Esempio di configurazione di WEP su un punto di accesso autonomo

Sommario

Introduzione

Questo documento descrive come utilizzare e configurare Wired Equivalent Privacy (WEP) su un Cisco Autonomous Access Point (AP).

Prerequisiti

Requisiti

per le successive spiegazioni, si presume che sia possibile stabilire una connessione amministrativa ai dispositivi WLAN e che i dispositivi funzionino normalmente in un ambiente non crittografato. Per configurare un protocollo WEP standard a 40 bit, è necessario disporre di due o più unità radio che comunichino tra loro.

Componenti usati

Per questo documento, è stato usato un access point serie 1140 con Cisco IOS® versione 15.2JB.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

WEP è l'algoritmo di crittografia integrato nello standard 802.11 (Wi-Fi). WEP utilizza la cifratura di flusso RC4 per la riservatezza, e il checksum Cyclic Redundancy Check-32 (CRC-32) per l'integrità .

Il protocollo WEP a 64 bit standard utilizza una chiave a 40 bit (nota anche come WEP-40), concatenata con un vettore di inizializzazione a 24 bit (IV) per formare la chiave RC4. Una chiave WEP a 64 bit viene in genere immessa come stringa di 10 caratteri esadecimali (base 16) (da zero a nove e da A-F). Ogni carattere rappresenta quattro bit e dieci cifre di quattro bit equivalgono ciascuno a 40 bit; se si aggiunge la chiave IV a 24 bit, verrà generata la chiave WEP completa a 64 bit.

Una chiave WEP a 128 bit viene in genere immessa come stringa di 26 caratteri esadecimali. Ventisei cifre di quattro bit ciascuna equivalgono a 104 bit; se si aggiunge la chiave IV a 24 bit, verrà generata la chiave WEP completa a 128 bit. La maggior parte dei dispositivi consente all'utente di immettere la chiave con 13 caratteri ASCII.

Metodi di autenticazione

Con WEP è possibile utilizzare due metodi di autenticazione: Autenticazione del sistema aperto e autenticazione con chiave condivisa.

Con l'autenticazione di sistema aperta, il client WLAN non deve fornire credenziali all'access point per l'autenticazione. Qualsiasi client può eseguire l'autenticazione con l'access point e quindi tentare l'associazione. In effetti, non viene eseguita alcuna autenticazione. Successivamente, è possibile utilizzare le chiavi WEP per crittografare i frame di dati. A questo punto, il client deve avere le chiavi corrette.

Con l'autenticazione a chiave condivisa, la chiave WEP viene utilizzata per l'autenticazione in un handshake in quattro passaggi con richiesta di verifica/risposta:

1. Il client invia una richiesta di autenticazione all'access point.
2. L'AP risponde con una sfida testuale.
3. Il client crittografa il testo della richiesta di verifica con la chiave WEP configurata e risponde con un'altra richiesta di autenticazione.
4. L'access point decrittografa la risposta. Se la risposta corrisponde al testo della richiesta, l'access point invia una risposta positiva.

Dopo l'autenticazione e l'associazione, viene utilizzata anche la chiave WEP precondivisa per crittografare i frame di dati con RC4.

A prima vista, potrebbe sembrare che l'autenticazione con chiave condivisa sia più sicura di quella con sistema aperto, poiché quest'ultima non offre un'autenticazione reale. Tuttavia, è vero il contrario. È possibile derivare il flusso di chiave utilizzato per l'handshake se si acquisiscono i frame di verifica in Autenticazione con chiave condivisa. È pertanto consigliabile utilizzare l'autenticazione di sistema aperto per l'autenticazione WEP anziché l'autenticazione con chiave condivisa.

Il protocollo TKIP (Temporal Key Integrity Protocol) è stato creato per risolvere questi problemi

WEP. Analogamente a WEP, TKIP utilizza la crittografia RC4. Tuttavia, TKIP migliora il WEP con l'aggiunta di misure come l'hashing della chiave per pacchetto, il controllo dell'integrità dei messaggi (MIC) e la rotazione della chiave di trasmissione per risolvere le vulnerabilità WEP conosciute. TKIP utilizza la cifratura di flusso RC4 con chiavi a 128 bit per la crittografia e chiavi a 64 bit per l'autenticazione.

Configurazione

Questa sezione fornisce le configurazioni GUI e CLI per WEP.

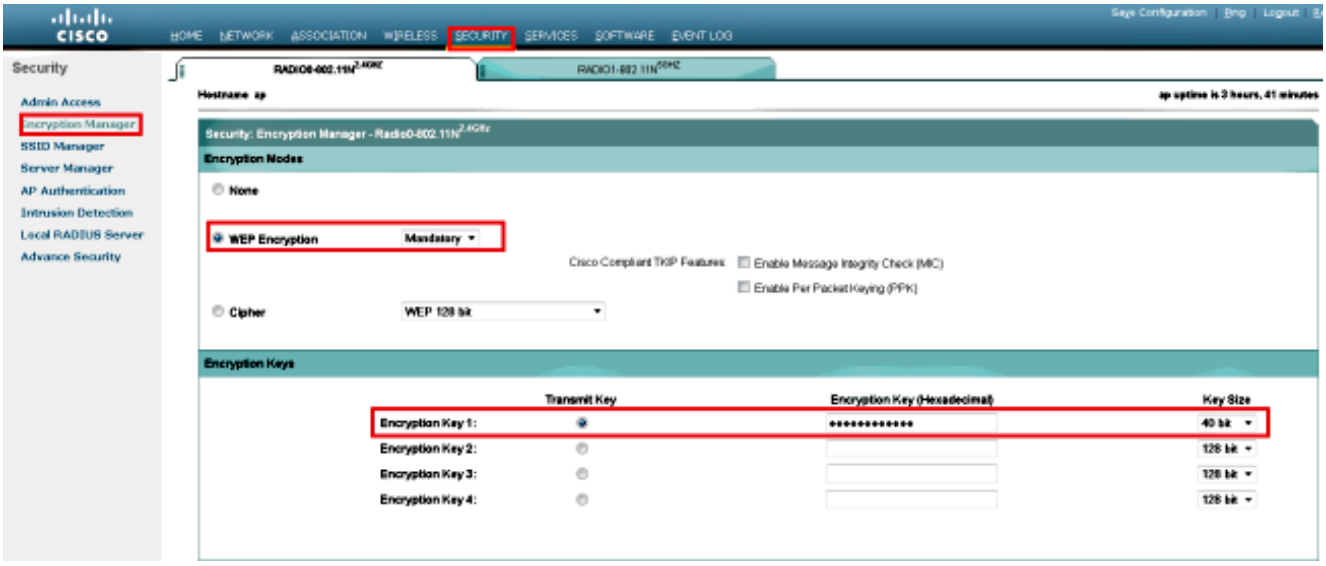
Configurazione GUI

Completare questa procedura per configurare WEP con la GUI.

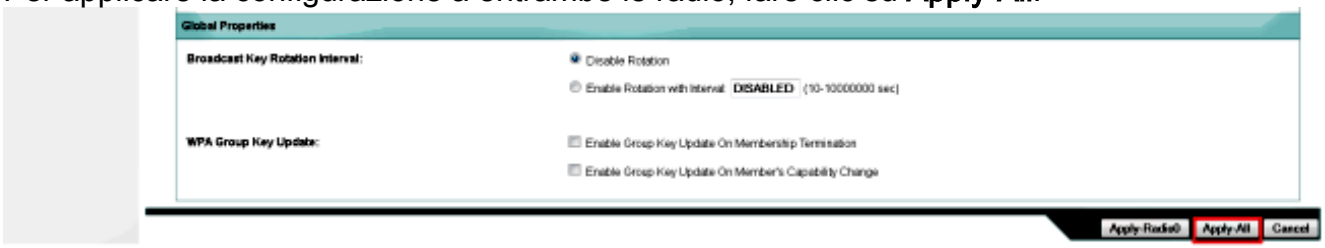
1. Connettersi all'access point tramite la GUI.
2. Dal menu Security (Protezione) sul lato sinistro della finestra, scegliere **Encryption Manager** per l'interfaccia radio su cui configurare le chiavi WEP statiche.
3. In Modalità di crittografia fare clic su **Crittografia WEP** e selezionare **Obbligatorio** dal menu a discesa del client.

   Le modalità di crittografia usate dalla stazione sono:
   Predefinito (senza crittografia) - Richiede ai client di comunicare con l'access point senza crittografia dei dati. Questa impostazione è sconsigliata.**Facoltativo**: consente ai client di comunicare con l'access point con o senza crittografia dei dati. In genere, questa opzione viene utilizzata quando sono presenti dispositivi client che non possono effettuare una connessione WEP, ad esempio client non Cisco in un ambiente WEP a 128 bit.**Obbligatorio (crittografia completa)**: richiede ai client di utilizzare la crittografia dei dati quando comunicano con l'access point. I client che non utilizzano la crittografia dei dati non possono comunicare. Questa opzione è consigliata se si desidera ottimizzare la sicurezza della WLAN.
4. In Chiavi di crittografia selezionare il pulsante di opzione **Trasmetti chiave** e immettere la chiave esadecimale a 10 cifre. Verificare che la proprietà Key Size sia impostata su **40 bit**.

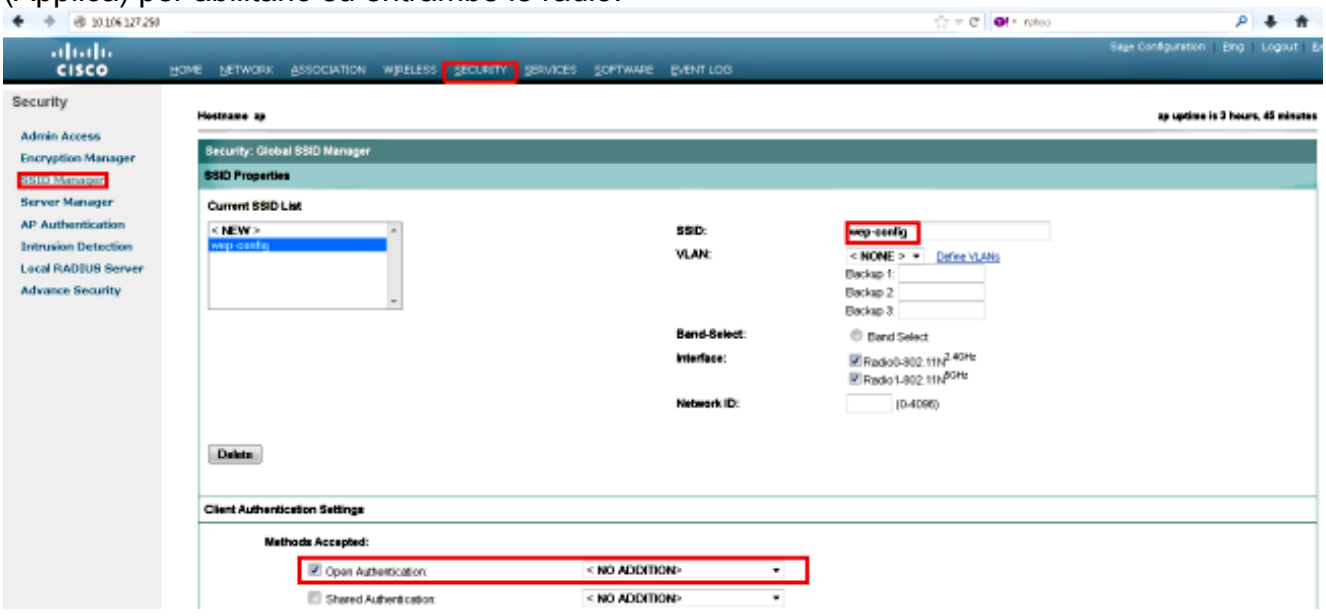
   Immettere 10 cifre esadecimali per le chiavi WEP a 40 bit o 26 cifre esadecimali per le chiavi WEP a 128 bit. I tasti possono essere costituiti da qualsiasi combinazione delle seguenti cifre:
   Da 0 a 9da a a fDa A a
   F



5. Per applicare la configurazione a entrambe le radio, fare clic su **Apply-All**.



6. Creare un SSID (Service Set Identifier) con **Open Authentication** e fare clic su **Apply** (Applica) per abilitarlo su entrambe le radio.



7. Accedere alla rete e attivare le radio da **2,4** e **5 GHz** per farle funzionare.

Configurazione CLI

Usare questa sezione per configurare WEP con la CLI.

```
ap#show run
Building configuration...

Current configuration : 1794 bytes
!
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
!
no aaa new-model
ip cef
!
!
!
dot11 syslog
!
 dot11 ssid wep-config
 authentication open
 guest-mode
!
!
crypto pki token default removal timeout 0
!
!
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
```

```
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1

 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
login local
transport input all
!
end
```

Verifica

Per verificare che la configurazione funzioni correttamente, immettere questo comando:

```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address    IP address      Device        Name           Parent         State
1cb0.94a2.f64c 10.106.127.251  unknown       -              self           Assoc
```

Risoluzione dei problemi

Consultare questa sezione per risolvere i problemi di configurazione.

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

I seguenti comandi **debug** sono utili per risolvere i problemi relativi alla configurazione:

- **debug dot11 events**: abilita il debug per tutti gli eventi dot1x.
- **debug dot11 packets**: abilita il debug per tutti i pacchetti dot1x.

Di seguito è riportato un esempio del log che viene visualizzato quando il client viene associato correttamente alla WLAN:

```
*Mar  1 02:24:46.246: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
1cb0.94a2.f64c Associated KEY_MGMT[NONE]
```

Quando il client immette la chiave errata, viene visualizzato questo errore:

```
*Mar  1 02:26:00.741: %DOT11-4-ENCRYPT_MISMATCH: Possible encryption key
mismatch between interface Dot11Radio0 and station 1cb0.94a2.f64c
*Mar  1 02:26:21.312: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating
Station 1cb0.94a2.f64c Reason: Sending station has left the BSS
*Mar  1 02:26:21.312: *** Deleting client 1cb0.94a2.f64c
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).