Panoramica della configurazione WPA

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per Wi-Fi Protected Access (WPA), lo standard di sicurezza provvisorio utilizzato dai membri di Wi-Fi Alliance.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenza approfondita delle reti wireless e dei problemi di sicurezza wireless
- Conoscenza dei metodi di protezione EAP (Extensible Authentication Protocol)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Access point (AP) basati su software Cisco IOS®
- Software Cisco IOS release 12.2(15)JA o successive**Nota:** preferibilmente, usare la versione più recente del software Cisco IOS, anche se WPA è supportato nel software Cisco IOS

versione 12.2(11)JA e successive. Per ottenere la versione più recente del software Cisco IOS, consultare il documento sui download (solo utenti registrati).
- Una scheda di interfaccia di rete (NIC) compatibile con WPA e il relativo software client compatibile con WPA

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.

Nozioni di base

Le funzioni di sicurezza di una rete wireless, ad esempio WEP, sono deboli. Il gruppo industriale Wi-Fi Alliance (o WECA) ha ideato uno standard di sicurezza intermedio di nuova generazione per le reti wireless. Lo standard fornisce una difesa contro le debolezze fino a quando l'organizzazione IEEE non lo ratifica.

Questo nuovo schema si basa sull'autenticazione corrente EAP/802.1x e sulla gestione dinamica delle chiavi, e aggiunge una crittografia più avanzata. Dopo che il dispositivo client e il server di autenticazione hanno creato un'associazione EAP/802.1x, la gestione delle chiavi WPA viene negoziata tra l'AP e il dispositivo client compatibile WPA.

I prodotti Cisco AP forniscono anche una configurazione ibrida in cui i client EAP basati su WEP legacy (con gestione delle chiavi legacy o assente) funzionano insieme ai client WPA. Questa configurazione viene definita modalità di migrazione. La modalità di migrazione consente un approccio a fasi per la migrazione a WPA. Questo documento non descrive la modalità di migrazione. Questo documento fornisce una struttura per una rete WPA pura.

Oltre ai problemi di sicurezza a livello aziendale o aziendale, WPA fornisce anche una versione a chiave già condivisa (WPA-PSK) destinata all'uso in reti wireless domestiche, per piccoli uffici o per piccoli uffici. Cisco Aironet Client Utility (ACU) non supporta WPA-PSK. L'utilità Wireless Zero Configuration di Microsoft Windows supporta WPA-PSK per la maggior parte delle schede wireless, così come queste utilità:

- Client AEGIS da Meetinghouse Communications**Nota:** fare riferimento all'annuncio di fine ciclo di vita e di fine ciclo di vita per la linea di prodotti AEGIS Meetinghouse.
- Client Odyssey di Funk Software**Nota:** fare riferimento al centro di assistenza clienti Juniper Networks .
- Utilità client OEM di alcuni produttori

Èpossibile configurare WPA-PSK quando:

- La modalità di crittografia viene definita come protocollo TKIP (Cipher Temporal Key Integrity Protocol) nella scheda Gestione crittografia.
- Il tipo di autenticazione, l'uso della gestione delle chiavi autenticate e la chiave già condivisa vengono definiti nella scheda Service Set Identifier (SSID) Manager della GUI.
- Nella scheda Server Manager non è richiesta alcuna configurazione.

Per abilitare WPA-PSK tramite l'interfaccia della riga di comando (CLI), immettere questi comandi. Avviare dalla modalità di configurazione:

```
AP(config)#interface dot11Radio 0
AP(config-if)#encryption mode ciphers tkip
```

```
AP(config-if)#ssid ssid_name
AP(config-if-ssid)#authentication open
AP(config-if-ssid)#authentication key-management wpa
AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

Nota: questa sezione fornisce solo la configurazione rilevante per WPA-PSK. La configurazione illustrata in questa sezione consente solo di comprendere come abilitare WPA-PSK e non è l'argomento principale di questo documento. Questo documento spiega come configurare WPA.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

WPA si basa sui metodi EAP/802.1x correnti. in questo documento si presume che l'utente disponga di una configurazione Light EAP (LEAP), EAP o Protected EAP (PEAP) che funziona prima di aggiungere la configurazione per utilizzare WPA.

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Autenticazione di rete EAP o aperta con EAP

In qualsiasi metodo di autenticazione basato su EAP/802.1x è possibile stabilire quali siano le differenze tra l'autenticazione EAP-rete e l'autenticazione aperta con EAP. Questi elementi fanno riferimento ai valori del campo Authentication Algorithm nelle intestazioni dei pacchetti di gestione e associazione. La maggior parte dei produttori di client wireless imposta questo campo sul valore 0 (autenticazione aperta), quindi segnala il proprio desiderio di eseguire l'autenticazione EAP in un secondo momento nel processo di associazione. Cisco imposta il valore in modo diverso dall'inizio dell'associazione al flag Network EAP.

Utilizzare il metodo di autenticazione indicato nell'elenco se la rete dispone di client:

- Client Cisco: utilizzare Network-EAP.
- Client di terze parti (che includono prodotti compatibili con Cisco Compatible Extensions [CCX]): utilizzare l'autenticazione aperta con EAP.
- Combinazione di client Cisco e di terze parti: scegliere l'autenticazione Network-EAP e l'autenticazione aperta con EAP.

Configurazione CLI

Nel documento vengono usate queste configurazioni:

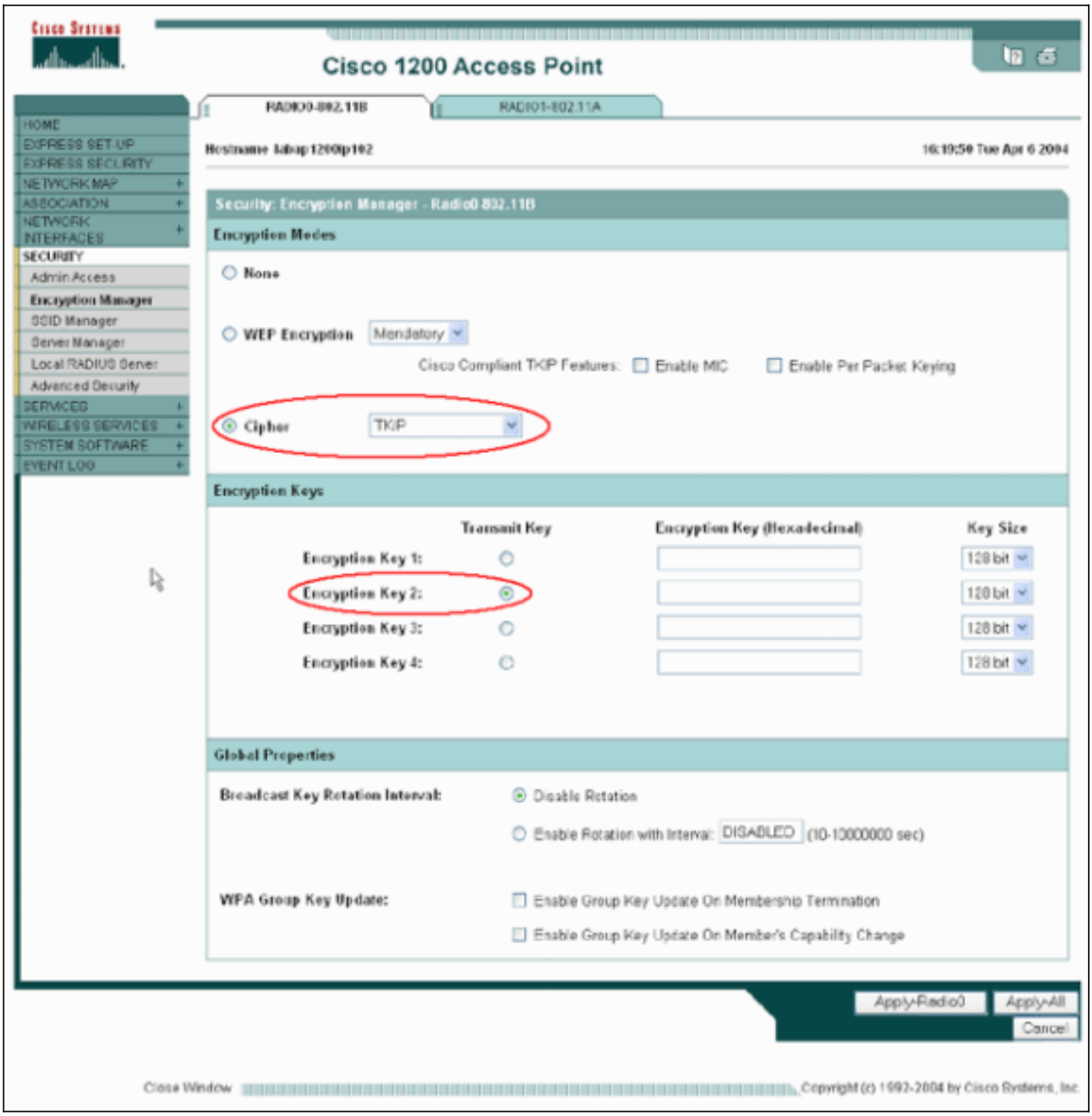
- Una configurazione LEAP esistente e funzionante
- Software Cisco IOS release 12.2(15)JA per i Cisco IOS Software-based AP

AP

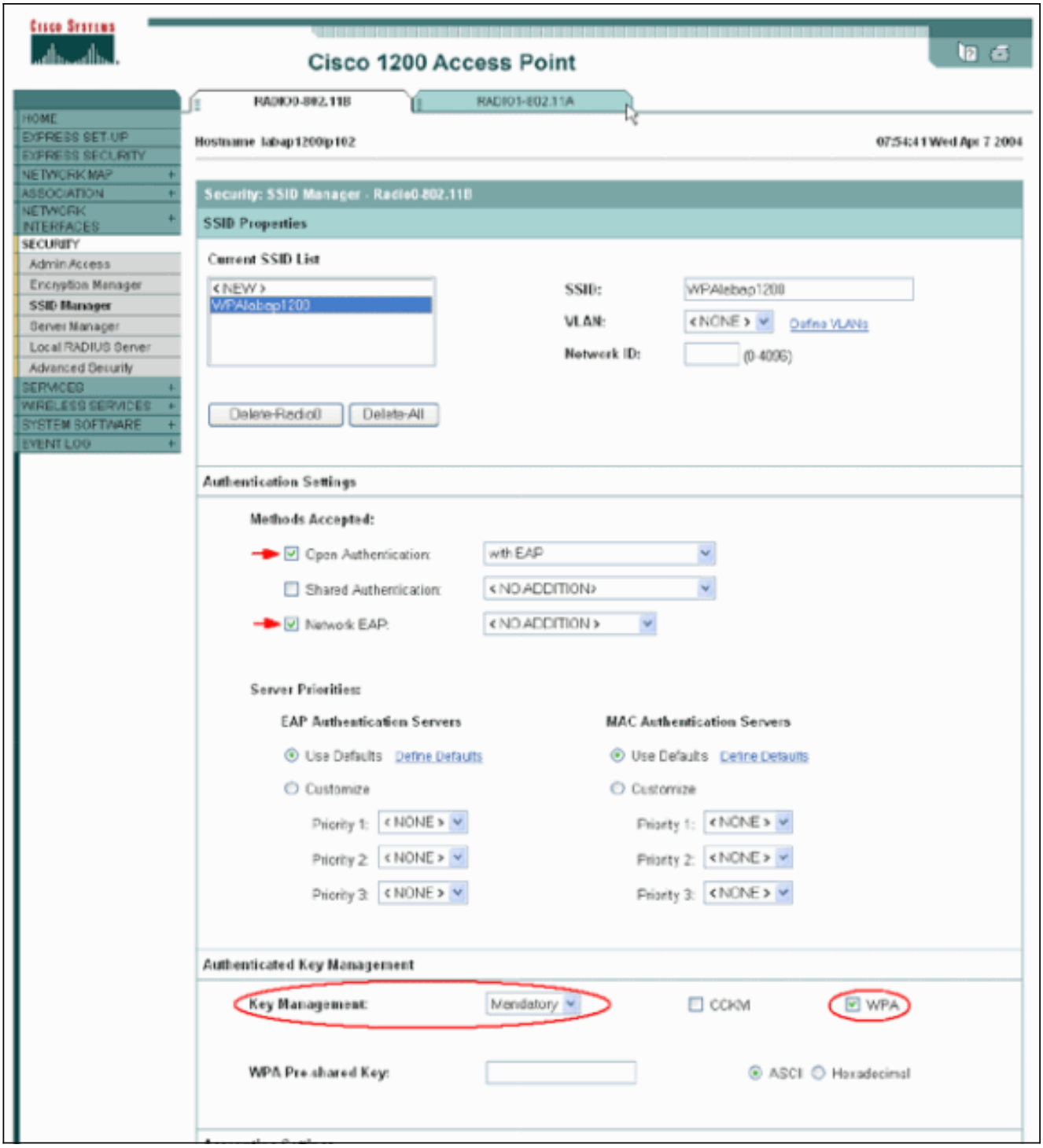
```
ap1#show running-config
 Building configuration...
 .
 .
 .
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip
!--- This defines the cipher method that WPA uses. The
TKIP !--- method is the most secure, with use of the Wi-
Fi-defined version of TKIP. ! ssid WPAlabap1200
authentication open eap eap_methods
!--- This defines the method for the underlying EAP when
third-party clients !--- are in use.     authentication
network-eap eap_methods
!--- This defines the method for the underlying EAP when
Cisco clients are in use.     authentication key-
management wpa
!--- This engages WPA key management. ! speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 rts threshold 2312
channel 2437 station-role root bridge-group 1 bridge-
group 1 subscriber-loop-control bridge-group 1 block-
unknown-source no bridge-group 1 source-learning no
bridge-group 1 unicast-flooding bridge-group 1 spanning-
disabled . . . interface FastEthernet0 no ip address no
ip route-cache duplex auto speed auto bridge-group 1 no
bridge-group 1 source-learning bridge-group 1 spanning-
disabled ! interface BVI1 ip address 192.168.2.108
255.255.255.0 !--- This is the address of this unit. no
ip route-cache ! ip default-gateway 192.168.2.1 ip http
server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
server community cable RO snmp-server enable traps tty
radius-server host 192.168.2.100 auth-port 1645 acct-
port 1646 key shared_secret !--- This defines where the
RADIUS server is and the key between the AP and server.
radius-server retransmit 3 radius-server attribute 32
include-in-access-req format %h radius-server
authorization permit missing Service-Type radius-server
vsa send accounting bridge 1 route ip ! ! line con 0
line vty 5 15 ! end ! end
```

Configurazione GUI

Completare questa procedura per configurare l'access point per WPA:

1. Per configurare Encryption Manager, completare la procedura seguente:Abilita crittografia per TKIP.Cancellare il valore nella chiave di crittografia 1.Impostare Encryption Key 2 come chiave di trasmissione.Selezionate **Apply-Radio#**
   .
   

2. Completare questa procedura per configurare SSID Manager:Selezionare il SSID desiderato dall'elenco SSID corrente.Scegliere un metodo di autenticazione appropriato.Basare questa decisione sul tipo di schede client utilizzate. Per ulteriori informazioni, vedere la sezione Autenticazione di rete EAP o aperta con EAP di questo documento. Se l'EAP ha funzionato prima dell'aggiunta di WPA, probabilmente non è necessaria una modifica.Per abilitare la gestione delle chiavi, completare i seguenti passaggi:Scegliere **Obbligatorio** dal menu a discesa Gestione chiavi.Selezionare la casella di controllo WPA.Selezionate **Apply-Radio#**
   .

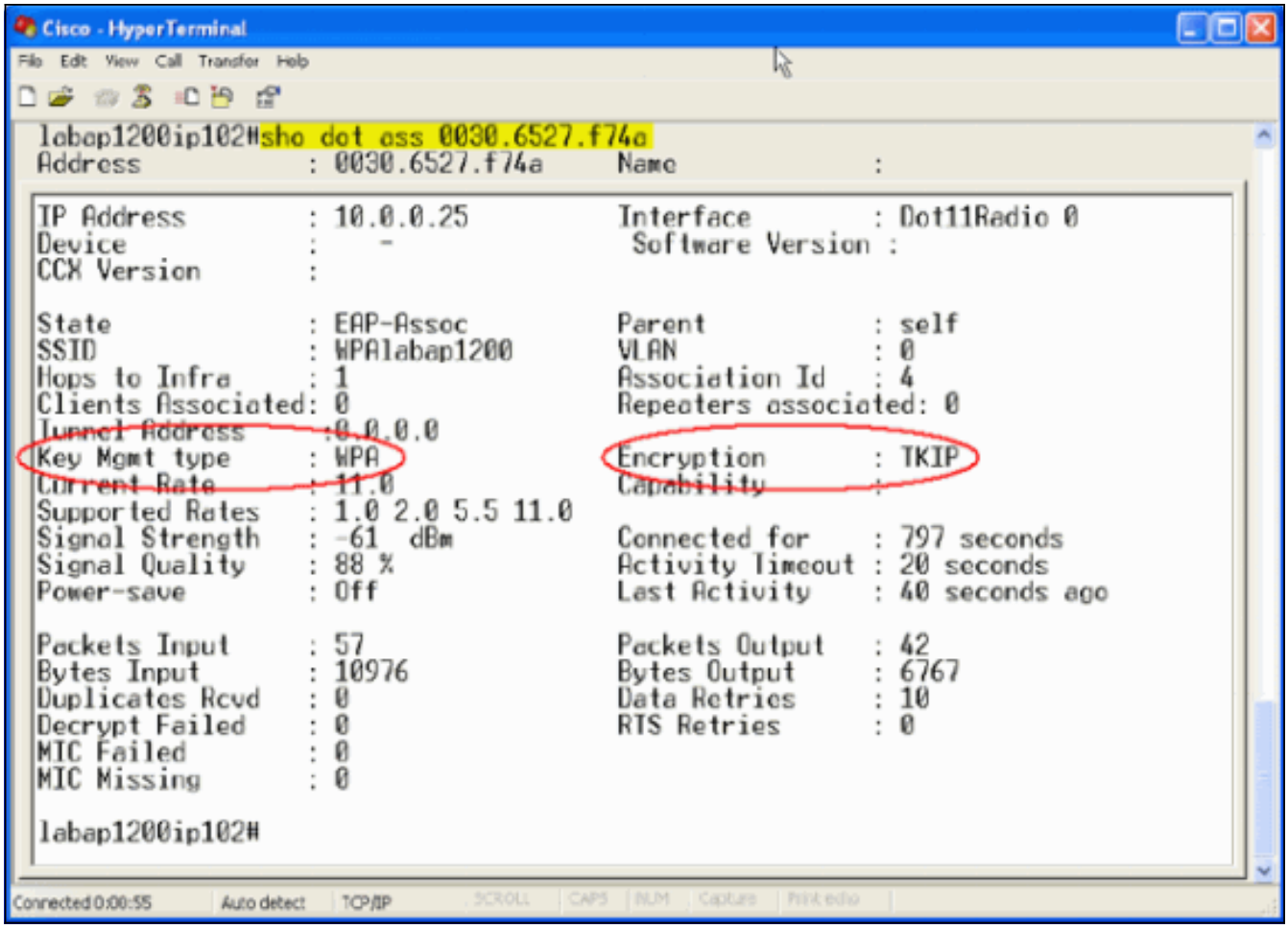


Verifica

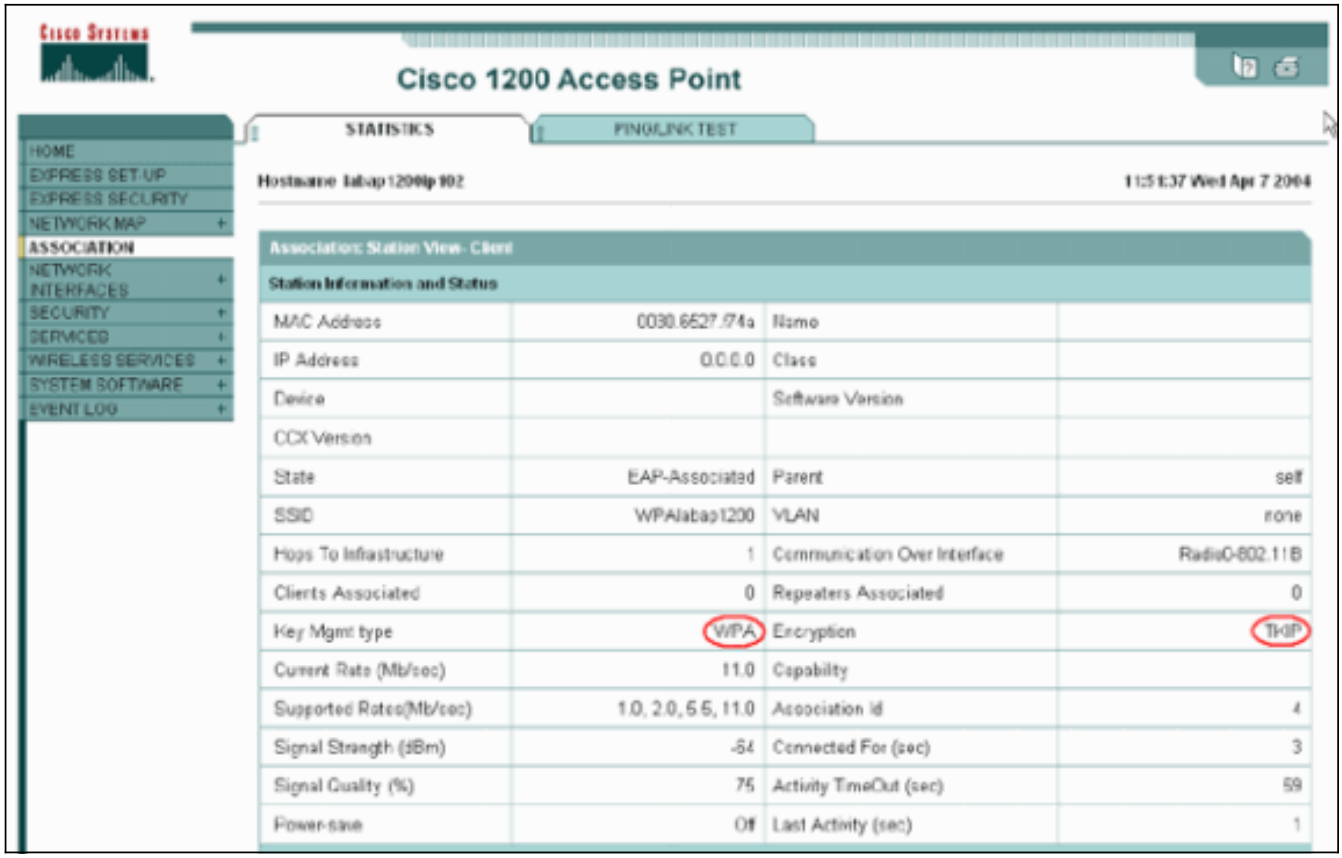
Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show dot11 association *mac_address*: questo comando visualizza informazioni su un client associato identificato in modo specifico.** Verificare che il client negozi la gestione delle chiavi come **WPA** e la crittografia come **TKIP**.



- La voce della tabella Association per un determinato client deve inoltre indicare Gestione chiavi come **WPA** e Crittografia come **TKIP**. Nella tabella Associazione fare clic su un indirizzo MAC specifico per un client per visualizzare i dettagli dell'associazione per tale client.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Procedura di risoluzione dei problemi

Queste informazioni sono rilevanti per la configurazione. Per risolvere i problemi relativi alla configurazione, completare la procedura seguente:

1. Se la configurazione LEAP, EAP o PEAP non è stata completamente testata prima dell'implementazione di WPA, completare i seguenti passaggi:Disabilitare temporaneamente la modalità di crittografia WPA.Riattivare l'EAP appropriato.Verificare che l'autenticazione funzioni.
2. Verificare che la configurazione del client corrisponda a quella dell'access point.Ad esempio, quando l'access point è configurato per WPA e TKIP, verificare che le impostazioni corrispondano a quelle configurate nel client.

Comandi per la risoluzione dei problemi

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

La gestione delle chiavi WPA prevede un handshake a quattro vie dopo il completamento dell'autenticazione EAP. Questi quattro messaggi si trovano nei debug. Se EAP non autentica correttamente il client o se i messaggi non vengono visualizzati, attenersi alla seguente procedura:

1. Disabilitare temporaneamente WPA.
2. Riattivare l'EAP appropriato.
3. Verificare che l'autenticazione funzioni.

Di seguito vengono descritti i debug:

- **debug dot11 aaa manager keys**: questo debug visualizza l'handshake che si verifica tra l'access point e il client WPA durante la negoziazione della chiave temporanea pairwise (PTK) e della chiave temporanea di gruppo (GTK). Questo debug è stato introdotto nel software Cisco IOS versione 12.2(15)JA.Se non vengono visualizzati output di debug, verificare quanto segue:Se si utilizza una sessione Telnet, il **termine mon del** monitor del terminale è abilitato.I debug sono attivati.Il client è configurato correttamente per WPA.Se durante il debug viene mostrato che gli handshake PTK e/o GTK sono stati compilati ma non verificati, controllare il software supplicant WPA per la configurazione corretta e la versione aggiornata.
- **debug dot11 aaa authentication state-machine**: questo debug mostra i vari stati delle negoziazioni attraverso cui deve passare un client quando viene associato e autenticato. I nomi degli stati indicano questi stati. Questo debug è stato introdotto nel software Cisco IOS versione 12.2(15)JA. Il comando debug obsoleta il comando **debug dot11 aaa dot1x state-machine** nel software Cisco IOS versione 12.2(15)JA e successive.
- **debug dot11 aaa dot1x state-machine**: questo debug mostra i vari stati delle negoziazioni attraverso cui deve passare un client quando viene associato e autenticato. I nomi degli stati indicano questi stati. Nelle versioni software Cisco IOS precedenti alla versione 12.2(15)JA,

questo debug mostra anche la negoziazione della gestione delle chiavi WPA.

- **debug dot11 aaa authenticator process**: questo debug è particolarmente utile per diagnosticare i problemi relativi alle comunicazioni negoziate. Le informazioni dettagliate mostrano ciò che ogni partecipante alla negoziazione invia e mostrano la risposta dell'altro partecipante. È possibile usare questo debug anche con il comando **debug radius authentication**. Questo debug è stato introdotto nel software Cisco IOS versione 12.2(15)JA. Il comando debug obsoleta il comando **debug dot11 aaa dot1x process** nel software Cisco IOS versione 12.2(15)JA e successive.
- **debug dot11 aaa dot1x process**: questo debug è utile per diagnosticare i problemi relativi alle comunicazioni negoziate. Le informazioni dettagliate mostrano ciò che ogni partecipante alla negoziazione invia e mostrano la risposta dell'altro partecipante. È possibile usare questo debug anche con il comando **debug radius authentication**. Nelle versioni software Cisco IOS precedenti alla versione 12.2(15)JA, questo debug mostra la negoziazione della gestione delle chiavi WPA.

Informazioni correlate

- Configurazione di suite di cifratura e WEP
- Configurazione dei tipi di autenticazione
- WPA2 - Accesso protetto Wi-Fi 2
- Configurazione Wi-Fi Protected Access 2 (WPA 2)
- Documentazione e supporto tecnico – Cisco Systems