Présentation de la configuration WPA

Contenu

Introduction

Ce document fournit un exemple de configuration pour le Wi-Fi Protected Access (WPA), la norme intérimaire de sécurité que les membres de Wi-Fi Alliance utilisent.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Avoir une connaissance complète des réseaux sans fil et des problèmes liés à la sécurité sans fil
- La connaissance des méthodes de sécurité du protocole EAP (Extensible Authentication Protocol)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Points d'accès (AP) basés sur le logiciel Cisco IOS®

- Logiciel Cisco IOS Version 12.2(15)JA ou ultérieure**Remarque :** Utilisez de préférence la dernière version du logiciel Cisco IOS, même si WPA est pris en charge dans le logiciel Cisco IOS Version 12.2(11)JA et ultérieure. Afin d'obtenir la version la plus récente de Cisco IOS, référez-vous aux téléchargements (clients enregistrés seulement).
- Une carte d'interface réseau (NIC) compatible WPA et son logiciel client compatible WPA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Théorie générale

Les fonctionnalités de sécurité dans un réseau sans fil, comme WEP, sont faibles. Le groupe de l'industrie Wi-Fi Alliance (ou WECA) a conçu une norme intérimaire de sécurité de la deuxième génération pour les réseaux sans fil. La norme assure la défense contre des faiblesses jusqu'à ce que l'organisation IEEE ratifie la norme 802.11i.

Ce nouveau système se fonde sur l'authentification EAP/802.1x et la gestion dynamique des clés, et ajoute un cryptage plus fort des chiffres. Après que le périphérique client et le serveur d'authentification font une association EAP/802.1x, la gestion des clés WPA est négociée entre AP et le périphérique client compatible WPA.

Les produits AP de Cisco prévoient également une configuration hybride dans laquelle les deux clients EAP existants basés sur WEP (avec gestion des clés ou gestion existante) travaillent avec les clients WPA. Cette configuration est désignée sous de « mode de transfert ». Le mode de migration permet une approche par étapes pour migrer vers WPA. Ce document ne couvre pas le mode de migration. Ce document trace les grandes lignes d'un pur réseau sécurisé par WPA.

En plus des questions de sécurité au niveau de l'entreprise ou du groupe entier, WPA fournit également une version de clé pré-partagée (WPA-PSK) qui est destinée aux bureaux de petite taille, aux travailleurs à domicile ou réseaux sans fil à la maison. L'utilitaire client Aironet de Cisco (ACU) ne prend pas en charge WPA-PSK. L'utilitaire de configuration sans fil de Microsoft Windows prend en charge WPA-PSK pour la plupart des cartes sans fil, de même que ces utilitaires :

- AEGIS Client de Meetinghouse Communications**Note :** Reportez-vous à Annonce de fin de vie et de fin de vie pour la gamme de produits AEGIS de Meetinghouse.
- Odyssey client de Funk Software**Remarque :** reportez-vous au Centre d'assistance à la clientèle de Juniper Networks .
- Utilitaires client OEM (Original Equipment Manufacturer) de quelques constructeurs

Vous pouvez configurer WPA-PSK quand :

- Vous définissez le mode de cryptage sur Cipher Temporal Key Integrity Protocol (TKIP) sur l'onglet Encryption Manager.
- Vous définissez le type d'authentification, l'utilisation de la gestion des clés authentifiées et la clé pré-partagée sur l'onglet Manager de Service Set Identifier (SSID) du GUI.
- Aucune configuration n'est requise sur l'onglet Server Manager.

Afin d'activer WPA-PSK par l'interface de commande en ligne (CLI), entrez ces commandes. Démarrez du mode de configuration :

```
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
```

Remarque : cette section fournit uniquement la configuration qui est pertinente pour WPA-PSK. La configuration dans cette section n'est que pour vous donner une compréhension sur la façon d'activer le WPA-PSK et n'est pas l'objet de ce document. Ce document explique comment configurer WPA.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

WPA se fonde sur les méthodes actuelles EAP/802.1x. Ce document suppose que vous avez une configuration Light EAP (LEAP), EAP ou Protected EAP (PEAP) qui fonctionne avant que vous ajoutiez la configuration afin d'engager WPA.

Cette section présente les informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Network EAP ou l'authentification ouverte avec EAP

Dans n'importe quelle méthode d'authentification basée sur EAP/802.1x, vous pouvez interroger ce que sont les différences entre Network-EAP et l'authentification ouverte avec EAP. Ces éléments se rapportent à des valeurs dans le domaine d'algorithme d'authentification dans les en-têtes des paquets de gestion et d'association. La plupart des constructeurs des clients sans fil définissent cette zone sur la valeur 0 (authentification ouverte), puis signalent leur désir de faire l'authentification EAP plus tard dans le processus d'association. Cisco définit la valeur différemment, depuis le début de l'association avec l'indicateur Network EAP.

Utilisez la méthode d'authentification que cette liste indique si votre réseau a des clients qui sont :

- clients Cisco - Utilisez Network-EAP.
- Clients tiers (qui incluent les produits conformes Cisco Compatible Extensions [CCX]) - utilisez l'authentification ouverte avec EAP.
- Une combinaison de chacun des deux clients Cisco et tiers - choisissez Network-EAP et l'authentification ouverte avec EAP.

Configuration CLI

Ce document utilise les configurations suivantes :

- Une configuration LEAP qui existe et fonctionne
- Cisco IOS Version 12.2(15)JA pour les AP Cisco IOS basés sur le logiciel Cisco IOS

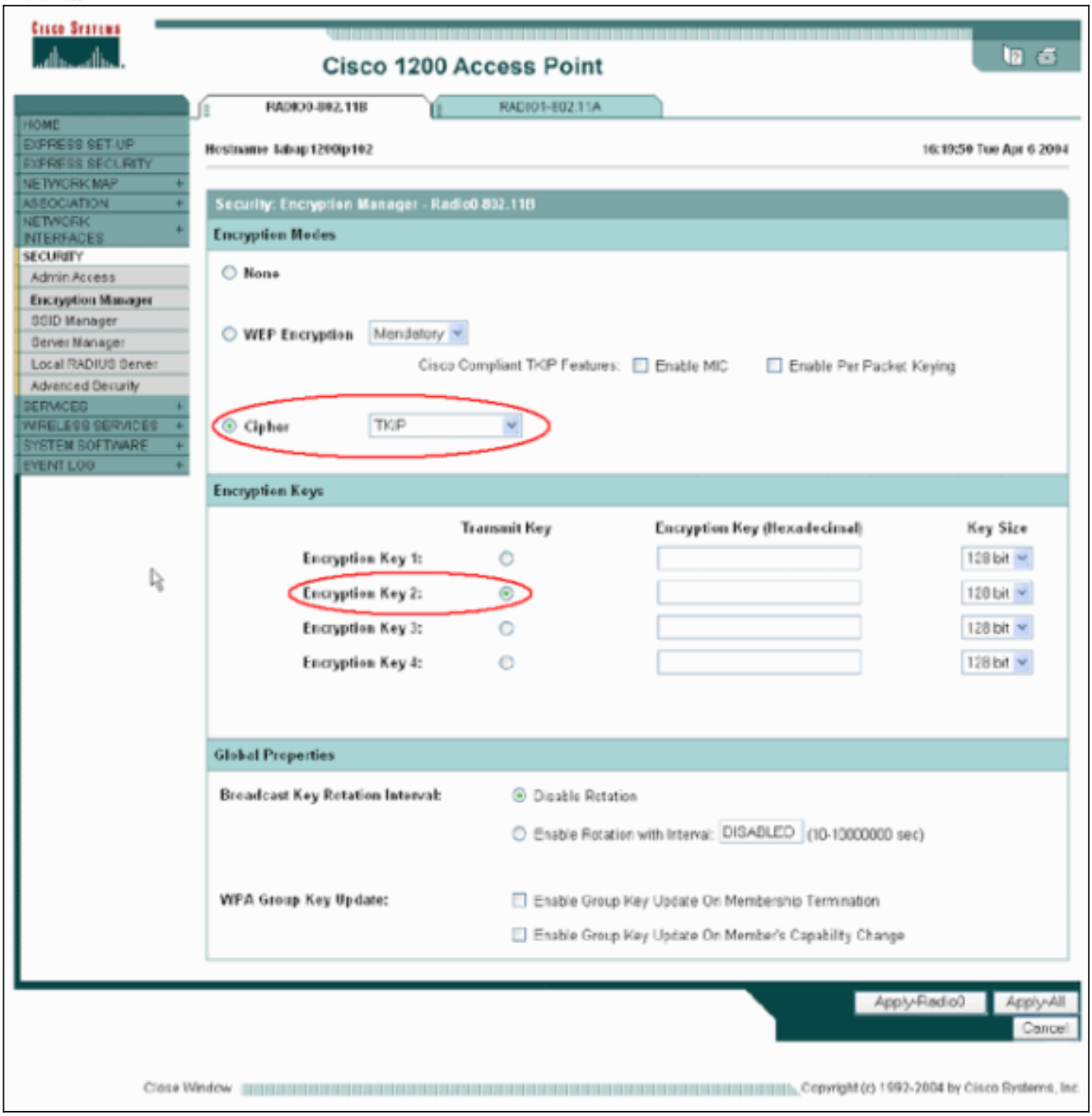
AP

```
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
```

Configuration de la GUI

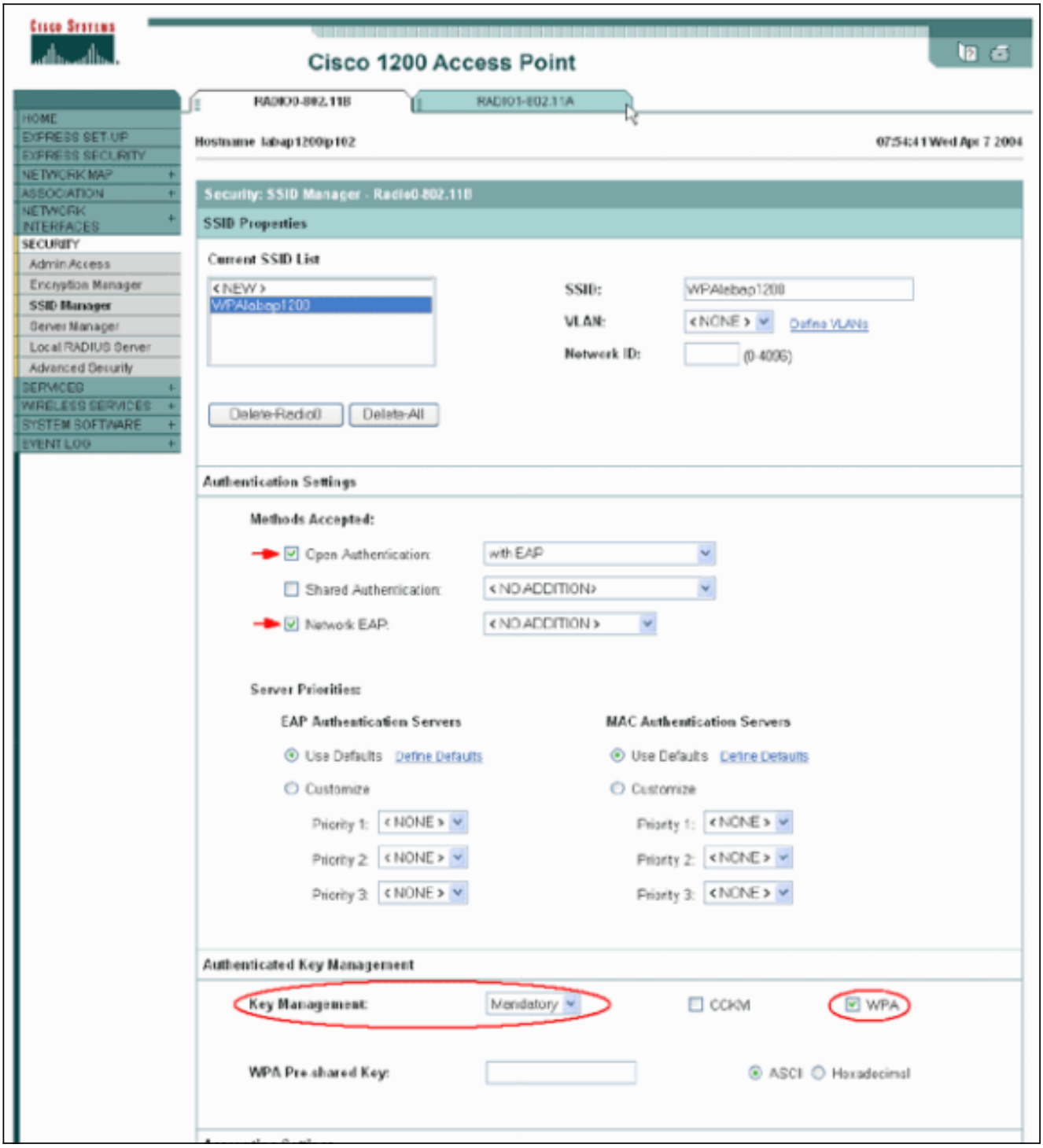
Complétez ces étapes afin de configurer l'AP pour WPA :

1. Complétez ces étapes pour configurer le gestionnaire de cryptage :Activez Cipher pour TKIP.Effacez la valeur dans la clé de cryptage 1.Définissez la clé de cryptage 2 comme la clé de transmission.Cliquez sur **Apply-Radio#**.



2. Complétez ces étapes pour configurer le gestionnaire SSID :Sélectionnez le SSID désiré de la liste actuelle des SSID.Choisissez la méthode d'authentification adéquate.Basez cette décision sur le type de cartes client que vous utilisez. Regardez la section Network EAP ou l'authentification ouverte avec EAP de ce document pour plus d'informations. Si EAP a fonctionné avant l'ajout de WPA, une modification n'est probablement pas nécessaire.Complétez ces étapes afin d'activer la gestion des clés :Choisissez **Mandatory dans le menu déroulant de gestion des clés.**Cochez la case à cocher WPA.Cliquez sur **Apply-**

Radio#.

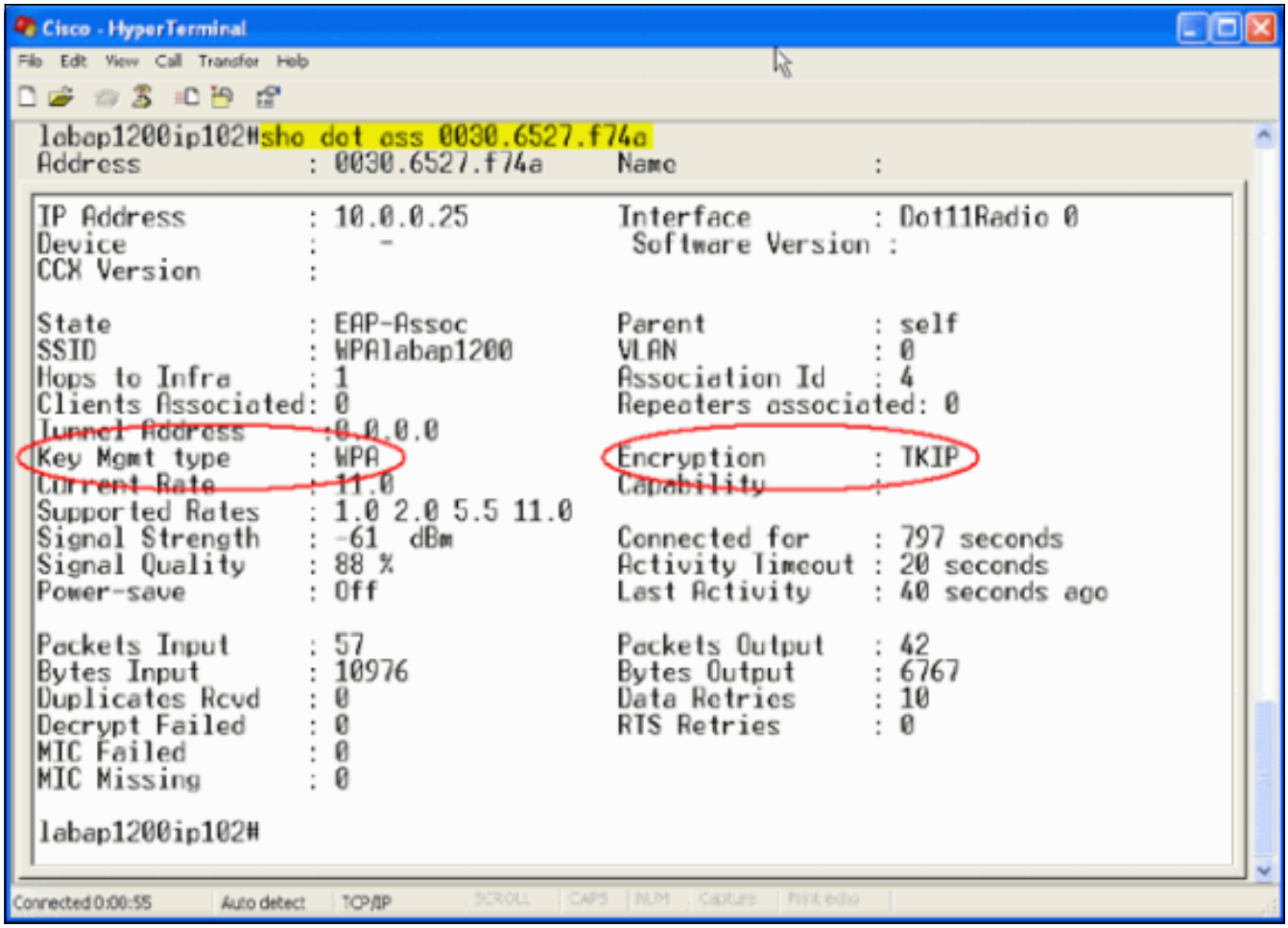


Vérification

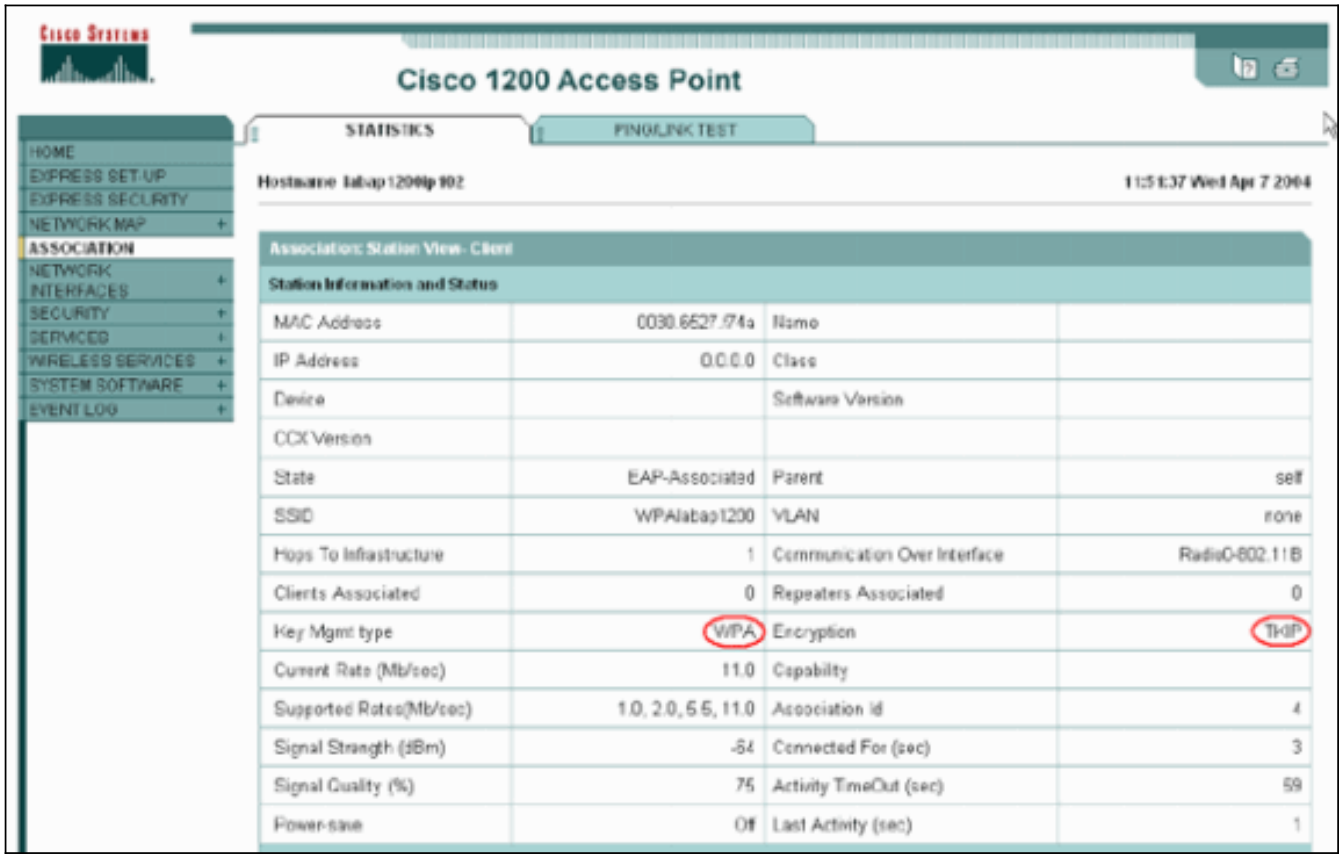
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show dot11 association** *mac_address* - Cette commande affiche des informations sur le client associé spécifiquement identifié. Vérifiez que le client négocie la gestion des clés en tant que **WPA et le cryptage en tant que**
  TKIP.



- L'entrée de la table d'association pour un client particulier doit également indiquer la gestion des clés comme étant **WPA et le cryptage comme étant TKIP**. Dans la table d'association, cliquez sur une adresse MAC particulière pour un client afin de voir les détails de l'association pour ce
client.



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Procédure de dépannage

Ces informations s'appliquent à cette configuration. Complétez ces étapes afin de dépanner votre configuration :

1. Si cette configuration LEAP, EAP ou PEAP n'a pas été complètement testée avant la mise en œuvre de WPA, vous devez compléter ces étapes :Désactivez temporairement le mode de cryptage WPA.Réactivez l'EAP adéquat.Confirmez que l'authentification fonctionne.
2. Vérifiez que la configuration du client correspond à celle de l'AP.Par exemple, quand l'AP est configuré pour WPA et TKIP, confirmez que les paramètres correspondent à ceux qui sont configurés dans le client.

Dépannage des commandes

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

La gestion des clés WPA implique une prise de contact à quatre voies après la réussite de l'authentification EAP. Vous pouvez voir ces quatre messages dans les débogages. Si l'EAP n'authentifie pas avec succès le client ou si vous ne voyez pas les messages, complétez ces étapes :

1. Désactivez temporairement WPA.
2. Réactivez l'EAP adéquat.
3. Confirmez que l'authentification fonctionne.

Cette liste décrit les débogages :

- **debug dot11 aaa manager keys - Ce débogage indique la prise de contact qui se produit entre l'AP et le WPA client tandis que les clés PTK (Pairwise Transient Key) et GTK (Group Transient Key) négocient.** Ce débogage a été introduit dans le logiciel Cisco IOS Version 12.2(15)JA.Si aucune sortie de débogage n'apparaît, vérifiez ces éléments :Le contrôle du terminal **term mon est activé (si vous utilisez une session Telnet).**Les débogages sont activés.Le client est convenablement configuré pour WPA.Si le débogage montre que des prises de contact PTK et/ou GTK sont établies mais pas vérifiées, examinez le logiciel de supplicant WPA pour vérifier que la configuration est correcte et la version à jour.
- **debug dot11 aaa authenticator state-machine - Ce débogage indique les divers états de négociation par lesquels passe un client pendant qu'il s'associe et s'authentifie.** Les noms d'état indiquent ces états. Ce débogage a été introduit dans le logiciel Cisco IOS Version 12.2(15)JA. Le débogage rend obsolète la commande **debug dot11 aaa dot1x state-machine dans le logiciel Cisco IOS Version 12.2(15)JA et ultérieure.**
- **debug dot11 aaa dot1x state-machine - Ce débogage indique les divers états de négociation par lesquels passe un client pendant qu'il s'associe et s'authentifie.** Les noms d'état indiquent ces états. Dans des versions de Cisco IOS qui sont antérieures à la version 12.2(15)JA, ce débogage montre également la négociation de la gestion des clés WPA.

- **debug dot11 aaa authenticator process - Ce débogage est très utile pour diagnostiquer les problèmes de transmissions négociées.** Les informations détaillées montrent ce que chaque participant à la négociation envoie ainsi que la réponse de l'autre participant. Vous pouvez également employer ce débogage avec la commande **debug radius authentication.** Ce débogage a été introduit dans le logiciel Cisco IOS Version 12.2(15)JA. Le débogage rend obsolète la commande **debug dot11 aaa dot1x process dans le logiciel Cisco IOS Version 12.2(15)JA et ultérieure.**
- **debug dot11 aaa dot1x process - Ce débogage est utile pour diagnostiquer les problèmes de transmissions négociées.** Les informations détaillées montrent ce que chaque participant à la négociation envoie ainsi que la réponse de l'autre participant. Vous pouvez également employer ce débogage avec la commande **debug radius authentication.** Dans les versions de Cisco IOS qui sont antérieures à la version 12.2(15)JA, ce débogage montre la négociation de la gestion des clés WPA.

Informations connexes

- Configuration des suites de chiffre et de WEP
- Configuration des types d'authentification
- WPA2 - Wi-Fi Protected Access 2
- Configuration de Wi-Fi Protected Access 2 (WPA 2)
- Support et documentation techniques - Cisco Systems