Detecção de invasores em redes sem fio unificadas

Contents

Introduction

As redes wireless estendem redes com fio e aumentam a produtividade dos trabalhadores e acessam às informações. Contudo, uma rede wireless não autorizada apresenta uma camada adicional de preocupações de segurança. Além disso, ela é colocada na segurança das portas em redes com fio, tendo as redes wireless como uma extensão simples de redes com fio. Portanto, um funcionário que traz seu próprio Ponto de Acesso (AP) Cisco em uma infraestrutura bem segura com ou sem fio e permite que usuários não autorizados acessem essa rede, até então segura, pode facilmente comprometer uma rede segura.

A detecção de invasores permite que o administrador de rede monitore e elimine essa preocupação com a segurança. O Cisco Unified Network Architecture fornece dois métodos de detecção de invasores que permitem uma solução completa de identificação e contenção de invasores sem a necessidade de redes e ferramentas de sobreposição caras e difíceis de justificar.

Visão geral do recurso

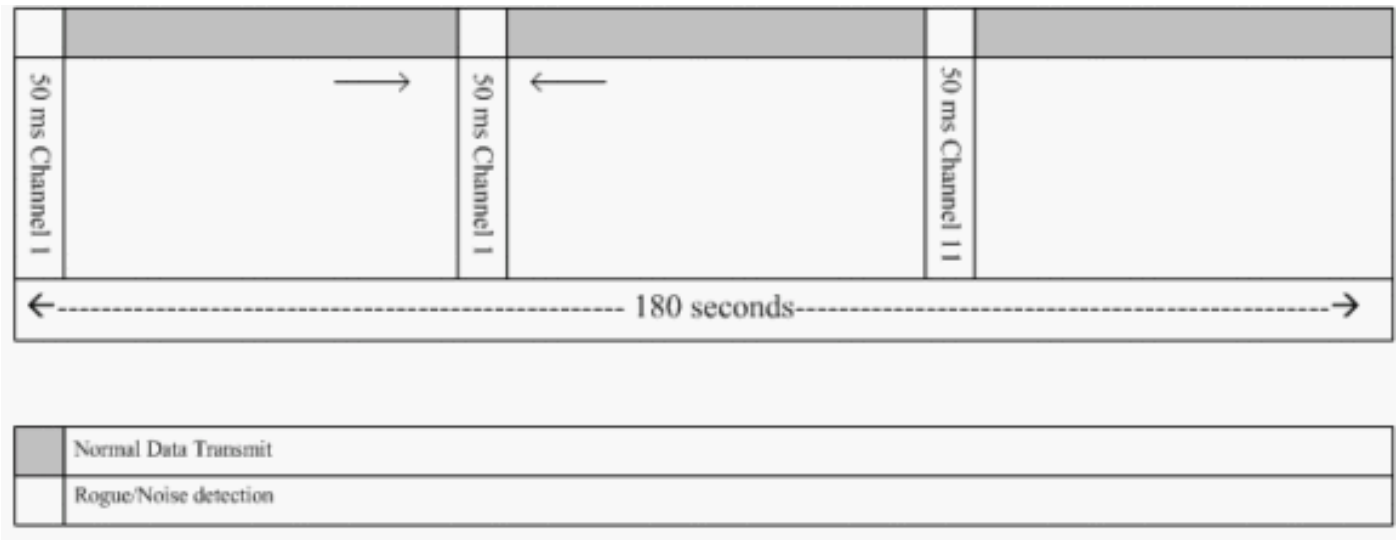
A detecção de invasores não está vinculada a nenhuma regulamentação e não é necessária nenhuma adesão legal para o seu funcionamento. No entanto, a contenção de invasores geralmente introduz problemas legais que podem colocar o provedor de infraestrutura em uma posição desconfortável se for deixado para operar automaticamente. A Cisco é extremamente sensível a esses problemas e fornece essas soluções. Cada controlador é configurado com um nome de Grupo de RF.Quando um AP Lightweight é registrado em um controlador, ele incorpora um **Elemento de Informação de Autenticação (IE)** que é específico para o Grupo de RF configurado no controlador em todos os seus beacons/frames de resposta de sonda. Quando o AP leve ouve beacons/ quadros de resposta de sondagem de um AP sem esse **IE** ou com **IE**

errado, o AP leve relata que o AP é um invasor, grava seu BSSID em uma tabela invasora e envia a tabela ao controlador. Existem dois métodos, o Protocolo de Descoberta de Localização por Rogue (RLDP - Rogue Location Discovery Protocol) e a operação passiva, que são explicados detalhadamente; consulte a seção Determine Ative Rogues.

Descoberta invasora de infraestrutura

A descoberta de invasores em um ambiente sem fio ativo pode ser cara. Esse processo pede que o AP em serviço (ou modo local) pare de atender, escutar ruído e executar detecção de invasão. O administrador de rede configura os canais para digitalizar e configura o período em que todas as estações são digitalizadas. O AP escuta 50 ms para beacons de clientes invasores e retorna ao canal configurado para atender novamente os clientes. Essa verificação ativa, combinada com mensagens de vizinhos, identifica quais APs são invasores e quais APs são válidos e parte da rede. Para configurar os canais digitalizados e o período de verificação, navegue até **Wireless > 802.11b/g Network** (**b/g**) ou "**a**", dependendo do requisito de rede) e selecione o botão **Auto RF** no canto superior direito da janela do navegador.

Você pode rolar para baixo até **Noise/Interference/Rogue Monitoring Channels** para configurar os canais a serem verificados quanto a problemas e ruídos. As opções disponíveis são: Todos os canais (de 1 a 14), Canais de países (de 1 a 11) ou Canais de Associação de Canal Dinâmico (DCA - Dynamic Channel Association) (por padrão, 1, 6 e 11). O período de verificação através desses canais pode ser configurado na mesma janela, em **Intervalos de monitoramento (60 a 3600 segundos)** junto com o intervalo de medição de ruído. Por padrão, o intervalo de escuta para ruídos e invasores fora do canal é de 180 segundos. Isso significa que cada canal é digitalizado a cada 180 segundos. Este é um exemplo dos canais DCA que são verificados a cada 180 segundos:



Como ilustrado, um alto número de canais configurados para serem verificados junto com os intervalos de verificação curtos deixa menos tempo para que o AP realmente atenda aos clientes de dados.

O AP leve espera para rotular clientes e APs como invasores, pois esses invasores possivelmente não serão relatados por outro AP até que outro ciclo seja concluído. O mesmo AP se move para o mesmo canal novamente para monitorar a existência de APs e clientes invasores, bem como ruído e interferência. Se os mesmos clientes e/ou APs forem detectados, eles serão listados como invasores no controlador novamente. O controlador agora começa a determinar se esses rogues estão conectados à rede local ou simplesmente a um AP vizinho. Em ambos os

casos, um AP que não faz parte da rede sem fio local gerenciada é considerado um invasor.

Detalhes do invasor

Um AP leve sai do canal por 50 ms para ouvir clientes invasores, monitorar ruído e interferência de canal. Qualquer cliente invasor detectado ou APs são enviados ao controlador, que coleta estas informações:

- O endereço MAC do AP invasor
- O nome do AP invasor
- O endereço MAC do(s) cliente(s) conectado(s) invasor(s)
- Se os quadros estão protegidos com WPA ou WEP
- O preâmbulo
- A razão sinal-ruído (SNR)
- O indicador de intensidade do sinal do receptor (RSSI)

Ponto de acesso de detecção de invasores

Você pode fazer com que um AP opere como um detector invasor, o que permite que ele seja colocado em uma porta de tronco para que possa ouvir todas as VLANs conectadas no lado com fio. Ele continua a encontrar o cliente na sub-rede com fio em todas as VLANs. O AP do detector de invasão escuta os pacotes do Address Resolution Protocol (ARP) para determinar os endereços da Camada 2 de clientes invasores identificados ou APs invasores enviados pelo controlador. Se um endereço de Camada 2 correspondente for encontrado, o controlador gera um alarme que identifica o AP invasor ou o cliente como uma ameaça. Esse alarme indica que o invasor foi visto na rede com fio.

Determinar Rogues ativos

Os APs invasores devem ser "vistos" duas vezes antes de serem adicionados como invasores pelo controlador. Os APs não autorizados não são considerados uma ameaça se não estiverem conectados ao segmento com fio da rede corporativa. Para determinar se o invasor está ativo, várias abordagens são usadas. Essas abordagens incluem o RLDP.

Protocolo de descoberta de local invasor (RLDP)

O RLDP é uma abordagem ativa, que é usada quando o AP invasor não tem autenticação (autenticação aberta) configurada. Esse modo, que é desativado por padrão, instrui um AP ativo a mover-se para o canal invasor e conectar-se ao invasor como um cliente. Durante esse período, o AP ativo envia mensagens de desautenticação a todos os clientes conectados e desliga a interface de rádio. Em seguida, ele se associará ao AP invasor como um cliente.

Em seguida, o AP tenta obter um endereço IP do AP invasor e encaminha um pacote UDP (User Datagram Protocol) (porta 6352) que contém o AP local e informações de conexão invasora para o controlador através do AP invasor. Se o controlador receber esse pacote, o alarme será definido para notificar o administrador de rede de que um AP invasor foi descoberto na rede com fio com o recurso RLDP.

Observação: use o comando **debug dot11 rldp enable** para verificar se o Lightweight AP associa e recebe um endereço DHCP do AP invasor. Esse comando também exibe o pacote UDP enviado

pelo Lightweight AP à controladora.

Um exemplo de um pacote UDP (porta de destino 6352) enviado pelo AP leve é mostrado aqui:

```
0020 0a 01 01 0d 0a 01 .......(..*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00
......x......... 0040 00 00 00 00 00 00 00 00 00 00 00 00
```

Os primeiros 5 bytes dos dados contêm o endereço DHCP fornecido ao AP de modo local pelo AP invasor. Os próximos 5 bytes são o endereço IP do controlador, seguido por 6 bytes que representam o endereço MAC do AP invasor. Em seguida, há 18 bytes de zeros.

Operação passiva:

Essa abordagem é usada quando o AP invasor tem alguma forma de autenticação, WEP ou WPA. Quando uma forma de autenticação é configurada em AP invasor, o AP Lightweight não pode se associar porque não sabe a chave configurada no AP invasor. O processo começa com o controlador quando ele passa na lista de endereços MAC de clientes invasores para um AP configurado como um detector invasor. O detector invasor verifica todas as sub-redes conectadas e configuradas em busca de solicitações ARP e o ARP procura um endereço correspondente da Camada 2. Se for descoberta uma correspondência, o controlador notifica o administrador de rede de que um invasor é detectado na sub-rede com fio.

Contenção invasora ativa

Quando um cliente invasor é detectado na rede com fio, o administrador da rede pode conter tanto o AP invasor quanto os clientes invasores. Isso pode ser feito porque os pacotes de desautenticação 802.11 são enviados aos clientes associados a APs invasores para que a ameaça que tal buraco cria seja atenuada. Cada vez que há uma tentativa de conter o AP invasor, quase 15% do recurso do AP Lightweight é usado. Portanto, é sugerido localizar e remover fisicamente o AP invasor assim que ele estiver contido.

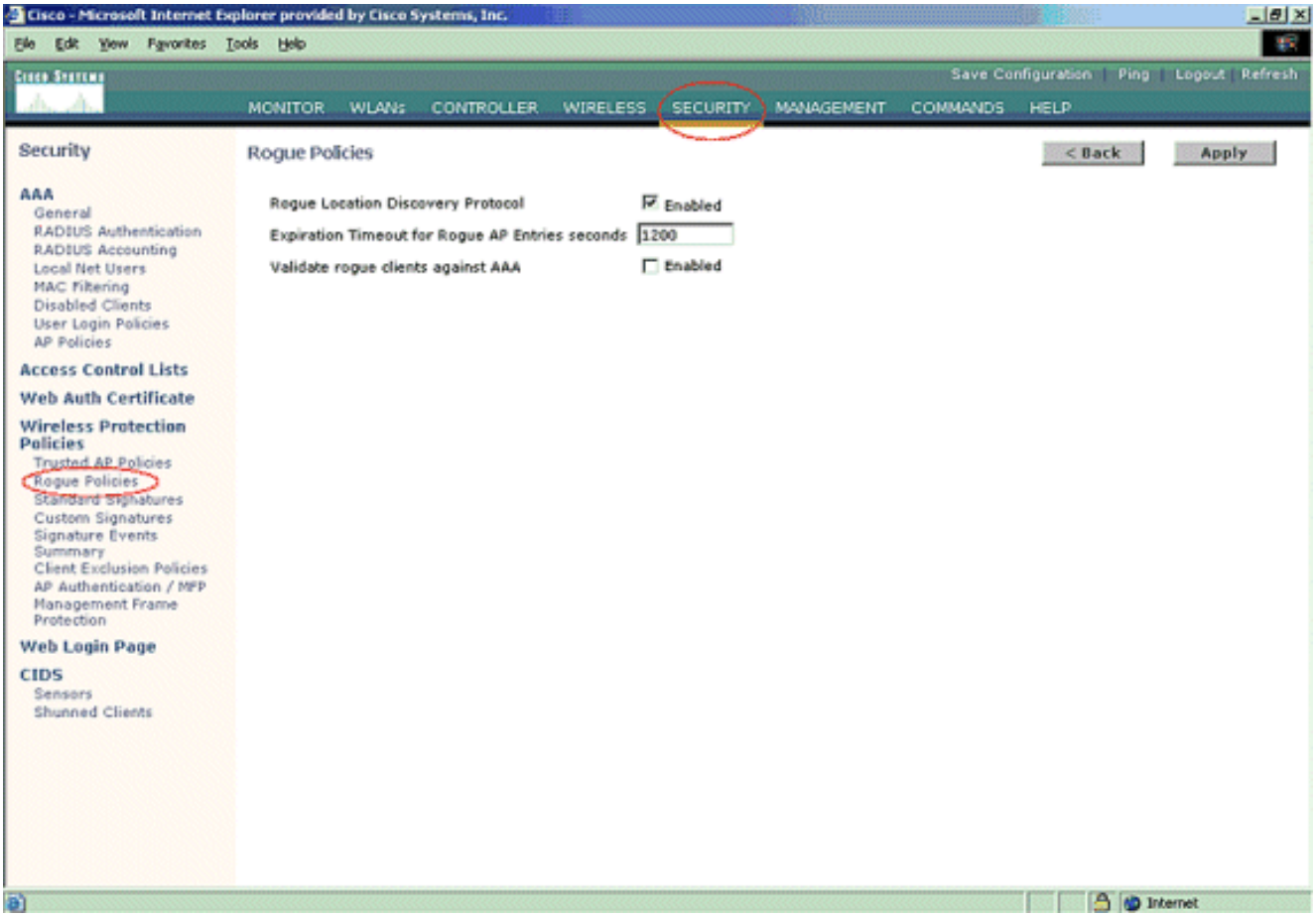
Observação: na versão 5.2.157.0 da WLC, quando o roteador for detectado, você poderá optar por conter o invasor detectado manualmente ou automaticamente. Nas versões de software do controlador anteriores à 5.2.157.0, a contenção manual é a única opção.

Detecção de invasores - Etapas de configuração

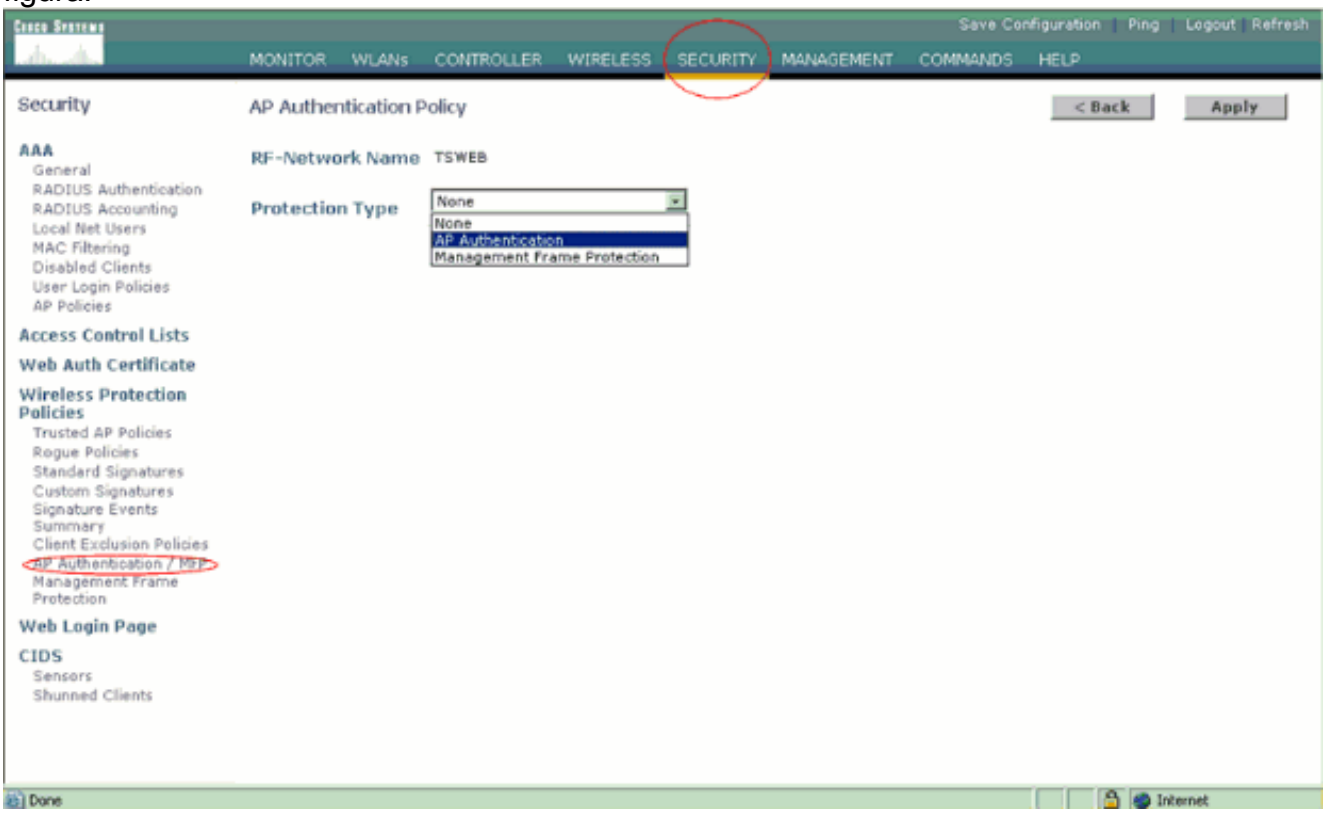
Quase toda a configuração de detecção de invasores é habilitada por padrão para permitir segurança de rede maximizada e pronta para uso. Essas etapas de configuração presumem que nenhuma detecção de invasor está configurada no controlador para esclarecer informações importantes de detecção de invasores.

Para configurar a detecção de invasores, faça o seguinte:

1. Verifique se o protocolo Rogue Location Discovery está ativado. Para ativá-lo, escolha **Security > Rogue Policies** e clique em **Enabled (Habilitado)** no **Rogue Location Discovery Protocol,** como mostrado na figura.**Observação:** se um AP invasor não for ouvido por um certo tempo, ele será removido da controladora. Este é o **tempo limite de expiração** para um AP invasor, que é configurado abaixo da opção
   RLDP.

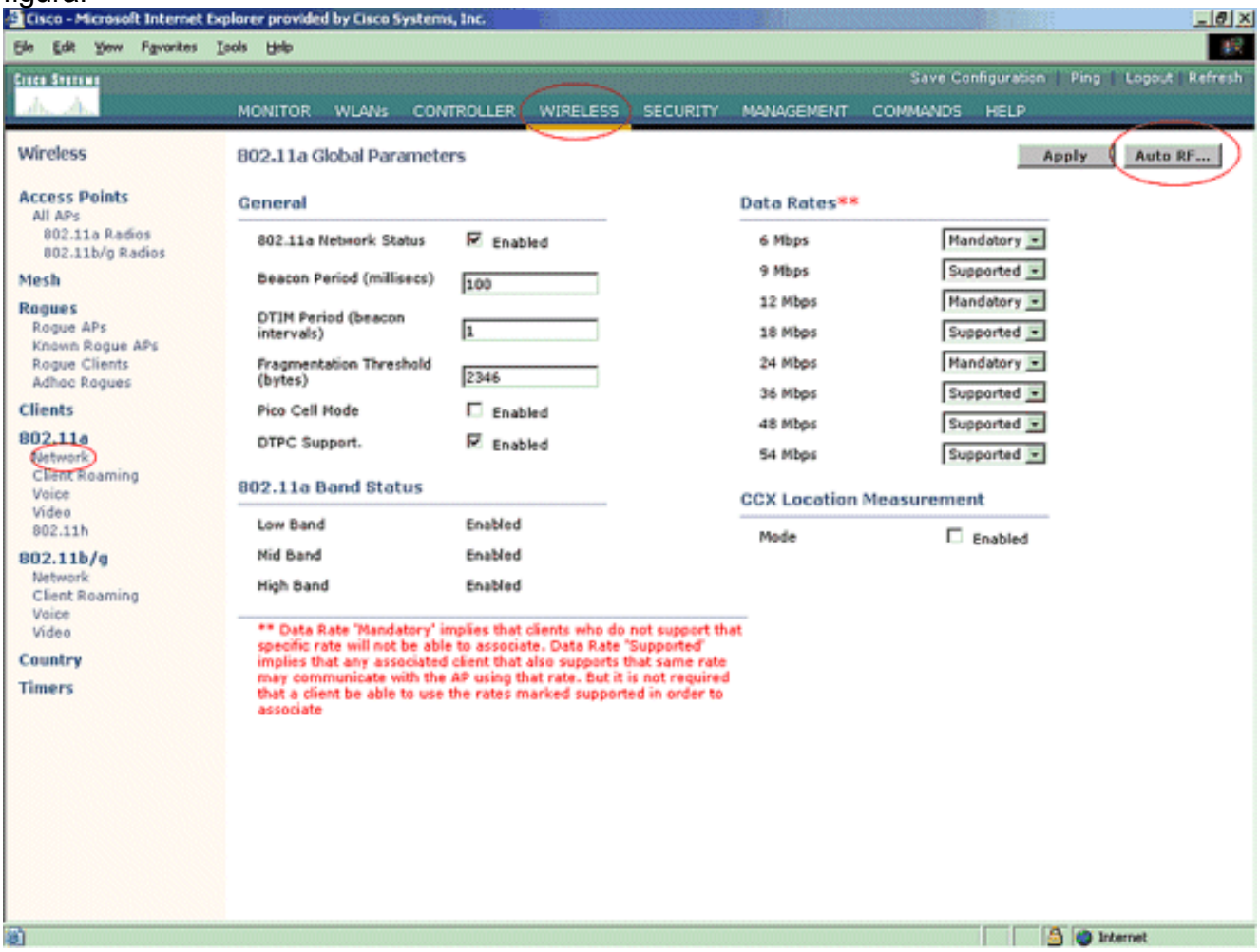


2. Esta é uma etapa opcional. Quando esse recurso é ativado, os APs que enviam pacotes de vizinhos RRM com diferentes nomes de **grupo RF** são relatados como invasores. Isso será útil no estudo do seu ambiente de RF. Para ativá-lo, escolha **Security-> AP Authentication**. Em seguida, escolha **Autenticação de AP** como o Tipo de Proteção como mostrado na figura.

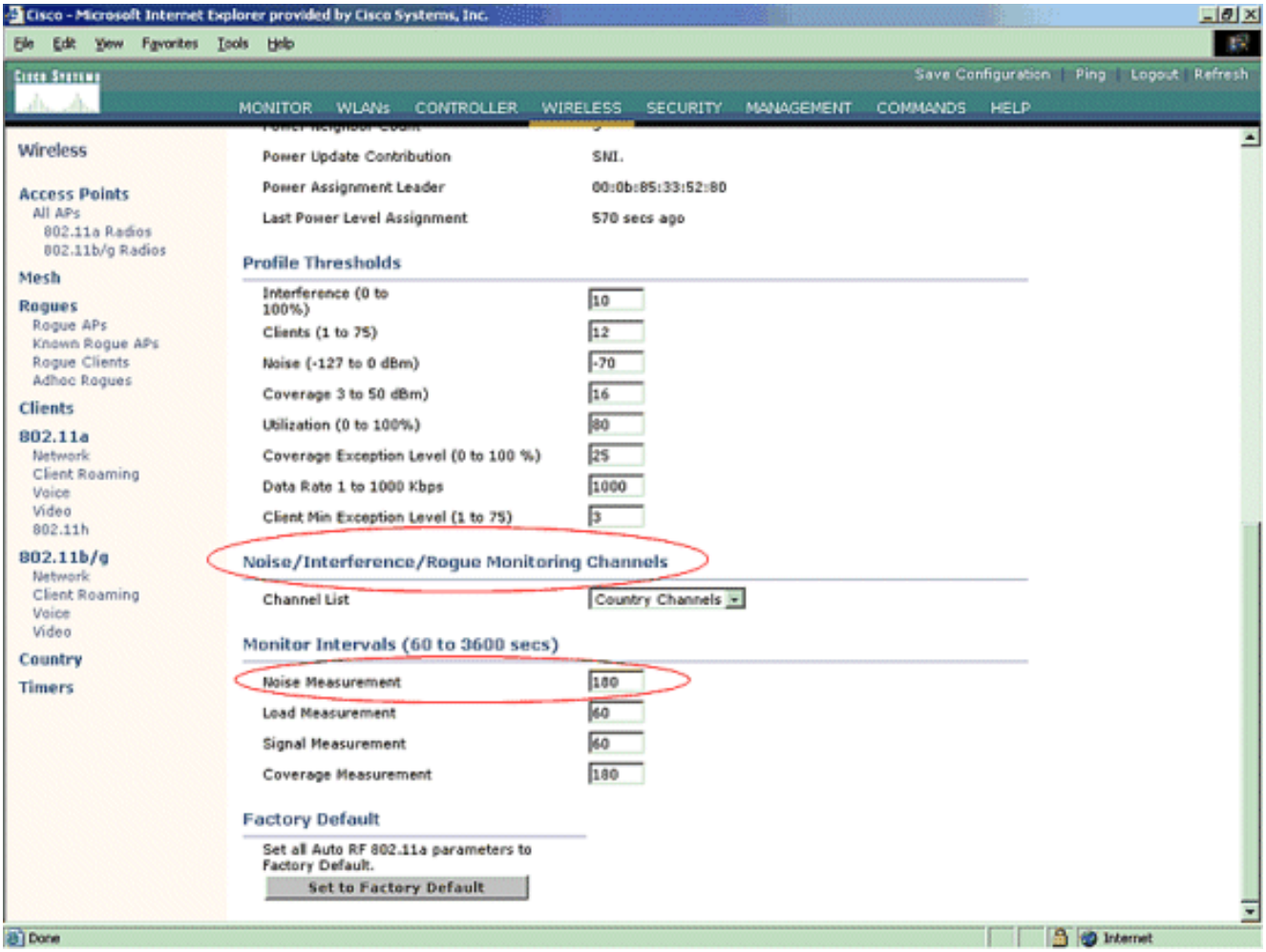


3. Verifique os canais a serem verificados nessas etapas:Selecione **Wireless > 802.11a Network** e, em seguida, **Auto RF** no lado direito como mostrado na

figura.



Na página **Auto RF**, role para baixo e escolha **Noise/Interference/Rogue Monitoring Channels**.



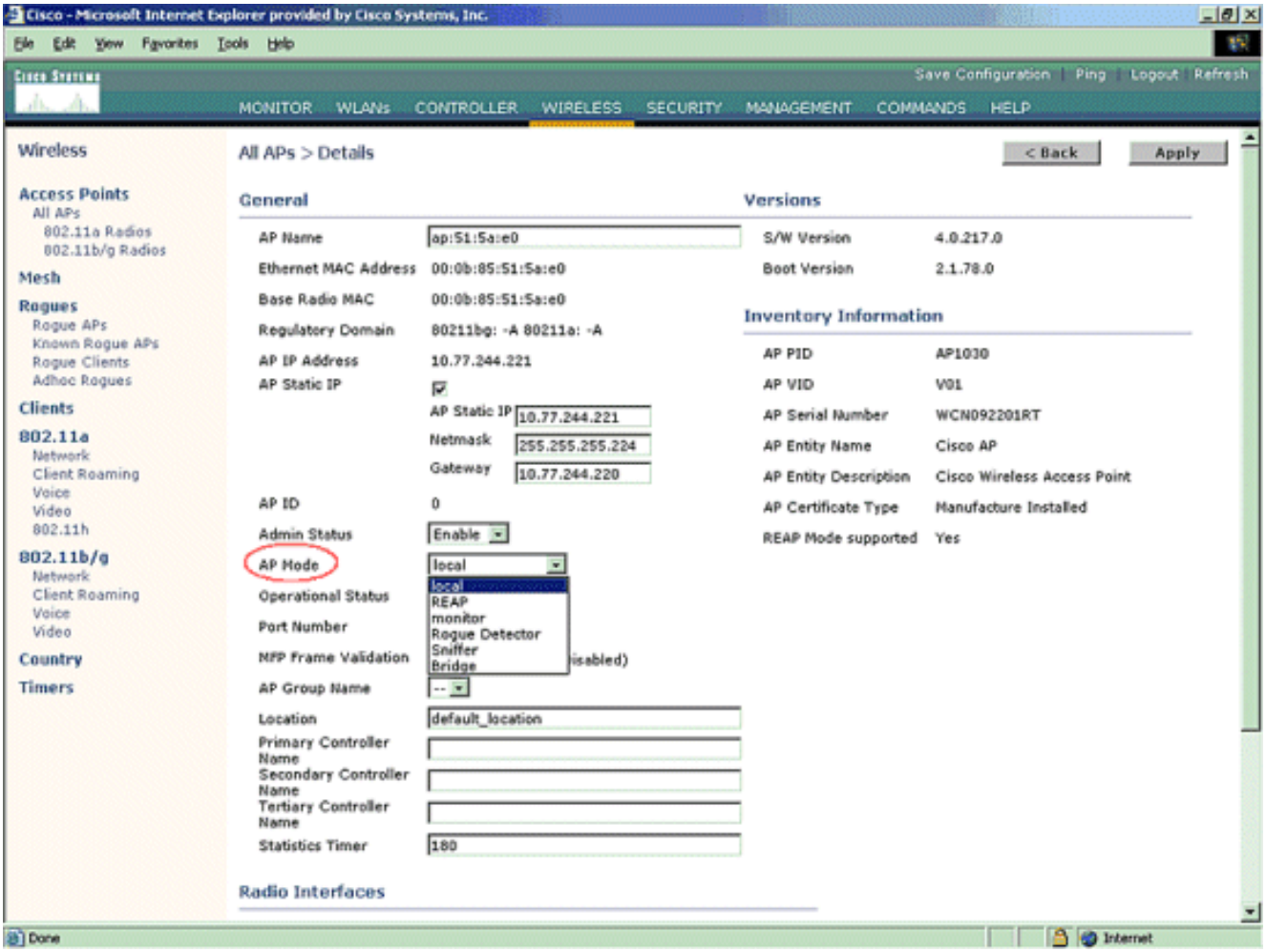
A lista de canais detalha os canais a serem verificados para monitoramento de invasores, além de outras funções de controlador e AP. Consulte FAQ do Lightweight Access Point para obter mais informações sobre APs Lightweight e Perguntas Frequentes sobre Troubleshooting do Wireless LAN Controller (WLC) para obter mais informações sobre controladores sem fio.

Channel Group Option	Channels Scanned for 802.11b/g	Channels Scanned for 802.11a
All Channels	1 - 14	
Country Channels	1 -11	
DCA Channels (Configurable)	1, 6, 11	36, 40, 44, 48, 52, 56, 60, 64

4. Defina o Período para a verificação dos canais selecionados:A duração da verificação do grupo definido de canais é configurada em **Monitor Interval > Noise Measurement**, e o intervalo permitido é de 60 a 3600 segundos. Se deixados no padrão de 180 segundos, os APs examinam cada canal no grupo de canais uma vez, por 50 ms, a cada 180 segundos. Durante esse período, o rádio AP muda de seu canal de serviço para o canal especificado, escuta e grava valores por um período de 50 ms e, em seguida, retorna ao canal original. O tempo de salto mais o tempo de permanência de 50 ms retira o AP do canal por aproximadamente 60 ms cada vez. Isso significa que cada AP gasta aproximadamente 840

ms do total de 180 segundos escutando invasões.O tempo de "escuta" ou "permanência" não pode ser modificado e não é alterado com um ajuste do valor de Medição de Ruído. Se o temporizador de Medição de Ruído for baixado, o processo de descoberta invasor provavelmente encontrará mais invasores e os encontrará mais rapidamente. No entanto, essa melhoria ocorre em detrimento da integridade dos dados e do serviço ao cliente. Um valor mais alto, por outro lado, permite uma melhor integridade dos dados, mas reduz a capacidade de encontrar invasores rapidamente.

5. Configure o modo de operação do AP:Um modo de operação do AP leve define a função do AP. Os modos relacionados às informações apresentadas neste documento são:**Local** — Esta é a operação normal de um AP. Esse modo permite que os clientes de dados sejam atendidos enquanto os canais configurados são verificados quanto a ruídos e problemas. Nesse modo de operação, o AP fica fora do canal por 50 ms e escuta invasores. Ele percorre cada canal, um de cada vez, durante o período especificado na configuração Auto RF.**Monitor** —Este é o modo somente de recebimento de rádio e permite que o AP examine todos os canais configurados a cada 12 segundos. Somente pacotes de não autenticação são enviados no ar com um AP configurado dessa maneira. Um AP do modo de monitor pode detectar invasores, mas não pode se conectar a um invasor suspeito como um cliente para enviar os pacotes RLDP.**Observação:** o DCA se refere a canais não sobrepostos configuráveis com os modos padrão.**Rogue Detector** —Neste modo, o rádio AP é desligado e o AP escuta apenas o tráfego com fio. O controlador passa os APs configurados como detectores invasores, bem como listas de clientes invasores suspeitos e endereços MAC do AP. O detector invasor escuta somente pacotes ARP e pode ser conectado a todos os domínios de broadcast através de um link de tronco, se desejado.Você pode configurar um modo de AP individual de forma simples, depois que o AP Lightweight estiver conectado ao controlador. Para alterar o modo AP, conecte-se à interface da Web do controlador e navegue até **Wireless**. Clique em **Details** ao lado do AP desejado para exibir uma tela semelhante a
esta:



Use o menu suspenso Modo AP para selecionar o modo de operação AP desejado.

Comandos para Troubleshooting

Use estes comandos para solucionar problemas de sua configuração no AP:

- **show rogue ap summary** — Este comando exibe a lista de APs não autorizados detectados pelos APs Lightweight.
- **show rogue detailed** *<MAC address of the rogue ap>* — Use este comando para exibir detalhes sobre um AP invasor individual. Esse é o comando que ajuda a determinar se o AP invasor está conectado à rede com fio.

Conclusão

A detecção e contenção de invasores na solução de controlador centralizado da Cisco é o método mais eficaz e menos intrusivo do setor. A flexibilidade fornecida ao administrador de rede permite um ajuste mais personalizado que pode acomodar quaisquer requisitos de rede.

Informações Relacionadas

- Visão geral dos grupos de RF
- Suporte Técnico e Documentação - Cisco Systems