Detecção desonesto sob redes Wireless unificadas

Índice

Introdução

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 desonesto permite que o administrador de rede monitore e elimine este interesse de segurança. Cisco unificou a arquitetura de rede fornece dois métodos da detecção desonesto que permitem uma solução desonesto completa da identificação e da retenção sem a necessidade para caro e duro-à-justificam redes e ferramentas de folha de prova.

Visão geral do recurso

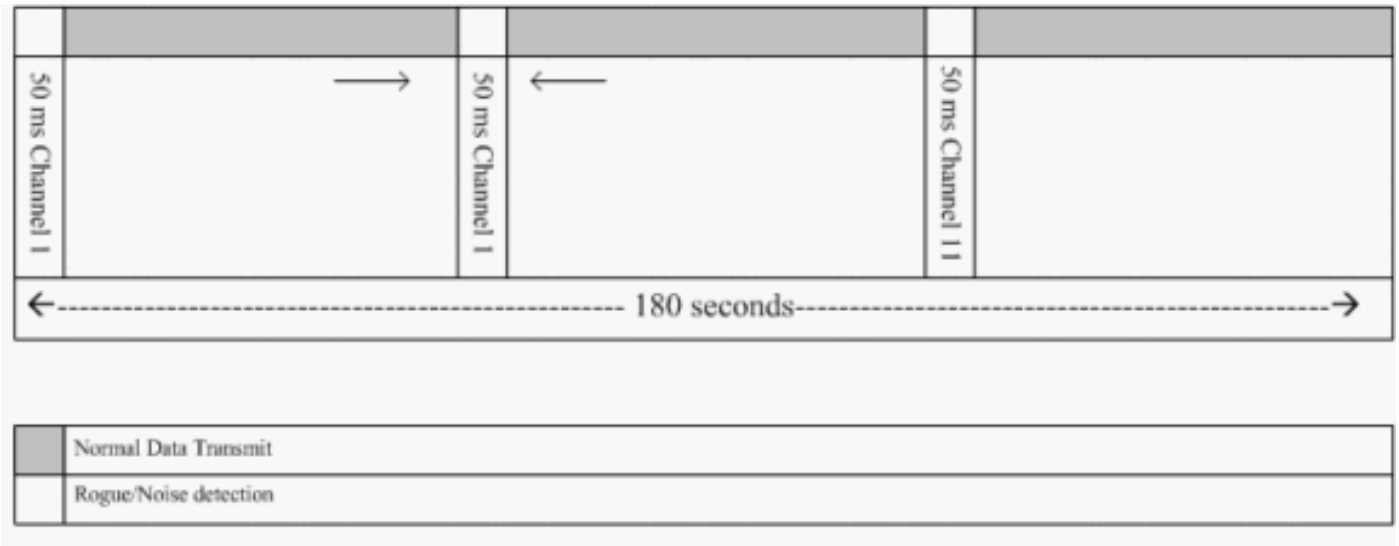
A detecção desonesto não é limitada por nenhuns regulamentos e nenhuma aderência legal é exigida para sua operação. Contudo, a retenção desonesto introduz geralmente as questões legais que podem pôr o fornecedor da infraestrutura em uma posição incômoda se saido para se operar automaticamente. Cisco é extremamente sensível a tais edições e fornece estas soluções. Cada controlador é configurado com um nome do grupo RF. Uma vez que um AP de pouco peso se registra com um controlador, encaixa um **elemento de informação da autenticação (IE)** que seja específico ao grupo RF configurado no controlador em todos seus balizas/frames de resposta da ponta de prova. Quando o AP de pouco peso ouve balizas sondar frames de resposta de um AP sem este **IE** ou com **IE errado**, a seguir o AP de pouco peso relata que o AP como um rogue, grava seu BSSID em uma tabela desonesto, e envia a tabela ao controlador. Há dois

métodos, a saber o protocolo de descoberta desonesto do lugar (RLDP) e a operação passiva, que são explicados em detalhe; veja a seção ativa dos rogues da determinação.

Descoberta desonesto da infraestrutura

A descoberta desonesto em um ambiente Wireless ativo pode ser cara. Este processo pede o AP no serviço (ou no modo local) para cessar o serviço, escutar o ruído, e para executar a detecção desonesto. O administrador de rede configura os canais para fazer a varredura, e configura o período de tempo em que todas as estações são feitas a varredura. O AP escuta a Senhora dos 50 pés para balizas desonestos do cliente, a seguir retorna ao canal configurado a fim prestar serviços de manutenção outra vez a clientes. Esta exploração ativa, combinada com as mensagens vizinhas, identifica que AP são rogues e que AP são válidos e parte da rede. A fim configurar os canais feitos a varredura e o período de tempo da exploração, consulte ao **Sem fio > à rede 802.11b/g** (“**b/g**” ou “**a**” segundo o requisito de rede) e selecione o **auto** botão **RF no** canto direito superior da janela de navegador.

Você pode enrolar para baixo **propalar/os canais monitoração da interferência/rogue** a fim configurar os canais a ser feitos a varredura para rogues e propalá-los. As escolhas disponíveis são: Todo o) dos canais (1 a 14, os canais do país (1 a 11) ou canais dinâmicos da associação do canal (DCA) (à revelia 1, 6 e 11). O período de tempo da exploração através destes canais pode ser configurado no mesmo indicador, sob **intervalos do monitor (60 a 3600 segundos)** junto com o intervalo da medida de ruído. À revelia, o intervalo de escuta para o ruído do fora-canal e os rogues são 180 segundos. Isto significa que cada canal está feito a varredura cada 180 segundos. Este é um exemplo dos canais DCA que são feitos a varredura cada 180 segundos:



Como ilustrado, um alto número de canais configurados para ser feito a varredura combinou com os intervalos curtos da exploração, deixa menos hora para os clientes dos dados de serviço AP realmente.

As esperas de pouco peso AP a fim etiquetar clientes e AP como rogues porque estes rogues não estão relatados possivelmente por um outro AP até que um outro ciclo estiver terminado. Os mesmos movimentos AP ao mesmo canal outra vez a fim monitorar para o rogue AP e os clientes, assim como o ruído e a interferência. Se os mesmos clientes e/ou AP são detectados, estão alistados como rogues no controlador outra vez. O controlador começa agora a determinar se estes rogues são anexados à rede local ou simplesmente a um AP vizinho. Em qualquer dos casos, um AP que não seja parte da rede Wireless local controlada é considerado um rogue.

Detalhes desonestos

Um AP de pouco peso vai fora-canal para a Senhora dos 50 pés a fim escutar clientes desonestos, monitor para o ruído, e interferência do canal. Todos os clientes ou AP desonestos detectados são enviados ao controlador, que recolhe esta informação:

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

Access point desonesto do detector

Você pode fazer um AP operar-se como um detector desonesto, que permita que seja colocado em uma porta de tronco de modo que possa ouvir todos os VLAN conectados prender-lado. Continua encontrar o cliente na sub-rede prendida em todos os VLAN. O detector desonesto AP escuta pacotes do Address Resolution Protocol (ARP) a fim determinar os endereços da camada 2 dos clientes do rogue ou do rogue identificado AP enviados pelo controlador. Se um endereço da camada 2 que combine é encontrado, o controlador gerencie um alarme que identifique o rogue AP ou o cliente como uma ameaça. Este alarme indica que o rogue esteve visto na rede ligada com fio.

Determine rogues ativos

Os AP desonestos devem “ser vistos” duas vezes antes que estejam adicionados como um rogue pelo controlador. Os AP desonestos não estão considerados ser uma ameaça se não são conectados ao segmento com fio da rede corporativa. A fim determinar se o rogue é aproximações ativas, várias é usada. Aquelas aproximações incluem RLDP.

Protocolo de descoberta desonesto do lugar (RLDP)

RLDP é uma aproximação ativa, que esteja usada quando o AP desonesto não tem nenhuma autenticação (autenticação aberta) configurada. Este modo, que é desabilitado à revelia, instrui um AP ativo para mover-se para o canal desonesto e para conectar ao rogue como um cliente. Durante este tempo, o AP ativo envia mensagens do deauthentication a todos os clientes conectados e fecha então a interface de rádio. Então, associará ao rogue AP como um cliente.

O AP tenta então obter um endereço IP de Um ou Mais Servidores Cisco ICM NT do rogue AP e para a frente de um pacote do User Datagram Protocol (UDP) (porta 6352) que contenha o AP local e a informação de conexão desonesto ao controlador com o rogue AP. Se o controlador recebe este pacote, o alarme está ajustado para notificar o administrador de rede que um rogue AP esteve descoberto na rede ligada com fio com a característica RLDP.

Nota: Use o **comando enable do rldp do dot11 debugar** a fim verificar se o AP de pouco peso associa e recebe um endereço de DHCP do rogue AP. Este comando igualmente indica o pacote de UDP enviado pelo AP de pouco peso ao controlador.

Uma amostra de um pacote UDP (porta do destino 6352) enviado pelo AP de pouco peso é mostrada 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
```

Os primeiros bytes 5 dos dados contêm o endereço de DHCP dado ao modo local AP pelo rogue AP. Os bytes 5 seguintes são o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador, seguido pelos bytes 6 que representa o MAC address do rogue AP. Então, há 18 bytes dos zero.

Operação passiva:

Esta aproximação é usada quando o AP desonesto tem algum formulário de autenticação, WEP ou WPA. Quando um formulário de autenticação é configurado no rogue AP, o AP de pouco peso não pode associar porque não conhece a chave configurada no rogue AP. O processo começa com o controlador quando passa sobre a lista de endereços MAC de cliente desonestos a um AP que esteja configurado como um detector desonesto. O detector desonesto faz a varredura de todas as sub-redes conectadas e configuradas para requisições ARP, e o ARP procura por um endereço de harmonização da camada 2. Se um fósforo é descoberto, o controlador notifica o administrador de rede que um rogue está detectado na sub-rede prendida.

Retenção desonesto do Active

Um cliente desonesto é detectado uma vez na rede ligada com fio, o administrador de rede pode conter o rogue AP e os clientes desonestos. Isto pode ser conseguido porque os pacotes da de-autenticação do 802.11 são enviados aos clientes que são associados para eliminar as plantas pouco vigorozas AP de modo que a ameaça que tal furo cria seja abrandada. Cada vez que há uma tentativa de conter o rogue AP, quase 15% do recurso do AP de pouco peso está usado. Consequentemente, sugere-se para encontrar e remover fisicamente o rogue AP uma vez que é contido.

Nota: Do WLC libere 5.2.157.0, uma vez que o vermelho lhe é detectado pode agora escolher para conter a manualmente ou automaticamente o rogue detectado. Em software release do controlador antes de 5.2.157.0, a retenção manual é a única opção.

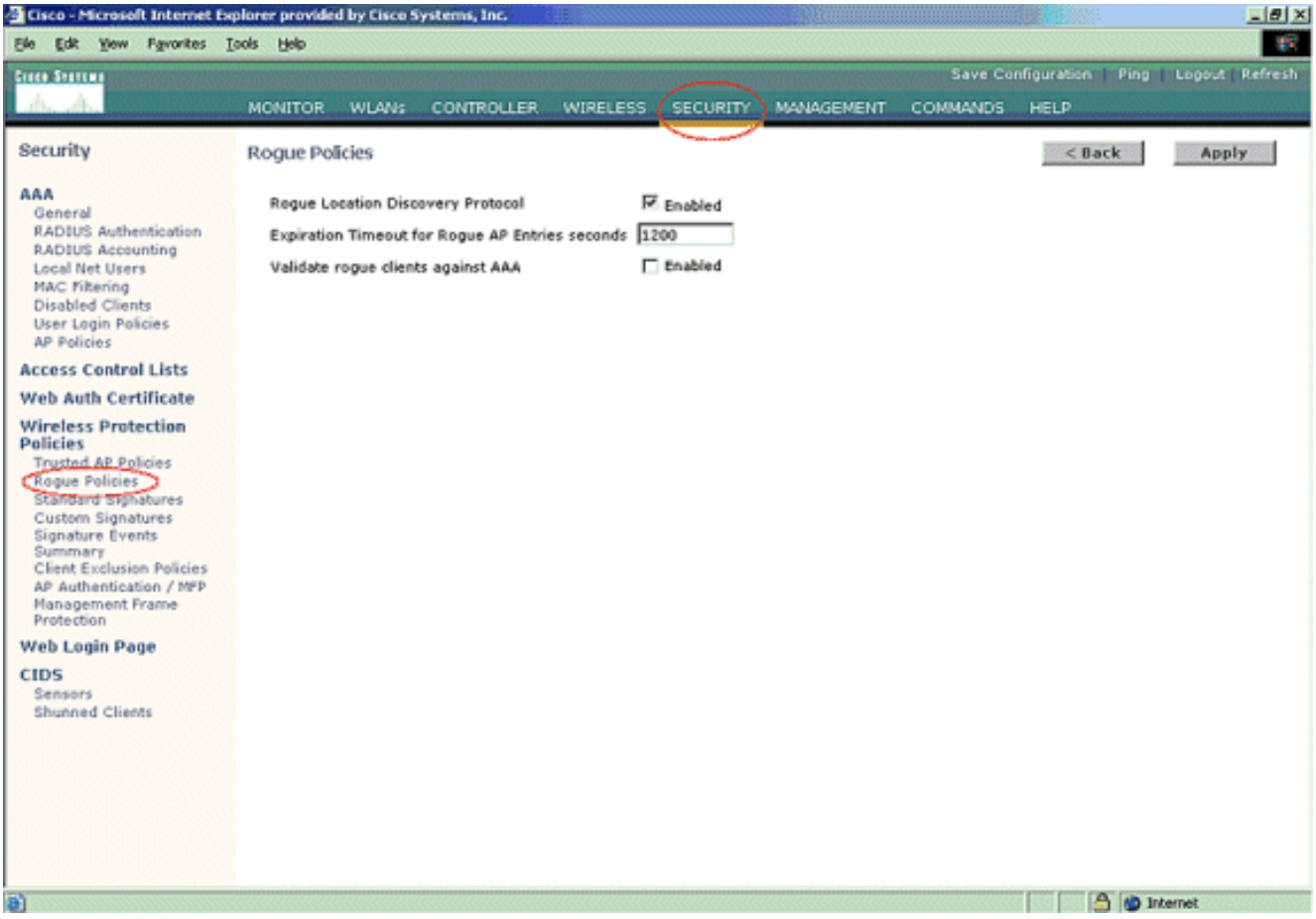
Detecção desonesto – Etapas de configuração

A configuração desonesto inteira da detecção é permitida quase à revelia de permitir maximizado, segurança de rede da para fora---caixa. Estas etapas de configuração supõem que nenhuma detecção desonesto se estabelece no controlador a fim esclarecer a informação desonesto importante da detecção.

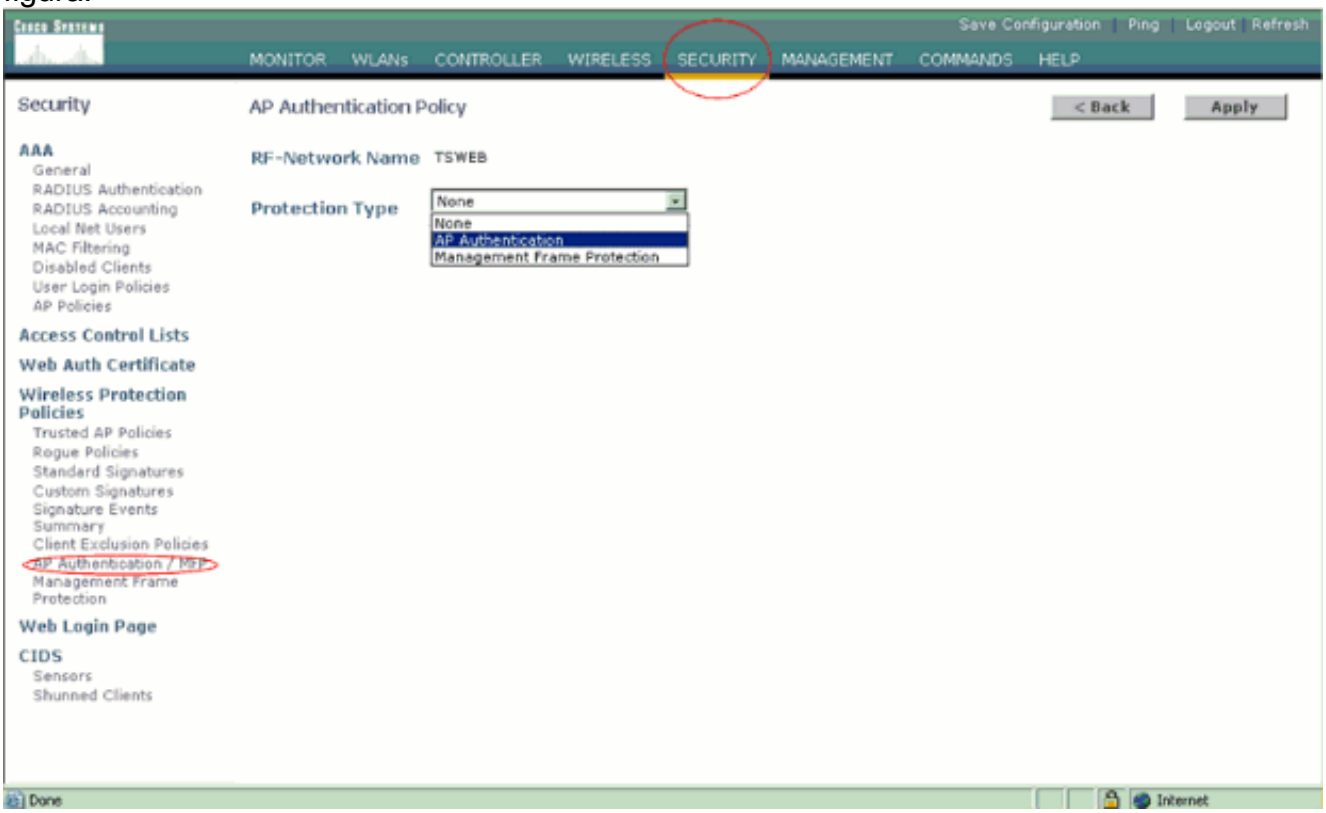
A fim estabelecer a detecção desonesto, termine estas etapas:

1. Assegure-se de que o protocolo de descoberta do lugar do rogue esteja girado sobre. A fim girá-lo sobre, para escolher **políticas da Segurança > do rogue** e para clicá-las **permitiu no protocolo de descoberta desonesto do lugar** segundo as indicações da figura.**Nota:** Se um rogue AP não é ouvido para uma certa quantidade de tempo, é formulário removido o controlador. Este é o **intervalo da expiração** para um rogue AP, que seja configurado abaixo

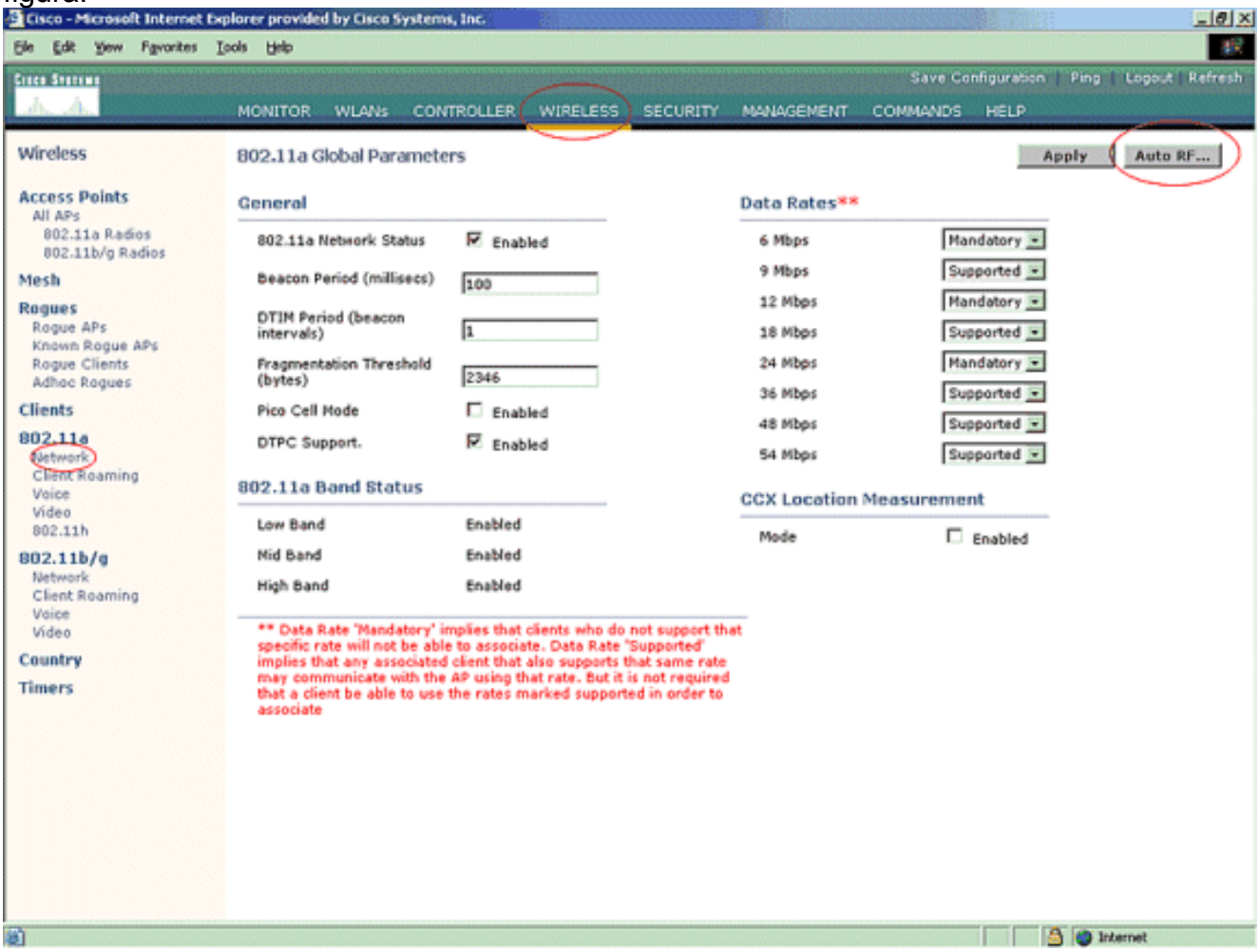
da opção
RLDP.



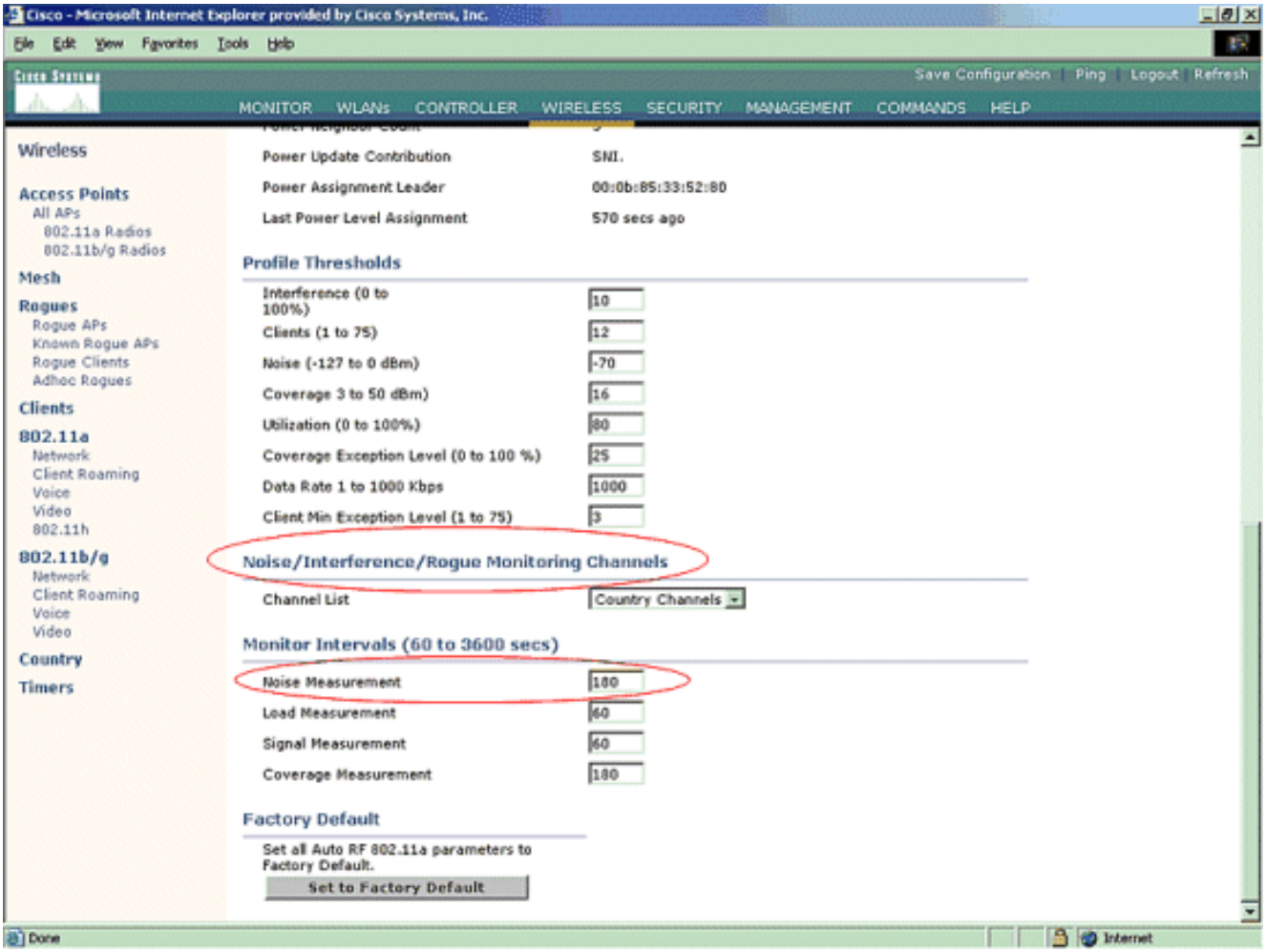
2. Esta é uma etapa opcional. Quando esta característica é permitida, os AP que enviam a RRM pacotes vizinhos com **nomes do grupo** diferentes **RF** estão relatados como rogues. Isto será útil em estudar seu ambiente RF. A fim permiti-lo, escolha a **autenticação de Security-> AP**. Então, escolha a **autenticação AP** como o tipo de proteção segundo as indicações da figura.



3. Verifique os canais a ser feitos a varredura nestas etapas:Selecione o **Sem fio > a rede 802.11a**, então **auto RF no** lado direito segundo as indicações da figura.



Na auto página **RF**, enrole para baixo e escolha os **canais de monitoração do ruído/interferência/rogue**.



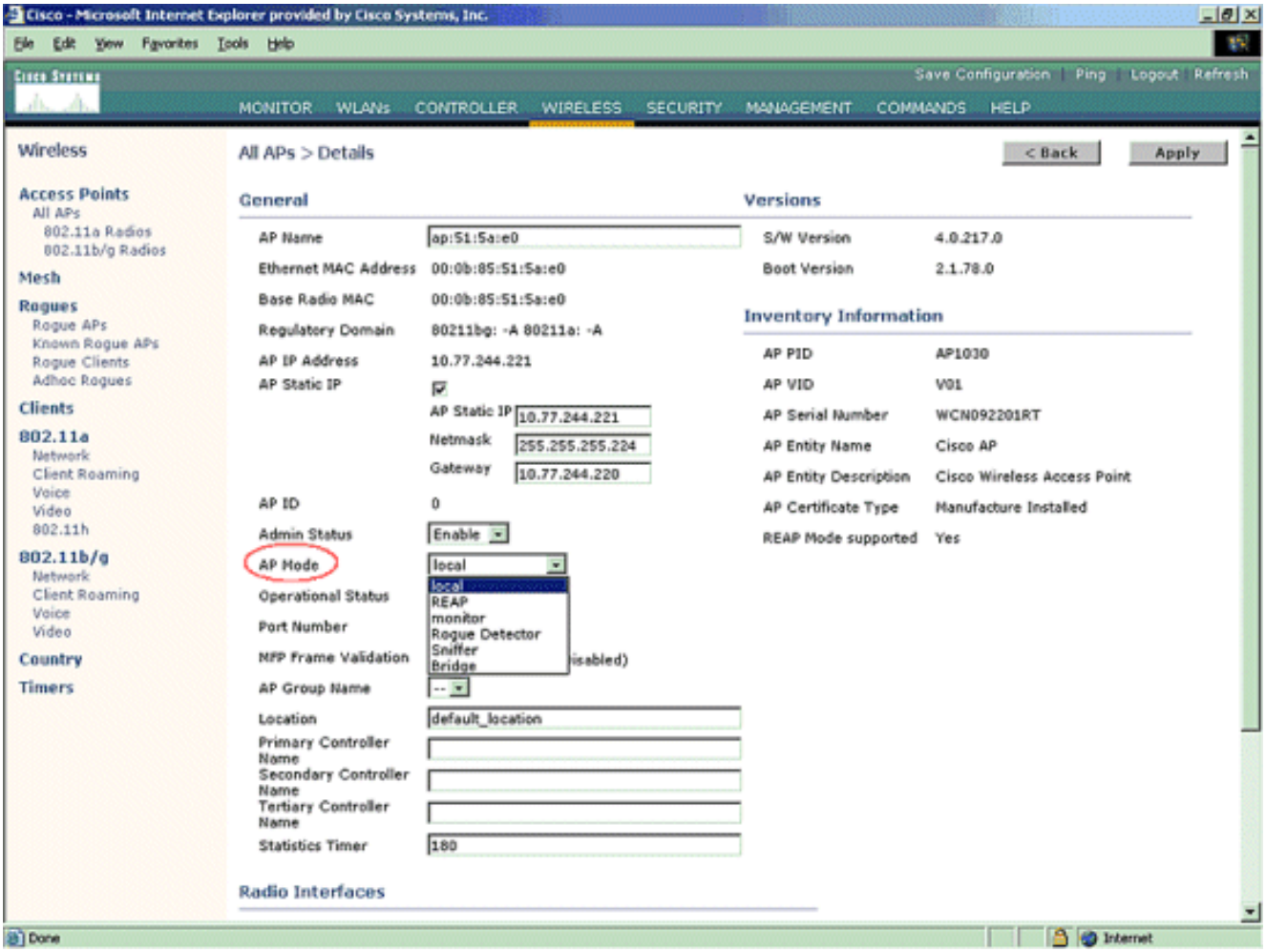
A lista do canal detalha os canais a ser feitos a varredura para a monitoração desonesto, além do que o outro controlador e as funções AP. Refira o Access point de pouco peso FAQ para obter mais informações sobre dos AP de pouco peso, e o controlador do Wireless LAN (WLC) pesquisa defeitos o FAQ para obter mais informações sobre dos controladores wireless.

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. Ajuste o período de tempo para fazer a varredura dos canais selecionados:A duração da exploração do grupo definido de canais é configurada sob **intervalos > medida de ruído do monitor**, e a escala permissível é 60 a 3600 segundos. Se saido no padrão de 180 segundos, os AP fazem a varredura de cada canal no grupo de canais uma vez, para a Senhora dos 50 pés, cada 180 segundos. Durante este período, as mudanças do rádio AP de seu canal do serviço ao canal especificado, escutam e gravam valores por um período de Senhora dos 50 pés, e retornam então ao canal original. O tempo do salto mais a época de interrupção da Senhora dos 50 pés toma o fora-canal AP para a Senhora aproximadamente 60 cada vez. Isto significa que cada AP gasta a Senhora aproximadamente 840 fora do total

180 segundos que escuta rogues.“Escute” ou o tempo da “interrupção” não pode ser alterado e não é mudado com um ajuste do valor da medida de ruído. Se o temporizador da medida de ruído é abaixado, o processo de descoberta desonesto é provável encontrar mais rogues e encontrá-los mais rapidamente. Contudo, esta melhoria vem às expensas da integridade de dados e do serviço de cliente. Um valor mais alto, por outro lado, permite a melhor integridade de dados mas abaixa a capacidade para encontrar rapidamente rogues.

5. Configurar o modo AP de operação:Um modo AP de pouco peso de operação define o papel do AP. Os modos relativos à informação apresentada em este documento são:**Local** — Esta é a operação normal de um AP. Este modo permite que os clientes dos dados sejam prestados serviços de manutenção quando os canais configurados forem feitos a varredura para o ruído e os rogues. Neste modo de operação, o AP vai fora-canal para a Senhora dos 50 pés e escuta rogues. Dá um ciclo através de cada canal, um de cada vez, para o período especificado sob a auto configuração RF.**Monitor** — Isto é de rádio recebe - somente o modo, e permite que o AP faça a varredura do todo o configurado canaliza cada 12 segundos. Somente os pacotes da de-autenticação são enviados no ar com um AP configuraram esta maneira. Um modo de monitor AP pode detectar rogues, mas não pode conectar a um rogue suspeito porque um cliente a fim enviar os pacotes RLDP.**Nota:** O DCA refere os canais desobreposição que são configuráveis com os modos padrão.**Detector desonesto** — Neste modo, o rádio AP é desligado, e o AP escuta o tráfego prendido somente. O controlador passa os AP configurados como detectores do rogue assim como lista de clientes desonestos suspeitados e de endereços AP MAC. O detector desonesto escuta pacotes ARP somente, e pode ser conectado a todos os domínios de transmissão através de um enlace de tronco se desejado.Você pode configurar um modo AP individual simplesmente, uma vez que o AP de pouco peso é conectado ao controlador. A fim mudar o modo AP, conecte à interface da WEB do controlador e navegue ao **Sem fio**. Clique sobre **detalhes** ao lado do AP desejado à fim indicar uma tela similar a esta:



Use o menu suspenso do modo AP a fim selecionar o modo AP desejado de operação.

Comandos para Troubleshooting

Você pode igualmente usar estes comandos a fim pesquisar defeitos sua configuração no AP:

- **mostre o sumário desonesto ap** — Este comando indica a lista do rogue AP detectado pelos AP de pouco peso.
- **mostre o ap desonesto detalhado** *< MAC address do ap> desonesto* — use este comando a fim ver detalhes sobre um rogue individual AP. Este é o comando que ajuda a determinar se o rogue AP é obstruído na rede ligada com fio.

Conclusão

A detecção desonesto e a retenção dentro da solução centralizada Cisco do controlador são método o mais eficaz e menos o mais intrusivo na indústria. A flexibilidade fornecida ao administrador de rede permite um ajuste mais personalizado que possa acomodar todos os requisitos de rede.

Informações Relacionadas

- Vista geral de grupos RF
- Suporte Técnico e Documentação - Cisco Systems