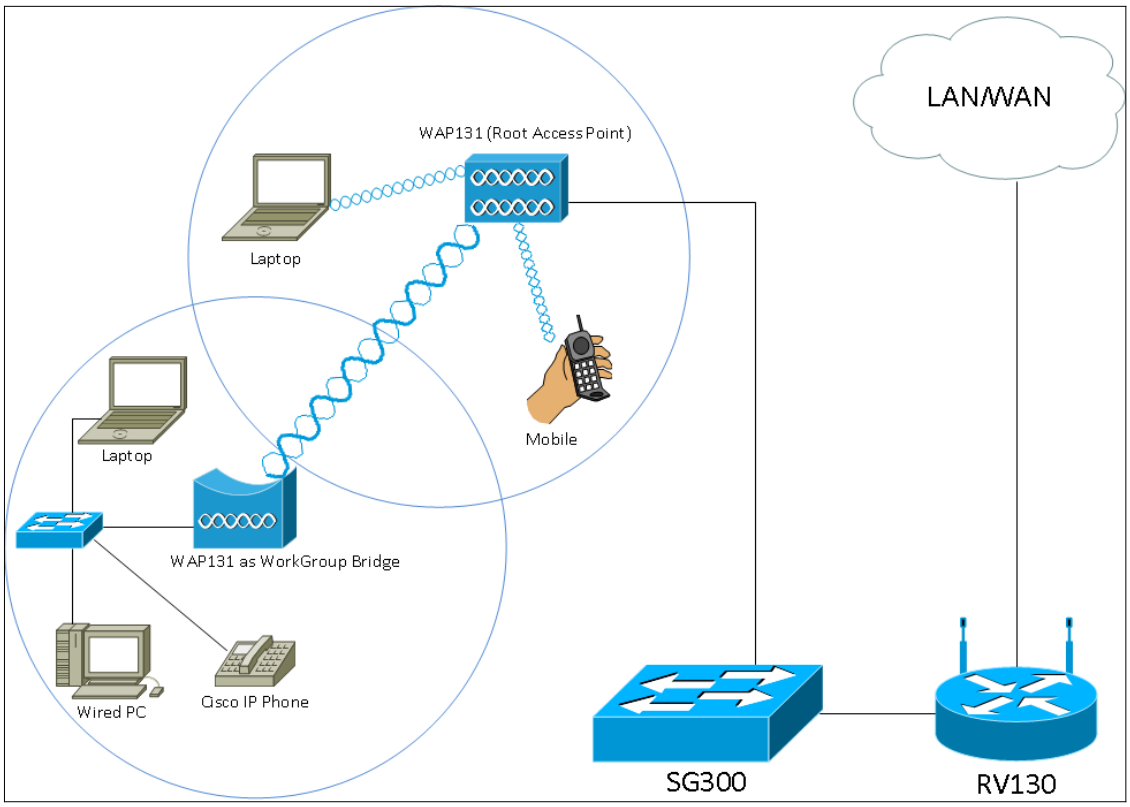
Configurar o bridge de grupo de trabalho no Access point WAP131

Objetivo

A característica do bridge de grupo de trabalho permite o ponto de acesso Wireless (WAP) de construir uma ponte sobre o tráfego entre um cliente remoto e o Wireless LAN que seja conectado com o modo do bridge de grupo de trabalho. O dispositivo WAP associado com a interface remota é sabido como uma relação do Access point, e essa associada com o Wireless LAN é chamado uma relação da infraestrutura. Embora Wireless Distribution System (WDS) seja a solução preferida da ponte para o WAP131, o modo do bridge de grupo de trabalho é recomendado quando a característica WDS é não disponível.



Nota: Quando a característica do bridge de grupo de trabalho é permitida, a característica da ponte WDS não trabalha. Para ver como a ponte WDS é configurada, refira o artigo que *configura a ponte de Wireless Distribution System (WDS) no WAP131 e no WAP351.*

O objetivo deste documento é explicar como configurar o bridge de grupo de trabalho no Access point WAP131.

Dispositivos aplicáveis

- WAP131

Versão de software

- 1.0.3.4

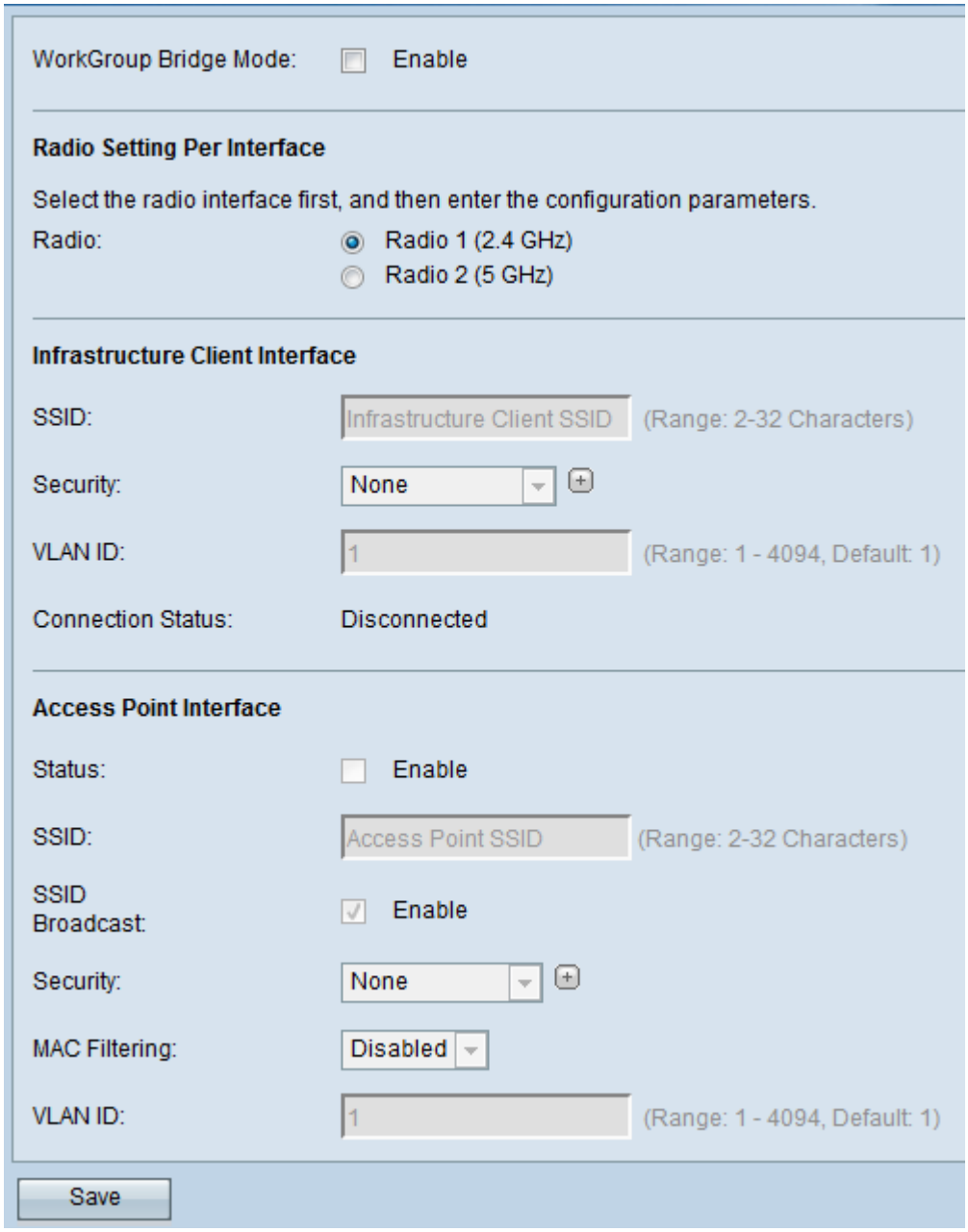
Configurar o bridge de grupo de trabalho

Nota: A fim permitir o bridge de grupo de trabalho, aglomerando-se deve ser permitida no WAP. Se se aglomerar é desabilitada, você precisa de desabilitar a única instalação do ponto para permitir a aglomeração. Todos os dispositivos WAP que participam no bridge de grupo de trabalho devem ter os seguintes ajustes idênticos:

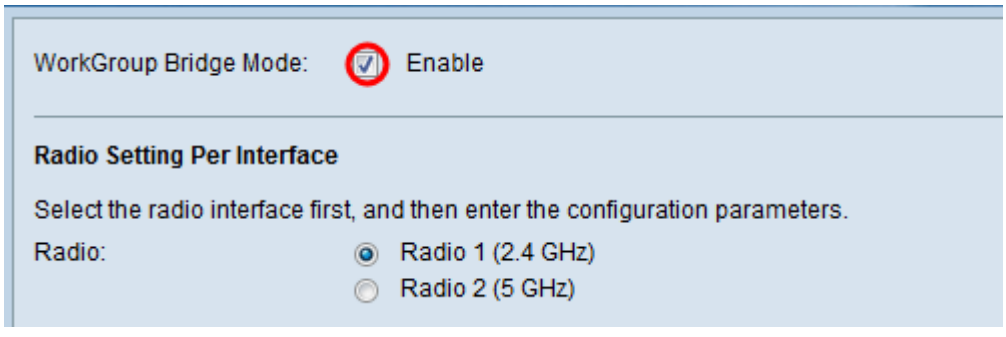
- Rádio
- Modo do IEEE 802.11
- Largura de banda de canal
- Canal (automóvel não recomendado)

Para assegurar estes ajustes em todos os dispositivos seja o mesmos, olham acima as configurações de rádio. Para configurar estes ajustes, refira o artigo que *configura configurações de rádio da tecnologia Wireless básica nos Access point WAP131 e WAP351*.

Etapa 1. Entre ao utilitário de configuração da Web e escolha o **Sem fio > o bridge de grupo de trabalho**. A página do *bridge de grupo de trabalho* abre:

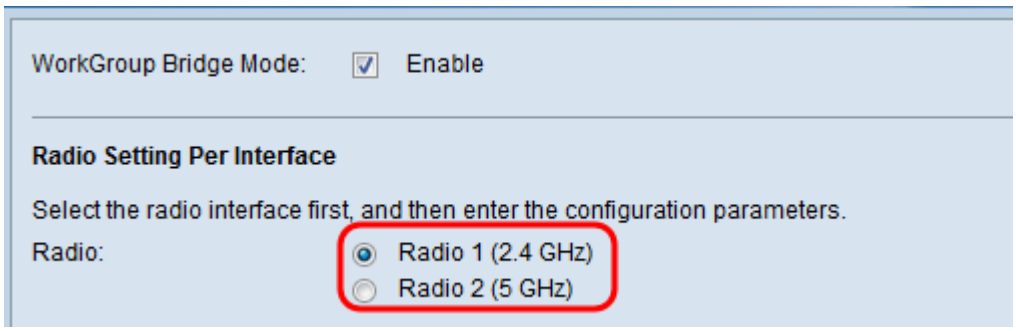


Etapa 2. Verifique a caixa de seleção da **possibilidade no** *campo de modo do bridge de grupo de trabalho* para permitir a característica do bridge de grupo de trabalho.



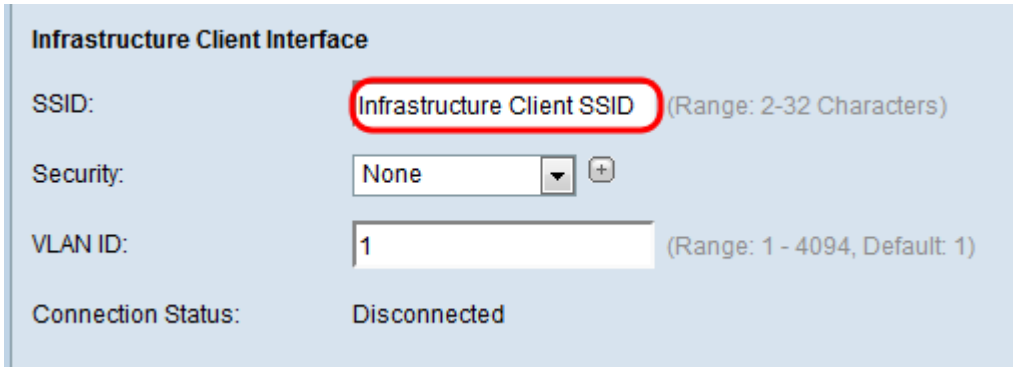
Configurações de rádio

Etapa 1. Selecione a interface de rádio para o bridge de grupo de trabalho. Quando você configura um rádio como um bridge de grupo de trabalho, o outro rádio permanece operacional. As interfaces de rádio correspondem às faixas de frequência de rádio do WAP131. O WAP131 é equipado para transmitir em duas interfaces de rádio diferentes. Configurar ajustes para uma interface de rádio não afetará a outro.



Interface de cliente da infraestrutura

Etapa 1. Dê entrada com o nome do Service Set Identifier (SSID) no campo *SSID*. O SSID deve ser 2-32 caráteres por muito tempo.



Etapa 2. Escolha o tipo de Segurança autenticar uma estação do cliente no dispositivo ascendente WAP da lista de drop-down da *Segurança*.

As opções disponíveis são definidas como segue:

• Nenhum — Abra ou nenhuma Segurança. Este é o valor padrão. Se você escolhe este, salte a etapa 14.

• WPA pessoal — O WPA pessoal pode apoiar chaves de caráteres do comprimento 8-63. O método de criptografia é RC4 para o WPA e o Advanced Encryption Standard (AES) para o WPA2. O WPA2 é recomendado porque tem um padrão de codificação mais poderoso. Se você escolhe este, passe a etapa 3.

• Empresa WPA — A empresa WPA é mais avançado do que o WPA pessoal e é a Segurança recomendada para a autenticação. Usa o protocolo extensible authentication protegido (PEAP) e o Transport Layer Security (TLS). Se você escolhe este, vá pisar 5.

WPA pessoal

Etapa 3. Selecione a caixa de seleção **WPA-TKIP** ou **WPA2-AES** para determinar que tipo da criptografia WPA a interface de cliente da infraestrutura usará. Se todos seus apoios de equipamento Wireless WPA2, ajustaram então a Segurança do cliente da infraestrutura para WPA2-AES. Se alguns de seus dispositivos Wireless, como PDA e outros dispositivos pequenos da rede Wireless, conectam somente com o WPA-TKIP, a seguir selecione WPA-TKIP.

Etapa 4. Entre na chave de criptografia WPA no *campo chave*. A chave deve ser 8-63 caráteres por muito tempo. Faixa clara a etapa 14.

Empresa WPA

Etapa 5. Selecione a caixa de seleção **WPA-TKIP** ou **WPA2-AES** para determinar que tipo da criptografia WPA a interface de cliente da infraestrutura usará. Se todo seu apoio de equipamento Wireless WPA2, ajustou então a Segurança do cliente da infraestrutura para WPA2-AES. Se alguns de seus dispositivos Wireless podem somente conectar com o WPA-TKIP, a seguir verifique as caixas de seleção **WPA-TKIP** e **WPA2-AES**. Nesta configuração, seus dispositivos WPA2 conectarão ao WPA2, e seus dispositivos WPA conectarão ao WPA.

Etapa 6. No campo do *método de EAP*, selecione o botão de rádio **PEAP** ou **TLS**. O protocolo extensible authentication protegido (PEAP) dá cada usuário Wireless sob os nomes de usuário e senha individuais WAP que apoiam padrões da criptografia de AES. O Transport Layer Security (TLS) exige cada usuário ter um certificado adicional para ser concedido o acesso. Se você seleciona o PEAP, salte a etapa 14.

Etapa 7. Incorpore o nome de usuário e senha ao campo do *nome de usuário e senha*.

Etapa 8. Selecione os botões de rádio **HTTP** ou **TFTP no** *método de transferência* colocam. O Trivial File Transfer Protocol (TFTP) é uma versão inseguro simplificada do File Transfer Protocol (FTP). É usado principalmente para distribuir o software ou autenticar dispositivos entre redes corporativas. O Hypertext Transfer Protocol (HTTP) fornece um framework de autenticação simples da resposta de desafio que possa ser usado por um cliente para fornecer o framework de autenticação. Se você seleciona o **TFTP**, salte a etapa 11.

Nota: Se um arquivo certificado está já atual no WAP, a seguir o campo da *data do presente* e de *expiração do certificado do arquivo certificado* estará preenchido já com a informação relevante. Se não, estarão vazios.

HTTP

Etapa 9. Clique o **botão Browse** para encontrar e selecionar um arquivo certificado. O arquivo deve ter a extensão de arquivo certificado apropriada (tal como o .pem ou o .pfx), se não o arquivo não será aceitado.

Etapa 10. **Transferência de arquivo pela rede do** clique para transferir arquivos pela rede o arquivo certificado selecionado. Faixa clara a etapa 14.

O campo da *data do presente* e de *expiração do certificado do arquivo certificado* será atualizado automaticamente.

TFTP

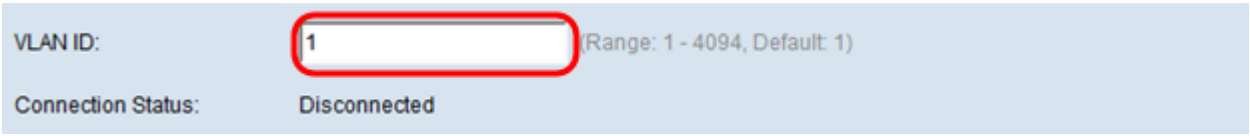
Etapa 11. Incorpore o nome de arquivo do arquivo certificado ao campo do *nome de arquivo* .

Etapa 12. Incorpore o endereço de servidor de TFTP ao *campo de endereço do IPv4 do servidor TFTP*.

Etapa 13. Clique o botão da **transferência de arquivo pela rede** para transferir arquivos pela rede o arquivo certificado especificado.

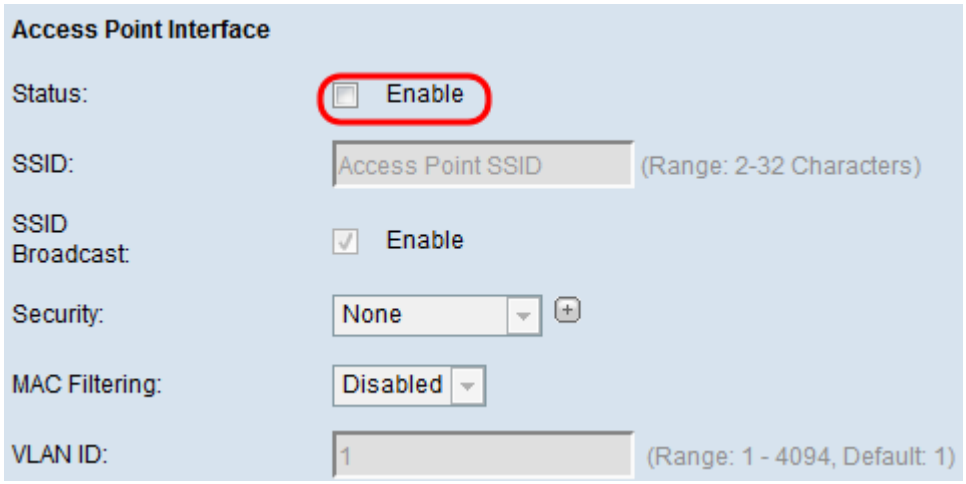
O campo da *data do presente* e de *expiração do certificado do arquivo certificado* será atualizado automaticamente.

Etapa 14. Incorpore o ID de VLAN para a interface de cliente da infraestrutura.

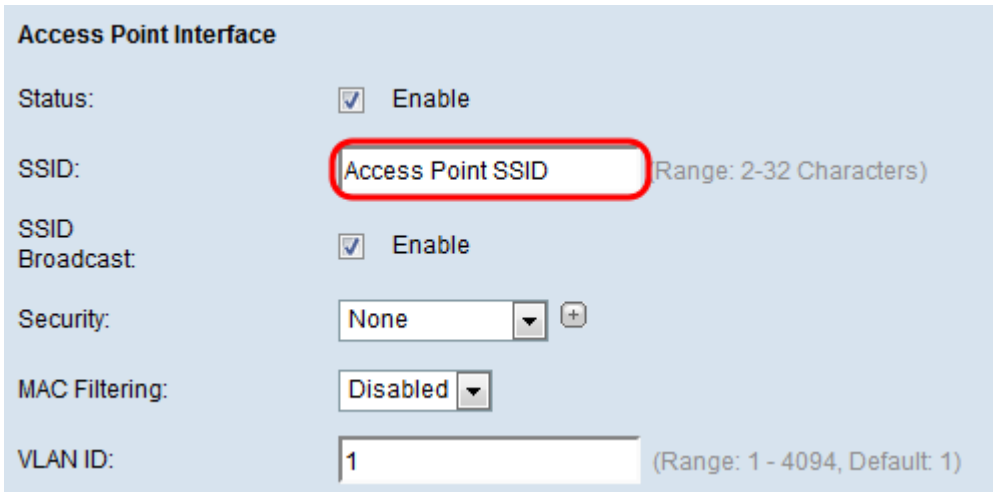


Relação do Access point

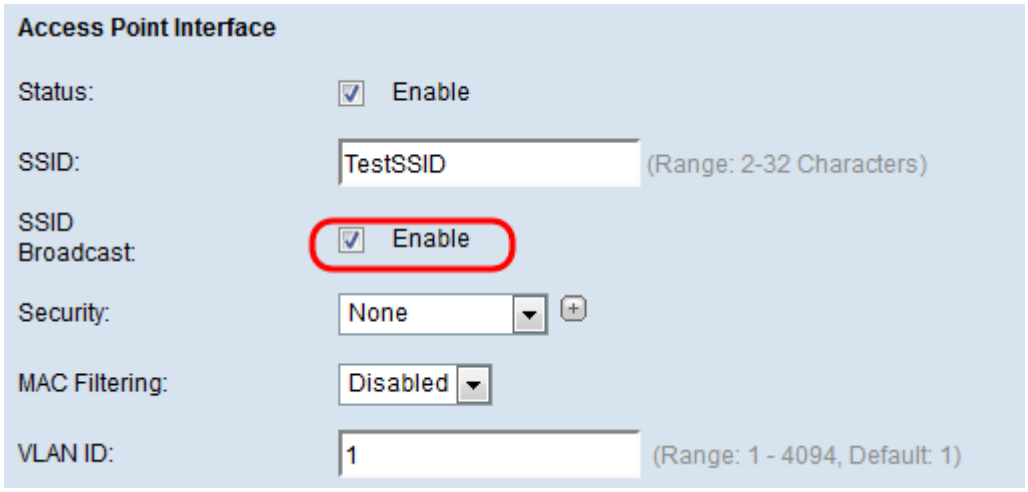
Etapa1. Verifique a caixa de seleção da **possibilidade no** campo de *estado* para permitir a construção de uma ponte sobre na relação do Access point.



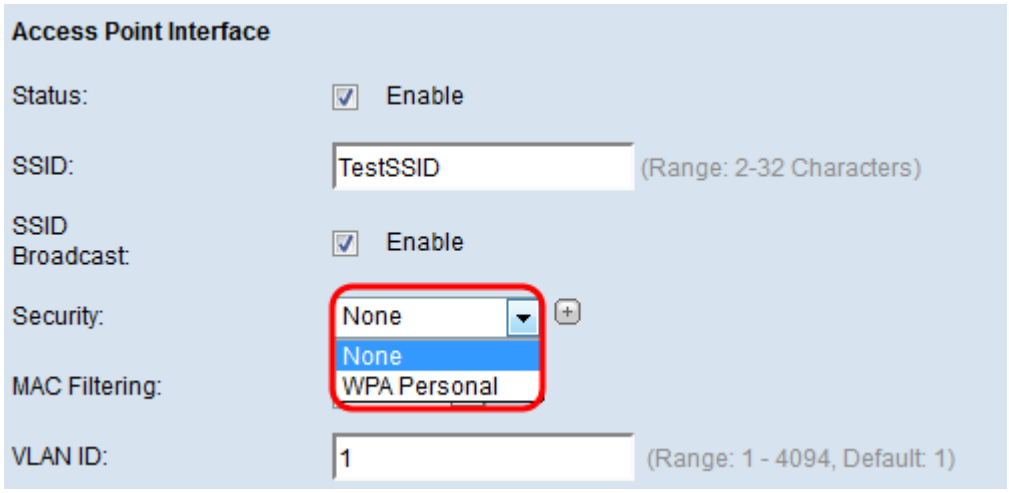
Etapa 2. Inscreva o Service Set Identifier (SSID) para o Access point no campo *SSID*. O comprimento SSID deve estar entre 2 a 32 caráteres.



Etapa 3. (opcional) se você não quer transmitir o SSID a jusante, desmarca a caixa de seleção da **possibilidade no** campo da transmissão SSID. É permitida à revelia.



Etapa 4. Escolha o tipo de Segurança autenticar estações do cliente de downstream ao dispositivo WAP da lista de drop-down da *Segurança*.



As opções disponíveis são definidas como segue:

- Nenhum — Abra ou nenhuma Segurança. Este é o valor padrão. Salte para pisar 10 se você escolhe este.

- WPA pessoal — O WPA pessoal e pode apoiar chaves de caráteres do comprimento 8 a 63. O método de criptografia é Temporal Key Integrity Protocol (TKIP) ou modo contrário da cifra com o bloco que acorrenta o protocolo do código de autenticação de mensagens (CCMP). O WPA2 com CCMP é recomendado como tem um padrão de codificação mais poderoso, Advanced Encryption Standard (AES) comparado ao TKIP que usa somente um padrão RC4 64-bit.

Etapa 5. Verifique as versões desejadas WPA do campo das *versões WPA*. Geralmente, o WPA é escolhido somente se alguns dos WAP envolvidos não apoiam o WPA2; se não, o WPA2 é recomendado. WPA2-AES é permitido sempre.

Etapa 6. Incorpore a chave compartilhada WPA ao *campo chave*. A chave deve ser 8-63 caráteres por muito tempo, e pode incluir caráteres alfanuméricos, caráteres maiúsculas e minúsculas, e caracteres especiais.

Etapa 7. Incorpore a taxa à *taxa de atualização chave da transmissão*. A taxa deve estar entre 0-86400, com um valor de 0 que desabilita a característica. O padrão é 300.

Etapa 8. Escolha o tipo de MAC que filtra o desejo para configurar para a relação do Access point da lista de drop-down de *filtração MAC*. Quando permitidos, os usuários são concedidos ou o acesso negado ao WAP é baseado no MAC address do cliente que se usam.

As opções disponíveis são definidas como segue:

- Deficiente — Todos os clientes podem alcançar a rede upstream. Este é o valor padrão.
- Local — O grupo de clientes que podem alcançar a rede upstream é restringido aos clientes especificado em uma lista localmente definida do MAC address.
- RAIO — O grupo de clientes que podem alcançar a rede upstream é restringido aos clientes especificado em uma lista do MAC address em um servidor Radius.

Etapa 9. Incorpore o ID de VLAN ao campo do *ID de VLAN* para a interface de cliente do Access point.

Nota: Para permitir a construção de uma ponte sobre dos pacotes, a configuração de VLAN para a relação do Access point e a relação prendida deve combinar aquela da interface de cliente da infraestrutura.

Etapa 10. **Salvaguarda do** clique para salvar suas mudanças.