Rilevamento di anomalie nelle reti wireless unificate

Sommario

Introduzione

Le reti wireless estendono le reti cablate e aumentano la produttività dei dipendenti e l'accesso alle informazioni. Tuttavia, una rete wireless non autorizzata presenta un livello aggiuntivo di problemi di sicurezza. La sicurezza delle porte nelle reti cablate è meno studiata e le reti wireless rappresentano una facile estensione delle reti cablate. Pertanto, un dipendente che inserisce il proprio punto di accesso Cisco (AP) in un'infrastruttura wireless o cablata ben protetta e consente a utenti non autorizzati di accedere a questa rete altrimenti protetta può facilmente compromettere la sicurezza della rete.

Il rilevamento dei server non autorizzati consente all'amministratore di rete di monitorare ed eliminare questo problema di sicurezza. L'architettura di rete unificata di Cisco offre due metodi di rilevamento rogue che consentono di identificare i rogue e soluzioni di contenimento complete senza la necessità di reti e strumenti di sovrapposizione costosi e difficili da giustificare.

Panoramica delle funzionalità

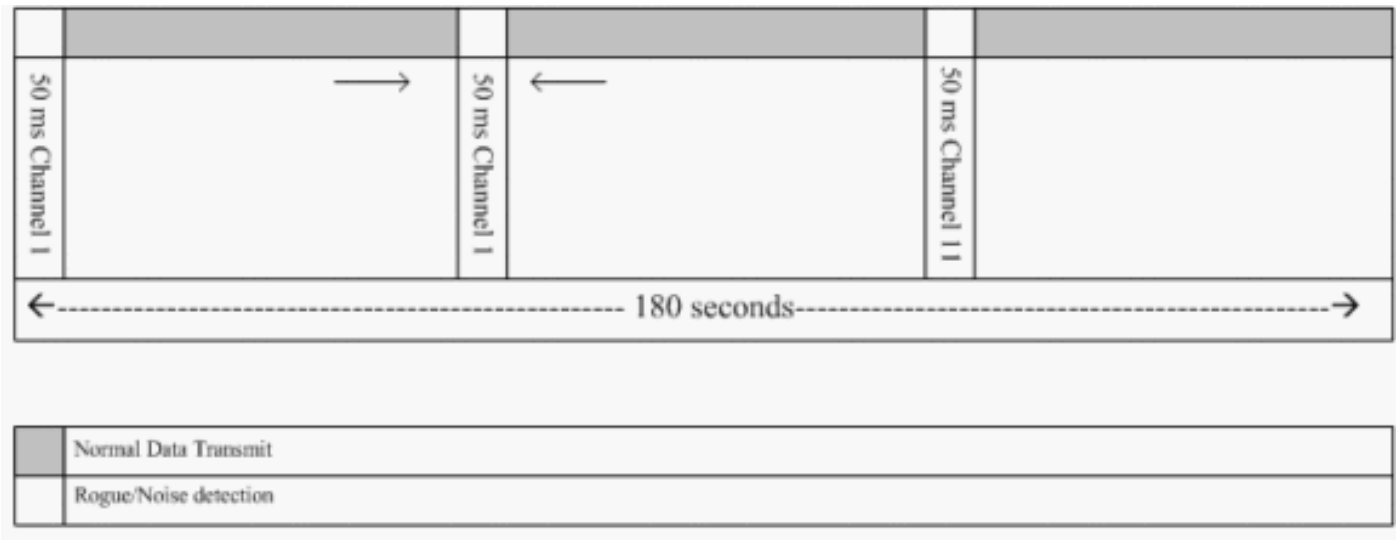
Il rilevamento dei server non autorizzati non è vincolato da alcuna normativa e non è necessaria alcuna conformità legale per il funzionamento di tale sistema. Tuttavia, i sistemi sigillati di solito introducono problemi legali che possono mettere il fornitore dell'infrastruttura in una posizione scomoda se lasciato operare automaticamente. Cisco è estremamente sensibile a tali problemi e fornisce queste soluzioni. Ogni controller è configurato con un nome di gruppo RF. Una volta registrato da un Lightweight AP con un controller, il Lightweight AP incorpora un **elemento di informazioni di autenticazione (IE)** specifico del Gruppo RF configurato sul controller in tutti i relativi frame di risposta beacon/sonda. Quando il punto di accesso Lightweight riceve i frame di risposta beacon/sonda da un punto di accesso senza il punto di **accesso** o con il punto di accesso **errato**, il punto di accesso Lightweight lo segnala come non autorizzato, registra il suo BSSID in

una tabella non autorizzata e invia la tabella al controller. Esistono due metodi, ossia il protocollo RLDP (Rogue Location Discovery Protocol) e il funzionamento passivo, che vengono spiegati in dettaglio; vedere la sezione Determinazione di regole attive.

Discovery dei server non autorizzati per l'infrastruttura

L'individuazione di anomalie in un ambiente wireless attivo può essere costosa. Questo processo richiede all'access point in servizio (o in modalità locale) di interrompere il servizio, ascoltare la presenza di rumore ed eseguire il rilevamento rogue. L'amministratore di rete configura i canali da analizzare e configura il periodo di tempo durante il quale tutte le stazioni vengono analizzate. L'access point resta in attesa di 50 ms per i beacon client non autorizzati, quindi torna al canale configurato per servire di nuovo i client. Questa analisi attiva, insieme ai messaggi adiacenti, identifica i punti di accesso non autorizzati, quelli validi e quelli che fanno parte della rete. Per configurare i canali digitalizzati e il periodo di tempo di scansione, selezionare **Wireless > 802.11b/g Network** (**b/g** o "**a**" a seconda dei requisiti di rete) e selezionare il pulsante **Auto RF** nell'angolo in alto a destra della finestra del browser.

Èpossibile scorrere verso il basso fino a **Noise/Interference/Rogue Monitoring Channels** (Rumori/interferenze/canali non autorizzati) per configurare i canali da scansionare alla ricerca di anomalie e disturbi. Le opzioni disponibili sono: Tutti i canali (da 1 a 14), i canali del paese (da 1 a 11) o i canali DCA (Dynamic Channel Association) (per impostazione predefinita 1, 6 e 11). Il periodo di tempo di scansione attraverso questi canali può essere configurato nella stessa finestra, in **Intervalli di monitoraggio (da 60 a 3600 secondi)** insieme all'intervallo di misurazione del rumore. Per impostazione predefinita, l'intervallo di ascolto per il rumore e i disturbi fuori canale è di 180 secondi. Ciò significa che ogni canale viene analizzato ogni 180 secondi. Questo è un esempio dei canali DCA che vengono analizzati ogni 180 secondi:



Come illustrato, un numero elevato di canali configurati per la scansione combinato con intervalli di scansione brevi lascia meno tempo all'access point per servire effettivamente i client dati.

Il Lightweight Access Point attende di etichettare i client e i punti di accesso come non autorizzati perché è possibile che questi non vengano segnalati da un altro punto di accesso fino al completamento di un altro ciclo. Lo stesso punto di accesso si sposta di nuovo sullo stesso canale per monitorare i punti di accesso e i client non autorizzati, oltre al rumore e alle interferenze. Se vengono rilevati gli stessi client e/o access point, questi vengono nuovamente elencati come non autorizzati sul controller. Il controller ora inizia a determinare se i router sono collegati alla rete locale o semplicemente a un access point adiacente. In entrambi i casi, un access point che non

fa parte della rete wireless locale gestita è considerato non autorizzato.

Dettagli Rogue

Un Lightweight AP esce dal canale per 50 ms per ascoltare i client non autorizzati, monitorare i disturbi e le interferenze dei canali. Tutti i client o gli access point non autorizzati rilevati vengono inviati al controller che raccoglie le seguenti informazioni:

- Indirizzo MAC punto di accesso non autorizzato
- Nome punto di accesso non autorizzato
- Indirizzo MAC dei client connessi non autorizzati
- Se i frame sono protetti con WPA o WEP
- Il preambolo
- Il rapporto segnale/rumore (SNR)
- L'indicatore di potenza del segnale del ricevitore (RSSI)

Access point rilevatore server non autorizzati

Èpossibile fare in modo che un access point funzioni come un rilevatore di anomalie, che consente di posizionarlo su una porta trunk in modo che possa sentire tutte le VLAN connesse dal lato cablato. Il client viene individuato nella subnet cablata su tutte le VLAN. L'access point rogue detector resta in ascolto dei pacchetti ARP (Address Resolution Protocol) per determinare gli indirizzi di layer 2 dei client non autorizzati identificati o dei punti di accesso non autorizzati inviati dal controller. Se viene rilevato un indirizzo di layer 2 corrispondente, il controller genera un allarme che identifica il punto di accesso o il client non autorizzato come minaccia. Questo allarme indica che la canaglia è stata rilevata sulla rete cablata.

Determinazione dei ruoli anomali attivi

Gli access point non autorizzati devono essere "visti" due volte prima di essere aggiunti come non autorizzati dal controller. I punti di accesso non autorizzati non sono considerati una minaccia se non sono collegati al segmento cablato della rete aziendale. Per determinare se la canaglia è attiva, vengono utilizzati vari approcci. Tali approcci includono il programma RLDP.

Protocollo RLDP (Rogue Location Discovery Protocol)

RLDP è un approccio attivo, utilizzato quando il punto di accesso non autorizzato non ha un'autenticazione (autenticazione aperta) configurata. Questa modalità, disabilitata per impostazione predefinita, indica a un punto di accesso attivo di spostarsi sul canale non autorizzato e di connettersi al server non autorizzato come client. Durante questo periodo, l'access point attivo invia messaggi di deautenticazione a tutti i client connessi e quindi chiude l'interfaccia radio. Quindi, verrà associato al punto di accesso non autorizzato come client.

L'access point tenta quindi di ottenere un indirizzo IP dal rogue AP e inoltra un pacchetto UDP (User Datagram Protocol) (porta 6352) contenente l'access point locale e le informazioni sulla connessione rogue al controller tramite il rogue AP. Se il controller riceve questo pacchetto, l'allarme viene impostato per notificare all'amministratore di rete che è stato rilevato un access point non autorizzato sulla rete cablata con la funzionalità RLDP.

Nota: utilizzare il comando **debug dot11 rldp enable** per verificare se il Lightweight AP è associato

e riceve un indirizzo DHCP dal Relay Access Point. Questo comando visualizza anche il pacchetto UDP inviato dal Lightweight AP al controller.

Di seguito è riportato un esempio di pacchetto UDP (porta di destinazione 6352) inviato dal Lightweight AP:

```
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
```

I primi 5 byte dei dati contengono l'indirizzo DHCP assegnato al punto di accesso in modalità locale dal punto di accesso non autorizzato. I successivi 5 byte sono l'indirizzo IP del controller, seguito da 6 byte che rappresentano l'indirizzo MAC del punto di accesso non autorizzato. Poi ci sono 18 byte di zeri.

Funzionamento passivo:

Questo approccio viene utilizzato quando un access point non autorizzato dispone di una forma di autenticazione, WEP o WPA. Quando una forma di autenticazione è configurata in un access point non autorizzato, il Lightweight Access Point non può associarsi perché non conosce la chiave configurata nel server non autorizzato. Il processo inizia con il controller quando passa l'elenco di indirizzi MAC client non autorizzati a un access point configurato come rilevatore di non autorizzati. Il rilevatore anomalo analizza tutte le subnet connesse e configurate per individuare le richieste ARP, mentre ARP cerca un indirizzo di layer 2 corrispondente. Se viene individuata una corrispondenza, il controller notifica all'amministratore di rete che è stato rilevato un server non autorizzato nella subnet cablata.

Contenimento automatico attivo

Una volta rilevato un client non autorizzato sulla rete cablata, l'amministratore di rete può contenere sia il punto di accesso non autorizzato che i client non autorizzati. Questa condizione può essere soddisfatta perché i pacchetti di deautenticazione 802.11 vengono inviati ai client associati ai punti di accesso non autorizzati in modo da ridurre la minaccia creata da un buco di questo tipo. Ogni volta che si tenta di contenere un access point non autorizzato, viene utilizzato quasi il 15% delle risorse del Lightweight Access Point. Pertanto, si consiglia di individuare e rimuovere fisicamente il punto di accesso non autorizzato una volta contenuto.

Nota: Dalla release 5.2.157.0 del WLC, una volta rilevato il router, è possibile scegliere di contenerlo manualmente o automaticamente. Nelle versioni software dei controller precedenti alla 5.2.157.0, l'unica opzione disponibile è il contenimento manuale.

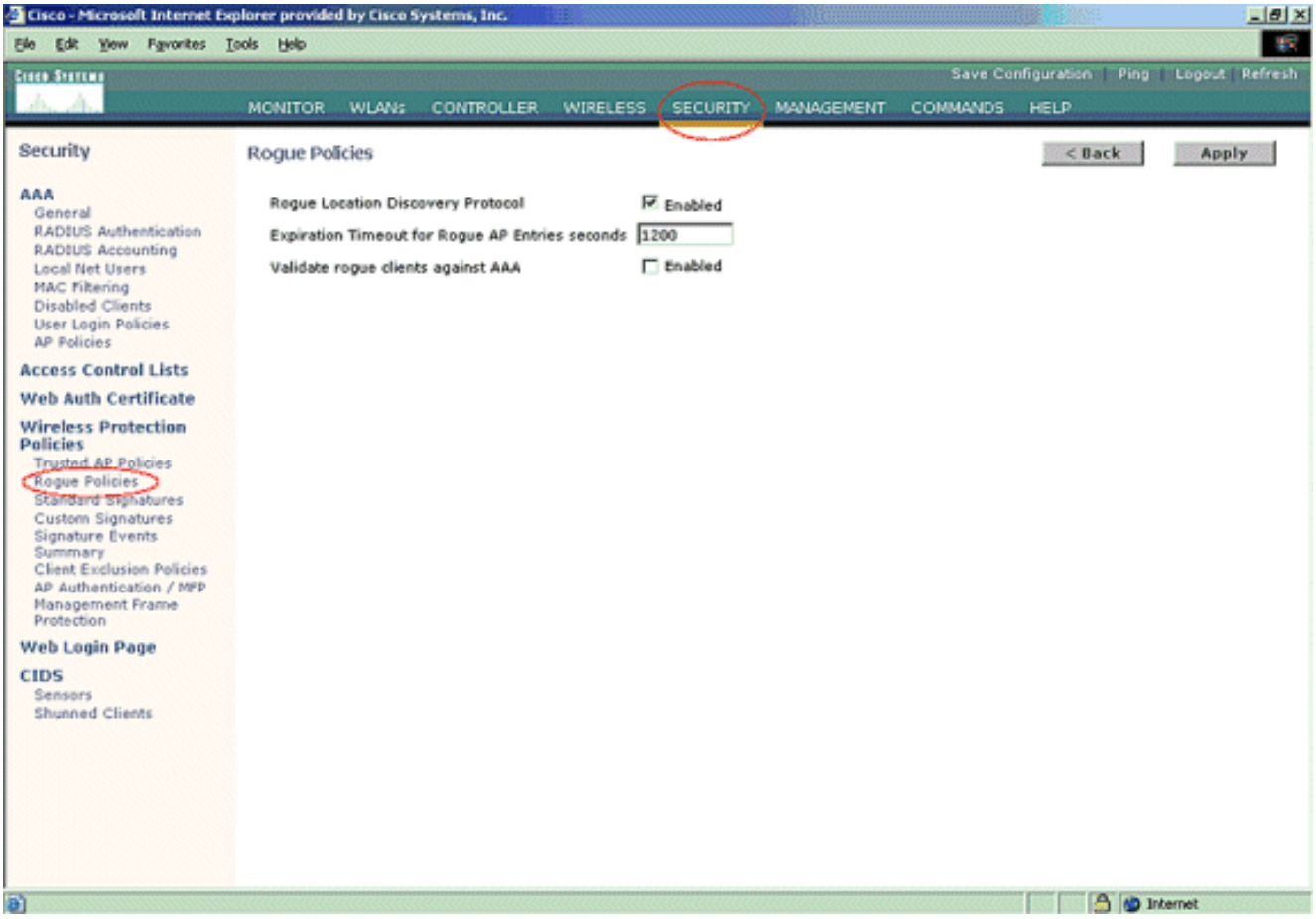
Rilevamento anomalie - Procedura di configurazione

Per impostazione predefinita, quasi l'intera configurazione del rilevamento rogue è abilitata in modo da garantire la sicurezza di rete immediata. Le procedure di configurazione descritte di seguito presuppongono che sul controller non sia configurato alcun rilevamento rogue per chiarire importanti informazioni relative al rilevamento rogue.

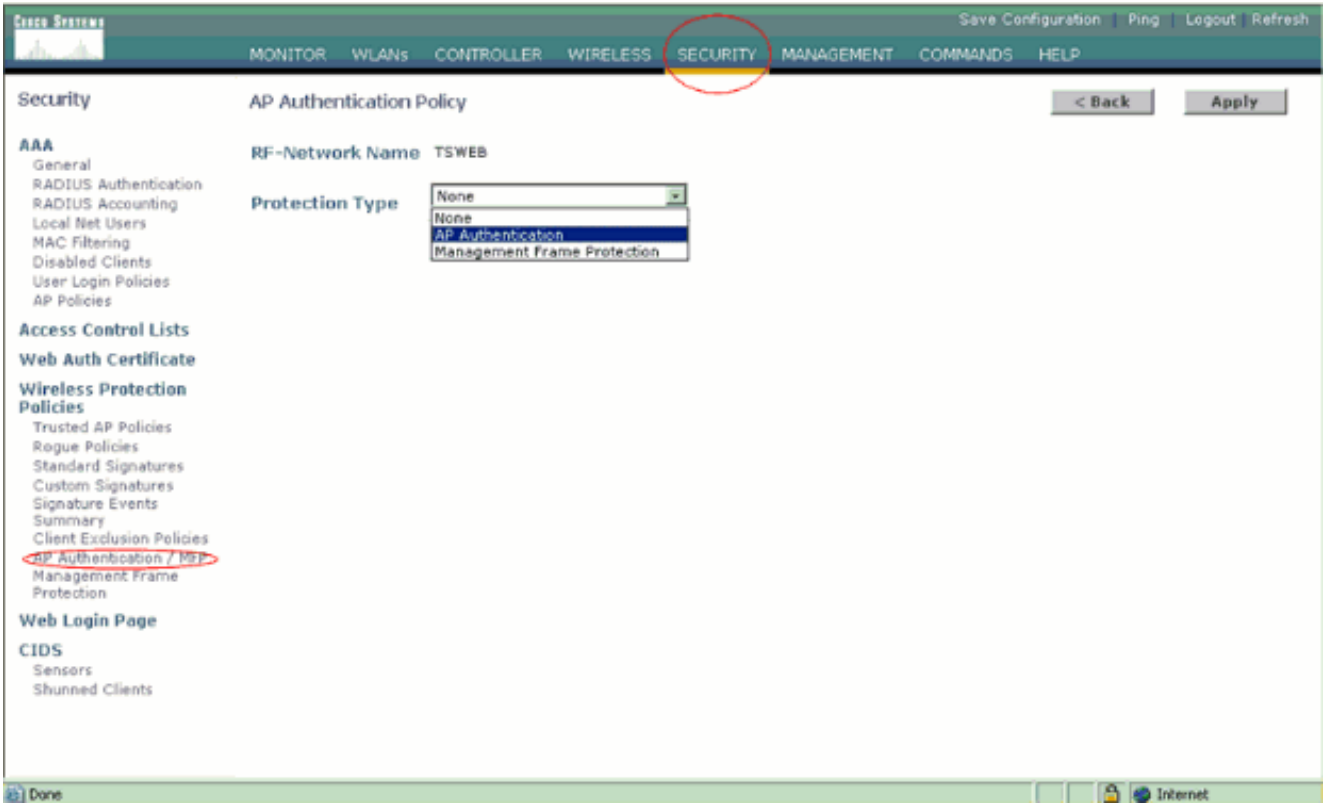
Per impostare il rilevamento rogue, procedere come segue:

1. Verificare che il protocollo Rogue Location Discovery sia attivato. Per attivarlo, scegliere **Sicurezza > Criteri non autorizzati** e fare clic su **Abilitato** nel **protocollo Rogue Location**

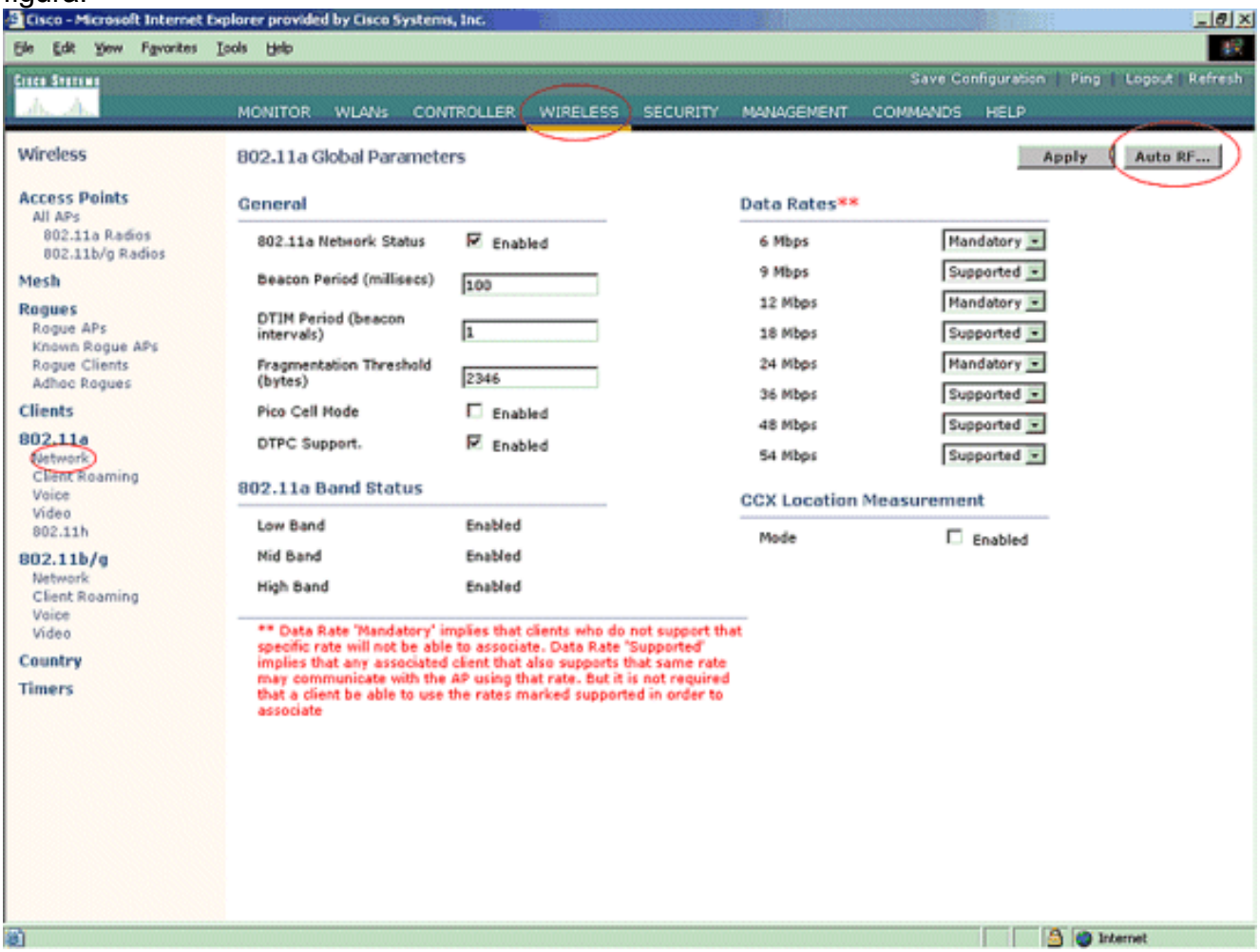
Discovery, come mostrato nella figura.**Nota:** se un access point non autorizzato non viene udito per un determinato periodo di tempo, viene rimosso dal controller. Questo è il **timeout di scadenza** per un access point anomalo, configurato sotto l'opzione RLDP.



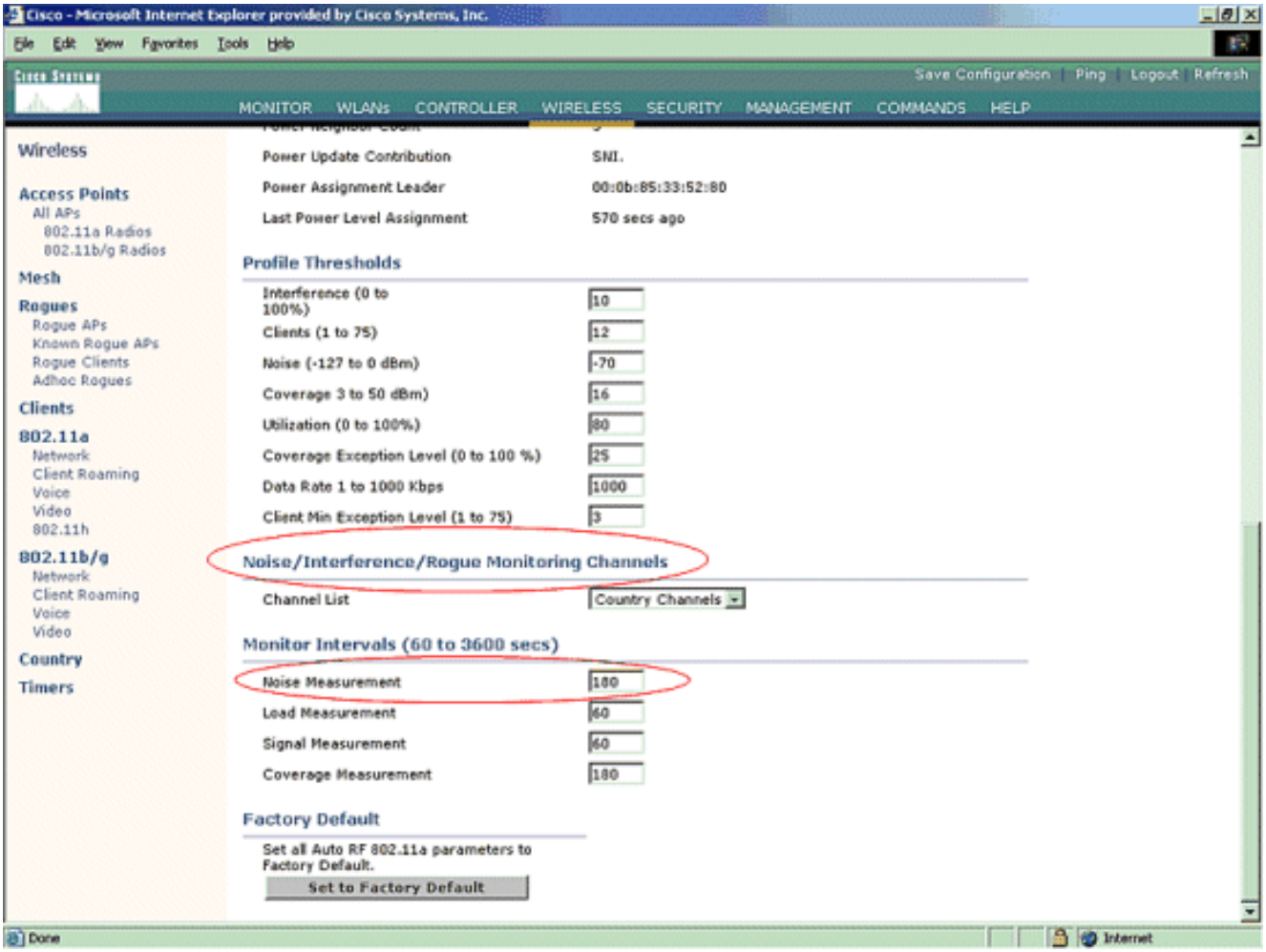
2. Questo passaggio è facoltativo. Quando questa funzione è abilitata, i punti di accesso che inviano pacchetti adiacenti RRM con nomi di **gruppi RF** diversi vengono segnalati come anomali. Questo sarà utile nello studio dell'ambiente RF. Per abilitarla, scegliere **Security-> AP Authentication** (Sicurezza - Autenticazione AP). Quindi, scegliere **Autenticazione AP** come Tipo di protezione, come mostrato nella figura.



3. Verificare i canali da scansionare attenendosi alla seguente procedura:Selezionare **Wireless > Rete 802.11a**, quindi **Auto RF** sul lato destro, come mostrato nella figura.



Nella pagina **Auto RF**, scorrere verso il basso e selezionare **Noise/Interference/Rogue Monitoring Channels** (Rumore/interferenze/canali di monitoraggio non autorizzati).



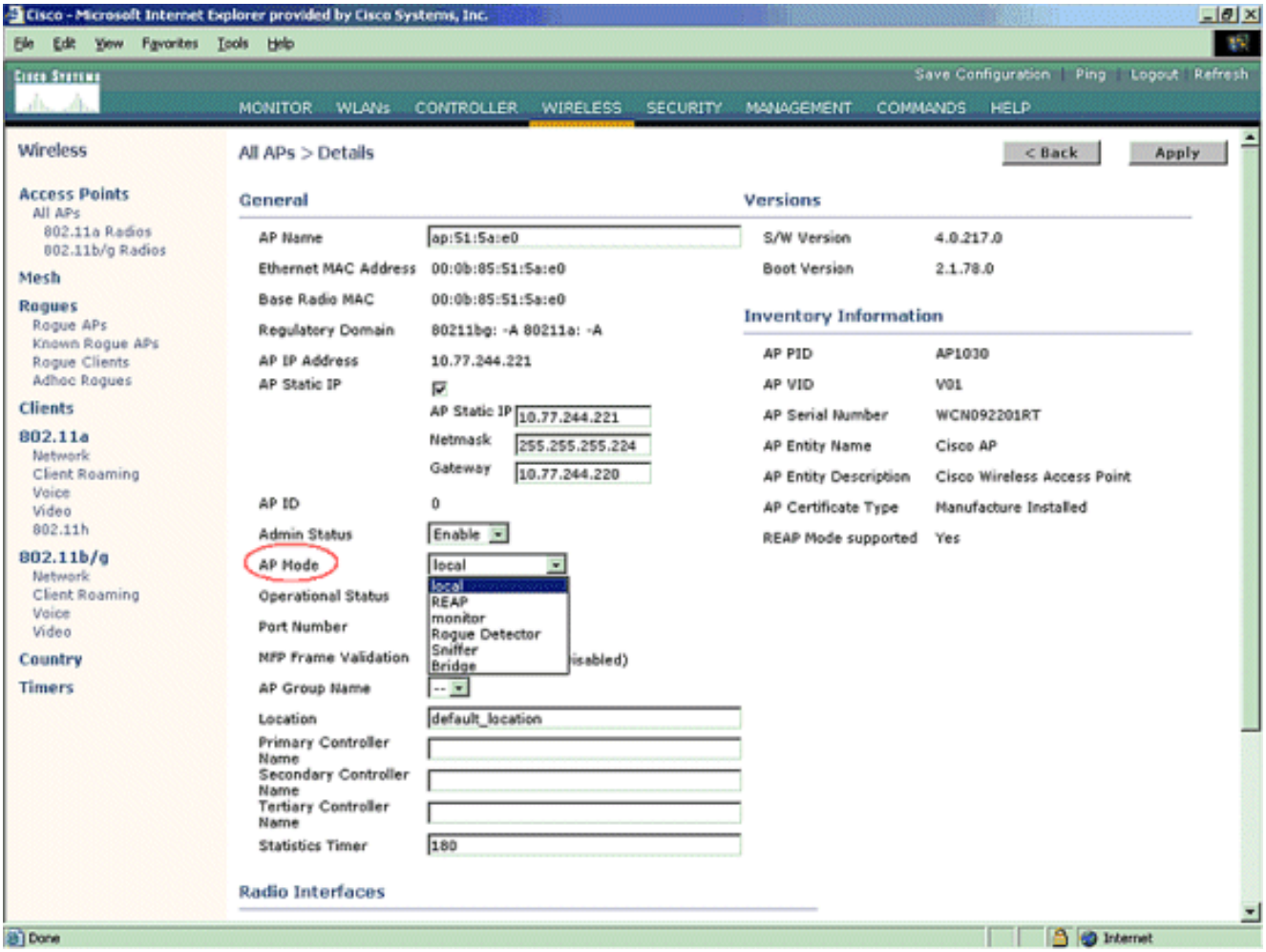
L'elenco dei canali mostra in dettaglio i canali da scansionare per il monitoraggio non autorizzato, oltre ad altre funzioni del controller e dell'access point. Per ulteriori informazioni sui Lightweight Access Point, fare riferimento alle domande frequenti sui Lightweight Access Point e alle Wireless LAN Controller (WLC) Troubleshoot FAQ (Risoluzione dei problemi sui Lightweight Access Point) per ulteriori informazioni sui controller 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. Impostare il periodo di tempo per la scansione dei canali selezionati:La durata della scansione del gruppo di canali definito viene configurata in **Intervalli monitor > Misura rumore** e l'intervallo consentito è compreso tra 60 e 3600 secondi. Se lasciati sul valore predefinito di 180 secondi, i punti di accesso eseguono la scansione di ciascun canale nel gruppo di canali una volta, per 50 ms, ogni 180 secondi. Durante questo periodo, la radio AP passa dal canale di servizio al canale specificato, ascolta e registra i valori per un periodo di 50 ms e quindi ritorna al canale originale. Il tempo di hop più il tempo di permanenza di 50 ms porta il punto di accesso fuori canale per circa 60 ms ogni volta. Ciò significa che ogni access point

impiega circa 840 ms su un totale di 180 secondi per l'ascolto di utenti non autorizzati.Il tempo di "ascolto" o di "permanenza" non può essere modificato e non viene modificato con una regolazione del valore di misurazione del rumore. Se il timer di misurazione del rumore è abbassato, è probabile che il processo di rilevamento rogue trovi più roghi e li trovi più rapidamente. Tuttavia, questo miglioramento avviene a scapito dell'integrità dei dati e del servizio client. Un valore più alto, invece, consente una maggiore integrità dei dati ma riduce la possibilità di trovare rapidamente i truffatori.

5. Configurare la modalità di funzionamento AP:Una modalità di funzionamento Lightweight AP definisce il ruolo dell'AP. Le modalità relative alle informazioni presentate nel presente documento sono le seguenti:**Locale**: si tratta del funzionamento normale di un punto di accesso. Questa modalità consente ai client di dati di essere serviti mentre i canali configurati vengono analizzati per verificare la presenza di disturbi e anomalie. In questa modalità operativa, l'access point rimane disattivato dal canale per 50 ms e rimane in ascolto dei router non autorizzati. e scorre attraverso ogni canale, uno alla volta, per il periodo specificato nella configurazione Auto RF.**Monitor**: si tratta della modalità di sola ricezione radio che consente all'access point di eseguire la scansione di tutti i canali configurati ogni 12 secondi. Con un access point configurato in questo modo, vengono inviati solo i pacchetti di deautenticazione. Un access point in modalità monitor può rilevare i router, ma non può connettersi a un router sospetto come client per inviare i pacchetti RLDP.**Nota:** DCA fa riferimento a canali non sovrapposti configurabili con le modalità predefinite.**Rilevatore server non autorizzati**: in questa modalità, la radio dell'access point è spenta e l'access point resta in ascolto solo del traffico cablato. Il controller trasmette i punti di accesso configurati come rilevatori di rogue, nonché gli elenchi dei client non autorizzati e degli indirizzi MAC dei punti di accesso. Il rogue detector resta in ascolto solo dei pacchetti ARP e, se lo si desidera, può essere connesso a tutti i domini di broadcast attraverso un collegamento trunk.Èpossibile configurare una singola modalità AP in modo semplice, una volta che il Lightweight AP è collegato al controller. Per modificare la modalità del punto di accesso, collegarsi all'interfaccia Web del controller e selezionare **Wireless**. Per visualizzare una schermata simile a questa, fare clic su **Details** (Dettagli) accanto all'access point desiderato:



Utilizzare il menu a discesa Modalità punto di accesso per selezionare la modalità di funzionamento desiderata.

Comandi per la risoluzione dei problemi

Èpossibile usare questi comandi anche per risolvere i problemi di configurazione sull'access point:

- **show rogue ap summary**: questo comando visualizza l'elenco dei punti di accesso non autorizzati rilevati dai punti di accesso leggeri.
- **show rogue ap detail** ***<Indirizzo MAC del rogue ap>*** - Utilizzare questo comando per visualizzare i dettagli di un singolo rogue AP. Questo comando aiuta a determinare se il punto di accesso non autorizzato è collegato alla rete cablata.

Conclusioni

Il rilevamento e il contenimento dei problemi all'interno della soluzione di controller centralizzato Cisco è il metodo più efficace e meno intrusivo del settore. La flessibilità fornita all'amministratore di rete consente di adattare il sistema a qualsiasi esigenza di rete.

Informazioni correlate

- Panoramica dei gruppi RF
- Documentazione e supporto tecnico – Cisco Systems