detecta ataques ao escutar quadros 802.11 e aciona alarmes para notificar o administrador.
- **Classificação de dispositivos:** o WIPS identifica os dispositivos Wireless ouvindo os quadros 802.11 e classifica os dispositivos com base nas regras de classificação.
- **Contramedidas:** o WIPS permite que você tome contramedidas contra dispositivos desonestos.

5.5.1.1. Ativação do WIPS

Antes de ativar o WIPS para um rádio de um AP, você deve adicionar o AP a um domínio de segurança virtual (VSD).

5.5.1.2. VSD

Você pode aplicar uma política de classificação, uma política de detecção de ataques, uma política de assinatura ou uma política de contramedida a um VSD para permitir que a política entre em vigor nos rádios do VSD.

5.5.1.3. Classificação do dispositivo

Política de classificação

Você pode habilitar o WIPS para classificar dispositivos usando um dos seguintes métodos:

- **Classificação automática:** o WIPS classifica automaticamente os dispositivos adicionando os endereços MAC, OUIs ou SSIDs dos dispositivos às listas especificadas. O WIPS também permite classificar APs usando regras de classificação de APs definidas pelo usuário.
- **Classificação manual:** você especifica manualmente uma categoria para um dispositivo. A classificação manual é aplicável apenas a APs.

Se você configurar a classificação automática e a classificação manual, a classificação manual terá efeito.

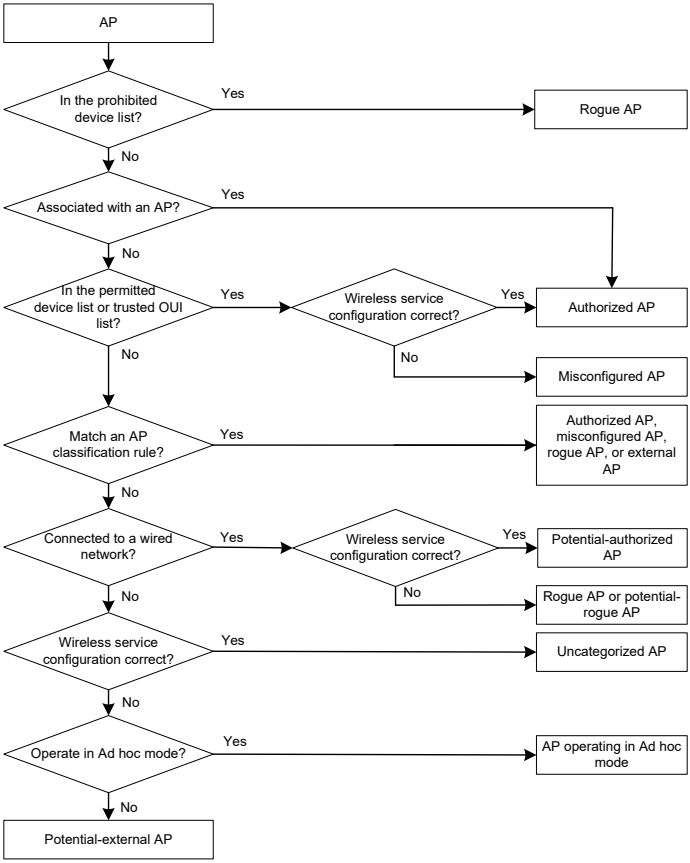
Classificação AP

Conforme mostrado na , o WIPS classifica os APs detectados de acordo com as regras de classificação predefinidas.

Categoria	Descrição	Regra de classificação
AP autorizado	Um AP que é permitido na WLAN.	Não está na lista de dispositivos proibidos. Foi conectado ao AC. Configurado como um AP autorizado.
Rogue AP	Um AP que não pode ser usado na WLAN.	Na lista de dispositivos proibidos. Não no arquivo de configuração da OUI. Configurado como um AP desonesto.
AP mal configurado	Um AP que pode ser usado na WLAN, mas que tem uma configuração incorreta.	Na lista de dispositivos permitidos, mas com um SSID incorreto. Não na lista de dispositivos proibidos, mas no arquivo de configuração da OUI. Na lista de OUIs confiáveis ou na lista de dispositivos permitidos, mas não conectado ao AC.
AP externo	Um AP que está em uma WLAN adjacente.	N/A

Categoria	Descrição	Regra de classificação
Ad hoc	Um AP operando no modo Ad hoc. O WIPS detecta APs Ad hoc ouvindo os quadros de beacon.	N/A
AP potencialmente autorizado	Um AP que possivelmente está autorizado.	Não está em nenhuma das listas a seguir: Lista de dispositivos permitidos. Lista de dispositivos proibidos. Lista de OUIs confiáveis.
AP potencialmente desonesto	Um AP que possivelmente é um AP desonesto.	Tem configuração Wireless incorreta e não está em nenhuma das listas a seguir: Lista de dispositivos permitidos. Lista de dispositivos proibidos. Lista de OUIs confiáveis. Se a porta com fio em um AP tiver sido conectada à rede, o AP é um AP desonesto.
AP potencial-externo	Um AP que possivelmente é um AP externo.	Possui configuração incorreta do serviço Wireless. A porta com fio não foi conectada à rede. Não está em nenhuma das listas a seguir: Lista de dispositivos permitidos. Lista de dispositivos proibidos. Lista de OUIs confiáveis.
AP sem categoria	Um AP cuja categoria não pode ser determinada.	N/A

O WIPS classifica os APs detectados seguindo o procedimento mostrado em *Fluxo de classificação AP.*

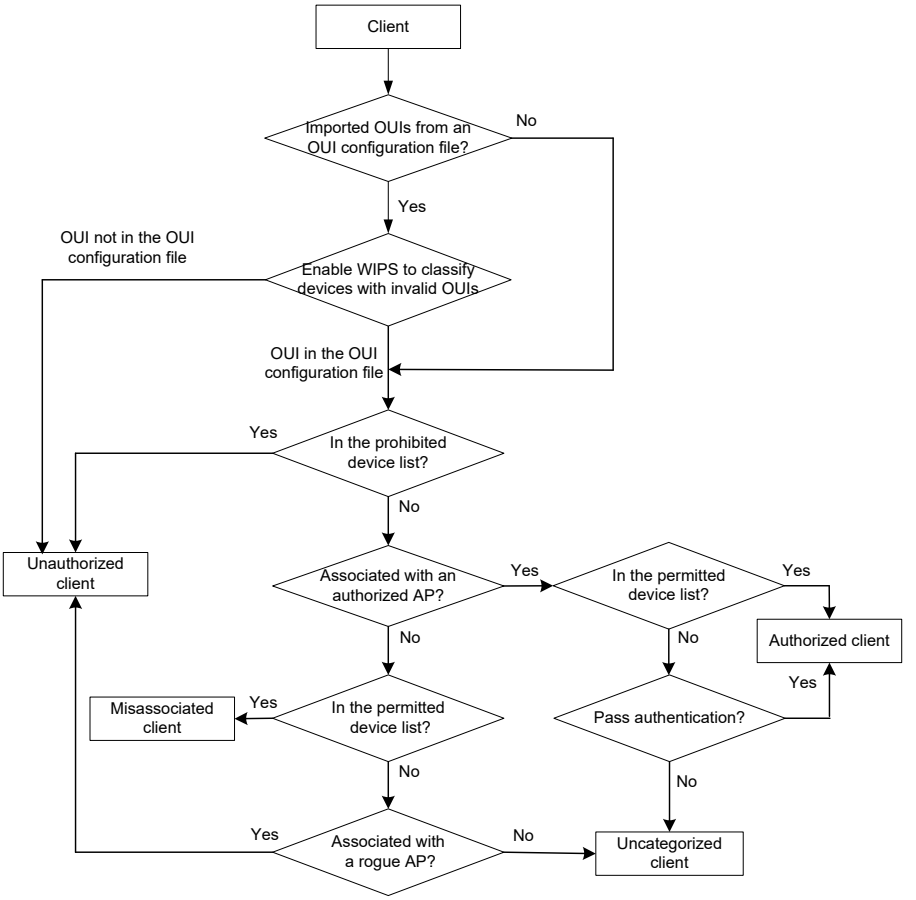


Classificação de clientes

Conforme mostrado em , o WIPS classifica os clientes detectados de acordo com as regras de classificação predefinidas.

Categoria	Descrição	Regra de classificação
Cliente autorizado	Um cliente que é permitido na WLAN.	Na lista de dispositivos permitidos e associados a um AP autorizado. Foi aprovado na autenticação e está associado a um AP autorizado.
Cliente não autorizado	Um cliente que não pode ser usado na WLAN.	Na lista de dispositivos proibidos. Associado a um AP desonesto. Não no arquivo de configuração da OUI.
Cliente associado incorretamente	Um cliente que está associado a um AP não autorizado.	Na lista de dispositivos permitidos, mas associado a um AP não autorizado. Um cliente mal associado pode trazer ameaças à segurança da rede.
Cliente sem categoria	Um cliente cuja categoria não pode ser determinada.	N/A

O WIPS classifica os clientes detectados seguindo o procedimento mostrado em *Fluxo de classificação de clientes*.



5.5.1.4. Detecção de ataques

O WIPS detecta ataques ouvindo os quadros 802.11 e dispara alarmes para notificar o administrador.

Detecção de ataque de entrada de dispositivo

Os invasores podem enviar pacotes inválidos ao WIPS para aumentar os custos de processamento. O WIPS examina periodicamente as entradas de dispositivos aprendidas para determinar se deve limitar a taxa de aprendizagem de entradas de dispositivos. Se o número de entradas de AP ou cliente aprendidas dentro do intervalo especificado exceder o limite, o WIPS aciona um alarme e para de aprender novas entradas.

Detecção de ataques de inundação

Um AP pode estar enfrentando um ataque de inundação se receber um grande número de quadros do mesmo tipo em um curto período de tempo. Para evitar que o AP fique sobrecarregado, o WIPS examina periodicamente as estatísticas dos pacotes recebidos e emite alarmes quando detecta um ataque de inundação suspeito. O WIPS pode detectar os seguintes ataques de inundação:

- **Ataque de inundação de solicitação de sonda/solicitação de associação/solicitação de reassociação:** inunda a tabela de associação de um AP imitando muitos clientes que enviam solicitações de sonda/solicitação de associação/solicitação de reassociação ao AP.
- **Ataque de inundação de solicitação de autenticação:** inunda a tabela de associação de um AP imitando muitos clientes que enviam solicitações de autenticação para o AP.
- **Ataque de inundação de beacon:** inunda quadros de beacon imitando um grande número de APs falsos para interromper a associação de clientes.
- **Ataque de inundação de Block Ack:** inunda quadros de Block Ack no AP para interromper a operação do mecanismo de Block Ack.
- **Ataque de inundação de RTS/CTS:** inunda quadros RTS/CTS para reservar o meio de RF e forçar outros dispositivos Wireless que compartilham o meio de RF a reter suas transmissões. Esse ataque tira proveito das vulnerabilidades do mecanismo de portadora virtual.
- **Ataque de inundação de desautenticação por broadcast/unicast:** envia frames de desautenticação do AP para os clientes associados para desassociar os clientes do AP. Esse ataque pode encerrar rapidamente os serviços sem fio para vários clientes.
- **Ataque de inundação de desassociação por difusão/unicast:** envia quadros de desassociação do AP para os clientes associados para desassociar os clientes do AP. Esse ataque pode encerrar rapidamente os serviços sem fio para vários clientes.
- Ataque **de inundação EAPOL-start:** esgota os recursos do AP imitando muitos clientes que enviam quadros EAPOL-start definidos no IEEE 802.1X para o AP.
- **Ataque de inundação de dados nulos:** envia quadros de dados nulos de um cliente para o AP. O AP determina que o cliente está no modo de economia de energia e armazena quadros em buffer para o cliente. Quando o tempo de envelhecimento dos quadros armazenados em buffer expira, o AP descarta os quadros. Isso interrompe a comunicação do cliente com o AP.
- Ataque **de inundação EAPOL-logoff: o** padrão IEEE 802.1X define o protocolo de autenticação usando o protocolo EAPOL (Extensible Authentication Protocol over LANs). Um cliente precisa enviar um quadro EAPOL-logoff para encerrar a sessão com um AP. Os quadros EAPOL-logoff não são autenticados, e um invasor pode falsificar quadros EAPOL-logoff para desassociar um cliente.
- Ataque **de inundação de EAP-success/failure:** em uma WLAN que usa a autenticação 802.1X, um AP envia um quadro EAP-success ou EAP-failure a um cliente para informar o sucesso ou a falha da autenticação. Um invasor pode falsificar o endereço MAC de um AP para enviar quadros EAP-success ou EAP-failure a um cliente e interromper o processo de autenticação.

Detecção de pacotes malformados

O WIPS determina que um quadro está malformado se o quadro corresponder aos critérios mostrados na e, em seguida, aciona alarmes e registros. O WIPS pode detectar 16 tipos de pacotes malformados.

Tipo de detecção	Molduras aplicáveis	Critérios de correspondência
Detecção de IE duplicado	Todos os quadros de gerenciamento	IE duplicado. Esse tipo de detecção não se aplica a IEs definidos pelo fornecedor.
Detecção de FATA-Jack	Quadros de autenticação	O valor do número do algoritmo de autenticação é 2.
Detecção de configuração anormal de IBSS e ESS	Quadros de farol Quadros de resposta da sonda	Tanto o IBSS quanto o ESS são definidos como 1.
Detecção de endereço de origem inválido	Todos os quadros de gerenciamento	O TO DS é 1, indicando que o quadro é enviado ao AP por um cliente. O endereço MAC de origem do quadro é um endereço multicast ou broadcast.
Detecção de quadros de solicitação de associação malformados	Quadros de solicitação de associação	O comprimento do quadro é 0.
Detecção de quadros de solicitação de autenticação malformados	Quadros de solicitação de autenticação	O número do algoritmo de autenticação não está em conformidade com o protocolo 802.11 e é maior que 3. O número de sequência da transação de autenticação é 1 e o código de status não é 0. O número de sequência da transação de autenticação é maior que 4.
Detecção de código de desautenticação inválido	Quadros de desautenticação	O código de motivo é 0 ou está no intervalo de 67 a 65535.
Detecção de código de desassociação inválido	Quadros de dissociação	O código de motivo é 0 ou está no intervalo de 67 a 65535.
Detecção de IE HT malformado	Quadros de farol Respostas da sonda Respostas da associação Solicitações de reassociação	O valor de economia de energia SM para o IE de recursos HT é 2. O valor de deslocamento do canal secundário para o IE de operação HT é 2.
Detecção de comprimento de IE inválido	Todos os quadros de gerenciamento	O comprimento do IE não está em conformidade com o protocolo 802.11.
Detecção de comprimento de pacote inválido	Todos os quadros de gerenciamento	O comprimento restante do IE não é zero depois que a carga útil do pacote é resolvida.
Detecção de quadros de resposta de sonda malformados	Quadros de resposta da sonda	O quadro não é um quadro de malha e seu comprimento de SSID é 0.
Detecção de chaves EAPOL superdimensionadas	Quadros de chaves EAPOL	O TO DS é 1 e o comprimento da chave é maior que 0.
Detecção de SSID superdimensionado	Quadros de farol Solicitações de sondagem Respostas da sonda Quadros de solicitação de associação	O comprimento do SSID é maior que 32.
Detecção de IE redundante	Todos os quadros de gerenciamento	O IE não é um IE necessário para o quadro e não é um IE reservado.
Detecção de duração superdimensionada	Quadros de gerenciamento unicast Quadros de dados unicast Quadros RTS, CTS e ACK	O valor da duração do pacote é maior do que o limite especificado.

Detecção de ataques

- **Detecção de ataques de falsificação:** em um ataque de falsificação, o invasor envia quadros em nome de outro dispositivo para ameaçar a rede. O WIPS suporta a detecção dos seguintes ataques de falsificação:
  - **Falsificação de quadros:** um AP falso falsifica um AP autorizado para enviar quadros de resposta de beacon ou sonda para induzir os clientes a se associarem a ele.
  - **Falsificação do endereço MAC do AP:** um cliente falsifica um AP autorizado para enviar quadros de desautenticação ou desassociação a outros clientes. Isso pode fazer com que os clientes fiquem off-line e afetar a operação correta da WLAN.
  - **Falsificação de endereço MAC de cliente:** um AP falso falsifica um cliente autorizado para se associar a um AP autorizado.
- **Detecção de IV fraca:** quando o algoritmo de criptografia RC4, usado pelo protocolo de segurança WEP, usa um IV inseguro, é mais provável que a chave WEP seja quebrada. Esse IV inseguro é chamado de IV fraco. O WIPS evita esse tipo de ataque detectando o IV em cada pacote WEP.
- **Detecção de ponte do Windows:** quando um cliente sem fio conectado a uma rede com fio estabelece uma ponte do Windows por meio da placa de rede com fio, o cliente pode fazer a ponte entre um AP externo e a rede interna. Isso pode trazer problemas de segurança para a rede interna. O WIPS detecta as pontes do Windows analisando os quadros de dados enviados pelos clientes associados.
- **Detecção em clientes com o modo de largura de banda de 40 MHz desativado:** os dispositivos 802.11n suportam os modos de largura de banda de 20 MHz e 40 MHz. Se o modo de largura de banda de 40 MHz estiver desativado em um cliente, outros clientes associados ao mesmo AP que o cliente também deverão usar a largura de banda de 20 MHz. Isso afeta a taxa de transferência e a eficiência da rede. O WIPS detecta esses clientes por meio da detecção de quadros de solicitação de sondagem enviados pelos clientes.
- **Omerta detecção de ataques:** omerta é uma ferramenta de ataque DoS baseada no protocolo 802.11. Ele envia quadros de desassociação com o código de motivo 0x01 para desassociar clientes. O código de motivo 0x01 indica um motivo de desassociação desconhecido. O WIPS detecta ataques Omerta detectando o código de motivo de cada quadro de dissociação.
- **Detecção de dispositivos não criptografados:** um AP ou cliente autorizado que esteja transmitindo quadros não criptografados pode trazer problemas de segurança para a rede. O WIPS detecta dispositivos não criptografados analisando os quadros enviados por APs ou clientes autorizados.
- **Detecção de ataque de ponto de acesso:** um invasor configura um AP desonesto com o mesmo SSID de um ponto de acesso para atrair os clientes a se associarem a ele. Depois que os clientes se associam ao AP malicioso, o invasor inicia outros ataques para obter informações do cliente. Você pode configurar um arquivo de hotspot para permitir que o WIPS detecte ataques de hotspot.
- **Detecção de AP HT-greenfield:** um AP operando no modo HT-greenfield pode causar colisões, erros e retransmissões porque não pode se comunicar com dispositivos 802.11a/b/g. O WIPS detecta APs HT-greenfield analisando os quadros de beacon ou os quadros de resposta de sonda enviados pelos APs.
- **Detecção de ataques DoS de associação/reassociação:** um ataque DoS de associação/reassociação inunda a tabela de associação de um AP imitando muitos clientes que enviam solicitações de associação ao AP. Quando o número de entradas na tabela atinge o limite superior, o AP não pode processar solicitações de clientes legítimos.
- **Detecção de ataques MITM:** em um ataque MITM, o invasor configura um AP desonesto e atrai um cliente para se associar a ele. Em seguida, o AP desonesto falsifica o endereço MAC do cliente para se associar ao AP autorizado. Quando o cliente e o AP autorizado se comunicam, o AP desonesto captura os pacotes do cliente e do AP autorizado. O AP desonesto pode modificar os quadros e obter as informações do quadro. O WIPS detecta ataques MITM ao detectar clientes que estão desassociados de um AP autorizado e associados a um AP honeypot.
- **Detecção de ponte Wireless:** um invasor pode invadir as redes internas por meio de uma ponte Wireless. Ao detectar uma ponte sem fio, o WIPS gera um alarme. Se a ponte sem fio estiver em uma rede mesh, o WIPS registrará o link mesh.
- **Detecção de mudança de canal do AP:** o WIPS detecta os eventos de mudança de canal para APs na WLAN.
- **Detecção de ataque de desassociação/desautenticação de transmissão:** um invasor falsifica um AP legítimo para enviar um quadro de desassociação ou desautenticação de broadcast para desconectar todos os clientes associados ao AP.
- **Detecção de ataque de personificação de AP:** em um ataque de personificação de AP, um AP mal-intencionado que tem o mesmo BSSID e ESSID que um AP legítimo atrai os clientes a se associarem a ele. Em seguida, esse AP falso inicia ataques a pontos de acesso ou engana o sistema de detecção. O WIPS detecta ataques de personificação de APs detectando o intervalo em que um AP envia quadros de beacon.
- **Detecção de ataque de inundação de AP:** o WIPS detecta o número de APs na WLAN e aciona um alarme para um ataque de inundação de APs quando o número de APs excede o limite especificado.

- **Detecção de AP de honeypot:** em um ataque de AP honeypot, o invasor configura um AP malicioso para atrair os clientes a se associarem a ele. O SSID do AP malicioso é semelhante ao SSID de um AP legítimo. Depois que um cliente se associa a um AP honeypot, o AP honeypot inicia outros ataques, como varredura de portas ou autenticação falsa para obter informações do cliente. O WIPS detecta APs honeypot detectando SSIDs de APs externos. Se a semelhança entre o SSID de um AP externo e o SSID de um AP legítimo atingir o limite especificado, o WIPS gera um alarme.
- **Detecção de ataque de economia de energia:** um invasor falsifica o endereço MAC de um cliente para enviar quadros de economia de energia a um AP. O AP armazena em cache os quadros para o cliente. O cliente atacado não pode receber quadros de dados porque o AP determina que o cliente ainda está no modo de economia de energia. Quando o tempo de envelhecimento dos quadros armazenados em cache expira, o AP descarta os quadros. O WIPS detecta ataques de economia de energia determinando a proporção de quadros com economia de energia em relação a quadros sem economia de energia.
- **Detecção suave de AP:** um soft AP refere-se a um cliente que atua como um AP e fornece serviços Wireless. Um invasor pode acessar a rede interna por meio de um soft AP e, em seguida, iniciar outros ataques. O WIPS detecta soft APs detectando o intervalo em que um dispositivo alterna suas funções entre cliente e AP.
- **Detecção de canal proibido:** depois que você configurar uma lista de canais permitidos e ativar a detecção de canais proibidos, o WIPS determinará que os canais que não estão na lista de canais permitidos são canais proibidos.

5.5.1.5. Detecção de ataques definidos pelo usuário com base na assinatura s

O WIPS oferece detecção de ataques definidos pelo usuário com base em assinaturas. Uma assinatura contém um método de identificação de pacotes e ações a serem tomadas em relação aos pacotes correspondentes. O sensor compara os pacotes detectados com a assinatura e executa as ações definidas na assinatura se um pacote corresponder à assinatura.

Uma assinatura pode conter no máximo seis subassinaturas, que podem ser definidas com base no tipo de quadro, endereço MAC, ID serial, comprimento do SSID, SSID e padrão de quadro. Um pacote corresponde a uma assinatura somente quando corresponde a todas as subassinaturas da assinatura.

5.5.1.6. Políticas de contramedidas

Os dispositivos não autorizados são suscetíveis a ataques e podem trazer problemas de segurança para a WLAN. O WIPS permite que você tome contramedidas contra dispositivos desonestos.

5.5.1.7. Lista de dispositivos ignorados por alarme

Para dispositivos Wireless em uma lista de dispositivos ignorados por alarme, o WIPS apenas os monitora, mas não aciona nenhum alarme.

5.5.2. Recursos de lista branca e lista negra

É possível configurar a lista de permissões ou as listas negras para filtrar quadros de clientes WLAN e implementar o controle de acesso de clientes. Os endereços MAC de multicast e broadcast não podem ser adicionados à lista branca ou à lista negra.

- **Whitelist:** contém os endereços MAC de todos os clientes que têm permissão para acessar a WLAN. Os quadros de clientes que não estão na lista de permissões são descartados. Essa lista é configurada manualmente.
- **Lista negra estática:** contém os endereços MAC de clientes proibidos de acessar a WLAN. Essa lista é configurada manualmente.
- **Lista negra dinâmica:** contém os endereços MAC de clientes proibidos de acessar a WLAN por meio de APs específicos dentro do tempo de envelhecimento especificado. Um cliente é adicionado dinamicamente à lista se um AP determinar que esse cliente é um cliente desonesto.

5.6. Aplicativos

5.6.1. Malha WLAN

A malha WLAN permite que os APs sejam conectados sem fio. Os APs em uma rede de malha WLAN podem ser conectados diretamente ou por meio de vários saltos. Quando um AP falha, os APs restantes ainda podem se comunicar uns com os outros. Para os usuários, uma rede mesh WLAN pode fornecer a mesma boa experiência de usuário que uma WLAN tradicional.

5.6.1.1. Funções de MP

Os APs em uma rede de malha WLAN são pontos de malha (MPs). Os MPs desempenham as seguintes funções:

- **MP de finalidade única:** fornece apenas serviços de malha
- **Ponto de acesso de malha (MAP):** fornece serviços de malha e de acesso.
- **Ponto de portal de malha (MPP**): fornece uma conexão com fio a uma rede com fio.

5.6.1.2. Perfil da malha

Um perfil de malha é um conjunto de recursos de processamento do protocolo de malha para que um AP opere em uma rede de malha. Um perfil de malha contém uma ID de malha, o modo de autenticação e gerenciamento de chaves e o intervalo de manutenção.

Antes que os MPs possam estabelecer um link de malha, eles precisam descobrir uns aos outros e estabelecer uma relação de pares. Os MPs estabelecem uma relação de pares entre si somente quando seus perfis de malha coincidem.

5.6.1.3. Política de malha

Uma política de malha contém um conjunto de atributos de configuração e manutenção de links de malha. Esses atributos são o recurso de iniciação de link de malha, o intervalo de solicitação de sondagem, o modo de taxa de link e o número máximo de links de malha. Apenas uma política de malha pode ser vinculada a um rádio de um MP, e a política entra em vigor em todos os links de malha no rádio.

Por padrão, uma política de malha definida pelo sistema é vinculada a cada rádio. Essa política de malha definida pelo sistema não pode ser excluída ou modificada. Para alterar as configurações de configuração e manutenção do link em um rádio, é possível vincular uma política de malha definida pelo usuário ao rádio para substituir a política de malha definida pelo sistema.

5.6.1.4. Lista de permissões de pares de malha

Use uma lista branca de pares de malha para garantir que um MP estabeleça links de malha somente com MPs legítimos

Um MP pode estabelecer relações de pares com qualquer vizinho MP se você não configurar uma lista de permissões.

5.6.2. Otimização de multicast de WLAN

5.6.2.1. Visão geral

A transmissão multicast tem limitações e não pode atender aos requisitos de aplicativos que não são sensíveis a atrasos, mas que são sensíveis à integridade dos dados. Para resolver esse problema, você pode configurar a otimização multicast da WLAN para permitir que um AP converta pacotes multicast em pacotes unicast.

A otimização multicast de WLAN usa entradas de otimização multicast para gerenciar o encaminhamento de tráfego. As entradas de otimização de multicast usam os endereços MAC dos clientes como índices. Uma entrada de otimização de multicast registra informações sobre grupos multicast aos quais os clientes aderem, fontes multicast das quais os clientes recebem tráfego, versão do grupo multicast e modo de otimização de multicast.

Sempre que um cliente ingressa em um grupo multicast, o AP cria uma entrada de otimização multicast para o grupo multicast. Se as fontes de multicast tiverem sido especificadas para um cliente quando ele ingressar no grupo de multicast, o AP também criará uma entrada de otimização de multicast para cada fonte de multicast. Quando um cliente sai de um grupo multicast ou rejeita uma fonte multicast, o AP exclui a entrada de otimização multicast relevante para o cliente.

5.6.2.2. Tempo de envelhecimento para entradas de otimização de multicast

Configure um timer de envelhecimento adequado para entradas de otimização de multicast. Um tempo de envelhecimento longo consome mais recursos do sistema e afeta a criação de novas entradas, enquanto um tempo de envelhecimento curto causa a geração e o envelhecimento frequentes de entradas.

5.6.2.3. Otimização de multicast policy

Uma política de otimização de multicast define o número máximo de clientes que a otimização de multicast de WLAN suporta e define as seguintes ações que um AP executa quando o limite é atingido:

- **Encaminhamento de unicast:** envia pacotes unicast convertidos de um pacote multicast para apenas *n* (*n* igual ao limite especificado) clientes selecionados aleatoriamente.
- **Encaminhamento de multicast:** encaminha o pacote multicast para todos os clientes.
- **Eliminação de pacote:** elimina o pacote multicast.

Se você não especificar uma ação, o AP realizará o encaminhamento unicast.

5.6.2.4. Limites de entrada de otimização de multicast

Limite para entradas de otimização de multicast

Você pode limitar o número de entradas de otimização multicast para economizar recursos do sistema.

Quando o número de entradas de otimização multicast atinge o limite, o AP para de criar novas entradas até que o número fique abaixo do limite

Limite de entradas de otimização multicast por cliente

É possível limitar o número de entradas de otimização multicast que um AP mantém para cada cliente para evitar que um cliente ocupe recursos excessivos do sistema.

5.6.2.5. Limites de taxa para pacotes IGMP de clientes

Você pode configurar o número máximo de pacotes IGMP que um AP pode receber de clientes dentro do intervalo especificado. O AP descarta os pacotes IGMP excessivos.

5.6.3. Sondagem do cliente

Depois que você ativa a sondagem de cliente no rádio de um AP, o AP varre os canais para coletar informações do cliente. Você pode visualizar as informações do cliente na página *Monitoramento> Sensor de proximidade do cliente.*

6. Configuração da rede

6.1. Interfaces

6.1.1. Interfaces

Você pode visualizar as informações das estatísticas de tráfego da interface e definir as configurações básicas da interface.

6.1.1.1. Configuração do modo duplex e da velocidade da interface

Você pode configurar uma interface Ethernet para operar em um dos seguintes modos duplex:

- **Modo full-duplex:** a interface pode enviar e receber pacotes simultaneamente.
- **Modo half-duplex:** a interface só pode enviar ou receber pacotes em um determinado momento.
- **Modo de negociação automática:** a interface negocia um modo duplex com seu par.

Você pode definir a velocidade de uma interface Ethernet ou permitir que ela negocie automaticamente uma velocidade com seu par.

6.1.1.2. Configuração do suporte a jumbo frame

Os Jumbo frames são frames maiores do que um tamanho específico do dispositivo e são normalmente recebidos por uma interface Ethernet durante trocas de dados de alta taxa de transferência, como transferências de arquivos. O tamanho específico do dispositivo varia de acordo com o modelo do dispositivo.

A interface Ethernet processa os quadros jumbo das seguintes maneiras:

- Quando a interface Ethernet está configurada para negar jumbo frames, ela descarta os jumbo frames.
- Quando a interface Ethernet é configurada com suporte a jumbo frame, a interface Ethernet executa as seguintes operações:
  - Processa quadros jumbo com o comprimento especificado.
  - Descarta os quadros jumbo que excedem o comprimento especificado.

6.1.1.3. Configuração do controle de fluxo genérico em uma interface Ethernet

Para evitar a perda de pacotes em um link, é possível ativar o controle de fluxo genérico em ambas as extremidades do link. Quando ocorre congestionamento de tráfego na extremidade receptora, esta envia um quadro de controle de fluxo (Pausa) para solicitar que a extremidade remetente suspenda o envio de pacotes. O controle de fluxo genérico inclui os seguintes tipos:

- **Controle de fluxo genérico no modo TxRx:** com o controle de fluxo genérico no modo TxRx ativado, uma interface pode enviar e receber quadros de controle de fluxo:
  - Quando ocorre um congestionamento, a interface envia um quadro de controle de fluxo para seu par.
  - Quando a interface recebe um quadro de controle de fluxo de seu par, ela suspende o envio de pacotes para seu par.

» **Controle de fluxo genérico no modo Rx:** com o controle de fluxo genérico no modo Rx ativado, uma interface pode receber quadros de controle de fluxo, mas não pode enviar quadros de controle de fluxo:
  » Quando ocorre um congestionamento, a interface não pode enviar quadros de controle de fluxo para seu par.
  » Quando a interface recebe um quadro de controle de fluxo de seu par, ela suspende o envio de pacotes para seu par.

Para lidar com o congestionamento de tráfego unidirecional em um link, configure o controle de fluxo genérico no modo Rx em uma extremidade e o controle de fluxo genérico no modo TxRx na outra extremidade. Para permitir que ambas as extremidades de um link lidem com o congestionamento de tráfego, configure o controle de fluxo genérico no modo TxRx em ambas as extremidades.

6.1.1.4. Supressão de tempestades

O recurso de supressão de tempestades garante que o tamanho de um tipo específico de tráfego (broadcast, multicast ou tráfego unicast desconhecido) não exceda o limite em uma interface. Quando o tráfego de broadcast, multicast ou unicast desconhecido na interface excede esse limite, o sistema descarta os pacotes até que o tráfego caia abaixo desse limite.

Tanto a supressão quanto o controle de tempestades podem suprimir tempestades em uma interface da Camada 2. A supressão de tempestades usa o chip para suprimir o tráfego. A supressão de tempestades tem menos impacto sobre o desempenho do dispositivo do que o controle de tempestades, que usa software para suprimir o tráfego.

6.1.2. Agregação de links

A agregação de links Ethernet agrupa vários links Ethernet físicos em um único link lógico, chamado de link agregado. A agregação de links tem as seguintes vantagens:

» Maior largura de banda além dos limites de um único link. Em um link agregado, o tráfego é distribuído entre as portas membros.
» Maior confiabilidade do link. As portas membros fazem backup dinamicamente umas das outras. Quando uma porta membro falha, seu tráfego é automaticamente transferido para outras portas membro.

6.1.2.1. Grupo de agregação

O agrupamento de links é implementado por meio do agrupamento de interfaces. Um grupo de agregação é um grupo de interfaces Ethernet agrupadas. Essas interfaces Ethernet são chamadas de portas-membro do grupo de agregação. Cada grupo de agregação tem uma interface lógica correspondente (chamada de interface agregada).

Quando você cria uma interface agregada, o dispositivo cria automaticamente um grupo de agregação do mesmo tipo e número que a interface agregada. Por exemplo, quando você cria a interface agregada de camada 2 1, é criado o grupo de agregação de camada 2 1.

Você pode atribuir interfaces Ethernet de camada 2 somente a um grupo de agregação de camada 2.

A taxa de porta de uma interface agregada é igual à taxa total de suas portas membros selecionadas. Seu modo duplex é o mesmo das portas membros selecionadas.

6.1.2.2. Estados de agregação das portas membros em um grupo de agregação

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

» **Selected : uma** porta selecionada pode encaminhar tráfego.
» **Unselected (Não selecionado):** uma porta não selecionada não pode encaminhar tráfego.

6.1.2.3. Chave operacional

Ao agregar portas, o sistema atribui automaticamente a cada porta uma chave operacional com base nas informações da porta, como a taxa da porta e o modo duplex. Qualquer alteração nessas informações aciona um novo cálculo da chave operacional.

Em um grupo de agregação, todas as portas selecionadas têm a mesma chave operacional.

6.1.2.4. Configurações de atributos

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

Recurso	Considerações
Isolamento de portas	Se a porta está em um grupo de isolamento. Grupo de isolamento ao qual a porta pertence.
VLAN	As configurações de atributos de VLAN incluem: VLAN IDs permitidas. PVID. Tipo de link. Modo de marcação de VLAN.

6.1.2.5. Modos de agregação de links

Um grupo de agregação opera em um dos seguintes modos:

- **A agregação estática é estável:** um grupo de agregação em modo estático é chamado de grupo de agregação estática. Os estados de agregação das portas membros em um grupo de agregação estática não são afetados pelas portas pares.
- **Dinâmico:** um grupo de agregação em modo dinâmico é chamado de grupo de agregação dinâmica. O sistema local e o sistema par mantêm automaticamente os estados de agregação das portas membros, o que reduz a carga de trabalho dos administradores.

Um grupo de agregação em qualquer modo deve escolher uma porta de referência e, em seguida, definir o estado de agregação de suas portas membros.

6.1.2.6. Agregação de links em modo estático

Ao definir os estados de agregação das portas em um grupo de agregação, o sistema escolhe automaticamente uma porta membro como a porta de referência. Uma porta selecionada deve ter as mesmas configurações de chave operacional e atributo que a porta de referência.

O sistema escolhe uma porta de referência entre as portas membro que estão em estado ativo e têm as mesmas configurações de atributo que a interface agregada.

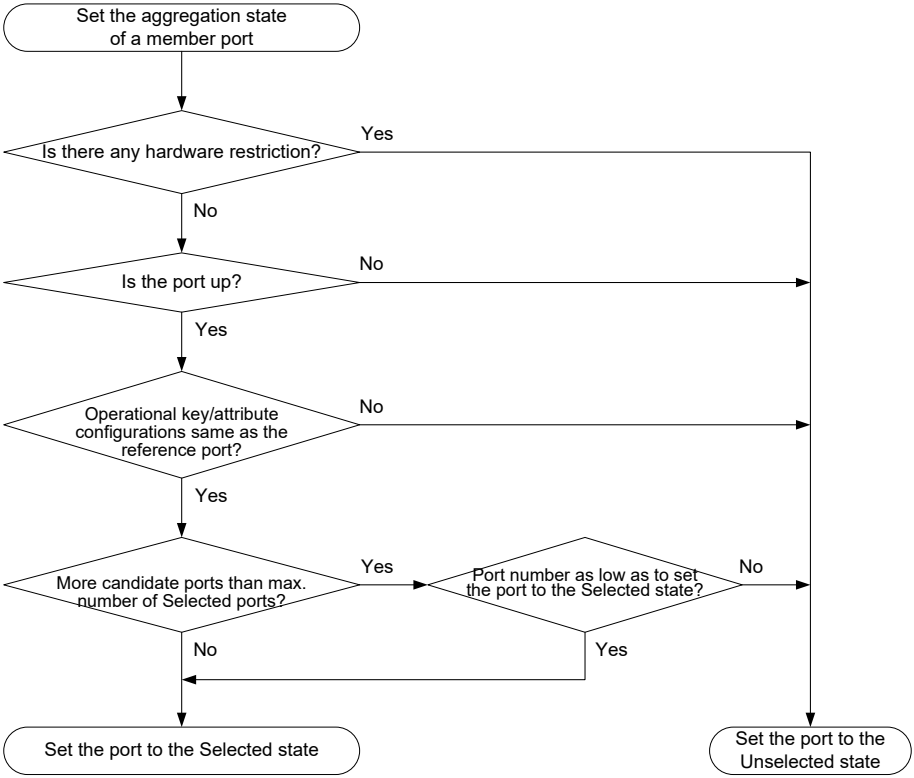
As portas candidatas são classificadas na seguinte ordem:

- Prioridade mais alta da porta
- Full duplex/alta velocidade
- Full duplex/baixa velocidade
- Half duplex/alta velocidade
- Half duplex/baixa velocidade

A porta candidata na parte superior é escolhida como a porta de referência.

- Se várias portas tiverem a mesma prioridade de porta, modo duplex e velocidade, a porta que foi selecionada (se houver) será escolhida. Se várias portas tiverem sido portas selecionadas, será escolhida a que tiver o menor número de porta.
- Se várias portas tiverem a mesma prioridade de porta, modo duplex e velocidade e nenhuma delas tiver sido uma porta selecionada, a porta com o menor número de porta será escolhida.

Depois que a porta de referência é escolhida, o sistema define o estado de agregação de cada porta membro no grupo de agregação estática.



Configuração do estado de agregação de uma porta membro em um grupo de agregação estática

6.1.2.7. Agregação de links no modo dinâmico

A agregação dinâmica é implementada por meio do protocolo de controle de agregação de links (LACP) IEEE 802.3ad.

O LACP usa LACPDUs para trocar informações de agregação entre dispositivos habilitados para LACP.

Cada porta membro em um grupo de agregação habilitado para LACP troca informações com seu par. Quando uma porta membro recebe um LACPDU, ela compara as informações recebidas com as informações recebidas nas outras portas membros. Dessa forma, os dois sistemas chegam a um acordo sobre quais portas são colocadas no estado Selected (Selecionado).

O sistema escolhe uma porta de referência entre as portas membros que estão em estado ativo e têm as mesmas configurações de atributo que a interface agregada. Uma porta selecionada deve ter a mesma chave operacional e as mesmas configurações de atributo que a porta de referência.

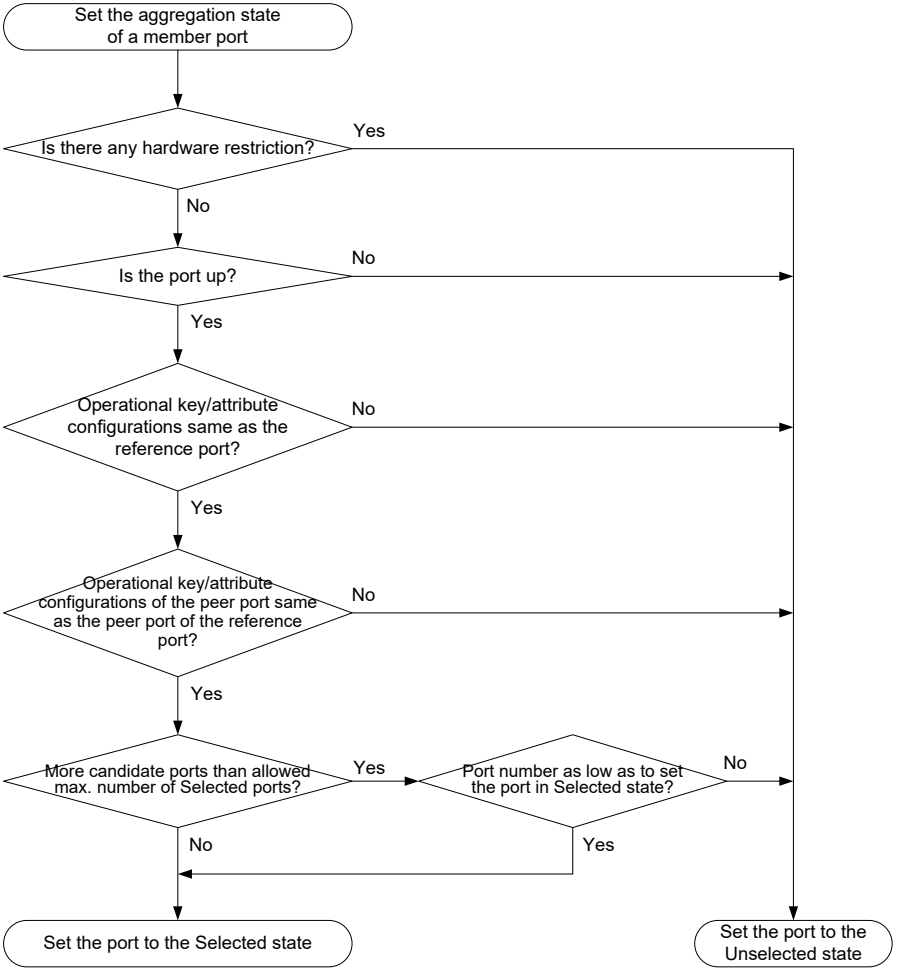
O sistema local (o ator) e o sistema par (o parceiro) negociam uma porta de referência usando o seguinte fluxo de trabalho:

- Os dois sistemas comparam suas IDs de sistema para determinar o sistema com a ID de sistema menor. Um ID do sistema contém a prioridade LACP do sistema e o endereço MAC do sistema.
- Os dois sistemas comparam seus valores de prioridade LACP. Quanto menor for a prioridade do LACP, menor será a ID do sistema. Se os valores de prioridade do LACP forem os mesmos, os dois sistemas passarão para a próxima etapa.
- Os dois sistemas comparam seus endereços MAC. Quanto menor for o endereço MAC, menor será a ID do sistema.

» O sistema com a menor ID de sistema escolhe a porta com a menor ID de porta como a porta de referência. Um ID de porta contém uma prioridade de porta e um número de porta. Quanto menor for a prioridade da porta, menor será o ID da porta.

» O sistema escolhe a porta com o valor de prioridade mais baixo como a porta de referência. Se as portas tiverem a mesma prioridade, o sistema passará para a próxima etapa.

» O sistema compara seus números de porta. Quanto menor for o número da porta, menor será a ID da porta. A porta com o menor número de porta e as mesmas configurações de atributo que a interface agregada é escolhida como a porta de referência. Depois que a porta de referência é escolhida, o sistema com a ID de sistema menor define o estado de cada porta membro em seu lado.



Configuração do estado de uma porta membro em um grupo de agregação dinâmica

Enquanto isso, o sistema com o ID de sistema mais alto está ciente das alterações de estado de agregação no sistema par. O sistema define o estado de agregação das portas membros locais da mesma forma que suas portas pares.

6.1.3. PPPoE

6.1.3.1. Sobre o PPPoE

O PPPoE (Point-to-Point Protocol over Ethernet) amplia o PPP transportando quadros PPP encapsulados em Ethernet por links ponto a ponto.

O PPPoE especifica os métodos para estabelecer sessões PPPoE e encapsular quadros PPP sobre Ethernet. O PPPoE requer uma relação ponto a ponto entre os pares, em vez de uma relação ponto a multiponto, como em ambientes de acesso múltiplo, como a Ethernet. O PPPoE fornece acesso à Internet para os hosts em uma Ethernet por meio de um dispositivo de acesso remoto e implementa controle de acesso, autenticação e contabilidade host. Integrando o baixo custo da Ethernet e as funções de escalabilidade e gerenciamento do PPP, o PPPoE ganhou popularidade em vários ambientes de aplicativos, como redes de acesso residencial.

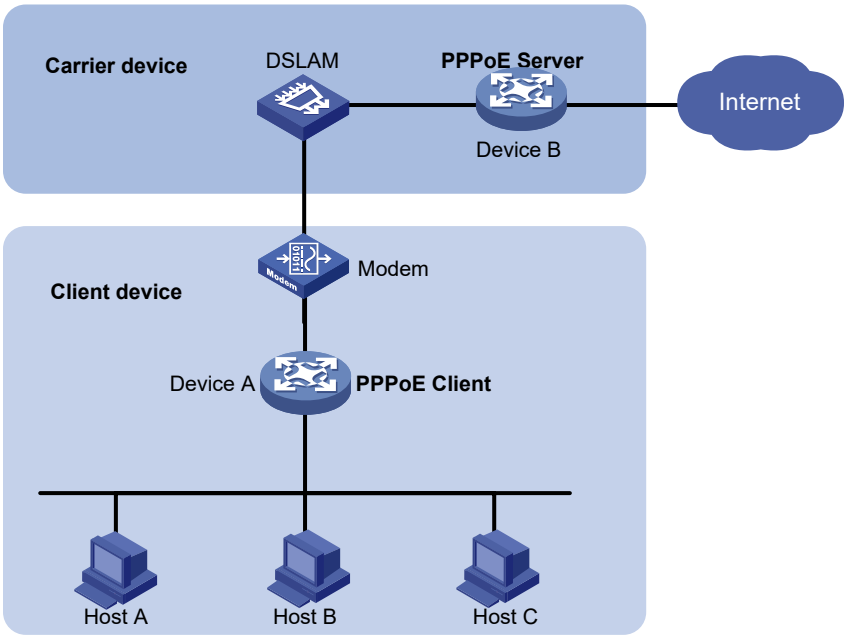
Para obter mais informações sobre o PPPoE, consulte a RFC 2516.

6.1.3.2. Estrutura da rede PPPoE

Importante: na versão atual do software, o dispositivo atua como cliente PPPoE.

O PPPoE usa o modelo cliente/servidor. O cliente PPPoE inicia uma solicitação de conexão com o servidor PPPoE. Após a conclusão da negociação da sessão entre eles, uma sessão é estabelecida entre eles e o servidor PPPoE fornece controle de acesso, autenticação e contabilidade ao cliente PPPoE.

Conforme mostrado em , a sessão PPPoE é estabelecida entre dispositivos (Dispositivo A e Dispositivo B). Todos os hosts compartilham uma sessão PPPoE para a transmissão de dados sem que seja instalado um software cliente PPPoE. Essa estrutura de rede é normalmente usada por empresas.



Estrutura da rede PPPoE

6.2. Links

6.2.1. VLAN

A tecnologia de rede local virtual (VLAN) divide uma LAN em várias LANs lógicas, que são chamadas de VLANs. Cada VLAN é um domínio de transmissão. Os hosts na mesma VLAN podem se comunicar diretamente uns com os outros. Os hosts em diferentes VLANs são isolados uns dos outros na Camada 2.

6.2.1.1. VLANs baseadas em portas

As VLANs baseadas em portas agrupam os membros da VLAN por porta. Uma porta encaminha pacotes de uma VLAN somente depois de ser atribuída à VLAN.

Você pode configurar uma porta como uma porta untagged ou tagged de uma VLAN.

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

Você pode configurar o tipo de link de uma porta como acesso, tronco ou híbrido. As portas de diferentes tipos de link usam diferentes métodos de tratamento de tags de VLAN.

- **Acesso:** uma porta de acesso pode encaminhar pacotes de apenas uma VLAN e enviá-los sem marcação. Atribua uma porta de acesso somente à lista de portas sem marcação de uma VLAN.
- **Tronco:** uma porta tronco pode encaminhar pacotes de várias VLANs. Com exceção dos pacotes da porta VLAN ID (PVID), os pacotes enviados por uma porta tronco são marcados com VLAN. Atribua uma porta tronco à lista de portas não marcadas do PVID da porta e às listas de portas marcadas de outras VLANs.
- **Híbrida:** uma porta híbrida pode encaminhar pacotes de várias VLANs. Você pode atribuir uma porta híbrida às listas de portas untagged de algumas VLANs e às listas de portas tagged de outras VLANs. Uma porta híbrida untagged de uma VLAN encaminha pacotes da VLAN sem tags de VLAN. Uma porta híbrida com tags de uma VLAN encaminha pacotes da VLAN com tags de VLAN.

6.2.1.2. Interface VLAN

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

6.2.2. MAC

Um dispositivo Ethernet usa uma tabela de endereços MAC para encaminhar quadros. Uma entrada de endereço MAC inclui um endereço MAC de destino, uma interface de saída (ou RB de saída) 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 fora da interface de saída na entrada correspondente se for encontrada uma correspondência.
- O dispositivo inunda o quadro na VLAN do quadro se nenhuma correspondência for encontrada.

6.2.2.1. Tipos de entradas de endereço 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 para fora da interface associada. Uma entrada dinâmica pode . 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 para fora da interface associada e nunca se . Uma entrada estática tem prioridade mais alta do que uma aprendida dinamicamente.
- **Entradas de blackhole:** uma entrada de blackhole é configurada manualmente e nunca se . Uma entrada de blackhole é configurada para filtrar quadros com um endereço MAC de origem ou destino específico. Por exemplo, para bloquear todos os quadros destinados a um usuário ou originados por ele, é possível configurar o endereço MAC do usuário como uma entrada de endereço MAC blackhole. A entrada de blackhole de um endereço MAC tem prioridade mais alta do que a entrada dinâmica do endereço MAC.

6.2.2.2. Temporizador de envelhecimento para entradas dinâmicas de endereço MAC

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

Uma rede estável requer um intervalo de envelhecimento mais longo, e 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 conseguir atualizar suas entradas para acomodar as últimas alterações na rede.

Um intervalo muito curto pode resultar na remoção de entradas válidas, o que causaria inundações desnecessárias e possivelmente afetaria 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 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 chegar a destinos não intencionais.

6.2.2.3. Aprendizado de endereço MAC

O aprendizado de endereço MAC é ativado por padrão. Para evitar que a tabela de endereços MAC fique saturada quando o dispositivo estiver sofrendo ataques, desative o aprendizado de endereços MAC. Por exemplo, você pode desativar o aprendizado de endereço MAC para evitar que o dispositivo seja atacado por uma grande quantidade de quadros com diferentes endereços MAC de origem.

Quando o aprendizado de endereço MAC global está ativado, é possível desativar o aprendizado de endereço MAC em uma única interface.

Você também pode configurar o limite de aprendizagem de MAC em uma interface para limitar o tamanho da tabela de endereços MAC. Uma tabela de endereços MAC grande prejudicará o desempenho do encaminhamento. Quando o limite é atingido, a interface para de aprender qualquer endereço MAC. Você também pode configurar se deseja encaminhar quadros cujo endereço MAC de origem não esteja na tabela de endereços MAC.

6.2.3. STP

Os protocolos de árvore de alcance executam as seguintes tarefas:

- Podar a estrutura de loop em uma estrutura de árvore sem loop para uma rede de Camada 2 bloqueando seletivamente as portas.
- Manter a estrutura em árvore da rede ativa.

Os protocolos de árvore de varredura incluem STP, RSTP, PVST e MSTP.

- **STP:** definido no IEEE 802.1d.
- **RSTP:** definido no IEEE 802.1w. O RSTP alcança uma convergência rápida da rede, permitindo que uma porta raiz recém-eleita ou uma porta designada entre no estado de encaminhamento muito mais rapidamente do que o STP.
- **PVST:** o PVST permite que cada VLAN tenha sua própria spanning tree, o que aumenta o uso de links e largura de banda. Como cada VLAN executa o RSTP de forma independente, uma árvore de abrangência atende apenas à sua VLAN.
- **MSTP:** definido no IEEE 802.1s. O MSTP supera as limitações do STP e do RSTP. Ele oferece suporte à rápida convergência da rede e permite que os fluxos de dados de diferentes VLANs sejam encaminhados por caminhos separados. Isso proporciona um melhor mecanismo de compartilhamento de carga para links redundantes.

6.2.3.1. Modos de árvore de abrangência

Os modos da árvore de abrangência incluem o seguinte:

- **Modo STP:** todas as portas do dispositivo enviam BPDUs STP. Selecione esse modo quando o dispositivo par de uma porta for compatível apenas com STP.
- **Modo RSTP:** todas as portas do dispositivo enviam BPDUs RSTP. Uma porta nesse modo passa automaticamente para o modo STP quando recebe BPDUs STP de um dispositivo par. A porta não passa para o modo MSTP quando recebe BPDUs MSTP de um dispositivo par. A porta não passa para o modo MSTP quando recebe BPDUs MSTP de um dispositivo par.

- **Modo PVST:** em uma porta de acesso, o modo PVST é compatível com outros modos de spanning tree em todas as VLANs. Em uma porta tronco ou porta híbrida, o modo PVST é compatível com outros modos de árvore de abrangência somente na VLAN padrão
- **Modo MSTP:** todas as portas do dispositivo enviam BPDUs MSTP. Uma porta nesse modo passa automaticamente para o modo STP quando recebe BPDUs STP de um dispositivo par. A porta não passa para o modo RSTP quando recebe BPDUs RSTP de um dispositivo par. A porta não passa para o modo RSTP quando recebe BPDUs RSTP de um dispositivo par.

6.2.3.2. Conceitos básicos do 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 árvore de abrangência é mapeada para VLANs específicas. Essa árvore de abrangência é chamada de instância de árvore de abrangência múltipla (MSTI). A árvore de abrangência comum (CST) é uma única árvore de abrangência que conecta todas as regiões MST na rede comutada. Uma árvore de abrangência interna (IST) é uma árvore de abrangência que é executada em uma região MST. Ela também é chamada de MSTI 0, uma MSTI especial para a qual todas as VLANs são mapeadas por padrão. A árvore de abrangência comum e interna (CIST) é uma única árvore de abrangência que conecta todos os dispositivos na rede comutada. Ela consiste nas ISTs em todas as regiões MST e na CST.

Os dispositivos em uma região MST têm as seguintes características:

- Um protocolo de árvore de abrangência ativado.
- Mesmo nome de região.
- Mesma configuração de mapeamento de VLAN para instância.
- Mesmo nível de revisão do MSTP.
- Fisicamente ligados entre si.

6.2.3.3. Funções de porta

O cálculo da árvore de abrangência envolve as seguintes funções de porta:

- **Porta raiz:** encaminha dados de uma ponte não raiz para a ponte raiz. A ponte raiz não tem nenhuma porta raiz.
- **Porta designada:** encaminha dados para o segmento de rede ou dispositivo downstream.
- **Porta alternativa:** atua como porta de backup para uma porta raiz ou porta principal. Quando a porta raiz ou a porta principal é bloqueada, a porta alternativa assume o controle.
- **Porta de backup:** atua como porta de backup de uma porta designada. Quando a porta designada é inválida, a porta de backup torna-se a nova porta designada. Um loop ocorre quando duas portas do mesmo dispositivo de spanning tree estão conectadas, de modo que o dispositivo bloqueia uma das portas. A porta bloqueada atua como backup.
- **Porta mestre: a**tua como uma porta no caminho mais curto da região MST local até a ponte raiz comum. A porta mestre nem sempre está localizada na raiz regional. Ela é uma porta raiz no IST ou CIST e ainda é uma porta mestre nos outros MSTIs.

O cálculo do STP envolve portas raiz, portas designadas e portas alternativas. O cálculo do RSTP envolve as portas raiz, as portas designadas, as portas alternativas e as portas de backup. O cálculo do MSTP envolve todas as funções de porta.

6.2.3.4. Estados das portas

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

Estado	Descrição
Encaminhamento	A porta recebe e envia BPDUs e encaminha o tráfego de usuários.
Aprendizagem	A porta recebe e envia BPDUs, mas não encaminha tráfego de usuário. O aprendizado é um estado intermediário da porta.
Descarte	A porta recebe e envia BPDUs, mas não encaminha tráfego de usuário.

O STP define os seguintes estados de porta: Desativado, Bloqueio, Escuta, Aprendizado e Encaminhamento. Os estados Disabled (Desativado), Blocking (Bloqueio) e Listening (Escuta) correspondem ao estado Discarding (Descarte) no RSTP e no MSTP.

6.3. Roteamento

6.3.1. Tabela de roteamento

Você pode exibir informações da tabela de roteamento, incluindo informações breves da tabela de roteamento e estatísticas de rota.

6.3.2. Roteamento estático

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

As rotas estáticas não podem se adaptar às mudanças na topologia da rede. Se ocorrer uma falha ou uma mudança topológica na rede, o administrador da rede deverá 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.

6.4. IP

6.4.1. NAT

O NAT (Network Address Translation) traduz um endereço IP no cabeçalho do pacote IP para outro endereço IP. Normalmente, o NAT é configurado em gateways para permitir que hosts privados acessem redes externas e hosts externos acessem recursos de rede privada, como um servidor Web.

6.4.1.1. NAT estático

O NAT estático cria um mapeamento fixo entre um endereço privado e um endereço público. Ele suporta conexões iniciadas por usuários internos para a rede externa e de usuários externos para a rede interna. A NAT estática se aplica a comunicações regulares.

6.4.1.2. NAT dinâmico

O NAT dinâmico usa um pool de endereços para traduzir endereços. Aplica-se ao cenário em que um grande número de usuários internos acessa a rede externa.

NO-PAT

O Not Port Address Translation (NO-PAT) traduz um endereço IP privado em um endereço IP público, mapeando o endereço IP privado para o endereço IP público. O endereço IP público não pode ser usado por outro host interno até que seja liberado.

O NO-PAT é compatível com todos os pacotes IP e cria uma entrada NO-PAT para cada mapeamento de endereço IP.

PAT

O PAT (Port Address Translation) converte vários endereços IP privados em um único endereço IP público, mapeando os endereços IP privados e as portas de origem para o endereço IP público e uma porta exclusiva.

O PAT suporta apenas pacotes TCP e UDP e pacotes de solicitação ICMP.

6.4.1.3. Servidor NAT

O recurso NAT Server mapeia um endereço público e um número de porta para o endereço IP privado e o número de porta de um servidor interno. Esse recurso permite que os servidores da rede privada forneçam serviços para usuários externos.

A tabela a seguir descreve os mapeamentos de endereço-porta entre uma rede externa e uma rede interna para o NAT Server.

Rede externa	Rede interna
Um endereço público	Um endereço particular.
Um endereço público e um número de porta pública	Um endereço privado e um número de porta privada.
Um endereço público e N números consecutivos de portas públicas	Um endereço privado e um número de porta privada.
	N endereços privados consecutivos e um número de porta privada.
	Um endereço privado e N números consecutivos de portas privadas.

Rede externa	Rede interna
N endereços públicos consecutivos	Um endereço particular.
	N endereços privados consecutivos.
N endereços públicos consecutivos e um número de porta pública	Um endereço privado e um número de porta privada.
	N endereços privados consecutivos e um número de porta privada.
	Um endereço privado e N números consecutivos de portas privadas.
Um endereço público e um número de porta pública	Um grupo de servidores privados.
Um endereço público e N números consecutivos de portas públicas	
N endereços públicos consecutivos e um número de porta pública	

6.4.1.4. NAT 444

O NAT444 oferece NAT de nível de operadora. É a solução preferida das operadoras para atenuar o esgotamento de endereços IPv4. Ele introduz uma segunda camada de NAT no lado da operadora, com poucas alterações no lado do cliente e no lado do servidor de aplicativos. Sua função de registro de usuários fornece o serviço de rastreamento de usuários.

Conforme mostrado em , a arquitetura NAT444 inclui as seguintes entidades:

- **CPE:** fornece serviços NAT no lado do cliente.
- **BRAS:** fornece serviços de acesso à Internet.
- **Gateway NAT444:** fornece serviços NAT de nível de operadora.
- **Servidor AAA:** coopera com o BRAS para fornecer serviços de autenticação, autorização e contabilidade de usuários.
- **Servidor de logs:** registra os logs de acesso do usuário e responde a consultas de informações de acesso do usuário.

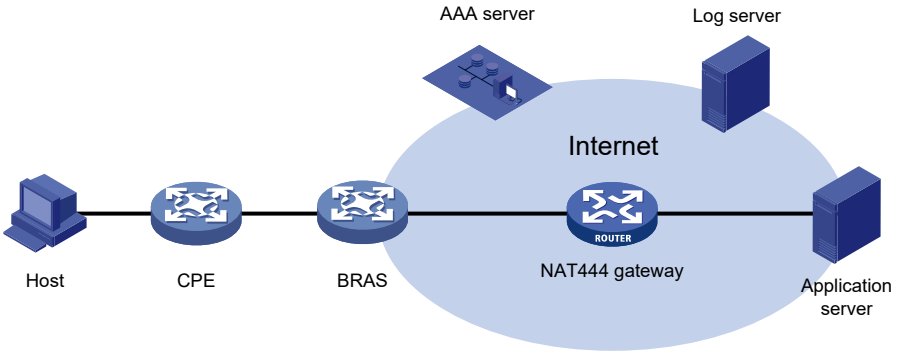


Diagrama do aplicativo NAT444

O gateway NAT444 oferece tradução PAT baseada em blocos de portas. Ele mapeia vários endereços IP privados para um endereço IP público e usa um bloco de portas diferente para cada endereço IP privado.

Por isso, o endereço IP privado 10.1.1.1 de um host interno é mapeado para o endereço IP público 202.1.1.1 e para o bloco de portas 10001 a 10256. Quando o host interno acessa hosts públicos, o endereço IP de origem 10.1.1.1 é convertido para 202.1.1.1 e as portas de origem são convertidas para portas no bloco de portas 10001 a 10256.

O NAT444 inclui o NAT444 estático e o NAT444 dinâmico.

- **NAT444 estático:** o gateway NAT444 calcula um mapeamento NAT444 estático antes da conversão de endereços. O mapeamento é entre um endereço IP privado e um endereço IP público com um bloco de portas.
  - O gateway NAT444 usa endereços IP privados, endereços IP públicos, um intervalo de portas e um tamanho de bloco de portas para calcular mapeamentos estáticos:
  - Divide o intervalo de portas pelo tamanho do bloco de portas para obter o número de blocos de portas

disponíveis para cada endereço IP público
  - » Esse valor é o número base para o mapeamento.
  - » Classifica os blocos de portas em ordem crescente do número da porta inicial em cada bloco.
  - » Classifica os endereços IP privados e os endereços IP públicos separadamente em ordem crescente.
  - » Mapeia o primeiro número base de endereços IP privados para o primeiro endereço IP público e seus blocos de portas em ordem crescente.
  - » Por exemplo, o número de blocos de portas disponíveis de cada endereço IP público é m. Os primeiros m endereços IP privados são mapeados para o primeiro endereço IP público e os m blocos de portas em ordem crescente. Os próximos m endereços IP privados são mapeados para o segundo endereço IP e os m blocos de portas em ordem crescente. Os outros mapeamentos NAT444 estáticos são criados por analogia.
- » **NAT444 dinâmico:** o Dynamic NAT444 funciona da seguinte forma:
  - » Cria um mapeamento do endereço IP privado do host interno para um endereço IP público e um bloco de portas quando o host inicia uma conexão com a rede pública.
  - » Traduz o endereço IP privado para o endereço IP público e as portas de origem para portas no bloco de portas selecionado para conexões subsequentes do endereço IP privado
  - » Exclui o bloqueio de porta e exclui o mapeamento NAT444 dinâmico quando todas as conexões do endereço IP privado são desconectadas.
  - » O Dynamic NAT444 usa ACLs para implementar o controle de tradução. Ele processa somente os pacotes que correspondem a uma regra de permissão de ACL.
  - » O Dynamic NAT444 oferece suporte à extensão de blocos de portas. Se todas as portas do bloco de portas de um endereço privado estiverem ocupadas, o NAT444 dinâmico traduz a porta de origem para uma porta em um bloco de portas estendido.

6.4.1.5. Configurações avançadas

Grupo de endereços NAT

Um grupo de endereços NAT é um conjunto de intervalos de endereços. O NAT dinâmico usa um grupo de endereços NAT para traduzir um grupo maior de endereços IP privados.

Grupo de endereços NAT444

Um grupo de endereços NAT444 é usado para executar o NAT444 dinâmico. Um grupo de endereços NAT444 é semelhante a um grupo de endereços NAT. A diferença é que um grupo de endereços NAT444 inclui parâmetros de bloco de portas, como um intervalo de portas, um tamanho de bloco de portas e um número de bloco de portas estendido.

Grupo de blocos de portas

Um grupo de blocos de portas é usado para realizar NAT444 estático. Um grupo de blocos de portas inclui endereços IP privados, endereços IP públicos, um intervalo de portas e um tamanho de bloco de portas. O gateway NAT444 usa esses parâmetros para calcular os mapeamentos NAT444 estáticos e executa o NAT444 adequadamente.

Grupo de servidores internos

Um grupo de servidores internos é usado para configurar o NAT Server com compartilhamento de carga. Os servidores internos do grupo fornecem o mesmo serviço a hosts externos. Quando um host externo envia uma solicitação para o endereço IP público mapeado para o grupo de servidores internos, o dispositivo NAT escolhe um servidor interno com base no peso e no número de conexões dos servidores.

PAT

O PAT é compatível com os seguintes mapeamentos:

- » **Endpoint-Independent Mapping (Mapeamento independente do ponto final):** usa o mesmo mapeamento de IP e porta (entrada EIM) para pacotes do mesmo IP e porta de origem para qualquer destino. O EIM permite que hosts externos acessem os hosts internos usando o endereço IP e a porta traduzidos. Ele permite que hosts internos atrás de diferentes gateways NAT acessem uns aos outros.
- » **Mapeamento dependente de endereço e porta:** usa mapeamentos de IP e porta diferentes para pacotes do mesmo IP e porta de origem para endereços IP e portas de destino diferentes. O APDM permite que um host externo acesse um host interno somente sob a condição de que o host interno tenha acessado o host externo anteriormente. Ele é seguro, mas não permite que hosts internos atrás de diferentes gateways NAT

acessem uns aos outros.

NAT com mapeamento de DNS

O NAT com mapeamento de DNS permite que um host interno acesse um servidor interno na mesma rede privada usando o nome de domínio do servidor interno quando o servidor DNS estiver na rede pública.

O NAT com mapeamento de DNS deve operar com o servidor NAT. O mapeamento de DNS mapeia o nome de domínio para o endereço IP público, o número da porta pública e o tipo de protocolo do servidor interno. O NAT Server mapeia o IP e a porta públicos para o IP e a porta privados do servidor interno.

O mapeamento de DNS também pode ser usado pelo DNS ALG. A resposta de DNS do servidor DNS externo contém apenas o nome de domínio e o endereço IP público do servidor interno na carga útil. A interface NAT pode ter vários servidores internos configurados com o mesmo endereço IP público, mas com endereços IP privados diferentes. O DNS ALG pode encontrar um servidor interno incorreto usando apenas o endereço IP público. Se um mapeamento de DNS estiver configurado, o DNS ALG poderá obter o endereço IP público, o número da porta pública e o tipo de protocolo do servidor interno usando o nome de domínio. Em seguida, ele pode localizar o servidor interno correto usando o endereço IP público, o número da porta pública e o tipo de protocolo do servidor interno.

Grampo de cabelo NAT

O NAT hairpin permite que os hosts internos acessem uns aos outros por meio do NAT.

O hairpin NAT inclui os modos P2P e C/S:

- **P2P:** permite que hosts internos acessem uns aos outros por meio de NAT. Para configurar o modo P2P, você deve configurar o PAT de saída na interface conectada à rede externa e ativar o modo de mapeamento EIM. Os hosts internos primeiro registram seus endereços públicos em um servidor externo. Em seguida, os hosts se comunicam entre si usando os endereços IP registrados.
- **C/S - Permite que hosts internos acessem servidores internos por meio de NAT:** no modo C/S, os endereços IP de origem e destino de um pacote são traduzidos na interface conectada à rede interna. O endereço IP de destino do pacote que vai para o servidor interno é traduzido de acordo com a configuração do servidor NAT. O endereço IP de origem é traduzido de acordo com as entradas NAT dinâmicas ou estáticas de saída. O NAT hairpin normalmente opera com NAT Server, NAT dinâmico de saída ou NAT estático de saída. Eles devem ser configurados em interfaces da mesma placa de interface. Caso contrário, o NAT hairpin não poderá funcionar corretamente.

NAT com ALG

O NAT com ALG traduz as informações de endereço ou porta nas cargas úteis da camada de aplicativos para garantir o estabelecimento da conexão.

Registro de NAT

- **Registro de sessão NAT:** o registro de sessão NAT registra as informações da sessão NAT, incluindo informações de tradução, informações de acesso e informações de fluxo. Um dispositivo NAT gera registros de sessão NAT para os seguintes eventos:
  - Estabelecimento de sessão NAT.
  - Remoção de sessão NAT. Esse evento ocorre quando você adiciona uma configuração com prioridade mais alta, remove uma configuração e altera ACLs, quando uma sessão NAT se esgota ou quando você exclui manualmente uma sessão NAT.
  - Registro de sessão NAT ativa.
- **Registro de usuários NAT444:** os registros de usuários do NAT444 são usados para rastreamento de usuários. O gateway NAT444 gera um registro de usuário sempre que atribui ou retira um bloqueio de porta. O registro inclui o endereço IP privado, o endereço IP público e o bloco de portas. É possível usar o endereço IP público e os números de porta para localizar o endereço IP privado do usuário nos registros de usuários. Um gateway NAT444 gera registros de usuários NAT quando ocorre um dos seguintes eventos:
  - **Um bloco de portas é atribuído:** para NAT444 estático, o gateway NAT444 gera um registro de usuário quando traduz a primeira conexão de um endereço IP privado. Para o NAT444 dinâmico, o gateway NAT444 gera um registro de usuário quando atribui ou estende um bloco de portas para um endereço IP privado.
  - **Um bloqueio de porta é retirado:** para NAT444 estático, o gateway NAT444 gera um registro de usuário quando todas as conexões de um endereço IP privado são desconectadas. Para o NAT444 dinâmico, o gateway NAT444 gera um registro de usuário quando todas as condições a seguir são atendidas:
    - Todas as conexões de um endereço IP privado são desconectadas.

- Os blocos de portas (inclusive estendidos) atribuídos ao endereço IP privado são retirados.

- **Registro de alarmes do NAT444:** se os endereços IP públicos, os blocos de portas ou as portas dos blocos de portas selecionados (inclusive os estendidos) estiverem todos ocupados, o gateway NAT444 não poderá executar a conversão de endereços e os pacotes serão descartados. Para monitorar o uso de endereços IP públicos e recursos de blocos de portas, é possível configurar o registro de alarme do NAT444. Um gateway NAT444 gera registros de alarme quando ocorre uma das seguintes situações:
  - As portas no bloco de portas selecionado de um mapeamento NAT444 estático estão todas ocupadas.
  - As portas nos blocos de portas selecionados (incluindo as estendidas) de um mapeamento NAT444 dinâmico estão todas ocupadas.
  - Os endereços IP públicos e os blocos de portas para o NAT444 dinâmico estão todos atribuídos.

Restrições e diretrizes

Quando você configurar o NAT, siga estas restrições e diretrizes:

- Não configure o NAT estático de entrada sozinho. Normalmente, o NAT estático de entrada funciona com NAT dinâmico de saída, servidor NAT ou NAT estático de saída para implementar o NAT bidirecional.
- A seguir, são mostradas as prioridades dos diferentes recursos NAT em ordem decrescente:
  - Servidor NAT.
  - NAT estático.
  - NAT444 estático.
  - NAT dinâmico e NAT444 dinâmico. O NAT dinâmico e o NAT444 dinâmico têm a mesma prioridade. Eles são combinados na ordem decrescente dos números de ACL.
- Os intervalos de endereços em um grupo de endereços NAT não podem se sobrepor uns aos outros.
- O número de endereços IP em um grupo de endereços NAT não pode ser menor do que o número de mecanismos de segurança.
- Em um grupo de servidores internos, um servidor interno com um peso maior fornece uma porcentagem maior de serviço.
- Antes de configurar o registro de usuários e alarmes do NAT444, é necessário configurar as funções personalizadas de geração e saída de registros do NAT444.

6.4.2. IP

6.4.2.1. Classes de endereços IP

O endereçamento IP usa um endereço de 32 bits para identificar cada host em uma rede IPv4. Para facilitar a leitura, os endereços são escritos em notação decimal com pontos, sendo que cada endereço tem quatro octetos de comprimento. Por exemplo, o endereço 00001010000000010000000100000001 em binário é escrito como 10.1.1.1.

Cada endereço IP é dividido nas seguintes seções:

- **ID de rede:** identifica uma rede. Os primeiros bits de uma ID de rede, conhecidos como campo de classe ou bits 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 e os intervalos de endereços IP. As três primeiras classes são mais comumente usadas.

Classe	Faixa 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 na inicialização para comunicação temporária. Esse endereço nunca é um endereço de destino válido. Os endereços que começam com 127 são reservados para teste de loopback. Os pacotes destinados a esses endereços são processados localmente como pacotes de entrada em vez de serem enviados ao link.
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 multicast.

Classe	Faixa de endereços	Observações
E	240.0.0.0 a 255.255.255.255	Reservado para uso futuro, exceto para o endereço de broadcast 255.255.255.255.

6.4.2.2. Sub-rede e mascaramento

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

O mascaramento identifica o limite entre o ID do host e a combinação de ID de rede e ID de sub-rede.

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

Antes de serem sub-redeadas, as redes de 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 sub-rede aumenta o número de endereços que não podem ser atribuídos a hosts. Portanto, usar sub-redes significa acomodar menos hosts.

Por exemplo, uma rede Classe B sem sub-rede pode acomodar 1.022 hosts a mais do que a mesma rede com 512 sub-redes.

- **Sem sub-rede:** 65534 (2^{16} - 2) hosts. (Os dois endereços deduzidos são o endereço de broadcast, que tem um ID de host totalmente um, e o endereço de rede, que tem um ID de host totalmente zero).
- **Com sub-rede:** o uso dos primeiros nove bits do ID do host para a sub-rede fornece 512 (2^9) sub-redes. No entanto, apenas sete bits permanecem disponíveis para o ID do host. Isso permite 126 (2^7 - 2) hosts em cada sub-rede, um total de 64512 (512× 126) hosts.

6.4.2.3. Métodos de configuração de endereço IP

Você pode usar os seguintes métodos para permitir que uma interface obtenha um endereço IP:

- Atribuir manualmente um endereço IP à interface.
- Configure a interface para obter um endereço IP por meio de DHCP.

6.4.2.4. 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 a fragmentação, o dispositivo o descartará.
- Se o pacote permitir a fragmentação, o dispositivo o fragmentará e encaminhará os fragmentos.

A fragmentação e a remontagem consomem recursos do sistema, portanto, defina um MTU apropriado para uma interface com base no ambiente da rede para evitar a fragmentação.

6.4.3. ARP

O ARP resolve endereços IP em endereços MAC em redes Ethernet.

6.4.3.1. Tipos de entradas da tabela ARP

Uma tabela ARP armazena entradas ARP dinâmicas e estáticas.

Entrada ARP dinâmica

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

As entradas ARP dinâmicas podem ser convertidas em entradas ARP estáticas. Essas entradas ARP estáticas não podem ser convertidas novamente em entradas dinâmicas.

Para evitar que uma interface mantenha muitas entradas ARP, você pode definir o número máximo de entradas ARP dinâmicas que a interface pode aprender.

Entrada ARP estática

Uma entrada ARP estática é configurada manualmente ou convertida de uma entrada ARP dinâmica. Ela não envelhece e não pode ser substituída por nenhuma entrada ARP dinâmica

As entradas de ARP estático protegem a comunicação entre dispositivos porque os pacotes de ataque não podem modificar o mapeamento de IP para MAC em uma entrada de ARP estático.

Para se comunicar com um host usando um mapeamento fixo de IP para MAC, configure uma entrada ARP estática no dispositivo

Para se comunicar com um host usando um mapeamento fixo de IP para MAC por meio de uma interface em uma VLAN, é necessário especificar a VLAN e a interface de saída na entrada ARP. Certifique-se de que o endereço IP esteja na mesma sub-rede que o endereço IP da interface da VLAN.

6.4.3.2. Proxy ARP

O ARP proxy permite que um dispositivo em uma rede responda a solicitações de ARP para um endereço IP em outra rede. Com o ARP proxy, os hosts em diferentes domínios de broadcast podem se comunicar entre si como se estivessem no mesmo domínio de broadcast

O proxy ARP inclui o proxy ARP comum e o proxy ARP local.

- **ARP de proxy comum:** permite a comunicação entre hosts que se conectam a diferentes interfaces da Camada 3 e residem em diferentes domínios de broadcast.
- **ARP de proxy local:** permite a comunicação entre hosts que se conectam à mesma interface da Camada 3 e residem em diferentes domínios de broadcast.

Você pode especificar um intervalo de endereços IP para o qual o proxy ARP local está ativado.

6.4.3.3. ARP gratuito

Em um pacote ARP gratuito, o endereço IP do remetente e o endereço IP de destino são os endereços IP do dispositivo de envio.

Um dispositivo envia um pacote ARP gratuito para uma das seguintes finalidades:

- Determinar se seu endereço IP já está sendo usado por outro dispositivo. Se o endereço IP já estiver sendo usado, o dispositivo será informado do conflito por uma resposta ARP.
- Informar outros dispositivos sobre uma alteração de endereço MAC.

Aprendizado gratuito de pacotes ARP

Essa função permite que um dispositivo crie ou atualize entradas ARP usando os endereços IP e MAC do remetente nos pacotes ARP gratuitos recebidos

Quando essa função está desativada, o dispositivo usa os pacotes ARP gratuitos recebidos apenas para atualizar as entradas ARP existentes. As entradas ARP não são criadas com base nos pacotes ARP gratuitos recebidos, o que economiza espaço na tabela ARP.

Respondendo com pacotes ARP gratuitos

Essa função permite que um dispositivo envie pacotes ARP gratuitos ao receber solicitações ARP cujo endereço IP do remetente esteja em uma sub-rede diferente.

Envio periódico de pacotes ARP gratuitos

A ativação do envio periódico de pacotes ARP gratuitos ajuda os dispositivos downstream a atualizar as entradas ARP ou MAC em hábil.

Esse recurso pode implementar as seguintes funções:

- **Impedir a falsificação de gateway:** a falsificação de gateway ocorre quando um invasor usa o endereço do gateway para enviar pacotes ARP gratuitos para os hosts em uma rede. Em vez disso, o tráfego destinado ao gateway dos hosts é enviado ao invasor. Como resultado, os hosts não podem acessar a rede externa. Para evitar esses ataques de falsificação de gateway, você pode habilitar o gateway para enviar pacotes ARP gratuitos em intervalos. Os pacotes ARP gratuitos contêm o endereço IP primário e os endereços IP secundários configurados manualmente do gateway, para que os hosts possam saber as informações corretas do gateway.
- **Evitar que as entradas ARP envelheçam:** se o tráfego da rede for intenso ou se o uso da CPU do host for alto, os pacotes ARP recebidos poderão ser descartados ou não serão processados imediatamente. Eventualmente, as entradas dinâmicas de ARP no host receptor se esgotam. O tráfego entre o host e os dispositivos correspondentes é interrompido até que o host recrie as entradas ARP. Para evitar esse problema, você pode ativar o gateway para enviar pacotes ARP gratuitos periodicamente. Os pacotes ARP gratuitos contêm o endereço IP primário e os endereços IP secundários configurados manualmente do gateway, para que os hosts receptores possam atualizar as entradas ARP em tempo hábil.

6.4.3.4. Proteção contra ataques ARP

Os ataques ARP e os vírus estão ameaçando a segurança da LAN. Embora o ARP seja fácil de implementar, ele não fornece nenhum mecanismo de segurança e é vulnerável a ataques à rede. Vários recursos são usados para detectar e impedir ataques ARP

- O gateway oferece suporte aos seguintes recursos
  - Roteamento ARP blackhole.
  - Supressão de fonte ARP.
  - Verificação da consistência do MAC de origem do pacote ARP.
  - Confirmação ativa de ARP.

- Detecção de ataques ARP baseados em MAC de origem.
- ARP autorizado.
- Varredura de ARP e ARP fixo.

» O dispositivo de acesso oferece suporte aos seguintes recursos:

- Proteção de gateway ARP.
- Filtragem de ARP.
- Detecção de ARP.

Proteção contra ataques de IP não solucionáveis

Se um dispositivo receber um grande número de pacotes IP não resolvíveis de um host, poderão 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 esses ataques de IP, você pode configurar os seguintes recursos:

» **Supressão de fonte ARP:** interrompe a resolução de pacotes de um host se o número de pacotes IP não resolvíveis do host exceder o limite superior em 5 segundos. O dispositivo continua a resolução de ARP quando o intervalo termina. Esse recurso é aplicável se os pacotes de ataque tiverem os mesmos endereços de origem.

» **Roteamento ARP blackhole:** cria uma rota blackhole destinada a um endereço IP não resolvível. O dispositivo descarta todos os pacotes correspondentes até que a rota blackhole se . Esse recurso é aplicável independentemente do fato de os pacotes de ataque terem os mesmos endereços de origem.

Verificação da consistência do MAC de origem do pacote ARP

Esse recurso permite que um gateway filtre os pacotes ARP cujo endereço MAC de origem no cabeçalho Ethernet seja diferente do endereço MAC do remetente no corpo da mensagem. Esse recurso permite que o gateway aprenda as entradas ARP corretas.

Confirmação ativa de ARP

Configure esse recurso nos gateways para evitar falsificação de usuário.

A confirmação ativa de ARP impede que um gateway gere entradas de ARP incorretas.

No modo estrito, um gateway executa verificações de validade mais rigorosas 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:

- Em caso afirmativo, o gateway executa a confirmação ativa. Quando a resposta ARP é verificada como válida, o gateway cria uma entrada ARP.
- Caso contrário, o gateway descarta o pacote.

Detecção de ataques ARP baseados em MAC de origem

Esse recurso 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 adicionará o endereço MAC a uma entrada de ataque ARP. Antes de a entrada ser , o dispositivo trata o ataque usando um dos seguintes métodos:

» **Monitor-Only:** gera mensagens de registro.

» **Filter (Filtro):** gera mensagens de registro e filtra os pacotes ARP subsequentes desse endereço MAC.

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

ARP autorizada

As entradas ARP autorizadas são geradas com base nas concessões de endereço dos clientes DHCP no servidor DHCP ou nas entradas de cliente dinâmico no agente de retransmissão DHCP.

Com o ARP autorizado ativado, uma interface é impedida de aprender entradas dinâmicas de ARP. Esse recurso evita a falsificação de usuários e permite que apenas clientes autorizados acessem os recursos da rede.

Varredura de ARP e ARP fixo

A varredura ARP é normalmente usada junto com o recurso ARP fixo em redes de pequena escala.

A varredura ARP cria automaticamente entradas ARP para dispositivos em um intervalo de endereços. O dispositivo executa a varredura de ARP usando as etapas a seguir:

» Envia solicitações ARP para cada endereço IP no intervalo de endereços.
» Obtém seus endereços MAC por meio de respostas ARP recebidas.
» Cria entradas ARP dinâmicas.

O ARP fixo converte as entradas dinâmicas de ARP existentes (inclusive as geradas pela varredura de ARP) em entradas estáticas de ARP. Esse recurso impede que as entradas de ARP sejam modificadas por invasores.

Limite de taxa de pacotes ARP

O recurso de limite de taxa de pacotes ARP permite que você limite a taxa de pacotes ARP entregues à CPU. Um dispositivo com detecção de ARP ativada enviará todos os pacotes ARP recebidos à CPU para inspeção. O processamento excessivo de pacotes ARP fará com que o dispositivo funcione mal ou até mesmo trave. Para resolver esse problema, configure o limite de taxa de pacotes ARP.

Configure esse recurso quando a detecção de ARP estiver ativada ou quando forem detectados ataques de inundação de ARP

Se o registro em log para o limite de taxa de pacotes ARP estiver ativado, o dispositivo enviará a taxa de pacotes ARP mais alta cruzada pelo limite dentro do intervalo de envio em uma mensagem de registro para o centro de informações. Você pode configurar o módulo do centro de informações para definir as regras de saída de registro.

Detecção de ARP

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

A detecção de ARP oferece as seguintes funções:

» **Verificação da validade do usuário:** se você ativar apenas a detecção de ARP para uma VLAN, a detecção de ARP fornecerá apenas a verificação de validade do usuário. Ao receber um pacote ARP de uma interface não confiável ARP, o dispositivo faz a correspondência dos endereços IP e MAC do remetente com as seguintes entradas:
  » Entradas de vinculação de proteção de fonte IP estática.
  » Entradas de DHCP snooping.

  Se for uma correspondência, o pacote ARP é considerado válido e é encaminhado. Se nenhuma correspondência for encontrada, o pacote ARP será considerado inválido e descartado.
» **Verificação da 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 do remetente:** 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 será encaminhado. Caso contrário, o pacote será descartado.
  » **Target MAC:** verifica o endereço MAC de destino das respostas ARP. Se o endereço MAC de destino for totalmente zero, totalmente um ou inconsistente com o endereço MAC de destino no cabeçalho da Ethernet, o pacote será considerado inválido e descartado.
  » **IP:** verifica os endereços IP do remetente e do destino das respostas ARP e o endereço IP do remetente das solicitações ARP. Os endereços IP all-one ou multicast são considerados inválidos e os pacotes correspondentes são descartados.
» **Encaminhamento restrito de ARP:** o encaminhamento restrito de ARP controla o encaminhamento de pacotes ARP recebidos em interfaces não confiáveis e que passaram pela 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 de ARP, eles serão encaminhados de acordo com o endereço MAC de destino. Se não for encontrada nenhuma correspondência na tabela de endereços MAC, eles serão encaminhados pela interface confiável.

6.4.4. DNS IPv4

O DNS (Domain Name System, sistema de nomes de domínio) é um banco de dados distribuído usado por aplicativos TCP/IP para traduzir nomes de domínio em endereços IP. O DNS IPv4 converte nomes de domínio em endereços IPv4. O DNS IPv6 converte nomes de domínio em endereços IPv6. O mapeamento de nome de domínio para endereço IP é chamado de entrada de DNS.

6.4.4.1. 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 de DNS ao servidor DNS para resolução de nomes de domínio.

Você pode configurar uma lista de sufixos de nome 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 o sufixo de aabbcc.com. O usuário só precisa digitar *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 trata 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 considerará o nome de domínio como um nome de host. Ele adiciona um sufixo DNS ao nome do host antes de executar 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 de DNS para outra operação de consulta.
- Se o usuário digitar um nome de domínio com um ponto (.) no final (por exemplo, aabbcc.com.), o resolvedor considerará o nome de domínio como um FQDN e retornará o resultado da consulta com êxito ou com falha. O ponto no final do nome de domínio é considerado um símbolo de terminação.

6.4.4.2. Resolução estática de nomes de domínio

Resolução estática de nomes de domínio significa criar manualmente mapeamentos entre nomes de domínio e endereços IP. Por exemplo, você pode criar um mapeamento de DNS estático para um dispositivo de modo que possa fazer Telnet no dispositivo usando o nome de domínio.

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

6.4.4.3. Proxy DNS

O proxy DNS executa as seguintes tarefas:

- Encaminha a solicitação do cliente DNS para o servidor DNS designado.
- Transmite a resposta do servidor DNS para o cliente.

O proxy DNS simplifica o gerenciamento da 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.

6.5. IPv6

6.5.1. IPv6

O IPv6, também chamado de IP next generation (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.

6.5.1.1. Formatos de endereço 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:0000:0000:0000:09C0:876A: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:0:0:0:9C0:876A:130B.
- Se um endereço IPv6 contiver um ou mais grupos consecutivos de zeros, eles poderão ser substituídos por dois pontos (::). Por exemplo, o endereço acima pode ser representado no formato mais curto como 2001:0:130F::9C0:876A:130B.

Um endereço IPv6 consiste em um prefixo de endereço e um ID 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 IPv6-address/prefix-length. O comprimento do prefixo é um número decimal que indica quantos bits mais à esquerda do endereço IPv6 estão no prefixo do endereço.

6.5.1.2. 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 (normalmente pertencentes a nós diferentes), 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 difusão são substituídos por endereços multicast no IPv6.
- **Endereço anycast:** um identificador para um conjunto de interfaces (normalmente pertencentes a nós diferentes). Um pacote enviado a 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 de prefixo de formato. A tabela a seguir mostra os mapeamentos entre os tipos de endereço e os prefixos de formato:

Tipo		Prefixo do formato (binário)	ID do prefixo IPv6	Observações
Endereço unicast	Endereço não especificado	00...0 (128 bits)	::/128	Ele 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 endereço IPv6 de destino.
	Endereço de loopback	00...1 (128 bits)	::1/128	Ele tem a mesma função que o endereço de loopback no IPv4. Não pode ser atribuído a nenhuma interface física. Um nó usa esse endereço para enviar um pacote IPv6 para si mesmo.
	Endereço local do link	1111111010	FE80::/10	Usado para comunicação entre nós locais de link para descoberta de vizinhos e autoconfiguração sem estado. Os pacotes com endereços de origem ou destino link-local não são encaminhados para outros links.
	Endereço unicast global	Outras formas	N/A	Equivalentes aos endereços IPv4 públicos, os endereços unicast globais são fornecidos para os provedores de serviços de Internet. Esse 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		Os endereços anycast usam o espaço de endereço unicast e têm a mesma estrutura dos endereços unicast.		N/A

6.5.1.3. Identificadores de interface baseados em endereços 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 endereços EUI-64 de forma diferente.

- **Em uma interface IEEE 802 (como uma interface Ethernet e uma interface VLAN):** o identificador de interface é derivado do endereço da 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) atrás do 24º bit de alta ordem do endereço MAC.
  - Inverter o bit universal/local (U/L) (o sétimo bit de ordem alta). Essa operação faz com que o identificador de interface tenha o mesmo significado local ou global que o endereço MAC.

- **Em uma interface de túnel:** os 32 bits inferiores do identificador de interface baseado em endereço EUI-64 são o endereço IPv4 de origem da interface de túnel. Os 32 bits superiores do identificador de interface baseado em endereço EUI-64 de uma interface de túnel ISATAP são 0000:5EFE, enquanto os de outras interfaces de túnel são todos zeros.
- **Em uma interface de outro tipo:** o identificador de interface baseado em endereço EUI-64 é gerado aleatoriamente pelo dispositivo.

6.5.1.4. Métodos de configuração de endereços unicast globais IPv6

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

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

É possível configurar vários endereços unicast globais IPv6 em uma interface.

6.5.1.5. Métodos de configuração de endereços IPv6 link-local

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

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

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

- Se você usar primeiro a geração automática e depois a atribuição manual, o endereço link-local atribuído manualmente substituirá o automaticamente.
- Se você usar primeiro a atribuição manual e depois a geração automática, ocorrerão as duas situações a seguir:
  - O endereço local do link ainda é o atribuído manualmente.
  - O endereço local de link gerado automaticamente não entra em vigor. Se você Excluir o endereço atribuído manualmente, o endereço de link-local gerado automaticamente entrará em vigor.

6.5.2. ND

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

- Resolução de endereços
- Detecção de acessibilidade do vizinho
- DAD
- Descoberta de roteador/prefixo
- Autoconfiguração de endereço sem estado
- Redirecionamento
- Descreve as mensagens ICMPv6 usadas pelo ND.

Mensagem ICMPv6	Tipo	Função
Solicitação de vizinho (NS)	135	Adquire o endereço da camada de link de um vizinho.
		Verifica se um vizinho é alcançável.
		Detecta endereços duplicados.
Anúncio de vizinho (NA)	136	Responde a uma mensagem NS.
		Notifica os nós vizinhos sobre alterações na camada de link.
Solicitação de roteador (RS)	133	Solicita um prefixo de endereço e outras informações de configuração para autoconfiguração após a inicialização.

Mensagem ICMPv6	Tipo	Função
Anúncio de roteador (RA)	134	Responde a uma mensagem RS.
		Anuncia informações, como as opções de informações de prefixo e os bits de sinalização.
Redirecionamento	137	Informa o host de origem sobre um próximo salto melhor no caminho para um destino específico quando determinadas condições são .

6.5.2.1. Entradas de vizinhos

Uma entrada de vizinho armazena informações sobre um nó vizinho no link. As entradas de vizinhança podem ser dinamicamente por meio de mensagens NS e NA ou manualmente.

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

- **Método 1:** associar o endereço IPv6 e o endereço da camada de link de um vizinho à interface local da Camada 3. Se você usar o Método 1, o dispositivo localizará automaticamente a porta da Camada 2 conectada ao vizinho.
- **Método 2:** associar o endereço IPv6 e o endereço da camada de link de um vizinho a uma porta da Camada 2 em uma VLAN. Se você usar o Método 2, verifique se a interface VLAN correspondente existe e se a porta da Camada 2 pertence à VLAN.

6.5.2.2. Mensagens RA

Uma mensagem RA é anunciada por um roteador a todos os hosts no mesmo link. A mensagem RA contém o prefixo do endereço e outras informações de configuração para que os hosts gerem endereços IPv6 por meio da autoconfiguração de endereços sem estado

Você pode habilitar uma interface para enviar mensagens RA, especificar os intervalos máximo e mínimo de envio 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.

Descreve os parâmetros configuráveis em uma mensagem RA.

Parâmetro	Descrição
Prefixo IPv6/comprimento do prefixo	O comprimento do prefixo/prefixo IPv6 para que um host gere um endereço unicast global IPv6 por meio da autoconfiguração sem estado.
Vida útil válida	Especifica o tempo de vida válido de um prefixo. O endereço IPv6 gerado é válido dentro do tempo de vida válido e torna-se inválido quando o tempo de vida válido expira.
Vida útil preferida	Especifica o tempo de vida preferencial de um prefixo usado para autoconfiguração sem estado. Após a expiração do tempo de vida preferencial, o nó não poderá usar o endereço IPv6 gerado para estabelecer novas conexões, mas poderá receber pacotes destinados ao endereço IPv6. O tempo de vida preferencial não pode ser maior que o tempo de vida válido.
Sinalizador No-autoconfig	Notifica os hosts para que não usem o prefixo de endereço para autoconfiguração stateless.
Bandeira off-link	Especifica o endereço com o prefixo a ser acessado indiretamente no link.
MTU	Garante que todos os nós do link usem o mesmo MTU.
Bandeira de lúpulo ilimitada	Especifica lúpulos ilimitados em mensagens RA.
Bandeira M	Determina se um host usa a autoconfiguração com estado para obter um endereço IPv6. Se o sinalizador M estiver definido, o host usará a autoconfiguração com estado (por exemplo, de um servidor DHCPv6) para obter um endereço IPv6. Se o sinalizador não estiver definido, o host usará a autoconfiguração sem estado para gerar um endereço IPv6 de acordo com seu endereço de camada de link e as informações de prefixo na mensagem RA.
O sinalizador	Determina se um host usa a autoconfiguração com estado para obter informações de configuração diferentes do endereço IPv6. Se o sinalizador O estiver definido, o host usará a autoconfiguração com estado (por exemplo, de um servidor DHCPv6) para obter informações de configuração que não sejam o endereço IPv6. Se o sinalizador não estiver definido, o host usará a autoconfiguração sem estado.
Vida útil do roteador	Anuncia o tempo de vida de um roteador de publicidade. Se o tempo de vida for 0, o roteador não poderá ser usado como gateway padrão.

Parâmetro	Descrição
Temporizador de retransmissão	Especifica o intervalo para retransmitir a mensagem NS depois que o dispositivo não recebe uma resposta para uma mensagem NS em um período de tempo.
Preferência de roteador	Especifica a preferência do roteador em uma mensagem RA. Um host seleciona um roteador como gateway padrão de acordo com a preferência do roteador. Se as preferências do roteador forem as mesmas, o host selecionará o roteador do qual a primeira mensagem RA for recebida.
Tempo de alcance	Especifica o período alcançável para um vizinho depois que o dispositivo detecta que um vizinho é alcançável. Se o dispositivo precisar enviar um pacote ao vizinho após o período alcançável, o dispositivo confirmará novamente se o vizinho está alcançável.

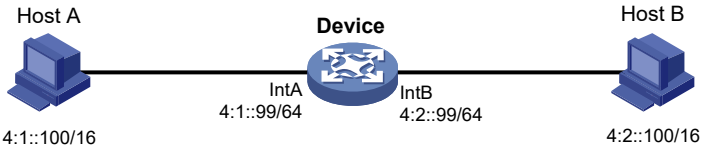
6.5.2.3. Proxy ND

O proxy ND permite que um dispositivo responda a uma mensagem NS solicitando o endereço de hardware de um host em outra rede. Com o proxy ND, os hosts em diferentes domínios de broadcast podem se comunicar uns com os outros como se estivessem na mesma rede.

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

Proxy ND comum

Conforme mostrado em , 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 residem na mesma rede, mas em domínios de broadcast diferentes.



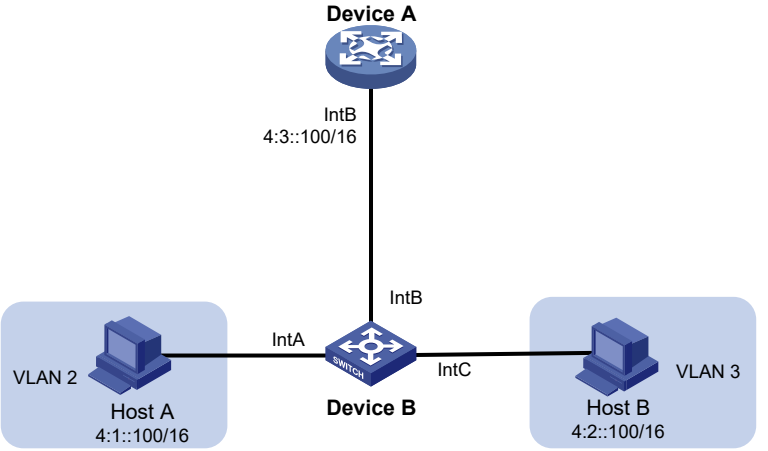
Ambiente de aplicativos do proxy ND comum

Como o endereço IPv6 do Host A está na mesma sub-rede que o do 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, ative o proxy ND comum na Interface A e na Interface B do Dispositivo. O dispositivo responde à mensagem NS do host A e encaminha os pacotes de outros hosts para o host B.

Proxy ND local

Conforme mostrado em , o host A pertence à VLAN 2 e o host B pertence à VLAN 3. O host A e o host B se conectam à interface A e à interface C, respectivamente.



Ambiente de aplicativos do proxy ND local

Como o endereço IPv6 do Host A está na mesma sub-rede que o do 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, ative o proxy ND local na Interface B do roteador para que o roteador possa encaminhar mensagens entre o Host A e o Host B.

6.5.3. DNS IPv6

O DNS (Domain Name System, sistema de nomes de domínio) é um banco de dados distribuído usado por aplicativos TCP/IP para traduzir nomes de domínio em endereços IP. O DNS IPv4 converte nomes de domínio em endereços IPv4. O DNS IPv6 converte nomes de domínio em endereços IPv6. O mapeamento de nome de domínio para endereço IP é chamado de entrada de DNS.

6.5.3.1. 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 de DNS ao servidor DNS para resolução de nomes de domínio.

Você pode configurar uma lista de sufixos de nome 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 o sufixo de aabbcc.com. O usuário só precisa digitar *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 trata as consultas com base nos nomes de domínio que o usuário insere:

- Se o usuário digitar um nome de domínio sem um ponto (.) (por exemplo, aabbcc), o resolvedor considerará o nome de domínio como um nome de host. Ele adiciona um sufixo DNS ao nome do host antes de executar 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 de DNS para outra operação de consulta.
- Se o usuário digitar um nome de domínio com um ponto (.) no final (por exemplo, aabbcc.com.), o resolvedor considerará o nome de domínio como um FQDN e retornará o resultado da consulta com êxito ou com falha. O ponto no final do nome de domínio é considerado um símbolo de terminação.

6.5.3.2. Resolução estática de nomes de domínio

Resolução estática de nomes de domínio significa criar manualmente mapeamentos entre nomes de domínio e endereços IP. Por exemplo, você pode criar um mapeamento de DNS estático para um dispositivo de modo que possa fazer Telnet no dispositivo usando o nome de domínio.

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

6.5.3.3. Proxy DNS

O proxy DNS realiza as seguintes operações:

- Encaminha a solicitação do cliente DNS para o servidor DNS designado.
- Transmite a resposta do servidor DNS para o cliente.

O proxy DNS simplifica o gerenciamento da 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.

6.6. Protocolos de gerenciamento

6.6.1. DHCP

O DHCP (Dynamic Host Configuration Protocol) fornece uma estrutura para atribuir informações de configuração a dispositivos de rede.

Um cenário típico de aplicativo DHCP tem 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.

6.6.1.1. Servidor DHCP

O servidor DHCP é adequado para redes onde:

- A configuração manual e o gerenciamento centralizado são difíceis de implementar.
- Os endereços IP são limitados. Por exemplo, um ISP limita o número de usuários on-line simultâneos, e os usuários precisam adquirir endereços IP dinamicamente.
- A maioria dos hosts não precisa de endereços IP fixos.

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

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

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

Pool de endereços DHCP

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

- **Alocação estática de endereços:** vincule manualmente o endereço MAC ou a 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 ao cliente o endereço IP na associação estática.
- **Alocação dinâmica de endereços:** especifique intervalos de endereços IP em um pool de endereços DHCP. Ao receber uma solicitação de DHCP, o servidor DHCP seleciona dinamicamente um endereço IP do intervalo de endereços IP correspondente no pool de endereços.

Você pode especificar a duração da concessão dos 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 em que um endereço IP esteja estaticamente vinculado ao endereço MAC ou à ID do cliente, o servidor DHCP selecionará esse pool de endereços e atribuirá o endereço IP estaticamente vinculado e outros parâmetros de configuração ao cliente.
- Se nenhum pool de endereços estáticos estiver configurado, o servidor DHCP selecionará um pool de endereços dependendo da 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 for encontrada uma correspondência, o servidor selecionará o pool de endereços com a sub-rede de correspondência 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 for encontrada uma correspondência, o servidor selecionará o pool de endereços com a sub-rede de correspondência mais longa.

Sequência de alocação de endereços IP

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

- Endereço IP vinculado estaticamente ao endereço MAC ou ID do cliente.
- Endereço IP que já foi atribuído ao cliente.
- Endereço IP designado pelo campo Option 50 na mensagem DHCP-DISCOVER enviada pelo cliente. A opção 50 é a opção Requested IP Address (Endereço IP solicitado). O cliente usa essa opção para especificar o endereço IP desejado em uma mensagem DHCP-DISCOVER. O conteúdo da Option 50 é definido pelo usuário.
- Primeiro endereço IP atribuível encontrado na forma de seleção de um pool de endereços.
- Endereço IP que foi um conflito ou que ultrapassou o período de concessão. Se nenhum endereço IP puder ser atribuído, o servidor não responderá.

Opções de DHCP

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

Você pode personalizar as opções para as seguintes finalidades:

» Adicionar opções de DHCP recém-lançadas.
» Adicione opções para as quais o fornecedor define o conteúdo, por exemplo, a Opção 43. Os servidores e clientes DHCP podem usar opções específicas do fornecedor para trocar informações de configuração específicas do fornecedor.
» Adicione opções para as quais a interface da Web não fornece uma página de configuração dedicada. Por, você pode usar a Opção 4 para especificar o endereço do servidor de horário 1.1.1.1 para clientes DHCP.
» Adicione todos os valores de opção 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 usadas.

Número da opção	Nome da opção	Formato de preenchimento recomendado
3	Roteador	Endereço IP
6	Servidor de nomes de domínio	Endereço IP
15	Nome de domínio	Cadeia ASCII
44	Servidor de nomes NetBIOS sobre TCP/IP	Endereço IP
46	NetBIOS sobre TCP/IP Tipo de nó	Cadeia hexadecimal
66	Nome do servidor TFTP	Cadeia ASCII
67	Nome do arquivo de inicialização	Cadeia ASCII
43	Informações específicas do fornecedor	Cadeia hexadecimal

Detecção de conflito de endereço IP

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

» Se o servidor receber uma resposta dentro do período especificado, ele seleciona e faz ping em outro endereço IP.
» Se não receber resposta, o servidor continuará a executar o ping no endereço IP até que um número específico de pacotes de ping seja enviado. Se ainda assim não houver resposta, o servidor atribuirá o endereço IP ao cliente solicitante.

6.6.1.2. Agente de retransmissão DHCP

O agente de retransmissão DHCP permite que os clientes obtenham endereços IP de um servidor DHCP em outra sub-rede. Esse recurso evita a implementação de um servidor DHCP para cada sub-rede para centralizar o gerenciamento e reduzir o investimento.

Registro de entrada de retransmissão DHCP

Essa função permite que o agente de retransmissão DHCP registre automaticamente as associações de IP para 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 os pacotes recebidos e bloquear os pacotes que não correspondem a nenhuma entrada. Dessa forma, os hosts ilegais não conseguem acessar redes externas por meio do agente de retransmissão. Exemplos de funções de segurança são verificação de endereço ARP, ARP autorizado e proteção de origem IP.

Atualização periódica de entradas dinâmicas de retransmissão DHCP

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

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

» Se o servidor retornar uma mensagem DHCP-ACK ou não retornar nenhuma mensagem em 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 manterá a entrada de retransmissão.

6.6.2. HTTP/HTTPS

O dispositivo fornece um servidor da Web incorporado. Depois de ativar o servidor da Web no dispositivo, os usuários podem fazer login na interface da Web para gerenciar e monitorar o dispositivo.

O servidor da Web incorporado ao dispositivo é compatível com o Hypertext Transfer Protocol (HTTP) (versão 1) e com o Hypertext Transfer Protocol Secure (HTTPS). O HTTPS é mais seguro que o HTTP devido aos seguintes itens:

- O HTTPS usa SSL para garantir a integridade e a segurança dos dados trocados entre o cliente e o servidor
- O HTTPS permite que você defina uma política de controle de acesso baseada em atributos de certificado para permitir que apenas clientes legais acessem a interface da Web.

Você também pode especificar uma ACL básica para HTTP ou HTTPS para impedir o acesso não autorizado à Web.

- Se você não especificar uma ACL para HTTP ou HTTPS, ou se 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 da Web por meio de HTTP ou HTTPS.

6.6.3. Telnet

O dispositivo pode atuar como um servidor Telnet para permitir o login Telnet. Depois de 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 os logins Telnet.

- Se você não especificar uma ACL para o serviço Telnet, ou se 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 fazer Telnet no dispositivo.

6.6.4. SSH

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

O SSH usa o modelo cliente-servidor típico para estabelecer um canal para transferência segura de dados com base no TCP.

O dispositivo pode atuar como um servidor SSH e fornecer os seguintes serviços para clientes SSH:

- **Telnet seguro:** o Telnet fornece serviços seguros e confiáveis de acesso a terminais de rede.
- **O Secure FTP-SFTP:** usa conexões SSH para oferecer transferência segura de arquivos com base no SSH2.
- **O Secure Copy-SCP:** oferece um método seguro para copiar arquivos com base no SSH2.

O SSH inclui duas versões: SSH1.x e SSH2.0 (doravante denominadas SSH1 e SSH2), que não são compatíveis. O SSH2 oferece melhor desempenho e segurança do que o SSH1. No modo não-FIPS, o dispositivo que atua como servidor SSH é compatível com SSH2 e SSH1. No modo FIPS, ele é compatível apenas com o SSH2.

Quando o dispositivo atua como um servidor SSH, ele suporta o uso de autenticação de senha local para examinar a validade do nome de usuário e da senha de um cliente SSH. Depois que o cliente SSH passa pela autenticação, as duas partes estabelecem uma sessão para troca de dados.

6.6.5. NTP

Sincronize seu dispositivo com uma fonte de horário confiável usando o Network Time Protocol (NTP) ou alterando o horário do sistema antes de executá-lo em uma rede ativa.

O NTP usa stratum para definir a precisão de cada servidor. O valor está no intervalo de 1 a 15. Um valor menor representa uma precisão maior.

Se os dispositivos em uma rede não puderem ser sincronizados com uma fonte de hora autorizada, você poderá realizar 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 da Web.

6.6.6. LLDP

O Link Layer Discovery Protocol (LLDP) opera na camada de enlace de dados para trocar informações sobre o dispositivo entre dispositivos diretamente conectados. Com o LLDP, um dispositivo envia informações sobre o dispositivo local como tripletos TLV (tipo, comprimento e valor) em unidades de dados LLDP (LLDPDUs) para os dispositivos diretamente conectados. As informações do dispositivo local incluem os recursos do sistema, o endereço IP de gerenciamento, a ID do dispositivo, a ID da porta e assim por diante. O dispositivo armazena as informações do dispositivo em 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 da rede da Camada 2.

6.6.6.1. Agente LLDP

Um agente LLDP é um mapeamento de uma entidade em que 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 próximo.
- Agente de ponte do cliente mais próximo.
- Agente de ponte não-TPMR mais próximo.

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

6.6.6.2. Transmissão de quadros LLDP

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

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

- Um novo quadro LLDP é recebido e contém novas informações do dispositivo para o dispositivo local.
- O modo de operação LLDP do agente LLDP muda de Disable 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 normal de transmissão de quadros LLDP é retomado.

6.6.6.3. Recebimento de quadros LLDP

Um agente LLDP operando no modo TxRx ou no modo Rx confirma a validade dos TLVs transportados em cada quadro LLDP recebido. Se os TLVs forem válidos, o agente LLDP salvará as informações e iniciará um cronômetro de envelhecimento. Quando o valor TTL no TLV Time To Live contido no quadro LLDP se torna zero, as informações envelhecem imediatamente.

Ao definir o multiplicador de TTL, você pode configurar o TTL dos LLDPDUs enviados localmente. O TTL é expresso por meio da seguinte fórmula:

TTL= Min (65535, (multiplicador TTL× intervalo de transmissão de quadros LLDP+ 1))

Como mostra a expressão, o TTL pode ser de até 65535 segundos. TTLs maiores que 65535 serão arredondados para 65535 segundos.

6.6.6.4. Atraso de reinicialização do LLDP

Quando o modo de operação do LLDP muda em uma porta, ela inicializa as máquinas de estado do protocolo após um atraso na reinicialização do LLDP. Ao ajustar o atraso, você pode evitar inicializações frequentes causadas por alterações frequentes no modo de operação LLDP em uma porta.

6.6.6.5. Trapping de LLDP

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

6.6.6.6. TLVs LLDP

Um TLV é um elemento de informação que contém os campos de tipo, comprimento e valor. As TLVs da 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 final de mídia)

Os TLVs de gerenciamento básico são essenciais para o gerenciamento do dispositivo.

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

6.6.6.7. Compatibilidade com CDP

A compatibilidade com CDP permite que seu dispositivo receba e reconheça os pacotes CDP de um telefone IP da Cisco e responda com pacotes CDP.

7. Segurança da rede

7.1. Políticas de tráfego

7.1.1. Filtro de pacotes

O filtro de pacotes usa ACLs para filtrar pacotes de entrada ou saída nas interfaces. Uma interface permite a passagem de pacotes que correspondem às instruções de permissão e nega os pacotes que correspondem às instruções de negação. A ação padrão se aplica a pacotes que não correspondem a nenhuma regra de ACL.

7.1.2. Mapeamento de prioridades

Quando um pacote chega, um dispositivo atribui valores de parâmetros de prioridade ao pacote para fins de agendamento de fila e controle de congestionamento.

O mapeamento de prioridade permite que você modifique os valores de prioridade do pacote de acordo com as regras de mapeamento de prioridade. Os parâmetros de prioridade decidem a prioridade de agendamento e a prioridade de encaminhamento do pacote.

7.1.2.1. Prioridade da porta

Quando uma porta é configurada com um modo de prioridade confiável, o dispositivo confia nas prioridades incluídas nos pacotes de entrada. O dispositivo resolve automaticamente as prioridades ou os bits de sinalização incluídos nos pacotes. Em seguida, o dispositivo mapeia a prioridade confiável para os tipos e valores de prioridade de destino de acordo com os mapas de prioridade

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

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

- **Untrust:** não confia em nenhuma prioridade incluída nos pacotes
- **Dot1p:** confia nas prioridades 802.1p incluídas nos pacotes
- **DSCP:** confia nas prioridades DSCP incluídas nos pacotes IP

7.1.2.2. Mapa de prioridades

O dispositivo fornece vários mapas de prioridade. Se um mapa de prioridade padrão não atender às suas necessidades, você poderá modificar o mapa de prioridade conforme necessário.

7.2. ACL

Uma lista de controle de acesso (ACL) é um conjunto de regras (ou instruções de permissão ou negação) 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 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 ACLs.

7.2.1. ACL tipos e critérios de correspondência

Mostra os tipos de ACL disponíveis no switch e os campos que podem ser usados para filtrar ou combinar o tráfego.

Tipo	Número 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 de protocolo. Outros campos de cabeçalho de Camada 3 e Camada 4.
		IPv6	Endereço IPv6 de origem. Endereço IPv6 de destino. Prioridade do pacote. Número de 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 da camada 2, incluindo: Endereços MAC de origem e destino. Prioridade 802.1p. Tipo de protocolo da camada de enlace.

7.2.2. Ordem de partida

As regras em uma ACL são classificadas 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 contiver regras sobrepostas ou conflitantes, o resultado da correspondência e a ação a ser tomada dependerão da ordem das regras

Os seguintes pedidos de correspondência ACL estão disponíveis:

- **config:** classifica as regras ACL em ordem crescente de ID de regra. Uma regra com um ID mais baixo é correspondida antes de uma regra com um ID mais alto. Se você usar esse método, verifique cuidadosamente as regras e sua ordem.
- Classifica automaticamente as regras ACL em ordem de profundidade. A ordenação em profundidade assegura que qualquer subconjunto de uma regra seja sempre correspondido antes da regra. Lista a sequência de desempates que a ordenação em profundidade usa para classificar as regras de cada tipo de ACL.

Categoria ACL	Sequência de desempates
ACL básica IPv4	Instância de VPN. Mais 0s no curinga do endereço IPv4 de origem (mais 0s significa um intervalo de endereços IPv4 mais restrito). Regra configurada anteriormente.
ACL avançada IPv4	Instância de VPN. Número de protocolo específico. Mais 0s na máscara curinga do endereço IPv4 de origem. Mais 0s no curinga do endereço IPv4 de destino. Intervalo de números de porta de serviço TCP/UDP mais restrito. Regra configurada anteriormente.
ACL básica IPv6	Instância de VPN. Prefixo mais longo para o endereço IPv6 de origem (um prefixo mais longo significa um intervalo de endereços IPv6 mais restrito). Regra configurada anteriormente.
ACL avançada IPv6	Instância de VPN. Número de protocolo específico. Prefixo mais longo para o endereço IPv6 de origem. Prefixo mais longo para o endereço IPv6 de destino. Intervalo de números de porta de serviço TCP/UDP mais restrito. Regra configurada anteriormente.

Categoria ACL	Sequência de desempates
Cabeçalho do quadro Ethernet ACL	Mais 1s na máscara do endereço MAC de origem (mais 1s significa um endereço MAC menor). Mais 1s na máscara de endereço MAC de destino. Regra configurada anteriormente.

Obs.: *uma máscara curinga, também chamada de máscara inversa, é um número binário de 32 bits representado em notação decimal pontilhada. Em contraste com uma máscara de rede, os bits 0 em uma máscara curinga representam bits "importantes" e os bits 1 representam bits "". Se os bits "do care" em um endereço IP forem idênticos aos bits "do care" em um critério de endereço IP, o endereço IP corresponderá ao critério. Todos os bits "" são ignorados. Os 0s e 1s em uma máscara curinga podem ser não contíguos. Por exemplo, 0.255.0.255 é uma máscara curinga válida.*

7.2.3. Numeração de regras

As regras de ACL podem ser manualmente ou automaticamente

7.2.3.1. Etapa de numeração da regra

Se você não atribuir uma ID à regra que está criando, o sistema atribuirá automaticamente uma ID de regra a ela. A etapa de numeração da regra define o incremento pelo qual o sistema numera automaticamente as regras. Por exemplo, a etapa padrão de numeração de regras ACL é 5. Se você não atribuir IDs às regras que estiver criando, elas serão automaticamente numeradas como 0, 5, 10, 15 e assim por diante. Quanto maior a de numeração, mais regras você poderá inserir entre duas regras

Ao introduzir um intervalo 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 configurada, em que as regras da ACL são correspondidas em ordem crescente de ID de regra

7.2.3.2. Numeração e renumeração automática de regras

A ID atribuída automaticamente a uma regra ACL é o múltiplo mais alto mais próximo da etapa de numeração da ID de regra mais alta atual, começando com 0.

Por , se a etapa de numeração for 5 (o padrão) e houver cinco regras ACL numeradas como 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 a etapa muda, as regras são renumeradas, começando em 0. Por exemplo, se houver cinco regras numeradas como 5, 10, 13, 15 e 20, mudar a etapa de 5 para 2 faz com que as regras sejam renumeradas como 0, 2, 4, 6 e 8.

7.3. Autenticação de acesso

7.3.1. Autenticação MAC

A autenticação MAC controla o acesso à rede autenticando os endereços MAC de origem em um modelo de serviço. O recurso não requer software cliente, e os usuários não precisam digitar um nome de usuário e uma senha para acessar a rede. O dispositivo inicia um processo de autenticação MAC quando detecta um endereço MAC de origem desconhecida em um modelo de serviço habilitado para autenticação MAC. Se o endereço MAC for aprovado na autenticação, o usuário poderá acessar os recursos autorizados da rede. Se a autenticação falhar, o dispositivo marcará o endereço MAC como um endereço MAC silencioso, descartará o pacote e iniciará um cronômetro de silêncio. O dispositivo descarta todos os pacotes subsequentes do endereço MAC dentro do tempo de silêncio. O mecanismo de silêncio evita a autenticação repetida em um curto período de tempo.

7.3.2. 802.1X

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

7.3.2.1. Arquitetura 802.1X

O 802.1X inclui as seguintes entidades:

- **Cliente:** um terminal de usuário que busca acesso à LAN. O terminal deve ter o software 802.1X para se autenticar no dispositivo de acesso.
- **Dispositivo de acesso:** autentica o cliente para controlar o acesso à LAN. Em um ambiente 802.1X típico, 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 primeiro autentica os clientes 802.1X usando os dados enviados pelo dispositivo de acesso. Em seguida, o servidor retorna os resultados da autenticação ao dispositivo de acesso para tomar decisões de acesso. Normalmente, o servidor de autenticação é um servidor RADIUS. Em uma LAN pequena, é possível usar o dispositivo de acesso como servidor de autenticação.

7.3.2.2. Métodos de autenticação 802.1X

O dispositivo de acesso pode executar o relé EAP ou a terminação EAP para se comunicar com o servidor RADIUS.

» **Encerramento do EAP:** o dispositivo de acesso executa as seguintes operações no modo de encerramento do EAP:
  » Termina os pacotes EAP recebidos do cliente.
  » Encapsula as informações de autenticação do cliente em pacotes RADIUS padrão.
  » Usa PAP ou CHAP para autenticação no servidor RADIUS.
  O CHAP não envia a senha de texto simples para o servidor RADIUS, e o PAP envia a senha de texto simples para o servidor RADIUS.

» **Retransmissão de EAP:** o dispositivo de acesso usa pacotes EAPOR para enviar informações de autenticação ao servidor RADIUS.

7.3.2.3. Métodos de controle de acesso

O Comware implementa o controle de acesso baseado em portas, conforme definido no protocolo 802.1X, e amplia o protocolo para oferecer suporte ao controle de acesso baseado em MAC.

» **Controle de acesso baseado em portas:** quando um usuário 802.1X passa pela autenticação em uma porta, todos os usuários subsequentes podem acessar a rede pela porta sem autenticação. Quando o usuário autenticado faz , todos os outros usuários são .

» **Controle de acesso baseado em MAC:** cada usuário é autenticado separadamente em uma porta. Quando um usuário faz , nenhum outro usuário on-line é afetado.

7.3.2.4. Estado de autorização da porta

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

» **Authorized:** coloca a porta no estado autorizado, permitindo que os usuários da porta acessem a rede sem autenticação.

» **Unauthorized:** coloca a porta no estado não autorizado, negando quaisquer solicitações de acesso de usuários na porta.

» **Automático:** coloca a porta inicialmente em estado não autorizado para permitir a passagem apenas de pacotes EAPOL. Depois que um usuário passa pela autenticação, define a porta no estado autorizado para permitir o acesso à rede. Você pode usar essa opção na maioria dos cenários.

7.3.2.5. Reautenticação periódica do usuário on-line

A reautenticação periódica do usuário on-line rastreia o status da conexão dos usuários on-line e atualiza os atributos de autorização atribuídos pelo servidor. Os atributos incluem a ACL, a VLAN e a QoS baseada no perfil do usuário. O intervalo de reautenticação é configurável pelo usuário.

7.3.2.6. Handshake do usuário on-line

O recurso de handshake de usuário on-line verifica o status de conectividade dos usuários 802.1X on-line. O dispositivo de acesso envia mensagens de handshake aos usuários on-line no intervalo de handshake. Se o dispositivo não receber nenhuma resposta de um usuário on-line depois de ter feito o máximo de tentativas de handshake, o dispositivo colocará o usuário no estado off-line.

Também é possível ativar o recurso de segurança de handshake do usuário on-line para verificar as informações de autenticação nos pacotes de handshake dos clientes. Com esse recurso, o dispositivo evita que os usuários 802.1X que usam software cliente ilegal contornem a verificação de segurança do iNode, como a detecção de placas de interface de rede (NICs) duplas.

7.3.2.7. Acionador de autenticação

O dispositivo de acesso inicia a autenticação se um cliente não puder enviar pacotes EAPOL-Start. Um exemplo é o cliente 802.1X disponível no Windows XP.

O dispositivo de acesso é compatível com os seguintes modos:

» **Modo de disparo unicast:** ao receber um quadro de um endereço MAC desconhecido, o dispositivo de acesso envia um pacote Identity EAP-Request da porta de recepção para o endereço MAC. O dispositivo retransmite o pacote se nenhuma resposta for recebida dentro do intervalo especificado.

» **Modo de disparo de multicast:** o dispositivo de acesso envia pacotes Identity EAP-Request periodicamente (a cada 30 segundos, por padrão) para iniciar a autenticação 802.1X.

7.3.2.8. Assistente de EAD

O Endpoint Admission Defense (EAD) é uma solução integrada de controle de acesso a endpoints da Intelbras para melhorar a capacidade de defesa contra ameaças de uma rede. A solução permite que o cliente de segurança, o servidor de política de segurança, o dispositivo de acesso e o servidor de terceiros operem juntos. Se um dispositivo terminal quiser acessar uma rede EAD, ele deverá ter um cliente EAD, que realiza a autenticação 802.1X.

O recurso de assistente de EAD permite que o dispositivo de acesso redirecione um usuário que esteja tentando acessar a rede para fazer download e instalar um cliente EAD. Esse recurso elimina a tarefa administrativa de implantar clientes EAD.

7.3.2.9. 802.1X SmartOn

O recurso SmartOn é mutuamente exclusivo do recurso de Handshake de usuário on-line 802.1X.

Quando o dispositivo envia um pacote EAP-Request/Notification unicast para o cliente, ele inicia o cronômetro de tempo limite do cliente SmartOn.

- Se o dispositivo não receber nenhum pacote EAP-Response/Notification do cliente dentro do cronômetro de tempo limite, ele retransmitirá o pacote EAP-Request/Notification para o cliente. Depois que o dispositivo tiver feito o máximo de tentativas de retransmissão, mas não tiver recebido nenhuma resposta, ele interromperá o processo de autenticação 802.1X para o cliente.

Se o dispositivo receber um pacote EAP-Response/Notification dentro do cronômetro ou antes que o máximo de tentativas de retransmissão tenha sido feito, ele iniciará a autenticação SmartOn. Se a ID do switch SmartOn e o resumo MD5 da senha SmartOn no pacote corresponderem aos do dispositivo, a autenticação 802.1X continuará para o cliente. Caso contrário, o dispositivo negará a solicitação de autenticação 802.1X do cliente.

7.3.3. Portal

A autenticação do portal controla o acesso do usuário às redes. O portal autentica um usuário pelo nome de usuário e pela senha que ele digita em uma página de autenticação do portal. Portanto, a autenticação de portal também é conhecida como autenticação da Web. Quando a autenticação de portal é implantada em uma rede, um dispositivo de acesso redireciona os usuários não autenticados para o site fornecido por um servidor da Web de portal. Os usuários podem acessar os recursos do site sem autenticação. Se os usuários quiserem acessar outros recursos da rede, deverão passar pela autenticação no site.

A autenticação de portal é classificada nos seguintes tipos:

- **Autenticação ativa:** os usuários visitam o site de autenticação fornecido pelo servidor da Web do portal e inserem seu nome de usuário e senha para autenticação.
- **Autenticação forçada:** os usuários são redirecionados para o site de autenticação do portal para autenticação quando visitam outros sites.

A autenticação de portal impõe de forma flexível o controle de acesso à camada de acesso e às entradas de dados vitais. Ela tem as seguintes vantagens:

- Permite que os usuários realizem a autenticação por meio de um navegador da Web sem instalar software cliente.
- Oferece aos ISPs opções de gerenciamento diversificadas e funções ampliadas. Por exemplo, os ISPs podem colocar anúncios, fornecer serviços comunitários e publicar informações na página de autenticação.

7.3.4. Segurança da 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 da porta oferece as seguintes funções:

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

Um quadro é ilegal se o 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. O recurso de segurança de porta executa automaticamente uma ação predefinida em quadros ilegais. Esse mecanismo automático aumenta a segurança da rede e reduz a intervenção humana.

7.4. AAA

7.4.1. Domínios ISP

O dispositivo gerencia usuários com base em domínios ISP. Um domínio ISP inclui métodos de autenticação, autorização e contabilidade para os 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.

O dispositivo é compatível com os seguintes métodos de autenticação:

- **Sem autenticação:** esse método confia em todos os usuários e não executa a autenticação. Para fins de segurança, não use esse método.
- **Autenticação local:** o dispositivo autentica os usuários por si só, com base nas informações de 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 podem ser armazenadas é limitada pelo tamanho do espaço de armazenamento.
- **Autenticação RADIUS remota:** o dispositivo funciona com um servidor RADIUS remoto para autenticar usuários. O servidor gerencia as informações do usuário de forma 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.

O dispositivo é compatível com os seguintes métodos de autorização:

- **Sem autorização:** o dispositivo não realiza nenhuma troca de autorização. As informações de autorização padrão a seguir se aplicam depois que os usuários passam pela autenticação:
  - Usuários sem login podem acessar a rede.
  - O diretório de trabalho dos usuários de FTP, SFTP e SCP é o diretório raiz do dispositivo. No entanto, os usuários não têm permissão para acessar o diretório raiz.
  - Outros usuários de login obtêm a função de usuário padrão.
- **Autorização local:** o dispositivo realiza a autorização de acordo com os atributos de usuário configurados localmente para os usuários.
- **Autorização RADIUS remota:** o dispositivo trabalha com um servidor RADIUS remoto 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 forem incluídas no pacote Access-Accept. Você pode configurar métodos de backup a serem usados quando o servidor remoto não estiver disponível.

O dispositivo é compatível com os seguintes 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 RADIUS remota:** o dispositivo funciona com um servidor RADIUS remoto para contabilidade. Você pode configurar métodos de backup a serem usados quando o servidor remoto não estiver disponível.

No dispositivo, cada usuário pertence a um domínio ISP. O dispositivo determina o domínio ISP ao qual um usuário pertence com base no nome de usuário inserido pelo usuário no 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 de usuário:

- Os usuários da LAN-LAN devem passar pela autenticação 802.1X para ficar on-line.
- Login: os usuários de login incluem usuários de Telnet, FTP e terminal que fazem login no dispositivo. Os usuários de terminal podem acessar por meio de uma porta de console.
- Usuários do Portal-Portal.

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

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

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

7.4.2. RADIUS

7.4.2.1. Protocolo RADIUS

O Remote Authentication Dial-In User Service (RADIUS) é um protocolo de interação de informações distribuídas que usa um modelo cliente/servidor. O protocolo pode proteger as redes contra acesso não autorizado e é frequentemente usado em ambientes de rede que exigem alta segurança e acesso remoto do usuário.

O cliente RADIUS é executado nos NASs localizados em toda a rede. Ele passa as informações do usuário para os servidores RADIUS e age de acordo com as respostas para, por exemplo, rejeitar ou aceitar solicitações de acesso do usuário.

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

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

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

7.4.2.2. Recursos aprimorados do RADIUS

O dispositivo oferece suporte aos seguintes recursos aprimorados do RADIUS:

- **Contabilização: esse** recurso permite que o dispositivo envie automaticamente um pacote de contabilização para o servidor RADIUS após uma reinicialização. Ao receber o pacote de contabilização, o servidor RADIUS faz o logout de todos os usuários on-line para que eles possam fazer login novamente pelo dispositivo. Sem esse recurso, os usuários não podem fazer login novamente após a reinicialização, porque o servidor RADIUS considera que eles estão on-line.

  Você pode configurar o intervalo pelo qual o dispositivo espera para reenviar o pacote de contabilização e o número máximo de tentativas.

  O servidor RADIUS deve ser executado no Inccloud para fazer o logout correto dos usuários quando um cartão for reinicializado no dispositivo distribuído ao qual os usuários se conectam.

- **Controle de sessão:** um servidor RADIUS em execução no Inccloud pode usar pacotes de controle de sessão para informar solicitações de desconexão ou de alteração de autorização dinâmica. Ative o controle de sessão no dispositivo para receber pacotes de controle de sessão RADIUS na porta UDP 1812.

7.4.3. Autenticação local

O dispositivo executa a autenticação, a autorização e a contabilidade locais com base nas informações do usuário configuradas localmente, incluindo o nome de usuário, a senha e os atributos de autorização. Cada usuário é identificado por um nome de usuário.

Os grupos de usuários simplificam a configuração e o gerenciamento de usuários locais. Um grupo de usuários contém um grupo de usuários locais e tem um conjunto de atributos de usuários locais. Os atributos de usuário de um grupo de usuários se aplicam a todos os usuários desse grupo.

7.5. Gerenciamento de usuários

O dispositivo executa a autenticação, a autorização e a contabilidade locais com base nas informações do usuário configuradas localmente, incluindo o nome de usuário, a senha e os atributos de autorização. Cada usuário é identificado por um nome de usuário.

Os grupos de usuários simplificam a configuração e o gerenciamento de usuários locais. Um grupo de usuários contém um grupo de usuários locais e tem um conjunto de atributos de usuários locais. Os atributos de usuário de um grupo de usuários se aplicam a todos os usuários desse grupo.

8.1. Registro

8.1.1. Registro de eventos

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

Valor da gravidade	Nível	Descrição
0	Emergência	O sistema está inutilizável. Por exemplo, a autorização do sistema .
1	Alerta	A 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 alimentação falha ou a bandeja do ventilador falha.
3	Erro	Condição de erro. Por exemplo, o estado do link muda ou um cartão de armazenamento é desconectado.
4	Advertência	Condição de aviso. Por exemplo, uma interface está desconectada ou os recursos de memória estão
5	Notificação	Condição normal, mas significativa. Por exemplo, um terminal faz login no dispositivo ou o dispositivo é reinicializado.
6	Informativo	Mensagem informativa. Por exemplo, um comando ou uma operação de ping é executada.
7	Depuração	Mensagem de depuração.

8.1.2. Configurações

O sistema envia os logs para destinos como o buffer de log e o host de log. Os destinos de saída de log são independentes e você pode configurá-los na interface da Web.

8.2. Recursos

8.2.1. Intervalo de tempo

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

Os seguintes tipos de intervalos de tempo estão disponíveis:

- **Intervalo de tempo periódico:** ocorre 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 por um nome. Um intervalo de tempo pode conter um ou vários intervalos de tempo periódicos e absolutos. Nesse caso, o período ativo de um intervalo de tempo é calculado da seguinte forma:

- Combinação de todos os demonstrativos periódicos.
- Combinação de todas as declarações absolutas.
- Tomando a interseção dos dois conjuntos de declarações como o período ativo do intervalo de tempo.

8.3. Gerenciamento de arquivos

8.3.1. Gerenciamento de arquivos

8.3.1.1. Sobre o gerenciamento de arquivos

Essa função é usada principalmente para atualizar a versão do dispositivo e gerenciar arquivos no dispositivo. Para solucionar vulnerabilidades na versão atual do software ou atualizar os recursos do aplicativo, use a função de atualização de versão. O gerenciamento de arquivos suporta as seguintes operações:

- **Upload:** fazer upload de arquivos locais para o dispositivo. Por exemplo, antes de atualizar o sistema do dispositivo, você deve carregar o arquivo IPE no dispositivo.
- **Excluir:** excluir arquivos no dispositivo. Ao fazer upload de arquivos para o dispositivo, se o espaço de memória for insuficiente para armazenar o arquivo, você deverá Excluir alguns arquivos não essenciais para liberar espaço de armazenamento.
- **Download:** baixar arquivos salvos no dispositivo para seu sistema local. Você pode fazer download de

arquivos do dispositivo para backup ou análise de dados.

8.3.1.2. Carregar

- Navegue até *System > File Management > File Management.*
- Clique em *Upload.*
- Navegue até o arquivo de destino.
- Clique em *OK.*

8.3.1.3. Excluir

Cuidado!

Para evitar erros de operação do dispositivo, não exclua os arquivos de versão.

- Navegue até *System > File Management > File Management.*
- Selecione os arquivos a serem excluídos.
- Clique em *Excluir.*

8.3.1.5. Baixar

- Navegue até *System > File Management > File Management.*
- Selecione os arquivos a serem baixados.
- Clique em *Download.*

8.4. Conexões em Cloud

8.4.1. Conexões em Cloud

Você pode configurar o nome de domínio do servidor de nuvem em um dispositivo para permitir que o dispositivo estabeleça uma conexão de nuvem com o servidor de nuvem. Em seguida, você pode gerenciar o dispositivo remotamente.

8.4.2. Desvinculação de dispositivos

Você pode desvincular um dispositivo do servidor Cloud usando um código de verificação.

8.5. QuickNet

8.5.1. Gerenciamento do QuickNet

Você pode ativar ou desativar o gerenciamento do QuickNet conforme necessário.

Obs.: *o suporte para as funções QuickNet depende do modelo do dispositivo.*

8.6. Gerenciamento de dispositivos

8.6.1. Administradores

Um administrador configura e gerencia o dispositivo nos seguintes aspectos:

- **Gerenciamento de conta de usuário:** gerencia informações e atributos da conta de usuário (por exemplo, nome de usuário e senha).
- **Controle de acesso baseado em função:** gerencia as permissões de acesso do usuário por função de usuário.
- **Controle de senhas:** gerencia as senhas dos usuários e controla o status de login dos usuários com base em políticas predefinidas.

O tipo de serviço de um administrador pode ser HTTP, HTTPS, SSH, Telnet, FTP, PAD ou terminal. Um usuário de terminal pode acessar o dispositivo por meio da porta do console.

8.6.1.1. 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 o nome de usuário, a senha, os serviços e os parâmetros de controle de senha.

8.6.1.2. Controle de acesso baseado em função

O controle das permissões do usuário de login é obtido por meio da atribuição de funções específicas aos usuários. Uma função define as funções do sistema que um usuário tem permissão para executar, por exemplo, definindo regras de função do usuário para permitir que os usuários configurem funções específicas ou para impedir que os usuários configurem funções específicas.

Regras de função do usuário

As regras de função do usuário permitem ou negam acesso a comandos, recursos, grupos de recursos, páginas da Web ou elementos XML. Você pode definir uma regra de menu da Web para controlar o acesso a páginas da Web por tipo de Web. Uma página da Web é identificada pelo menu da Web que pode abrir a página da Web.

Os menus da Web são divididos nos seguintes tipos:

- Menus Read-Web que exibem informações de configuração e manutenção.
- Escreva os menus da Web que configuram o recurso no sistema.
- Execute: menus da Web que executam funções específicas.

Definir uma regra é equivalente a estabelecer convenções para quais permissões de operação os usuários têm para um determinado tipo de entidade. Para menus de entidade da Web, é possível configurar regras para controlar menus da Web para determinar se é permitido operar itens específicos do menu da Web. Como cada item de menu tem atributos correspondentes de leitura, gravação ou execução, a definição de regras com base em menus da Web pode controlar com precisão as operações de controles de leitura, gravação ou execução nos itens de menu.

Funções de usuário predefinidas

O sistema fornece funções de usuário predefinidas. Essas funções de usuário têm diferentes permissões de acesso aos recursos do sistema, conforme mostrado na tabela abaixo.

Nome da função do usuário	Permissões
administrador de rede	Acessa todos os recursos e funções do sistema, exceto os recursos e funções permitidos pela função de auditoria de segurança.
operador de rede	Acessa todos os recursos e monitora o status operacional do dispositivo no sistema, exceto os recursos permitidos pela função security-audit.
nível-n (n= 0 a 15	Nível 0 a nível 14 - Para obter mais informações sobre as permissões de função de usuário, consulte a configuração do RBAC no Guia de configuração básica. É possível configurar regras personalizadas para ajustar as permissões das funções de usuário de nível 0 a nível 14, mas não é possível alterar as permissões de execução padrão. level-15 - Tem os mesmos direitos que network-admin.
auditoria de segurança	Gerente de registro de segurança. A função de usuário tem permissões de leitura, gravação e execução para arquivos de log de segurança. **Importante:** somente a função security-audit tem acesso aos arquivos de registro de segurança.
gerente de hóspedes	Acessa apenas páginas da Web relacionadas a convidados e não tem acesso a comandos.

Atribuição de função de usuário

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

- **Autorização local:** se o usuário for aprovado na autorização local, o dispositivo atribuirá as funções de usuário especificadas na conta de usuário local.
- **Autorização remota:** se o usuário for aprovado na autorização remota, o servidor AAA remoto atribuirá as funções de usuário especificadas no servidor.

Um usuário que não consegue obter uma função de usuário é desconectado do dispositivo.

Se várias funções de usuário forem atribuídas a um usuário, ele poderá usar a coleção de itens e recursos acessíveis a todas as funções de usuário.

8.6.1.3. Controle de senha

O controle de senha permite implementar os seguintes recursos:

- Gerencie a configuração de login e super senha, expirações e atualizações para usuários de gerenciamento de dispositivos.
- Controle o status de login do usuário com base em políticas predefinidas.

Os usuários locais são divididos em dois tipos: usuários de gerenciamento de dispositivos e usuários de acesso à rede. Esse recurso se aplica somente aos usuários de gerenciamento de dispositivos.

Comprimento mínimo da senha

É possível definir o tamanho mínimo das senhas de usuário. Se um usuário inserir uma senha menor do que o comprimento mínimo, o sistema rejeitará a senha.

Política de composição de senhas

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.

Nome do personagem	Símbolo	Nome do personagem	Símbolo
Sinal de E comercial	&	Apóstrofe	‘
Asterisco	*	No sinal	@
Citação anterior	`	Corte traseiro	\
Espaço em branco	N/A	Caret	^
Cólon	:	Vírgula	,
Sinal de dólar	$	Ponto	.
Sinal de igual	=	Ponto de exclamação	!
Suporte de ângulo esquerdo	<	Braçadeira esquerda	{
Suporte esquerdo	[	Parêntese esquerdo	(
Sinal de menos	-	Sinal de porcentagem	%
Sinal de mais	+	Sinal de libra	#
Aspas	“	Suporte de ângulo reto	>
Braçadeira direita	}	Suporte direito	]
Parêntese direito	)	Ponto e vírgula	;
	/	Tilde	~
Underscore	_	Barra vertical	|

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 tabela abaixo.

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, somente a combinação de nível 4 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 da complexidade da senha

Uma senha menos complicada, como uma senha que contenha o nome de usuário ou caracteres repetidos, tem maior probabilidade de ser quebrada. Para aumentar a segurança, você pode configurar uma política de verificação da complexidade da senha para garantir que todas as senhas de usuários sejam relativamente complicadas. Com essa política configurada, quando um usuário configura uma senha, o sistema verifica a complexidade da senha. Se a senha for incompatível com a complexidade, a configuração falhará

Você pode aplicar os seguintes requisitos de complexidade de senha:

- Uma senha não pode conter o nome de usuário ou o inverso do nome de usuário. Por exemplo, se o nome de usuário for abc, uma senha como abc982 ou 2cba não é suficientemente complexa.
- Um caractere ou número não pode ser incluído três ou mais vezes consecutivas. Por exemplo, a senha a111 não é suficientemente complexa.

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 como 48 horas, um usuário não poderá alterar a senha duas vezes em 48 horas.

O intervalo mínimo definido não entra em vigor quando um usuário é solicitado a alterar a senha no primeiro login ou após a do tempo de envelhecimento da senha.

Expiração da senha

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

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

Os usuários de Telnet, SSH e console podem alterar suas próprias senhas. O administrador deve alterar as senhas dos usuários de FTP.

Aviso antecipado sobre expiração de senha pendente

Quando um usuário faz login, o sistema verifica se a senha expirará em um tempo igual ou inferior ao período de notificação especificado. Em caso afirmativo, o sistema notifica o usuário quando a senha expirará e oferece uma opção para o usuário alterar a senha. Se o usuário definir uma nova senha que esteja em conformidade com a complexidade, o sistema registrará a nova senha e o tempo de configuração. Se o usuário optar por não alterar a senha ou se não conseguir alterá-la, o sistema permitirá que o usuário faça login usando a senha atual

Os usuários de Telnet, SSH e console podem alterar suas próprias senhas. O administrador deve alterar as senhas dos usuários de FTP.

Fazer login com uma senha expirada

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

Histórico de senhas

Com esse recurso ativado, o sistema armazena as senhas que um usuário usou. Quando um usuário altera a senha, o sistema compara a nova senha com a senha atual e com as armazenadas nos registros do histórico de senhas. A nova senha deve ser diferente da atual e das armazenadas nos registros do histórico em pelo menos quatro caracteres. Os quatro caracteres devem ser diferentes uns dos outros. Caso contrário, o sistema exibirá uma mensagem de erro e a senha não será alterada.

É possível definir o número máximo de registros de histórico de senhas que o sistema manterá para cada usuário. Quando o número de registros de histórico de senhas exceder a sua configuração, o registro mais recente substituirá o antigo.

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

Limite de tentativas de login

Limitar o número de falhas de login consecutivas pode impedir efetivamente a adivinhação de senhas.

O limite de tentativas de login entra em vigor para usuários de FTP e VTY. Ele não tem efeito sobre os seguintes tipos de usuários:

- Usuários inexistentes (usuários não configurados no dispositivo).
- Usuários que fazem login no dispositivo por meio de portas de console.

Se um usuário não conseguir usar uma conta de usuário para fazer login depois de fazer o número máximo de tentativas consecutivas, o limite de tentativas de login executará as seguintes ações:

- Adiciona a conta de usuário e o endereço IP do usuário à lista negra de controle de senhas. Essa conta é bloqueada apenas para esse usuário. Outros usuários ainda podem usar essa conta, e o usuário na lista negra pode usar outras contas de usuário.

- Limita o usuário e a conta de usuário de uma das seguintes maneiras:
  - Desativa a conta de usuário até que a conta seja removida manualmente da lista negra de controle de senhas.
  - Permite que o usuário continue a usar a conta de usuário. O endereço IP do usuário e a conta de usuário são removidos da lista negra de controle de senhas quando o usuário usa essa conta para fazer login com êxito no dispositivo.
  - Desativa a conta de usuário por um período de tempo

    O usuário pode usar a conta para fazer login quando houver uma das seguintes condições:
    - O cronômetro de bloqueio expira.
    - A conta é removida manualmente da lista negra de controle de senhas antes que o tempo de bloqueio expire.

Tempo máximo de inatividade da conta

É possível definir o tempo máximo de inatividade da conta para as contas de usuário. Quando uma conta fica inativa por esse período de tempo desde o último login bem-sucedido, a conta se torna inválida.

8.6.2. Configurações

Acesse a página *Settings (Configurações)* para alterar o nome do dispositivo, o local e a hora do sistema.

8.6.2.1. Fonte de tempo do sistemas

As configurações corretas da hora do sistema são essenciais para que o dispositivo coopere com outros dispositivos na rede. A hora do sistema é calculada com base no GMT, no fuso horário e no horário de verão.

Você pode usar os seguintes métodos para obter o GMT:

- Definir manualmente o GMT.
- Configure o NTP ou SNTP para obter o GMT.

O GMT obtido por meio de NTP ou SNTP é mais seguro do que o GMT configurado na CLI.

8.6.2.2. Protocolos de sincronização de relógio

O dispositivo é compatível com os seguintes protocolos de sincronização de relógio:

- **NTP - Network Time Protocol (Protocolo de horário da rede):** o NTP é normalmente usado em grandes redes para sincronizar dinamicamente a hora entre os dispositivos da rede. Ele oferece maior precisão do relógio do que a configuração manual da hora do sistema.
- **SNTP-Simple NTP:** uma implementação mais simples do NTP. O SNTP usa os mesmos formatos de pacotes e procedimentos de troca do NTP. No entanto, o SNTP simplifica o procedimento de sincronização do relógio. Em comparação com o NTP, o SNTP usa menos recursos e implementa a sincronização do relógio em menos tempo, mas oferece menor precisão de tempo.

8.6.2.3. Modos de operação NTP/SNTP

O NTP é compatível com dois modos operacionais: modo cliente/servidor e modo ativo/passivo simétrico. O dispositivo pode atuar apenas como cliente no modo cliente/servidor ou como par ativo no modo ativo/passivo simétrico.

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

Modo	Processo operacional	Princípio	Cenário de aplicação
Cliente/servidor	Um cliente envia uma mensagem de sincronização de relógio para os servidores NTP. Ao receber a mensagem, os servidores operam automaticamente no modo de servidor e enviam uma resposta. Se o cliente estiver sincronizado com vários servidores de horário, ele selecionará um relógio ideal e sincronizará seu relógio local com a fonte de referência ideal. Você pode configurar vários servidores de horário para um cliente. Esse modo de operação exige que você especifique os endereços IP dos servidores NTP no cliente.	Um cliente pode sincronizar com um servidor, mas um servidor não pode sincronizar com um cliente.	Esse modo é destinado a cenários em que dispositivos de um estrato mais alto sincronizam com dispositivos de um estrato mais baixo.

Modo	Processo operacional	Princípio	Cenário de aplicação
Ativo/passivo simétrico	Um par ativo simétrico envia periodicamente mensagens de sincronização de relógio para um par passivo simétrico O par passivo simétrico opera automaticamente no modo passivo simétrico e envia uma resposta. Se o par ativo simétrico puder ser sincronizado com vários servidores de horário, ele selecionará um relógio ideal e sincronizará seu relógio local com a fonte de referência ideal. Esse modo de operação exige que você especifique o endereço IP do par passivo simétrico no par ativo simétrico.	Um par ativo simétrico e um par passivo simétrico podem ser sincronizados um com o outro. Se ambos estiverem sincronizados, o par com um estrato mais alto será sincronizado com o par com um estrato mais baixo.	Esse modo é usado com mais frequência entre servidores com o mesmo estrato para operar 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.

8.6.2.4. Autenticação da fonte de tempo NTP/SNTP

O recurso de autenticação de fonte de horário permite que o dispositivo autentique os pacotes NTP ou SNTP recebidos. Esse recurso garante que o dispositivo obtenha o GMT correto.

8.6.3. Arquivo de configuração

Esse recurso permite que você visualize e gerencie a configuração do dispositivo.

8.6.3.1. Salvando a configuração em execução

A configuração em execução inclui configurações de inicialização inalteradas e novas configurações. A configuração em execução é armazenada na memória e é apagada em uma reinicialização ou desligamento do dispositivo. Para usar a configuração em execução após um ciclo de energia ou reinicialização, salve-a em um arquivo de configuração.

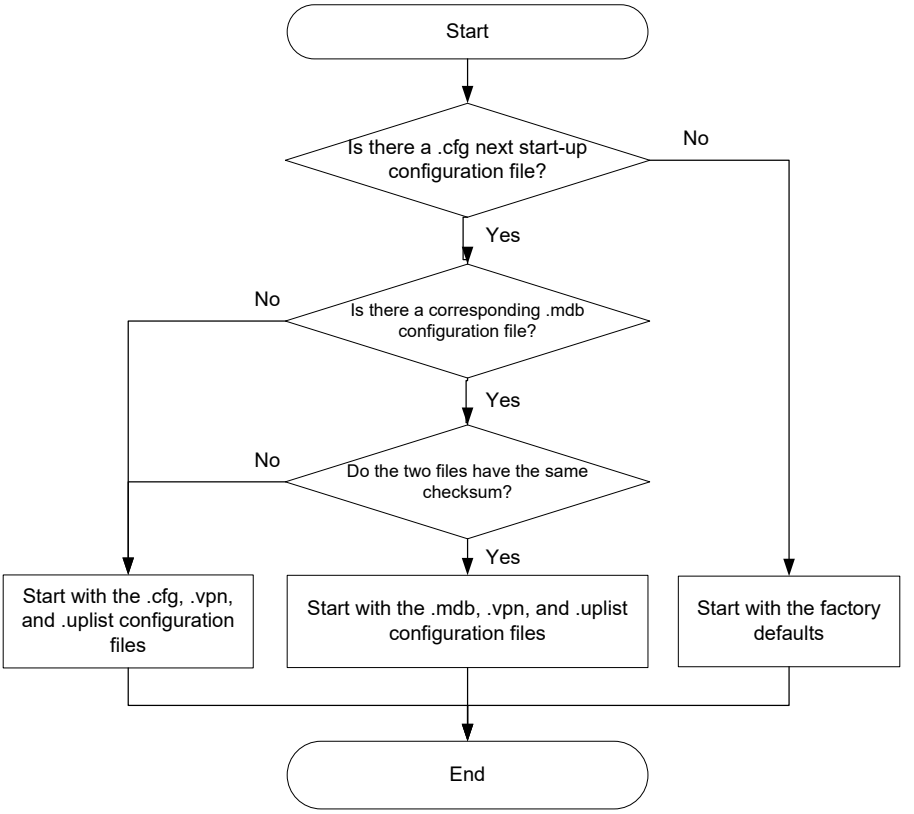
Você pode salvar a configuração em execução de uma das seguintes maneiras:

- Salve a configuração em execução no próximo arquivo de configuração de inicialização. A configuração atual ainda estará em vigor após a reinicialização do dispositivo. Se você não especificar um próximo arquivo de configuração de inicialização, o dispositivo restaurará os padrões de fábrica após a reinicialização.
- Salva a configuração em execução no arquivo de configuração especificado. A configuração será salva na memória flash do dispositivo.

Quando você salva a configuração, o sistema salva as definições em um arquivo de configuração .cfg e em um arquivo .mdb.

- Um arquivo de configuração .cfg é um arquivo de texto legível por humanos e seu conteúdo pode ser exibido com o uso do comando *more.* O conteúdo do arquivo pode ser modificado por meio de um editor de texto. Um arquivo de configuração do tipo texto pode ser salvo separadamente na mídia de armazenamento sem um arquivo de configuração do tipo binário correspondente.
- Um arquivo .mdb é um arquivo binário inacessível ao usuário que tem o mesmo nome do arquivo .cfg. Um arquivo de configuração do tipo binário não pode ser salvo somente na mídia de armazenamento e deve ter um arquivo de configuração do tipo texto correspondente. O dispositivo carrega um arquivo .mdb mais rapidamente do que um .cfg. Um dispositivo prefere um arquivo de configuração do tipo binário quando o dispositivo é iniciado.

Na inicialização, o dispositivo usa o procedimento exibido em para identificar o arquivo de configuração a ser carregado.



Fluxo de trabalho de seleção de arquivos de configuração

Salvo indicação em contrário, o termo arquivo de configuração neste documento refere-se a um arquivo de configuração .cfg.

8.6.3.2. Exportação do arquivo de configuração

Exporte a configuração em execução para um arquivo .cfg e salve o arquivo no disco local.

8.6.3.3. Importação do arquivo de configuração

Depois que você carregar o arquivo de configuração especificado no dispositivo, o arquivo será definido como o próximo arquivo de configuração de inicialização. A configuração importada entrará em vigor depois que o dispositivo for reinicializado.

Se você configurar o dispositivo para executar a configuração importada imediatamente, o sistema substituirá a configuração em execução pela configuração importada imediatamente, sem exigir uma reinicialização.

8.6.3.4. Visualização da configuração em execução

Você pode visualizar a configuração em execução do dispositivo nessa página.

8.6.3.5. Restauração dos padrões de fábrica

Os padrões de fábrica são configurações básicas personalizadas que acompanham o dispositivo.

O dispositivo será iniciado com os padrões de fábrica se não houver arquivos de configuração de próxima inicialização disponíveis.

Quando o cenário de uso muda ou o dispositivo falha, você pode restaurar o dispositivo para os padrões de fábrica, mantendo apenas os arquivos .bin e de licença, bem como a pasta apimge.

8.6.4. Atualização de software

A atualização de software permite que você atualize uma versão de software, adicione novos recursos e corrija erros de software.

Antes da atualização, obtenha o arquivo IPE do software compatível com o dispositivo de acordo com as notas de versão e salve o arquivo IPE no endpoint local. Você pode obter a versão mais recente do software no site oficial da Intelbras.

8.6.5. Reinicialização

Você pode reiniciar manualmente o dispositivo de uma das seguintes maneiras:

- Reinicie após salvar a configuração. O dispositivo mantém a configuração atual após a reinicialização.
- Reinicie sem nenhuma verificação. A configuração não salva será perdida após a reinicialização.

O dispositivo leva cerca de cinco minutos para ser reinicializado. Após a reinicialização, é necessário fazer login na interface da Web novamente.

8.6.6. Sobre

Você pode visualizar as seguintes informações nesta página:

- Informações sobre o dispositivo:
  - Nome do dispositivo.
  - Número de série do dispositivo.
  - Modelo do dispositivo.
  - Descrição do dispositivo.
  - Localização do dispositivo.
  - Informações de contato.
- Informações sobre a versão.
- Gravadora eletrônica.
- Declaração legal.

9. Ferramentas

9.1. Diagnóstico

O sistema fornece uma interface para coletar informações de diagnóstico para ajudar os usuários a diagnosticar e localizar problemas.

10. Exemplos de configuração de recursos Wireless

10.1. Exemplos de configuração de serviço Wireless

10.1.1. Exemplo de configuração de autenticação de chave compartilhada

10.1.1.1. Requisitos da rede

Conforme mostrado em , o cliente está na cobertura da WLAN. Configure a autenticação de chave compartilhada para permitir que o cliente acesse a rede usando a chave WEP *12345*.

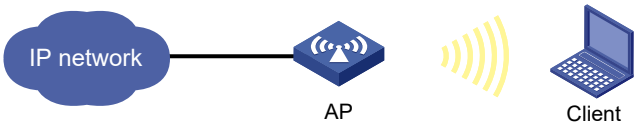


Diagrama de rede

10.1.1.2. Procedimento de configuração

- Configure um serviço Wireless:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Adicione um serviço Wireless:
    - Crie um serviço Wireless chamado *service1.*
    - Defina o SSID como *serviço.*
    - Ative o serviço Wireless.
- Clique em *Apply and Configure Advanced Settings* e, em seguida, clique na guia *Authentication (Autenticação).*
- Configurar a autenticação WEP estática:
  - Defina o tipo de segurança como WEP estático.
  - Defina o tipo de chave como *Passphrase.*
  - Selecione o pacote de cifras WEP40.
  - Defina a chave como string de texto simples *12345.*
- Aplique o serviço Wireless.
- Vincule o serviço de serviço sem *fio1* ao rádio:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Clique no ícone *Editar* na coluna *Ações para service1.*
  - Clique na guia **Binding (Vinculação**).
  - Selecione o rádio de 5 GHz do AP e clique em *Apply (Aplicar).*

10.1.1.3. Verificação da configuração

Veja os detalhes sobre o serviço wireless *service1* para verificar se a configuração está correta.

10.1.2. Exemplo de configuração da autenticação PSK e da autenticação de desvio

10.1.2.1. Requisitos da rede

Conforme mostrado em , o cliente está na cobertura da WLAN.

- Configure a autenticação de sistema aberto e a autenticação de desvio.
- Configure o cliente para usar a chave pré-compartilhada **12345678** para acessar a rede.

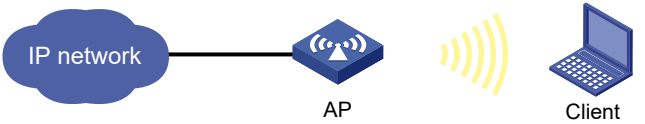


Diagrama de rede

10.1.2.2. Procedimento de configuração

- Configure um serviço Wireless:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Adicione um serviço Wireless:
    - Crie um serviço Wireless chamado *service1.*
    - Defina o SSID como *serviço.*
    - Ative o serviço Wireless.
- Clique em *Apply and Configure Advanced Settings* e, em seguida, clique na guia *Authentication (Autenticação).*
- Configure a autenticação PSK estática:
  - Defina o tipo de segurança como PSK estático.
  - Defina o modo de segurança como WPA.
  - Selecione o conjunto de cifras CCMP.
  - Defina o tipo de chave como *Passphrase* e a chave como 12345678.
- Aplique o serviço Wireless.

- Associe o serviço de serviço sem *fio1* ao rádio:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Clique no ícone *Editar* na coluna *Ações* para *service1.*
  - Clique na guia *Binding.*
  - Selecione o rádio de 5 GHz do AP e clique em *Apply (Aplicar).*

10.1.2.3. Verificação da configuração

Veja os detalhes sobre o serviço wireless *service1* para verificar se a configuração está correta.

10.1.3. Exemplo de configuração de autenticação PSK e autenticação MAC

10.1.3.1. Requisitos da rede

Conforme mostrado em , o cliente está na cobertura da WLAN.

- Configure a autenticação de sistema aberto e a autenticação MAC para clientes.
- Configure o cliente para usar a chave pré-compartilhada *12345678* para acessar a rede.

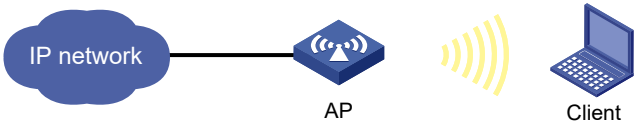


Diagrama de rede

10.1.3.2. Procedimento de configuração

- No servidor RADIUS, configure o endereço MAC do cliente como o nome de usuário e a senha usados para autenticação. O endereço MAC não pode conter hífens e letras maiúsculas.
- Configure o servidor RADIUS corretamente para fornecer funções de autenticação, autorização e contabilidade.
- Configure o RADIUS e um domínio de autenticação.
- Configure um serviço Wireless:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Adicione um serviço Wireless:
    - Crie um serviço Wireless chamado *service1.*
    - Defina o SSID como *serviço.*
    - Ative o serviço Wireless.
- Clique em *Apply and Configure Advanced Settings* e, em seguida, clique na guia *Authentication (Autenticação).*
- Configure a autenticação PSK estática e a autenticação MAC:
  - Defina o tipo de segurança como PSK estático e selecione a autenticação MAC.
  - Defina o modo de segurança como WPA.
  - Selecione o conjunto de cifras CCMP.
  - Defina o tipo de chave como *Passphrase* e a chave como *12345678.*
  - Defina o nome do domínio como *dom1.*
- Aplique o serviço Wireless.
- Associe o serviço de serviço sem *fio1* ao rádio:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Clique no ícone *Editar* na coluna *Ações* do serviço 1.
  - Clique na guia *Binding.*
  - Selecione o rádio de 5 GHz do AP e clique em *Apply (Aplicar).*

10.1.3.3. Verificação da configuração

Veja os detalhes sobre o serviço wireless *service1* para verificar se a configuração está correta.

10.2. Exemplos de configuração de QoS Wireless

10.2.1. Exemplo de configuração de limitação de taxa de clientes

10.2.1.1. Requisitos da rede

Conforme mostrado em , realize as seguintes tarefas no AP:

- Configure a limitação da taxa de clientes no modo estático para limitar a taxa de tráfego de clientes de entrada.
- Configure a limitação da taxa de clientes no modo dinâmico para limitar a taxa de tráfego de clientes de saída.

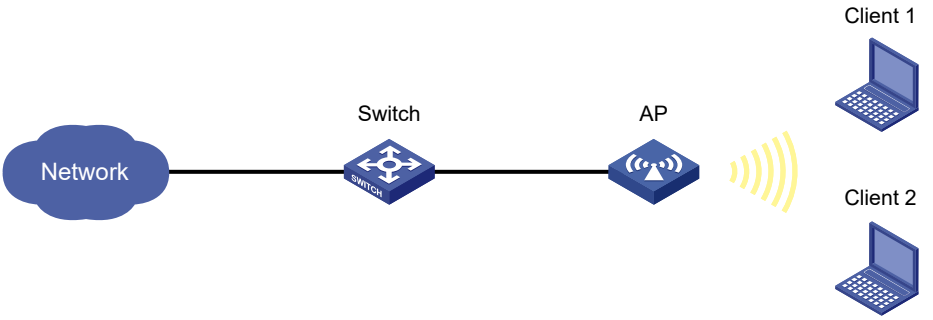


Diagrama de rede

10.2.1.2. Procedimento de configuração

- Configure um serviço Wireless:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Adicione um serviço Wireless:
    - Crie um serviço Wireless chamado *service.*
    - Defina o SSID como *serviço.*
    - Ative o serviço Wireless.
- Vincular o serviço ao rádio:
  - No painel de navegação, selecione *Wireless Configuration> AP Management> Bind WLAN Service.* Vincule o serviço de serviço ao rádio 1 do AP.
- Configurar a limitação da taxa do cliente:
  - No painel de navegação, selecione *Wireless Configuration (Configuração sem fio>Wireless QoS> Client Rate Limit (Limite de taxa do cliente).*
  - Clique no ícone *More (Mais)* na área de configuração baseada em serviço.
  - Selecione o nome do serviço *service* e clique no ícone de edição do *serviço* wireless service.
  - Na página de edição, execute as seguintes tarefas:
    - Defina o modo de limite como modo estático para o tráfego de entrada.
    - Defina a taxa de limite por cliente como *8000* para o tráfego de entrada.
    - Defina o modo de limite como modo dinâmico para o tráfego de saída.
    - Defina a taxa de limite por cliente como *4000* para o tráfego de saída.
- Ativar o rádio 1 para o AP:
  - No painel de navegação, selecione *Wireless Configuration (Configuração Wireless>Radio Management (Gerenciamento de rádios>Radio Configuration (Configuração de rádios).*
  - Ativar o rádio 1 do AP.

10.2.1.3. Verificação da configuração

Verifique se a taxa de download e a taxa de upload de cada cliente não excedem 8 Mbps e 4 Mbps, respectivamente.

10.2.2. Exemplo de configuração de garantia de largura de banda

10.2.2.1. Requisitos da rede

Conforme mostrado na , os Clientes 1, 2 e 3 acessam a rede por meio dos SSIDs research, office e entertain, respectivamente.

Para que a rede funcione corretamente, garanta 20% da largura de banda para o escritório do SSID, 80% para pesquisa e nenhum para entretenimento.

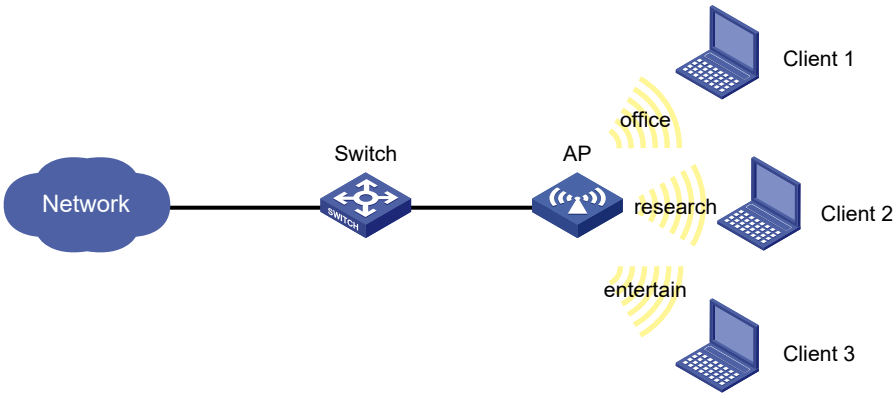


Diagrama de rede

10.2.2.2. Procedimento de configuração

- Configure os serviços Wireless:
  - Na árvore de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Adicione serviços Wireless:
    - Crie serviços sem fio denominados *escritório, pesquisa e entretenimento.*
    - Defina seu SSID como *escritório, pesquisa e entretenimento,* respectivamente.
    - Ative os serviços Wireless.
- Vincular serviços ao rádio:
  - Na árvore de navegação, selecione *Wireless Configuration > AP Management > Bind WLAN Service.* Associe os serviços *office, research e entertain* ao rádio 1 do AP.
- Configurar a garantia de largura de banda:
  - Na árvore de navegação, selecione *Wireless Configuration (Configuração sem fio)> Wireless QoS > Bandwidth Guarantee (Garantia de largura de banda).*
  - Clique no ícone mais na área de configuração do AP.
    - Habilitar a garantia de largura de banda.
    - Defina a porcentagem de largura de banda garantida como 20% para o *escritório de serviço wireless.*
    - Defina a porcentagem de largura de banda garantida como 80% para a *pesquisa de serviço Wireless.*
- Ativar o rádio 1 para o AP:
  - Na árvore de navegação, selecione *Wireless Configuration (Configuração Wireless)> Radio Management (Gerenciamento de rádios>Radio Configuration (Configuração de rádios).*
  - Ativar o rádio 1 do AP.

10.2.2.3. Verificação da configuração

Veja detalhes sobre a configuração do AP para verificar se a porcentagem de largura de banda efetiva para cada SSID não é maior que a porcentagem de largura de banda garantida.

10.3. Exemplo de configuração de gerenciamento de rádio

10.3.1. Exemplo de configuração de gerenciamento de rádio

10.3.1.1. Requisitos da rede

Conforme mostrado em , o cliente se conecta ao AP por meio da WLAN. Execute as seguintes tarefas para configurar o rádio de 5 GHz do AP:

- Defina o tipo de rádio, o canal de trabalho e a potência máxima de transmissão como 802.11ac, 153 e 18 dBm, respectivamente, para o rádio 1.
- Defina o tipo de rádio, o canal de trabalho e a potência máxima de transmissão como 802.11ac, 48 e 19 dBm, respectivamente, para o rádio 2.
- Defina o NSS máximo obrigatório, o NSS máximo suportado, o NSS multicast e o índice VHT-MCS multicast como 2, 3, 2 e 5, respectivamente.
- Ative os métodos de agregação A-MSDU e A-MPDU para melhorar a taxa de transferência da rede.

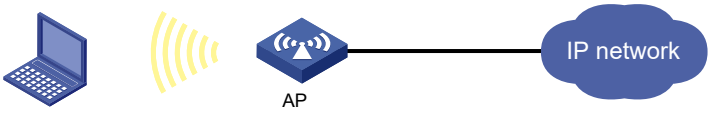


Diagrama de rede

10.3.1.2. Procedimento de configuração

- No painel de navegação, selecione *Wireless Configuration (Configuração Wireless>Radio Management (Gerenciamento de rádios>Radio Configuration (Configuração de rádios).*
- Clique no ícone *Editar* na coluna *Ações* do rádio de 5 GHz do AP. Você será colocado na guia *Basic (Básico).* Execute as seguintes tarefas para configurar o rádio 1 e o rádio 2:

  Na área de configurações básicas:

  - Defina o tipo de rádio como *802.11ac (5GHz)* para o rádio 1 e o rádio 2.
  - Defina o canal como 153 e 48 para o rádio 1 e o rádio 2, respectivamente.
  - Defina a potência máxima de transmissão como 18 dBm e 19 dBm para o rádio 1 e o rádio 2, respectivamente.

  Na área de configuração de tarifas:

  - Defina o NSS máximo obrigatório como *2.*
  - Defina o NSS máximo suportado como *3.*
  - Defina o NSS multicast como *2.*
  - Defina o índice VHT-MCS como *5.*

  Na área de configurações 802.11n/802.11ac/802.11ax:

  - Habilite o método de agregação A-MSDU.
  - Habilite o método de agregação A-MPDU.
- Aplique a configuração.

10.3.1.3. Verificação da configuração

- Acesse a página *Wireless Configuration> Radio Management> Radio Configuration.*
- Clique no ícone *Edit (Editar)* na coluna *Actions (Ações)* do de 5 GHz
- Verifique se a configuração está correta.

10.3.2. Exemplo de configuração de navegação de banda

10.3.2.1. Requisitos da rede

Tanto o rádio de 5 GHz quanto o de 2,4 GHz estão ativados no AP. Configure a navegação de banda para a navegação de banda para equilibrar a carga dos rádios.

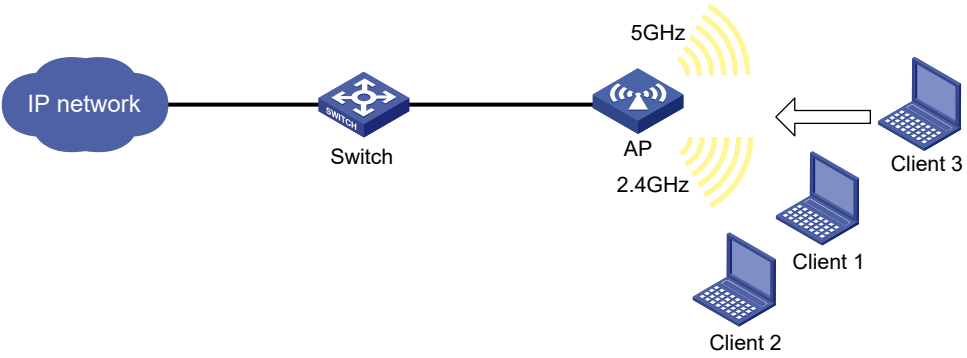


Diagrama de rede

10.3.2.2. Procedimento de configuração

- Configure um serviço Wireless:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Acesse a página para adicionar uma rede wireless para realizar as seguintes tarefas:
    - Defina o nome do serviço sem fio como *service.*
    - Defina seu SSID como *navegação por banda.*
    - Desativar a associação rápida.
    - Ative o serviço Wireless.
- Vincular o serviço ao AP:
  - Acesse a página *Wireless Configuration > Wireless Services > Wireless Services Configuration* e clique em *Edit for service* para acessar a página *Binding.*
  - Vincular **o** serviço aos rádios de 5 GHz e 2,4 GHz do AP.
- Configurar a navegação de banda:
  - No painel de navegação, selecione *Wireless Configuration> Radio Management> Band Navigation.*
  - Acesse a página de detalhes da configuração global para executar as seguintes tarefas:
    - Ativar a navegação por banda globalmente.
    - Defina o limite da sessão como 5.
    - Defina o limite de intervalo da sessão como 2.

10.3.2.3. Verificação da configuração

Verifique se os clientes que suportam 2,4 GHz e 5 GHz preferem acessar o rádio de 5 GHz (detalhes não mostrados).

Verifique se o sistema rejeita as solicitações de acesso do cliente ao rádio de 5 GHz quando as seguintes condições são atendidas:

- O número de clientes on-line no rádio de 5 GHz chega a 5.
- A diferença de quantidade de clientes entre os rádios de 5 GHz e 2,4 GHz chega a 2 (detalhes não mostrados).

Na página *Monitoramento de> Clientes> Informações do cliente,* verifique se o rádio de 5 GHz e o rádio de 2,4 GHz do AP 1 estão com balanceamento de carga.

10.4. Exemplos de configuração de segurança Wireless

10.4.1. WIPS exemplo de configuração de classificação de dispositivos e contramedidas

10.4.1.1. Requisitos da rede

Conforme mostrado em , o AP 1 e o AP 2 fornecem serviços Wireless aos clientes por meio do SSID **abc**. Execute as seguintes tarefas:

- Habilite o WIPS para o sensor.
- Configure a classificação de dispositivos Wireless para adicionar o endereço MAC *000f-1c35-12a5* à lista estática de dispositivos proibidos e o SSID *abc* à lista de SSIDs confiáveis.
- Configure contramedidas para permitir que o WIPS tome contramedidas contra APs externos em potencial e clientes não autorizados.

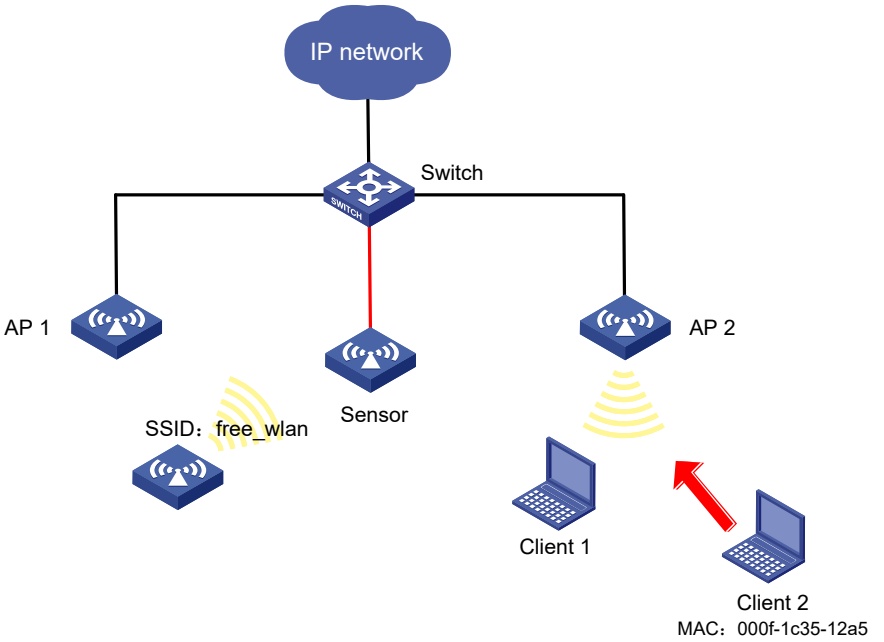


Diagrama de rede

10.4.1.2. Procedimento de configuração

- No painel de navegação, selecione *Wireless Configuration (Configuração sem fio>Wireless Security (Segurança sem fio>WIPS.*
- Clique na guia *VSD* e, em seguida, crie o VSD *VSD_1.*
- Clique na guia *WIPS Enable (Ativar WIPS),* clique em *Edit (Editar)* para o AP de destino e especifique uma lista de rádio e o nome VSD *VSD_1.*
- Clique na guia *Classification (Classificação)* e execute as seguintes tarefas:
  - Crie a política de classificação *class1.*
  - Adicione o endereço MAC do Cliente 2 à lista de dispositivos proibidos.
  - Adicione o SSID *abc* à lista de SSIDs confiáveis.
- Clique na guia *Contramedida* e execute as seguintes tarefas:
  - Crie a política de contramedida *de proteção.*
  - Configure o WIPS para tomar contramedidas contra clientes não autorizados e APs externos em potencial.
- Acesse a página de modificação de VSD para o VSD *VSD_1* para executar as seguintes tarefas:
  - Aplique a política de classificação *class1* ao VSD *VSD_1.*
  - Aplique a política de contramedida *protect* ao VSD *VSD_1.*

10.4.1.3. Verificação da configuração

Verifique se o AP com o endereço MAC *000f-e223-1616* é classificado como um AP potencialmente externo e se o cliente com o endereço MAC *000f-1c35-12a5* é classificado como um cliente não autorizado.

Verificar se o WIPS tomou contramedidas contra o cliente não autorizado com o endereço MAC *000f-1c35-12a5* e o AP potencialmente externo com o endereço MAC *000f-e223-1616.*

10.4.2. Exemplo de configuração de detecção de pacotes malformados e ataques de inundação do WIPS

10.4.2.1. Requisitos da rede

Conforme mostrado em , configure o AP como um sensor. Adicione o sensor ao VSD **VSD_1**. Configure a detecção de pacotes malformados e a detecção de ataques de inundação para permitir que o WIPS acione um alarme quando detectar ataques de inundação de beacon ou pacotes malformados com IE duplicado.

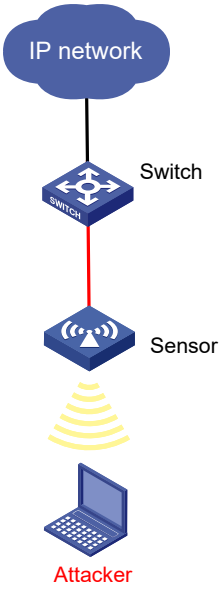


Diagrama de rede

10.4.2.2. Procedimento de configuração

- No painel de navegação, selecione *Wireless Configuration (Configuração sem fio>Wireless Security (Segurança sem fio>WIPS.*
- Clique na guia *VSD* e, em seguida, crie o VSD *VSD_1.*
- Clique na guia *WIPS Enable (Ativar WIPS),* clique em *Edit (Editar)* para o AP de destino e especifique uma lista de rádio e o nome VSD *VSD_1.*
- Clique na guia **Detection (Detecção)** e execute as seguintes tarefas:
  - Crie uma política de detecção de ataques.
  - Habilite a detecção de pacotes malformados com IE duplicado e defina o tempo de silêncio para 50 segundos.
  - Ative a detecção de ataque de inundação de beacon e defina o intervalo de estatísticas, o limite e o tempo de silêncio como 100 segundos, 200 e 50 segundos, respectivamente.
- Acesse a página de modificação do VSD *VSD_1* para aplicar a política de detecção de ataques ao VSD *VSD_1.*

10.4.2.3. Verificação da configuração

Verifique se não há pacotes malformados ou mensagens de ataque de inundação quando o WIPS não detecta nenhum ataque na WLAN.

Verifique se o número de pacotes malformados ou de mensagens de ataque de inundação não é zero quando o WIPS detecta ataques de inundação de beacon e pacotes malformados com IE duplicado.

10.4.3. Exemplo de configuração de detecção de ataques com base em assinatura

10.4.3.1. Requisitos da rede

Conforme mostrado em , o AP 1 e o AP 2 fornecem serviços Wireless para clientes por meio do SSID *abc*. Ative o WIPS para o sensor e configure uma assinatura para permitir que o WIPS acione um alarme quando detectar quadros de beacon cujos SSIDs não sejam *abc*.

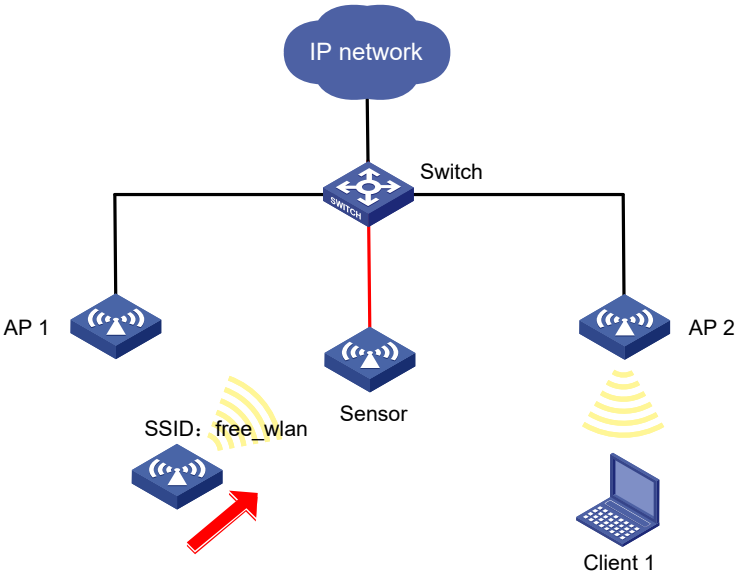


Diagrama de rede

10.4.3.2. Procedimento de configuração

- No painel de navegação, selecione *Wireless Configuration (Configuração sem fio>Wireless Security (Segurança sem fio>WIPS*.
- Clique na guia *VSD* e, em seguida, crie o VSD *VSD_1*.
- Clique na guia *WIPS Enable (Ativar WIPS),* selecione uma interface para ativar o WIPS e adicione a interface ao VSD *VSD_1*.
- Clique na guia *Signature rule (Regra de assinatura)* e execute as seguintes tarefas:
  - Criar assinatura 1.
  - Configure uma subsignatura para corresponder aos quadros de beacon.
  - Configure uma subsignatura para corresponder a quadros cujos SSIDs não sejam *abc*.
- Clique na guia *Signature (Assinatura)* e execute as seguintes tarefas:
  - Crie uma política de assinatura chamada *sig1*.
  - Vincular a assinatura 1 à política de assinatura *sig1*.
  - Defina o intervalo de detecção, o tempo de silêncio e o limite de alarme como 5 segundos, 60 segundos e 60, respectivamente.
- Acesse a página de modificação do VSD *VSD_1* para aplicar a política de assinatura *sig1* ao VSD *VSD_1*.

10.4.3.3. Verificação da configuração

Verifique se um alarme é acionado quando o sensor detecta o serviço Wireless com o SSID *free_wlan.*

Verifique se o número de mensagens detectadas para pacotes que correspondem à assinatura não é zero.

10.5. Exemplos de configuração de aplicativos

10.5.1. Exemplo de configuração de malha WLAN

10.5.1.1. Requisitos da rede

Conforme mostrado na , configure o MPP, o MAP 1 e o MAP 2 para usar o canal 149 e rádios de 5 GHz no modo 802.11n para estabelecer links de malha para o cliente acessar os recursos da rede.

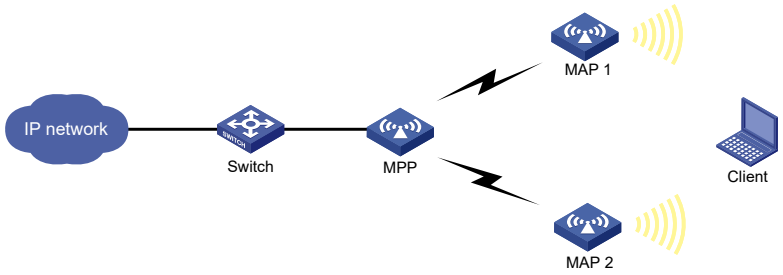


Diagrama de rede

10.5.1.2. Procedimento de configuração

- Configure um serviço wireless (somente para um MAP):
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Crie um serviço Wireless chamado *service.*
  - Defina o SSID como *rede mesh.*
  - Ative o serviço Wireless.
- Vincular o serviço ao rádio (somente para um MAP):
  - No painel de navegação, selecione *Wireless Configuration> AP Management> Bind WLAN Service.* Vincule o serviço de serviço ao rádio 1 do AP.
- Configurar um perfil de malha:
  - No painel de navegação, selecione *Wireless Configuration (Configuração Wireless>Applications (Aplicativos>Mesh Services (Serviços de malha).*
  - Clique no ícone *Add (Adicionar+na área Mesh Profile (Perfil de malha).*
  - Defina o número do perfil como 1.
  - Habilite o perfil de malha.
  - Defina a ID da malha como 1.
  - Defina o modo de autenticação e gerenciamento de chaves como *SAE* e especifique a chave para 12345678.
  - Mantenha as configurações padrão para os outros campos.
- Vincular o perfil de malha aos rádios:
  - No painel de navegação, selecione *Wireless Configuration (Configuração Wireless>Applications (Aplicativos>Mesh Services (Serviços de malha).*
  - Clique no ícone *More (Mais)* na área *Binding Info (Informações de encadernação).*
  - Selecione o rádio de 5 GHz e associe o perfil de malha 1 ao rádio.
- Configurar a lista de permissões de pares (somente para um MAP):
  - No painel de navegação, selecione *Wireless Configuration (Configuração Wireless>Applications (Aplicativos>Mesh Services (Serviços de malha).*
  - Clique no ícone *More (Mais)* na área *Mesh Peer Whitelist (Lista de permissões de pares de malha).*
  - Clique em *Edit* para o rádio de 5 GHz. Configure o endereço MAC do par para adicionar o MPP à lista de permissões do MAP 1 e do MAP 2 para que os MAPs estabeleçam links de malha somente com o MPP para evitar loops.

- Configure o modo e o canal do rádio:
  - No painel de navegação, selecione *Wireless Configuration (Configuração Wireless>Radio Management (Gerenciamento de rádios>Radio Configuration (Configuração de rádios).*
  - Configure o rádio de 5 GHz da seguinte forma:
    - Defina o modo de rádio como 802.11n (5 GHz).
    - Defina o canal como 149.
    - Ativar o rádio.

10.5.1.3. Verificação da configuração

Verifique se o cliente pode acessar a rede e se é possível visualizar as estatísticas de pacotes de links de malha na interface da Web.

10.5.2. Exemplo de configuração de otimização de multicast

10.5.2.1. Requisitos da rede

Conforme mostrado em , o AP se conecta ao switch. Configure a otimização de multicast IPv4 para gerenciar o encaminhamento de pacotes multicast.

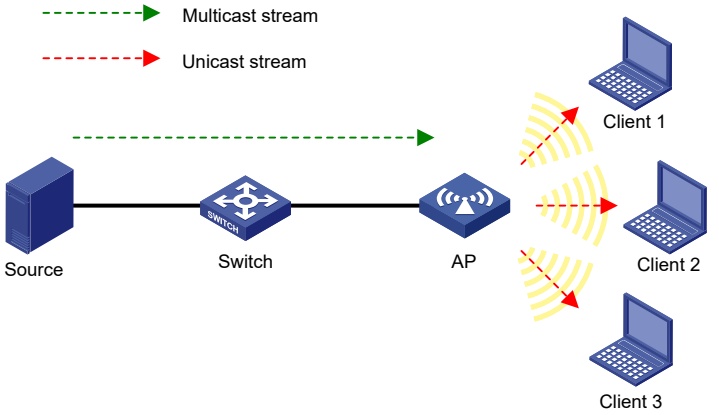


Diagrama de rede

10.5.2.2. Procedimento de configuração

- Configure um serviço Wireless:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Crie um serviço Wireless chamado *service1.*
  - Defina o SSID como *serviço.*
  - Ative o serviço Wireless.
- Vincular o serviço ao rádio:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Selecione service *service1* e clique em *Bind to Radio* para acessar a página *Bind to Radio.*
  - Selecione o rádio de 5 GHz do AP e clique em *Bind (Vincular).*
- Configurar a otimização de multicast:
  - No painel de navegação, selecione *Wireless Configuration (Configuração Wireless>Applications (Aplicativos>Multicast Optimization (Otimização de Multicast).*
  - Clique no ícone *More (Mais)* para otimização de multicast IPv4.
  - Habilite a otimização multicast para o *serviço* de serviço sem *fio1.*
  - Clique na guia *Advanced Configuration* e execute as seguintes tarefas:
    - Defina o tempo de envelhecimento da entrada como 300 segundos.
    - Defina o limite de entrada como 1024 e defina o limite de entrada por cliente como 256.
    - Defina o limite de clientes por grupo como 2 e defina a ação para descartar pacotes multicast.
    - Configure o dispositivo para aprender um máximo de 100 pacotes IGMP a cada 60 segundos.

10.5.2.3. Verificação da configuração

Conecte o Cliente 1, o Cliente 2 e o Cliente 3 ao serviço WLAN com o *serviço SSID*.

Enviar relatórios IGMP do Cliente 1 e do Cliente 2 para participar do grupo multicast IPv4 que a origem usa para encaminhar dados multicast IPv4. Tanto o Cliente 1 quanto o Cliente 2 podem receber os dados multicast IPv4.

Enviar um relatório IGMP do Cliente 3 para participar do grupo multicast IPv4. Nenhum dos clientes pode receber os dados multicast IPv4.

11. Exemplos de configuração de recursos de rede

11.1. Exemplos de configuração de interface

11.1.1. Exemplo de configuração de agregação estática de camada 2

11.1.1.1. Requisitos da rede

Conforme mostrado em , configure um grupo de agregação estática de camada 2 AP e switch para melhorar a confiabilidade do link. Esta seção usa a configuração do AP como exemplo.

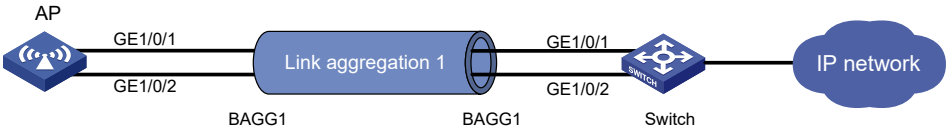


Diagrama de rede

11.1.1.2. Procedimento de configuração

- No painel de navegação, selecione *Network Configuration (Configuração de rede>Network Interfaces (Interfaces de rede>Link Aggregation (Agregação de links)*.
- Configure um grupo de agregação de camada 2:
  - Adicione o grupo de agregação de camada 2 1.
  - Configure o modo de agregação como *Estático*.
  - Atribua as portas GigabitEthernet 1/0/1 a GigabitEthernet 1/0/2 ao grupo de agregação.

11.1.1.3. Verificação da configuração

Acesse a página de agregação de links e verifique se as portas GigabitEthernet 1/0/1 a GigabitEthernet 1/0/2 foram atribuídas ao grupo de agregação de links 1.

11.1.2. Exemplo de configuração de agregação dinâmica de camada 2

11.1.2.1. Requisitos da rede

Conforme mostrado em , configure um grupo de agregação de camada 2 dinâmico AP e switch para melhorar a confiabilidade do link. Esta seção usa a configuração do AP como exemplo.

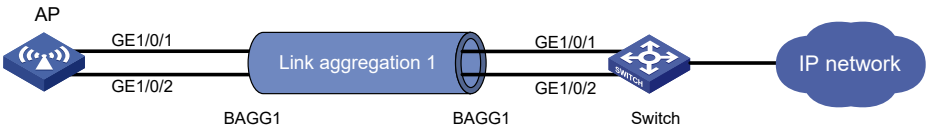


Diagrama de rede

11.1.2.2. Procedimento de configuração

- No painel de navegação, selecione *Network Configuration (Configuração de rede>Network Interfaces (Interfaces de rede>Link Aggregation (Agregação de links)*.
- Configure um grupo de agregação de camada 2:
  - Adicione o grupo de agregação de camada 2 1.
  - Configure o modo de agregação como *Dinâmico*.
  - Atribua as portas GigabitEthernet 1/0/1 a GigabitEthernet 1/0/2 ao grupo de agregação.

11.1.2.3. Verificação da configuração

Acesse a página de agregação de links e verifique se as portas GigabitEthernet 1/0/1 a GigabitEthernet 1/0/2 foram atribuídas ao grupo de agregação de links 1.

11.1.3. Cliente PPPoE exemplo de configuração

11.1.3.1. Requisitos da rede

Como mostrado em , conecte o AP gordo à Internet como um cliente PPPoE e certifique-se de que o servidor PPPoE e o cliente PPPoE possam se comunicar.

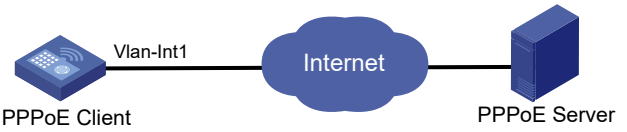


Diagrama de rede

11.1.3.2. Procedimento de configuração

Configure o servidor PPPoE para atribuir um nome de usuário e uma senha ao dispositivo. (Detalhes não mostrados.)

Configure o cliente PPPoE:

- Na árvore de navegação, selecione *Network Configuration (Configuração de rede) > Network Interfaces (Interfaces de rede >PPPoE.*
- Clique no ícone .
- Selecione a interface VLAN Vlan-interface 1.
- Digite o nome de usuário e a senha e selecione um modo on-line.
- Selecione *Abrir a função NAT* e clique em *Aplicar.*

11.1.3.3. Verificação da configuração

Verifique se o AP e o servidor PPPoE podem se comunicar.

11.2. Exemplos de configuração de links

11.2.1. Exemplo de configuração de endereço MAC

11.2.1.1. Requisitos da rede

Conforme mostrado em , os endereços MAC do Host A e do cliente são 000f-e235-dc71 e 000f-e235--abcd, respectivamente. O host A se conecta ao AP por meio da interface GigabitEthernet1/0/1. Tanto o host A quanto o cliente pertencem à VLAN 1. Defina as configurações de endereço MAC no AP para atender aos seguintes requisitos:

- Permita que os pacotes sejam encaminhados corretamente para o Host A adicionando uma entrada de endereço MAC estático.
- Proíba o cliente de receber pacotes da rede adicionando uma entrada de endereço MAC blackhole.
- O cronômetro de envelhecimento para entradas de endereço MAC dinâmico é de 500 segundos.

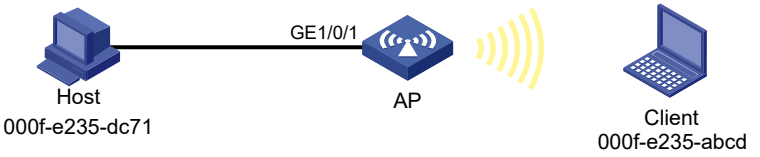


Diagrama de rede

11.2.1.2. Procedimento de configuração

No painel de navegação esquerdo, selecione *Network Configuration (Configuração de rede) > Links> MAC.* Execute as seguintes tarefas:

- Adicionar uma entrada de endereço MAC estático:
  - Especifique o endereço MAC *000f-e235-dc71.*
  - Especifique a interface de saída GigabitEthernet1/0/1.
  - Especifique a VLAN 1.
- Adicionar uma entrada de endereço MAC blackhole:
  - Especifique o endereço MAC *000f-e235-abcd.*
  - Especifique a VLAN 1.
- Clique em *Advanced settings (Configurações avançadas)* e configure o cronômetro de envelhecimento para entradas dinâmicas de endereço MAC como 500 segundos.

11.2.1.3. Verificação da configuração

Verifique se as entradas de endereço MAC estático e de blackhole foram criadas na lista com êxito. O host A não consegue fazer ping no cliente.

11.2.2. Exemplo de configuração de MSTP

11.2.2.1. Requisitos da rede

Conforme mostrado em , todos os dispositivos pertencem à região MST. O dispositivo A e o dispositivo B estão na camada de agregação e o AP 1 e o AP 2 estão na camada de acesso. Configure o MSTP para permitir que os pacotes da VLAN 10 sejam encaminhados ao longo da MSTI 1 e que os pacotes da VLAN 30 sejam encaminhados ao longo da MSTI 2.

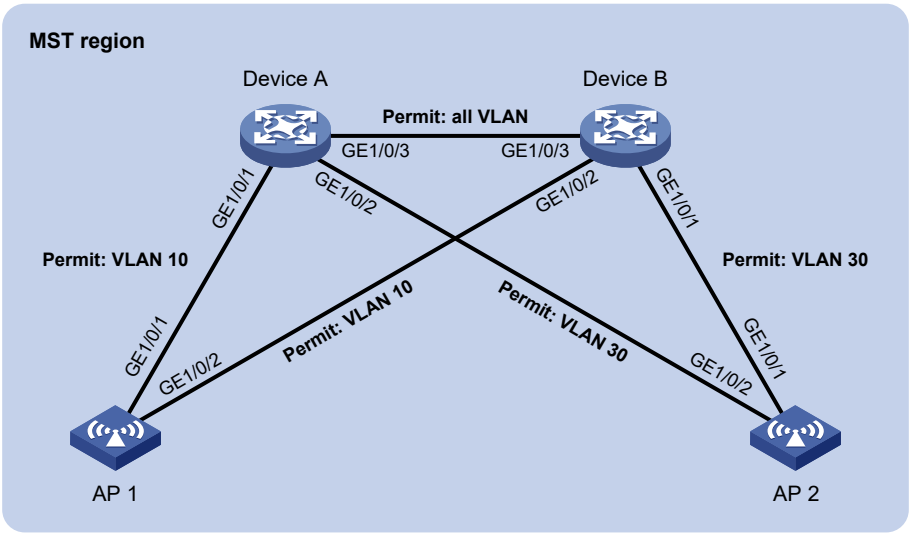


Diagrama de rede

11.2.2.2. Procedimento de configuração

- Configurar VLANs. No painel de navegação esquerdo, selecione *Network Configuration (Configuração de rede) > Links > VLAN.* Execute as seguintes tarefas:
  - Configure as VLANs no dispositivo A:
    - Criou a VLAN 10 e a VLAN 30.
    - Acesse a página de detalhes da VLAN 10 e adicione as interfaces GigabitEthernet1/0/1 e GigabitEthernet1/0/3 à lista de portas marcadas da VLAN 10.
    - Acesse a página de detalhes da VLAN 30 e adicione as interfaces GigabitEthernet1/0/2 e GigabitEthernet1/0/3 à lista de portas marcadas da VLAN 30.

- Configure VLANs no dispositivo B:
  - Criou a VLAN 10 e a VLAN 30.
  - Acesse a página de detalhes da VLAN 10 e adicione as interfaces GigabitEthernet1/0/2 e GigabitEthernet1/0/3 à lista de portas marcadas da VLAN 10.
  - Acesse a página de detalhes da VLAN 30 e adicione as interfaces GigabitEthernet1/0/1 e GigabitEthernet1/0/3 à lista de portas marcadas da VLAN 30.
- Configurar VLANs no AP 1:
  - Criou a VLAN 10.
  - Acesse a página de detalhes da VLAN 10 e adicione as interfaces GigabitEthernet1/0/1 e GigabitEthernet1/0/2 à lista de portas marcadas da VLAN 10.
- Configurar VLANs no AP 2:
  - Criou a VLAN 30.
  - Acesse a página de detalhes da VLAN 30 e adicione as interfaces GigabitEthernet1/0/1 e GigabitEthernet1/0/2 à lista de portas marcadas da VLAN 30.

- Configure o MSTP. No painel de navegação esquerdo, selecione *Network Configuration (Configuração de rede) > Network Links (Links de rede) > STP*. Execute as seguintes tarefas:
  - Ativar o STP globalmente.
  - Defina o modo de operação como MSTP para o Dispositivo A, Dispositivo B, AP 1 e AP 2.
  - Na página de região MST do Dispositivo A, Dispositivo B, AP 1 e AP 2, configure o nome da região como Web, mapeie a VLAN 10 e a VLAN 30 para MSTI 1 e MSTI 2, respectivamente, e configure o nível de revisão MSTP como 0.

11.2.2.3. Verificação da configuração

Verifique as funções e os estados das portas a partir do status da árvore de abrangência.

11.3. Exemplos de configuração de roteamento

11.3.1. Exemplo de configuração de rota estática IPv4

11.3.1.1. Requisitos da rede

Conforme mostrado na figura abaixo, configure rotas estáticas IPv4 no AP para que o cliente se comunique com o servidor WWW.

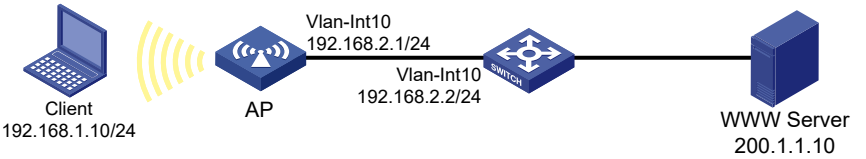


Diagrama de rede

11.3.1.2. Procedimento de configuração

- No painel de navegação, selecione *Network Configuration (Configuração de rede>Network Routing (Roteamento de rede>Static Routing (Roteamento estático)*.
- Clique em *roteamento estático IPv4*.
- Configure a rota padrão:
  - Defina o endereço IP de destino como *0.0.0.0*.
  - Defina o comprimento da máscara como *0*.
  - Defina o endereço do próximo salto como *192.168.2.2*.

11.3.1.3. Verificação da configuração

Verifique se o cliente pode acessar o servidor WWW.

11.3.2. Exemplo de configuração de rota estática IPv6

11.3.2.1. Requisitos da rede

Conforme mostrado em na figura abaixo, configure rotas estáticas de IPv6 no AP para que o cliente se comunique com o servidor WWW.

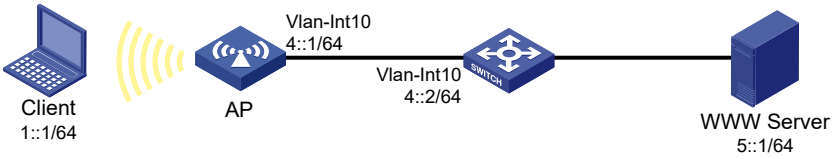


Diagrama de rede

11.3.2.2. Procedimento de configuração

- No painel de navegação, selecione *Network Configuration (Configuração de rede>Network Routing (Roteamento de rede>Static Routing (Roteamento estático).*
- Clique em *roteamento estático IPv6.*
- Configure a rota padrão IPv6:
  - Defina o endereço IP de destino como *::.*
  - Defina o comprimento da máscara como *0.*
  - Defina o endereço do próximo salto como *4::2.*

11.3.2.3. Verificação da configuração

Verifique se o cliente pode acessar o servidor WWW.

11.4. Exemplos de configuração de IP

11.4.1. Exemplo de configuração de NAT dinâmico de saída

11.4.1.1. Requisitos da rede

Conforme mostrado em , uma empresa tem um endereço privado 192.168.0.0/16 e dois endereços IP públicos 202.38.1.2 e 202.38.1.3. Configure o NAT dinâmico de saída para permitir que somente os usuários internos da sub-rede 192.168.1.0/24 acessem a Internet.

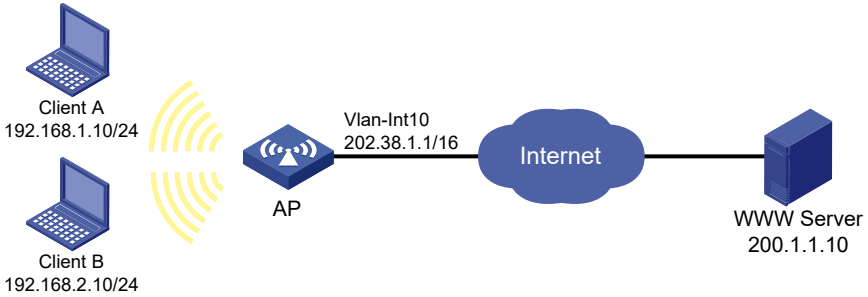


Diagrama de rede

11.4.1.2. Procedimentos de configuração

- No painel de navegação, selecione *Network Configuration (Configuração de rede>IP> NAT.*
- Clique no ícone de adição.
- Na página *New Dynamic NAT Rule,* execute as seguintes tarefas:
  - Adicione a ACL 2000 para permitir a de pacotes somente da sub-rede 192.168.1.0/24.
  - Adicione o grupo de endereços 0 e adicione um intervalo de endereços de 202.38.1.2 a 202.38.1.3 ao grupo.
- Aplique a regra de NAT dinâmico à interface Vlan 10.

11.4.1.3. Verificação da configuração

Verifique se o Cliente A consegue acessar o servidor WWW, mas o Cliente B não (detalhes não mostrados).

11.4.2. Exemplo de configuração de NAT estático de saída

11.4.2.1. Requisitos da rede

Configure o NAT estático para permitir que o cliente acesse o servidor WWW na rede externa.

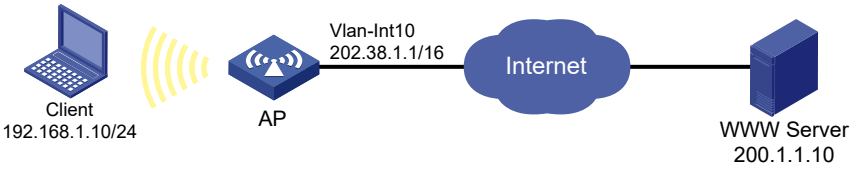


Diagrama de rede

11.4.2.2. Procedimento de configuração

- Na árvore de navegação, selecione *Network Configuration (Configuração de rede)> IP> NAT.*
- Clique em *Static NAT.*
- Clique na guia *Regras.*
- Clique no ícone  .
- Selecione o modo de tradução de *host para host.*
- Digite 192.168.1.10 no campo de endereço privado e 202.38.1.100 no campo de endereço público.
- Clique em *Aplicar.*
- Clique na guia *Aplicar.*
- Selecione a interface Vlan-interface 10.
- Clique em *Aplicar.*

11.4.2.3. Verificação da configuração

Verifique se o cliente pode acessar o servidor WWW na rede externa.

11.4.3. Exemplo de configuração de ARP proxy

11.4.3.1. Requisitos da rede

Conforme mostrado na , o Cliente 1 e o Cliente 2 têm o mesmo prefixo e máscara de IP, mas estão localizados em sub-redes diferentes separadas pelo AP. O Cliente 1 pertence à VLAN 10 e o Cliente 2 pertence à VLAN 20. Nenhum gateway padrão está configurado no Cliente 1 e no Cliente 2.

Configure o proxy ARP no AP para permitir a comunicação entre os dois clientes.

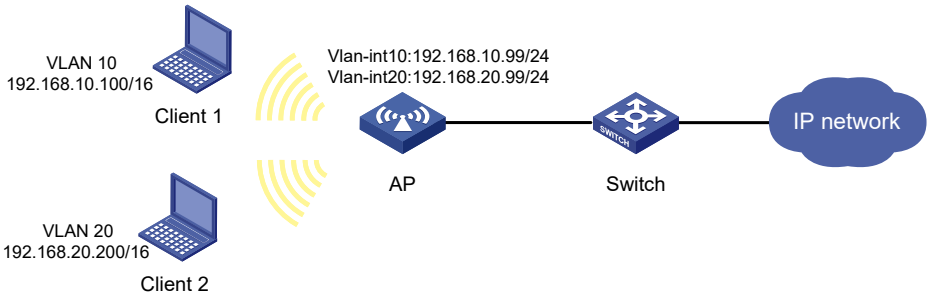


Diagrama de rede

11.4.3.2. Procedimento de configuração

- Configure a VLAN 10 e a VLAN 20 e atribua endereços IP à interface VLAN 10 e à interface VLAN 20:
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>Network Links (Links de rede>VLAN.*
  - Crie a VLAN 10 e atribua o endereço IP 192.168.10.99/24 à interface 10 da VLAN.
  - Crie a VLAN 20 e atribua o endereço IP 192.168.20.99/24 à interface 20 da VLAN.
- Habilite o ARP proxy na interface VLAN 10 e na interface VLAN 20.
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>IP> ARP.*
  - Acesse a página de configurações avançadas para configurar o proxy ARP.
    - Habilite o ARP proxy na interface VLAN 10.
    - Habilite o ARP proxy na interface VLAN 20.

11.4.3.3. Verificação da configuração

Verifique se o Cliente 1 e o Cliente 2 conseguem executar o ping um do outro com êxito.

11.4.4. Exemplo de configuração de DNS estático IPv4

11.4.4.1. Requisitos da rede

Conforme mostrado em , configure uma entrada de DNS estático no AP, para que o AP possa usar o nome de domínio *host.com* para acessar o host em 10.1.1.2.

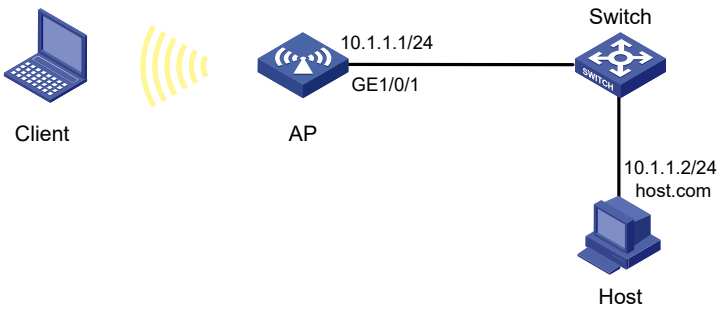


Diagrama de rede

11.4.4.2. Procedimento de configuração

- No painel de navegação, selecione *Network Configuration (Configuração de rede>IP> IPv4 DNS.*
- Na guia *Manual,* crie uma entrada de DNS estático:
  - Configure o nome do host como *host.com.*
  - Configure o endereço IPv4 como *10.1.1.2.*

11.4.4.3. Verificação da configuração

Use o comando *ping host.com* no AP para verificar os seguintes itens:

- A operação de ping foi bem-sucedida.
- O AP pode usar a resolução de nome de domínio estático para resolver o nome de domínio *host.com* no endereço IPv4 *10.1.1.2.*

11.4.5. Exemplo de configuração de DNS dinâmico IPv4

11.4.5.1. Requisitos da rede

Conforme mostrado em , o servidor DNS em 2.1.1.2/16 tem um domínio com que armazena o mapeamento entre o nome de domínio *host* e o endereço IPv4 3.1.1.1/16.

Configure o DNS dinâmico e o sufixo DNS com no AP que atua como um cliente DNS. O AP pode usar o nome de *domínio host* para acessar o host cujo nome de domínio é *host.com* e o endereço IPv4 é 3.1.1.1/16.

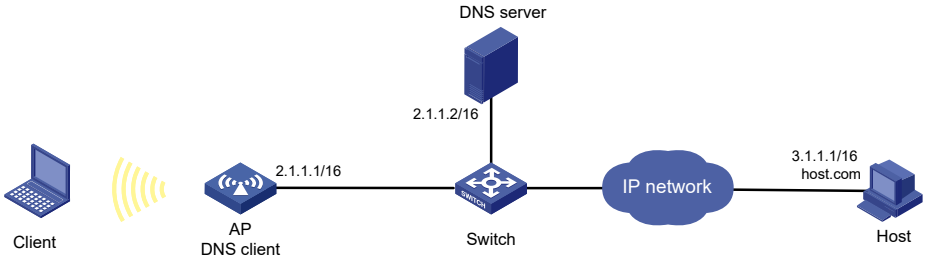


Diagrama de rede

11.4.5.2. Procedimento de configuração

- Mapeie o nome de domínio *host.com* para o endereço IPv4 3.1.1.1 no servidor DNS (detalhes não mostrados).
- Configure rotas estáticas ou protocolos de roteamento dinâmico nos dispositivos para garantir que os dispositivos possam se comunicar entre si. (Detalhes não mostrados.)
- Configurar o cliente DNS no AP:
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>IP> IPv4 DNS).*
  - Especifique o endereço do servidor DNS *2.1.1.2.*
  - Acesse a página de configurações avançadas e adicione o sufixo de nome de domínio **com**.

11.4.5.3. Verificação da configuração

Use o comando *ping host* no AP para verificar os seguintes itens:

- A operação de ping foi bem-sucedida.
- O AP pode resolver o nome de domínio *host.com* para o endereço IPv4 *3.1.1.1* por meio do servidor DNS.

11.4.6. Exemplo de configuração de proxy DNS IPv4

11.4.6.1. Requisitos da rede

Conforme mostrado em , a LAN tem um grande número de dispositivos implantados. Os dispositivos acessam o servidor DNS para resolução de nomes de domínio. Se o endereço IP do servidor DNS mudar, o administrador deverá modificar o endereço do servidor DNS em cada dispositivo, o que leva muito tempo.

Para simplificar a configuração, configure o AP como proxy de DNS. Especifique o endereço real do servidor DNS no AP. Especifique o endereço do proxy DNS como o endereço do servidor DNS nos outros dispositivos. Se o endereço do servidor DNS for alterado, o administrador só precisará modificar o endereço do servidor DNS no proxy DNS.

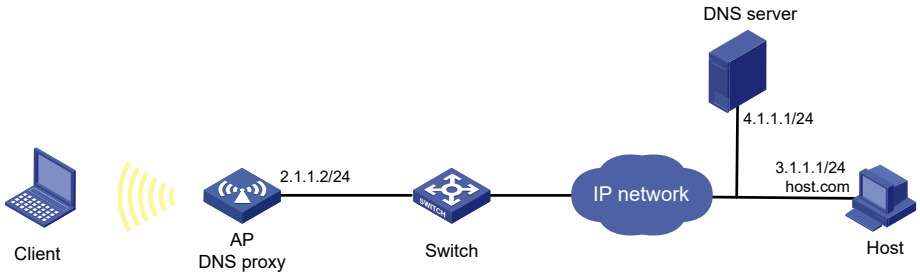


Diagrama de rede

11.4.6.2. Procedimento de configuração

- Configure rotas estáticas ou protocolos de roteamento dinâmico nos dispositivos para garantir que os dispositivos possam se comunicar entre si (detalhes não mostrados).
- Configure o servidor DNS (detalhes não mostrados).
- Configurar o proxy DNS no AP:
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>IP> IPv4 DNS.*
  - Especifique o endereço do servidor DNS *4.1.1.1.*
  - Na página de configurações avançadas, ative o proxy DNS.
- Configurar clientes DNS. Especifique o endereço de proxy DNS *2.1.1.2* como o endereço do servidor DNS nos outros dispositivos que atuam como clientes DNS.

11.4.6.3. Verificação da configuração

Use o comando *ping host.com* em um cliente DNS para verificar os seguintes itens:

- A operação de ping foi bem-sucedida.
- O cliente pode resolver o nome de domínio *host.com* para o endereço IPv4 *3.1.1.1* por meio do servidor DNS.

11.5. Exemplos de configuração de IPv6

11.5.1. Exemplo de configuração de endereço IPv6 estático

11.5.1.1. Requisitos da rede

Conforme mostrado em , o cliente gera um endereço IPv6 por meio da autoconfiguração de endereço sem estado.

Atribua um endereço IPv6 unicast global à interface VLAN 1 do AP.

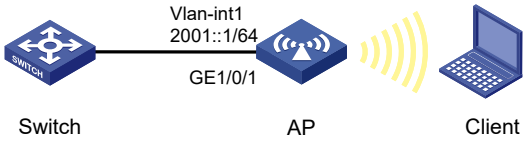


Diagrama de rede

11.5.1.2. Procedimento de configuração

- Configure o serviço Wireless e as definições de AP (detalhes não mostrados).
- Configure um endereço IPv6 para a interface VLAN 1:
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>IPv6> IPv6.*
  - Acesse a página de detalhes da interface VLAN 1 para executar as seguintes tarefas:
    - Configure o endereço IPv6 da interface como *2001::1.*
    - Defina o comprimento do prefixo como *64.*
- Configure a interface VLAN 1 para anunciar mensagens RA.
  - No painel de navegação, selecione *Configuração de rede> IPv6> ND.*
  - Acesse a página de configurações avançadas para definir as configurações de RA.
  - Configure a interface VLAN 1 para anunciar mensagens RA.
- Instale o IPv6 no cliente. O cliente gera automaticamente um endereço IPv6 com base nas informações de prefixo de endereço contidas na mensagem RA.

11.5.1.3. Verificação da configuração

Verifique se o cliente e o AP conseguem executar o ping um do outro com êxito.

11.5.2. Exemplo de configuração de DNS estático IPv6

11.5.2.1. Requisitos da rede

Conforme mostrado em , configure uma entrada de DNS estático no AP, para que o AP possa usar o nome de domínio *host.com* para acessar o host em 1::2.

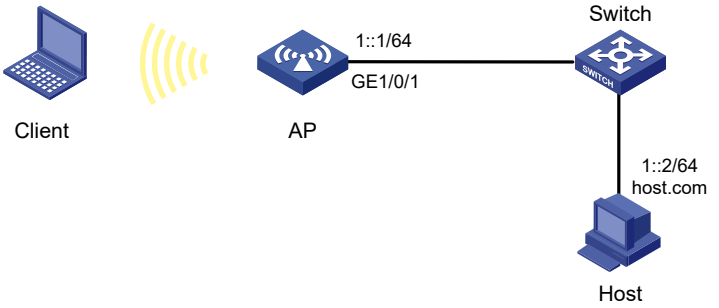


Diagrama de rede

11.5.2.2. Procedimento de configuração

- No painel de navegação, selecione *Network Configuration (Configuração de rede>IPv6> IPv6 DNS.*
- Crie uma entrada de DNS estático:
  - Configure o nome do host como *host.com.*
  - Configure o endereço IPv6 como *1::2.*

11.5.2.3. Verificação da configuração

Use o comando *ping ipv6 host.com* no AP para verificar os seguintes itens:

- A operação de ping foi bem-sucedida.
- O AP pode usar a resolução de nome de domínio estático para resolver o nome de domínio *host.com* no endereço IPv6 *1::2.*

11.5.3. Exemplo de configuração de DNS dinâmico IPv6

11.5.3.1. Requisitos da rede

Conforme mostrado em , o servidor DNS em 2::2/64 tem um domínio com que armazena o mapeamento entre o nome de domínio *host* e o endereço IPv6 1::1/64.

Configure o DNS dinâmico e o sufixo DNS com no AP que atua como um cliente DNS. O AP pode usar o nome de *domínio host* para acessar o host cujo nome de domínio é *host.com* e o endereço IPv6 é 1::1/64.

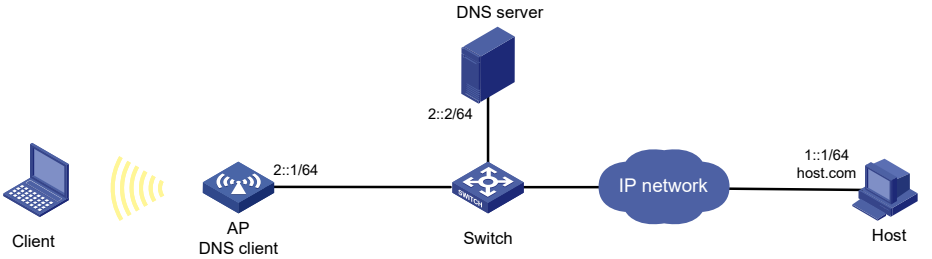


Diagrama de rede

11.5.3.2. Procedimento de configuração

- Mapeie o nome de domínio *host.com* para o endereço IPv6 1::1 no servidor DNS. (Detalhes não mostrados).
- Configure rotas estáticas ou protocolos de roteamento dinâmico nos dispositivos para garantir que os dispositivos possam se comunicar entre si (detalhes não mostrados).
- Configurar o cliente DNS no AP:
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>IPv6> IPv6 DNS.*
  - Especifique o endereço do servidor DNS *2::2.*
  - Acesse a página de configurações avançadas e adicione o sufixo de nome de domínio *com.*

11.5.3.3. Verificação da configuração

Use o comando *ping ipv6 host* no AP para verificar os seguintes itens:

- A operação de ping foi bem-sucedida.
- O AP pode resolver o nome de domínio *host.com* para o endereço IPv6 *1::1* por meio do servidor DNS.

11.5.4. Exemplo de configuração de proxy DNS IPv6

11.5.4.1. Requisitos da rede

Conforme mostrado em , a LAN tem um grande número de dispositivos implantados. Os dispositivos acessam o servidor DNS para resolução de nomes de domínio. Se o endereço IPv6 do servidor DNS for alterado, o administrador deverá modificar o endereço do servidor DNS em cada dispositivo, o que leva muito tempo.

Para simplificar a configuração, configure o AP como proxy de DNS. Especifique o endereço real do servidor DNS no AP. Especifique o endereço do proxy DNS como o endereço do servidor DNS nos outros dispositivos. Se o endereço do servidor DNS for alterado, o administrador só precisará modificar o endereço do servidor DNS no proxy DNS.

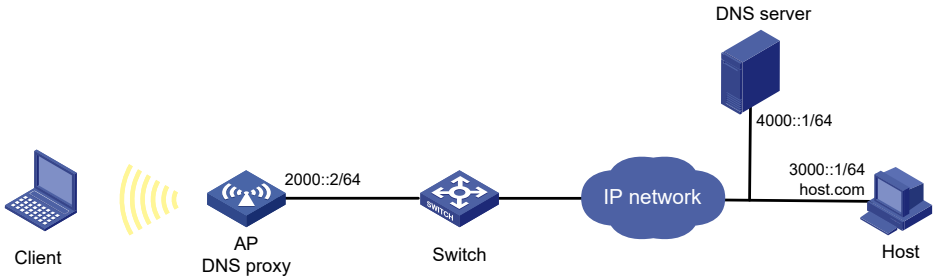


Diagrama de rede

11.5.4.2. Procedimento de configuração

- Configure rotas estáticas ou protocolos de roteamento dinâmico nos dispositivos para garantir que os dispositivos possam se comunicar entre si (detalhes não mostrados).
- Configure o servidor DNS (detalhes não mostrados).
- Configurar o proxy DNS no AP:
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>IPv6> IPv6 DNS.*
  - Especifique o endereço do servidor DNS *4000::1.*
  - Na página de configurações avançadas, ative o proxy DNS.
- Configurar clientes DNS. Especifique o endereço de proxy DNS *2000::2* como o endereço do servidor DNS nos outros dispositivos que atuam como clientes DNS.

11.5.4.3. Verificação da configuração

Use o comando *ping ipv6 host.com* em um cliente DNS para verificar os seguintes itens:

- A operação de ping foi bem-sucedida.
- O cliente pode resolver o nome de domínio *host.com* para o endereço IPv6 *3000::1* por meio do servidor DNS.

11.6. Exemplos de configuração do protocolo de gerenciamento

11.6.1. Exemplo de configuração do servidor DHCP

11.6.1.1. Requisitos da rede

Conforme mostrado na , o servidor DHCP (AP) atribui endereços IP ao switch e ao cliente DHCP na sub-rede 10.1.1.0/24, que é subdividida em 10.1.1.0/25 e 10.1.1.128/25. O AP está conectado ao cliente e ao switch por meio de duas interfaces de VLAN: VLAN-interface 10 em 10.1.1.1/25 e VLAN-interface 20 em 10.1.1.129/25.

Configure o servidor DHCP no AP para atribuir um endereço IP na sub-rede 10.1.1.0/25 ao switch e endereços IP na sub-rede 10.1.1.128/25 ao cliente DHCP.

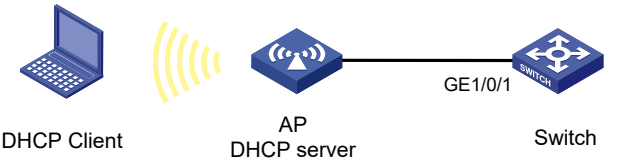


Diagrama de rede

11.6.1.2. Procedimento de configuração

- Configurar VLANs e interfaces de VLAN:
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>Network Links (Links de rede>VLAN.*
  - Criar VLANs e interfaces de VLAN:
    - Crie a *VLAN 10* e a interface VLAN 10.
    - Crie a *VLAN 20* e a interface VLAN 20.
  - Acesse *Network Configuration (Configuração de rede) > Network Interfaces (Interfaces de rede) > Interfaces,* clique em *Edit (Editar)* para a interface de destino e clique em *IP address/Mask (Endereço IP/Máscara):*
    - Atribua o endereço IP *10.1.1.1/25* à interface VLAN 10.
    - Atribua o endereço IP *10.1.1.129/25* à interface VLAN 20.
- Configure o servidor DHCP:
  - No painel de navegação, selecione *Configuração de rede> Protocolos de gerenciamento> DHCP.*
  - Ativar DHCP.
  - Especifique a interface de VLAN 10 e a interface de VLAN 20 como servidores DHCP.
  - Clique no link do pool de endereços e execute as seguintes tarefas:
    - Crie o pool de endereços *pool1,* especifique *10.1.1.0/25* como a sub-rede para atribuição dinâmica e especifique *10.1.1.1* como o gateway.
    - Crie o pool de endereços *pool2,* especifique *10.1.1.128/25* como a sub-rede para atribuição dinâmica e especifique *10.1.1.129* como o gateway.
  - Acesse a página de configurações avançadas para executar as seguintes tarefas:
    - Defina o número máximo de pacotes de ping como 1.
    - Defina o tempo limite de resposta do ping como 500 milissegundos.
- Configure um serviço Wireless:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Adicione um serviço Wireless:
    - Crie um serviço Wireless chamado *service.*
    - Defina o SSID como *escritório.*
    - Especifique a *VLAN 20* padrão.
    - Ative o serviço Wireless.
- Configurar o AP:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services > Wireless Services Configuration.*
  - Vincular **o** serviço de serviço ao rádio de 5 GHz do AP.

» Configure o rádio AP:
  » No painel de navegação, selecione *Wireless Configuration (Configuração Wireless>Radio Management (Gerenciamento de rádios>Radio Configuration (Configuração de rádios).*
  » Defina o status do rádio de 5 GHz do AP como *Ligado.*

11.6.1.3. Verificação da configuração

» Verifique se o switch pode obter um endereço IP na sub-rede 10.1.1.0/25 e o endereço de gateway do servidor DHCP.
» Verifique se o cliente DHCP pode obter endereços IP na sub-rede 10.1.1.128/25 e o endereço de gateway do servidor DHCP.

11.6.2. Exemplo de configuração do agente de retransmissão DHCP

11.6.2.1. Requisitos da rede

Conforme mostrado em , o cliente DHCP e o servidor DHCP estão em sub-redes diferentes. O cliente DHCP reside na sub-rede 10.10.1.0/24 e o servidor DHCP está em 10.1.1.1/24. Um AP é implantado entre os clientes DHCP e o servidor DHCP. O AP está conectado à rede na qual o cliente DHCP reside por meio da interface VLAN 10 em 10.10.1.1/24. O AP está conectado ao servidor DHCP por meio da interface VLAN 20 em 10.1.1.2/24.

Configure o agente de retransmissão DHCP no AP, para que o cliente DHCP possa obter um endereço IP e outros parâmetros de configuração do servidor DHCP.

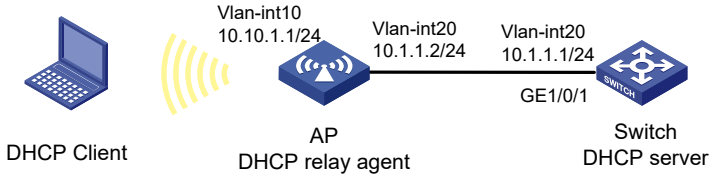


Diagrama de rede

11.6.2.2. Procedimento de configuração

» Atribuir endereços IP às interfaces. (Detalhes não mostrados).
» Configure o servidor DHCP. (Detalhes não mostrados.)
» Configurar as definições básicas no AP. (Detalhes não mostrados.)
» Configure o agente de retransmissão DHCP:
  » No painel de navegação, selecione *Configuração de rede> Protocolos de gerenciamento> DHCP.*
  » Execute as seguintes tarefas:
    » Ativar DHCP.
    » Especifique a interface VLAN 10 como o agente de retransmissão DHCP.
    » Especifique o endereço do servidor DHCP 10.1.1.1.

11.6.2.3. Verificação da configuração

Verifique se o cliente DHCP pode obter um endereço IP e outros parâmetros de configuração do servidor DHCP por meio do agente de retransmissão DHCP.

11.6.3. Exemplo de configuração de NTP

11.6.3.1. Requisitos da rede

Conforme mostrado em

» Configure o relógio local do AP 1 como uma fonte de referência, com o nível de estrato 2.
» Coloque o AP 2 no modo cliente e use o AP 1 como servidor NTP para o AP 2.

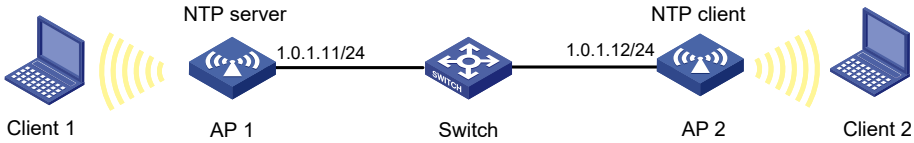


Diagrama de rede

11.6.3.2. Procedimento de configuração

- Configure o AP 1 (servidor NTP)
  - No painel de navegação, selecione *Configuração de rede> Protocolos de gerenciamento> NTP.*
  - Habilite o serviço NTP.
  - Especifique o endereço IP do relógio local como *127.127.1.0.*
  - Configure o nível de estrato do relógio local como *2.*
- Configurar o AP 2:
  - No painel de navegação, selecione *Sistema> Gerenciamento> Configurações.*
  - Selecione a sincronização automática de horário com uma fonte de horário confiável e, em seguida, selecione NTP como o protocolo de horário.
  - Especifique o endereço IP do Dispositivo A como *1.0.1.11* e configure o Dispositivo B para operar no modo de servidor.

11.6.3.3. Verificação da configuração

Verifique se o AP 2 está sincronizado com o AP 1 e se o nível de estrato do relógio é 3 no AP 2 e 2 no AP 1.

11.6.4. Exemplo de configuração LLDP

11.6.4.1. Requisitos da rede

Conforme mostrado em , configure o LLDP no AP e no switch para atender aos seguintes requisitos:

- O AP pode descobrir o switch e obter as informações de sistema e configuração do switch.
- O switch não consegue descobrir o AP.

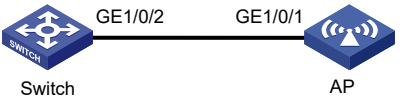


Diagrama de rede

11.6.4.2. Procedimento de configuração

- No painel de navegação esquerdo, selecione *Configuração de rede > Protocolos de gerenciamento > LLDP.*
- Configure as definições de LLDP no AP:
  - Habilite o LLDP globalmente no AP.
  - Acesse a página de status da interface e ative o LLDP na interface GigabitEthernet1/0/1.
  - Acesse a página de configurações da interface, ative o agente de ponte mais próximo na interface GigabitEthernet1/0/1 e defina o modo de operação da interface como Rx. Isso permite que o AP receba apenas pacotes LLDP e descubra vizinhos.
- Configure as definições de LLDP no switch:
  - Habilite o LLDP globalmente no switch.
  - Acesse a página de status da interface e ative o LLDP na interface GigabitEthernet1/0/2.
  - Acesse a página de configurações da interface, ative o agente de ponte mais próximo na interface GigabitEthernet1/0/2 e defina o modo de operação da interface como Tx. Isso permite que o switch envie apenas pacotes LLDP e desativa o switch para descobrir vizinhos.

11.6.4.3. Verificação da configuração

Verifique se é possível ver as informações do switch na página de vizinhos LLDP do AP, o que indica que a relação de vizinhança foi estabelecida, e se não é possível ver nenhuma informação de vizinhança na página de vizinhos LLDP do switch.

12. Exemplos de configuração de segurança de rede

12.1. Exemplos de configuração de controle de acesso

12.1.1. Exemplo de configuração de filtro de pacotes baseado em ACL

12.1.1.1. Requisitos da rede

Conforme mostrado em , uma empresa interconecta seus departamentos por meio dos APs. Configure o filtro de pacotes nos APs para atender aos seguintes requisitos:

- Permitir o acesso do escritório do Presidente a qualquer momento ao servidor do banco de dados financeiro.
- Permitir o acesso do Departamento Financeiro ao servidor do banco de dados financeiro somente durante o horário de trabalho (das 8:00 às 18:00) em dias úteis.
- Negar o acesso de qualquer outro departamento ao servidor do banco de dados financeiro.

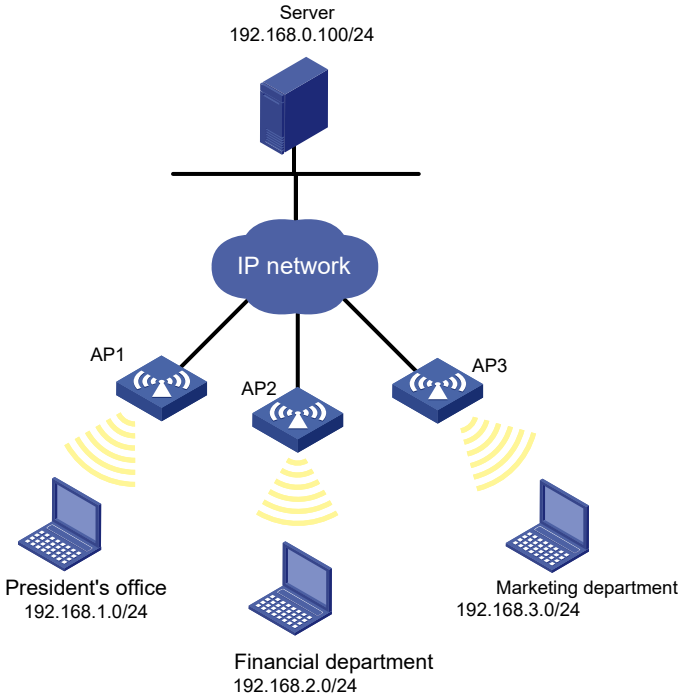


Diagrama de rede

12.1.1.2. Procedimento de configuração

- No painel de navegação, selecione *Network Security> Traffic Policy> Packet Filter.*
- Crie uma política de filtro de pacotes:
  - Selecione a interface Ethernet de uplink GE1/0/1.
  - Selecione a direção do aplicativo de saída.
  - Selecione o tipo de ACL IPv4 para o filtro de pacotes.
- Crie uma ACL IPv4 avançada e configure as seguintes regras na ordem em que estão descritas:

Ação	Tipo de protocolo	Máscara de IP/wildcard	Intervalo de tempo
Permissão	256	Fonte: 192.168.1.0/0.0.0.255 Destino: 192.168.0.100/0	N/A
Permissão	256	Fonte: 192.168.2.0/0.0.0.255 Destino: 192.168.0.100/0	Crie um intervalo de tempo denominado trabalho: Especifique a hora de início como 08:00. Especifique o horário final como 18:00. Selecione de segunda a sexta-feira.
Negar	256	Destino: 192.168.0.100/0	N/A

- Ativar a contagem de correspondências de regras para a ACL.

12.1.1.3. Verificação da configuração

- Faça ping no servidor de banco de dados de diferentes departamentos para verificar os seguintes itens:
  - Você pode acessar o servidor a partir do escritório do presidente a qualquer momento.
  - Você pode acessar o servidor no Departamento Financeiro durante o horário de expediente em dias úteis.
  - Não é possível acessar o servidor do Departamento de Marketing em nenhum momento.
- Acesse a interface da Web da regra ACL, verifique se as regras ACL estão ativas e se o número de pacotes correspondentes é exibido.

12.2. Exemplos de configuração de autenticação de acesso

12.2.1. Exemplo de configuração de autenticação 802.1X RADIUS

12.2.1.1. Requisitos da rede

Conforme mostrado em , configure o AP para atender aos seguintes requisitos:

- Use o servidor RADIUS para realizar autenticação, autorização e contabilidade para usuários 802.1X.
- Autenticar todos os usuários 802.1X que acessam o AP por meio da GigabitEthernet 1/0/1 no domínio *dm1X* do ISP.
- Exclua os nomes de domínio dos nomes de usuário enviados ao servidor RADIUS.
- Use o *nome* como chaves compartilhadas de autenticação e contabilidade para comunicação RADIUS segura entre o AP e o servidor RADIUS.
- Use as portas *1812 e 1813* para autenticação e contabilidade, respectivamente.

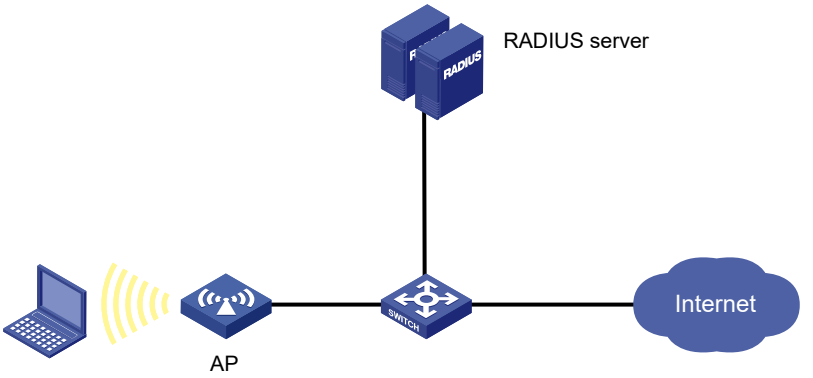


Diagrama de rede

12.2.1.2. Procedimento de configuração

- Atribua um endereço IP a cada interface, conforme mostrado em . (Detalhes não mostrados).
- No AP, Configure um esquema RADIUS no AP:
  - No painel de navegação, selecione *Segurança da rede> AAA> RADIUS.*
  - Adicionar e configurar um esquema RADIUS:
    - Defina o nome do esquema RADIUS como *802.1X.*
    - Configure o servidor de autenticação primário: defina seu endereço IP como *10.1.1.1,* defina o número da porta como *1812,* defina a chave compartilhada como *name* e defina o estado como *Active.*
    - Configure o servidor de contabilidade primário: defina seu endereço IP como *10.1.1.1,* defina o número da porta como *1813,* defina a chave compartilhada como *name* e defina o estado como *Active.*
    - Defina o formato dos nomes de usuário enviados ao servidor RADIUS como *Exclui o nome de domínio.*
- Configure um domínio ISP no AP:
  - No painel de navegação, selecione *Segurança da rede> AAA> Domínios ISP.*
  - Adicionar e configurar um domínio ISP:
    - Defina o nome de domínio como *dm1X.*
    - Defina o estado do domínio ISP como *Ativo.*
    - Defina o tipo de serviço como acesso à LAN.
    - Defina o método e o esquema de autenticação, autorização e contabilidade como *RADIUS e 802.1X,* respectivamente.
- Configure o 802.1X no AP:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.* Clique em *Add (Adicionar).*
  - Na área de configurações básicas, configure o nome do serviço e o SSID.
  - Na área de configurações de autenticação, selecione 802.1X e especifique o nome de domínio *dm1X.*
  - Clique em *Aplicar.*
- Configure o servidor RADIUS:
  - Adicione uma conta de usuário no servidor (detalhes não mostrados).
  - Configure as definições de autenticação, autorização e contabilidade (detalhes não mostrados).

12.2.1.3. Verificação da configuração

- Acesse a página *Network Security> AAA> RADIUS* para verificar informações breves do esquema RADIUS *802.1X.*
- Acesse a página *Network Security> AAA> ISP Domains* para verificar as informações breves do domínio ISP *dm1X.*
- Verifique se o uso pode ficar on-line:
  - Use o nome de usuário e a senha configurados para fazer .
  - Acesse a página *Network Security> Authentication> 802.1X* para verificar se o número de usuários on-line é *1* na GigabitEthernet 1/0/1.

12.2.2. Exemplo de configuração de autenticação local 802.1X

12.2.2.1. Requisitos da rede

Conforme mostrado em , adicione uma conta de usuário com o nome de usuário *dotuser* e a senha *12345* no AP. Configure o AP para atender aos seguintes requisitos:

- Execute a autenticação 802.1X local para controlar o acesso à rede dos usuários na GigabitEthernet 1/0/1.
- Autenticar os usuários no domínio *abc* do ISP
- Especifique o controle de acesso baseado em porta na GigabitEthernet 1/0/1. Depois que um usuário passa pela autenticação na porta, todos os usuários subsequentes podem acessar a rede sem autenticação.

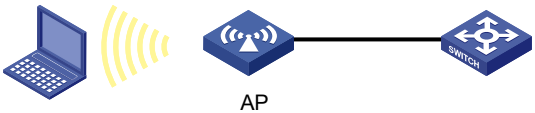


Diagrama de rede

12.2.2.2. Procedimento de configuração

- Atribua um endereço IP a cada interface, conforme mostrado em . (Detalhes não mostrados).
- Configure um usuário local:
  - No painel de navegação, selecione *Segurança da rede> Gerenciamento de usuários> Usuários locais.*
  - Adicionar e configurar um usuário local:
    - Defina o nome de usuário como *dotuser.*
    - Defina a senha como *12345.*
    - Defina o tipo de serviço como acesso à LAN.
- Configurar um domínio ISP:
  - No painel de navegação, selecione *Segurança da rede> AAA> Domínios ISP.*
  - Adicionar e configurar um domínio ISP:
    - Defina o nome de domínio do ISP como *abc.*
    - Defina o estado do domínio ISP como *Ativo.*
    - Defina o tipo de serviço como acesso à LAN.
    - Configure o domínio do ISP para usar o método local para autenticação e autorização de usuários da LAN e não execute a contabilidade para usuários da LAN.
- Configurar o 802.1X:
  - No painel de navegação, selecione *Wireless Configuration > Wireless Services> Wireless Services Configuration.* Clique em *Add (Adicionar).*
  - Na área de configurações básicas, configure o nome do serviço e o SSID.
  - Na área de configurações de autenticação, selecione 802.1X e especifique o nome de domínio *abc.*
  - Clique em *Aplicar.*

12.2.2.3. Verificação da configuração

- Acesse a página *Network Security> User Management> Local Users* para verificar a configuração do usuário local *dotuser.*
- Acesse a página *Network Security> AAA> ISP Domains* para verificar as informações breves do domínio ISP *abc.*
- Verifique se o uso pode ficar on-line:
  - Use o nome de usuário e a senha configurados para fazer .
  - Acesse a página *Network Security> Authentication> 802.1X* para verificar se o número de usuários on-line é *1* na GigabitEthernet 1/0/1.

12.2.3. Exemplo de configuração do AKM 802.1X

12.2.3.1. Requisitos da rede

Conforme mostrado em , o switch funciona como um servidor DHCP para atribuir endereços IP ao AP e ao cliente.

- Configure a autenticação de sistema aberto e a autenticação 802.1X para que o cliente possa acessar a rede usando o nome de usuário de login *abcdef* e a senha *123456.*
- Configure o 802.1X como o modo AKM.

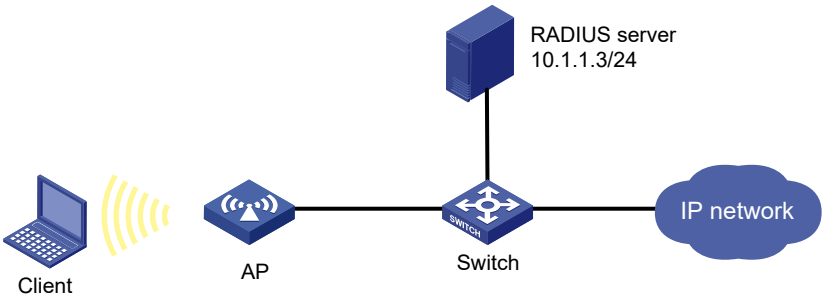


Diagrama de rede

12.2.3.2. Procedimento de configuração

- Configure o nome de usuário *abcdef* e a senha *123456* no servidor RADIUS e certifique-se de que o servidor RADIUS e o AP possam comunicar (detalhes não mostrados).
- Configure o RADIUS e um domínio de autenticação.
- Configure um serviço Wireless:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Adicione um serviço Wireless:
    - Crie um serviço Wireless chamado *service1.*
    - Defina o SSID como *serviço.*
    - Ative o serviço Wireless.
- Clique em *Apply and Configure Advanced Settings e, em seguida, clique na guia Authentication (Autenticação).*
- Configurar a autenticação 802.1X:
  - Defina o tipo de segurança como autenticação 802.1X.
  - Defina o modo de segurança como WPA.
  - Selecione o conjunto de cifras CCMP.
  - Defina o nome do domínio como *dom1.*
- Aplique o serviço Wireless.
- Associe o serviço de serviço sem *fio1* ao rádio:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Selecione service *service1* e clique em *Bind to Radio.*
  - Selecione o rádio de 5 GHz do AP e clique em *Bind (Vincular).*

12.2.3.3. Verificação da configuração

Veja detalhes sobre o serviço wireless **service1** para verificar se a configuração está correta.

12.2.4. Autenticação direta do portal IPv4 exemplo de configuração

12.2.4.1. Requisitos da rede

Conforme mostrado em , o AP encaminha diretamente o tráfego de usuário do cliente. O cliente é atribuído a um endereço IP público manualmente ou por meio de DHCP. Um servidor de portal atua como um servidor de autenticação de portal e um servidor Web de portal. Um servidor RADIUS atua como servidor de autenticação/contabilidade.

Configure a autenticação direta do portal, para que o cliente possa acessar somente o servidor da Web do portal antes de passar pela autenticação e acessar os recursos da Internet depois de passar pela autenticação.

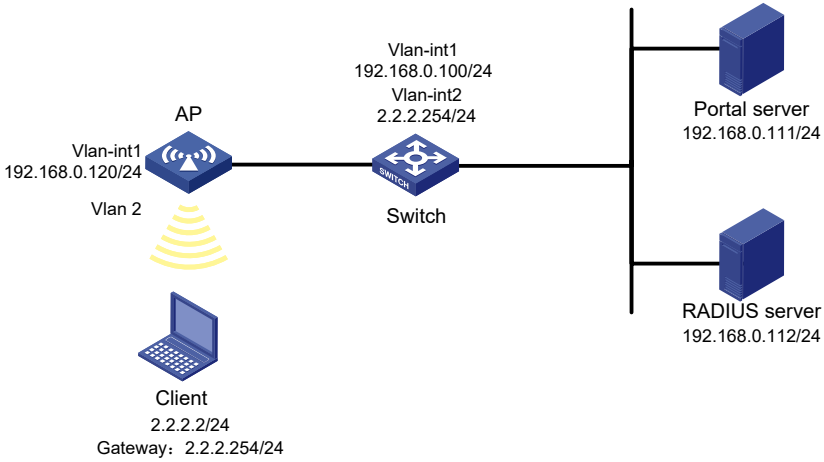


Diagrama de rede

12.2.4.2. Procedimentos de configuração

- Configure os endereços IP do cliente, do AP e dos servidores conforme mostrado em e certifique-se de que eles possam se comunicar entre si.
- Configure o servidor RADIUS corretamente para fornecer funções de autenticação e contabilidade.
- Configure o RADIUS e um domínio de autenticação.
  - Configure um serviço Wireless:
    - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Adicione um serviço Wireless:
    - Crie um serviço Wireless chamado **service1**.
    - Defina o SSID como **serviço**.
    - Ative o serviço Wireless.
- Configure o modo de autenticação do portal:
  - Clique no ícone de edição do serviço wireless *service1.* A página de configurações avançadas é aberta.
  - Clique na guia *Authentication (Autenticação).*
  - Selecione *IPv4 Portal Authentication (Autenticação do portal IPv4).*
  - Defina o nome do domínio como *dm1.*
  - Defina o URL do servidor como *newpt.*
  - Defina o BAS-IP como *192.168.0.110.*
  - Clique em *Aplicar.*
- Associe o *serviço Wireless1* ao rádio:
  - No painel de navegação, selecione *Wireless Configuration> Wireless Services> Wireless Services Configuration.*
  - Selecione service *service1* e clique em *Bind to Radio.*
  - Selecione o rádio de 5 GHz do AP e clique em *Bind (Vincular).*

12.2.4.3. Verificação da configuração

Exibir detalhes sobre o serviço *service1* para verificar se a configuração está correta.

13. Exemplos de configuração de recursos do sistema

13.1. Exemplos de configuração de gerenciamento de dispositivos

13.1.1. Exemplo de configuração de administradores

13.1.1.1. Requisitos da rede

Conforme mostrado em , configure uma conta de administrador com o nome de usuário *webuser* e a senha *12345* no AP para atender aos seguintes requisitos:

- Permitir que o usuário use a conta para fazer login no AP por meio de HTTP.
- Realize a autenticação local para o usuário que usa a conta de administrador para fazer login no AP.
- Atribua a função de usuário administrador da rede ao usuário autenticado.

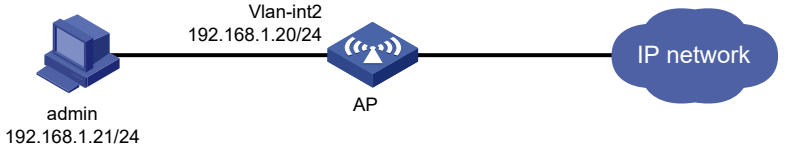


Diagrama de rede

13.1.1.2. Procedimento de configuração

- Configure a VLAN e a interface da VLAN:
  - No painel de navegação, selecione *Network Configuration (Configuração de rede>Network Links (Links de rede>VLAN.*
  - Crie a *VLAN 2.*
  - Acesse a página de edição da VLAN 2 para realizar as seguintes tarefas:
    - Adicione a interface que se conecta ao PC do administrador à lista de portas marcadas.
    - Criar interface VLAN 2.
    - Atribua o endereço IP *192.168.1.20/24* à interface VLAN 2.
- Configure uma conta de administrador:
  - No painel de navegação, selecione *System> Management> Administrators.*
  - Criar e configurar uma conta de administrador:
    - Defina o nome de usuário e a senha como *webuser e hello12345,* respectivamente.
    - Selecione a função de usuário administrador da rede.
    - Especifique HTTP e HTTPS como os tipos de acesso permitidos.

13.1.1.3. Verificação da configuração

- Acesse a página *System> Management> Administrators* para verificar se a conta de administrador foi adicionada com sucesso.
- Digite *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.

13.1.2. Exemplo de configuração do servidor SSH local

13.1.2.1. Requisitos da rede

Conforme mostrado em , configure o AP como um servidor Stelnet e o host como um cliente Stelnet e estabeleça uma conexão SSH entre os dois dispositivos para atender aos seguintes requisitos:

- O AP e o host podem se comunicar entre si. O AP usa a autenticação por senha para verificar o host e o processo de autenticação é concluído no AP localmente.
- O administrador da rede pode fazer login no host com o nome de usuário *client* e a senha *hello12345* e pode realizar todas as operações suportadas no dispositivo.

Obs.: *o software cliente Stelnet tem vários tipos, como PuTTY e OpenSSH. Esta seção usa o PuTTY0.58 como exemplo para configurar um cliente Stelnet.*

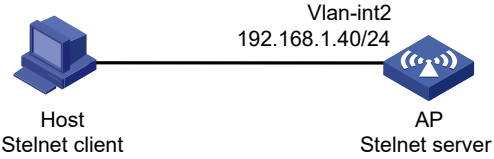


Diagrama de rede

13.1.2.2. Procedimento de configuração

- Configure o serviço SSH. No painel de navegação, selecione *Configuração de rede > Protocolos de gerenciamento > SSH.* Ative o serviço Stelnet.
- Configurar VLANs e interfaces de VLAN.
  - No painel de navegação, selecione *Network Configuration (Configuração de rede) > Network Links (Links de rede) > VLAN.*
  - Crie a VLAN 2.
  - Acesse a página de edição da VLAN 2 para executar as seguintes tarefas:
    - Adicione a interface GigabitEthernet1/0/2 à lista de portas marcadas.
    - Criar interface VLAN 2.
    - Atribua o endereço IP *192.168.1.40/24* à interface VLAN 2.
- Configure uma conta de administrador:
  - No painel de navegação, selecione *System > Management > Administrators.*
  - Criar e configurar uma conta de administrador:
    - Defina o nome de usuário e a senha como *client e hello12345,* respectivamente.
    - Selecione a função de usuário administrador da rede.
    - Especifique SSH como o tipo de acesso permitido.

13.1.2.3. Verificação da configuração

- Execute o PuTTY.exe no host.
- Digite o endereço IP do servidor Stelnet no campo *Nome do host (ou endereço IP)* e clique em *Abrir.*
- Verifique se é possível usar o nome de usuário *client* e a senha *hello12345* para acessar a página de configuração do AP com êxito.

Termo de garantia

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo: Nº de série:

Revendedor:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano – sendo este de 90 (noventa) dias de garantia legal e 9 (nove) meses de garantia contratual –, contado a partir da data da compra do produto pelo Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem vício de fabricação, incluindo as despesas com a mão de obra utilizada nesse reparo. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.
2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.
3. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.
4. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.
6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.
7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.
8. Descarte adequadamente seu produto após vida útil - entregue em pontos de coleta de produtos eletroeletrônicos, em alguma assistência técnica autorizada Intelbras ou consulte nosso site www.intelbras.com.br e suporte@intelbras.com.br ou (48) 2106-0006 ou 0800 7042767 para mais informações.

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

Todas as imagens deste manual são ilustrativas.

intelbras

fale com a gente

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

Importado no Brasil por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001 01.25
CNPJ 82.901.000/0014-41 – www.intelbras.com.br Origem: China