Übersicht über die WPA-Konfiguration

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für Wi-Fi Protected Access (WPA), den vorläufigen Sicherheitsstandard, den Mitglieder der Wi-Fi Alliance verwenden.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Umfassendes Wissen über Wireless-Netzwerke und Wireless-Sicherheitsfragen
- Kenntnisse der EAP-Sicherheitsmethoden (Extensible Authentication Protocol)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IOS® Software-basierte Access Points (APs)
- Cisco IOS Software Release 12.2(15)JA oder höher**Hinweis:** Verwenden Sie vorzugsweise

die neueste Version der Cisco IOS-Software, obwohl WPA in Version 12.2(11)JA und höher der Cisco IOS-Software unterstützt wird. Um die neueste Cisco IOS Software-Version zu erhalten, lesen Sie Downloads (nur registrierte Kunden).
- Eine WPA-konforme Netzwerkschnittstellenkarte (NIC) und die WPA-konforme Client-Software

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundtheorie

Die Sicherheitsfunktionen in einem Wireless-Netzwerk, z. B. WEP, sind schwach. Die WECA-Branchengruppe (Wi-Fi Alliance) hat einen vorläufigen Sicherheitsstandard der nächsten Generation für Wireless-Netzwerke entwickelt. Der Standard bietet Schutz vor Schwachstellen, bis die IEEE-Organisation den 802.11i-Standard ratifiziert.

Dieses neue Schema baut auf der aktuellen EAP/802.1x-Authentifizierung und der dynamischen Schlüsselverwaltung auf und bietet eine stärkere Verschlüsselung der Verschlüsselung. Nachdem das Client-Gerät und der Authentifizierungsserver eine EAP/802.1x-Verbindung herstellen, wird das WPA-Schlüsselmanagement zwischen dem AP und dem WPA-kompatiblen Client-Gerät ausgehandelt.

Cisco AP-Produkte bieten außerdem eine Hybridkonfiguration, bei der beide Legacy-WEP-basierten EAP-Clients (mit veralteter oder ohne Schlüsselverwaltung) mit WPA-Clients zusammenarbeiten. Diese Konfiguration wird als Migrationsmodus bezeichnet. Der Migrationsmodus ermöglicht einen schrittweisen Ansatz für die Migration zu WPA. In diesem Dokument wird der Migrationsmodus nicht behandelt. Dieses Dokument bietet einen Überblick über ein reines WPA-gesichertes Netzwerk.

Neben Sicherheitsbedenken auf Unternehmens- oder Unternehmensebene bietet WPA auch eine Pre-Shared Key-Version (WPA-PSK), die für den Einsatz in kleinen Büros, Heimbüros (SOHO) oder privaten Wireless-Netzwerken bestimmt ist. Das Cisco Aironet Client Utility (ACU) unterstützt WPA-PSK nicht. Das Dienstprogramm "Konfigurationsfreie drahtlose Verbindung" von Microsoft Windows unterstützt WPA-PSK für die meisten Wireless-Karten. Dies gilt auch für folgende Dienstprogramme:

- AEGIS-Client für Meetinghouse Communications**Hinweis:** Weitere Informationen zur AEGIS-Produktlinie für Meetinghouse finden Sie in der EOS- und EOL-Ankündigung.
- Odyssey-Client von Funk Software**Hinweis:** Weitere Informationen finden Sie im Kundensupport-Center von Juniper Networks.
- Utilitys von einigen Herstellern (Original Equipment Manufacturer, OEM)

Sie können WPA-PSK konfigurieren, wenn:

- Sie definieren den Verschlüsselungsmodus auf der Registerkarte Encryption Manager als Cipher Temporal Key Integrity Protocol (TKIP).
- Auf der Registerkarte "Service Set Identifier (SSID) Manager" der GUI legen Sie den Authentifizierungstyp, die Verwendung der Verwaltung authentifizierter Schlüssel und den vorinstallierten Schlüssel fest.
- Auf der Registerkarte Server Manager ist keine Konfiguration erforderlich.

Um WPA-PSK über die Befehlszeilenschnittstelle (CLI) zu aktivieren, geben Sie diese Befehle ein. Starten Sie im Konfigurationsmodus:

```
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
```

Hinweis: Dieser Abschnitt enthält nur die Konfiguration, die für WPA-PSK relevant ist. Die Konfiguration in diesem Abschnitt dient lediglich dazu, Ihnen ein Verständnis für die Aktivierung von WPA-PSK zu vermitteln. Sie wird in diesem Dokument nicht behandelt. In diesem Dokument wird die Konfiguration von WPA erläutert.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfiguration

WPA baut auf den aktuellen EAP/802.1x-Methoden auf. In diesem Dokument wird davon ausgegangen, dass Sie über eine Light EAP (LEAP)-, EAP- oder PEAP-Konfiguration (Protected EAP) verfügen, die vor dem Hinzufügen der Konfiguration zur Aktivierung von WPA funktioniert.

In diesem Abschnitt werden die Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen erläutert.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerk-EAP oder offene Authentifizierung mit EAP

Bei jeder EAP/802.1x-basierten Authentifizierungsmethode können Sie die Unterschiede zwischen der Netzwerk-EAP und der offenen Authentifizierung mit EAP infrage stellen. Diese Elemente beziehen sich auf Werte im Feld Authentifizierungsalgorithmus in den Headern der Management- und Zuordnungspakete. Die meisten Hersteller von Wireless-Clients setzen dieses Feld auf den Wert 0 (Open Authentication) und signalisieren dann ihren Wunsch, die EAP-Authentifizierung später im Zuordnungsprozess durchzuführen. Cisco legt den Wert anders fest, als bei Beginn der Verknüpfung mit dem Netzwerk-EAP-Flag.

Verwenden Sie die Authentifizierungsmethode, die in dieser Liste angegeben ist, wenn Ihr Netzwerk Clients hat, die:

- Cisco Clients - Verwenden Sie Network-EAP.
- Drittanbieter-Clients (die Cisco Compatible Extensions [CCX]-konforme Produkte enthalten) - Verwenden Sie die offene Authentifizierung mit EAP.
- Eine Kombination aus Cisco Clients und Clients von Drittanbietern - Wählen Sie Network-EAP und Open Authentication mit EAP.

CLI-Konfiguration

In diesem Dokument werden folgende Konfigurationen verwendet:

- Eine vorhandene und funktionierende LEAP-Konfiguration
- Cisco IOS Software Release 12.2(15)JA für die Cisco IOS Software-basierten APs

AP

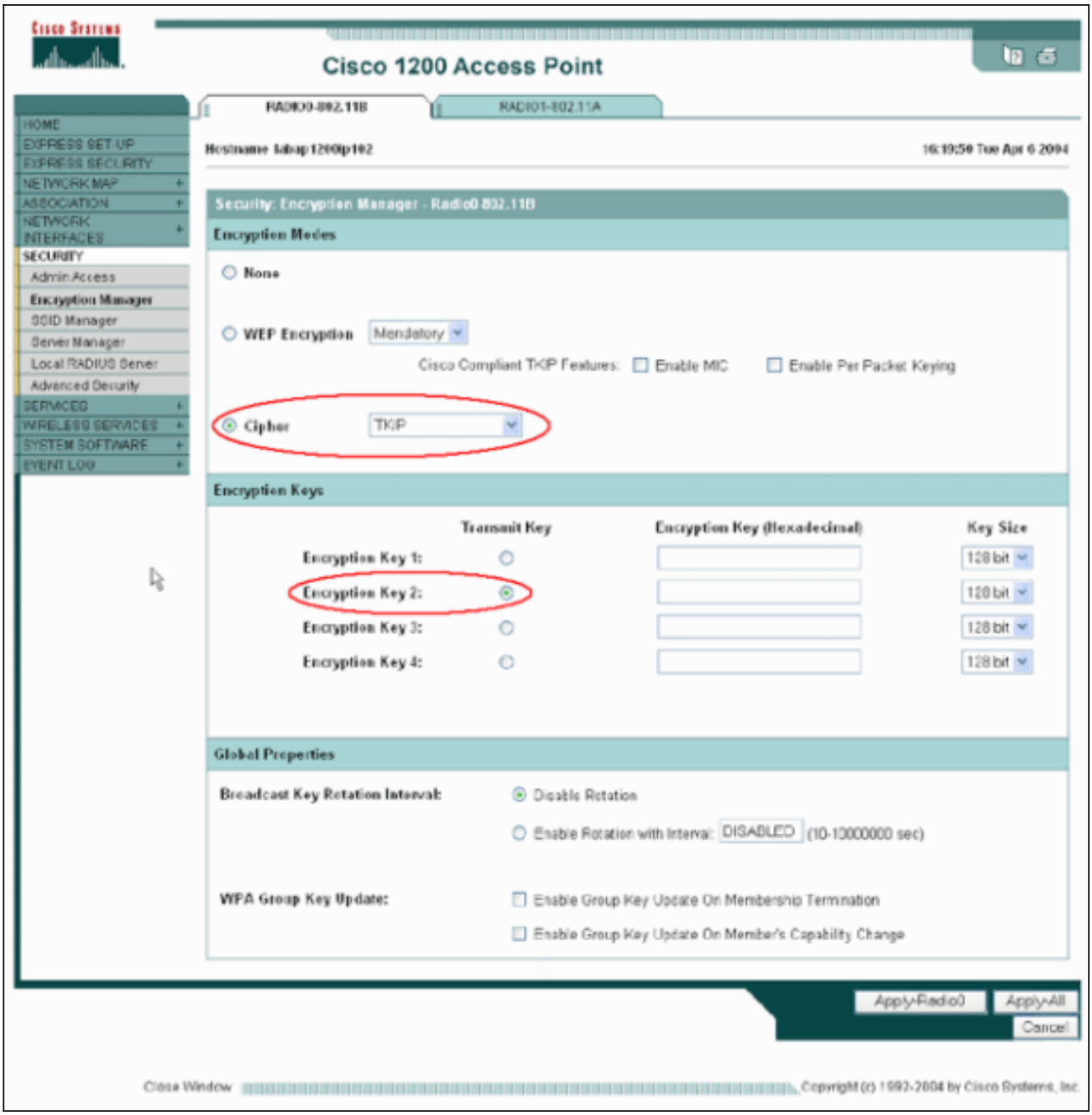
```
ap1#show running-config
 Building configuration...
 .
 .
 .
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption 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
```

GUI-Konfiguration

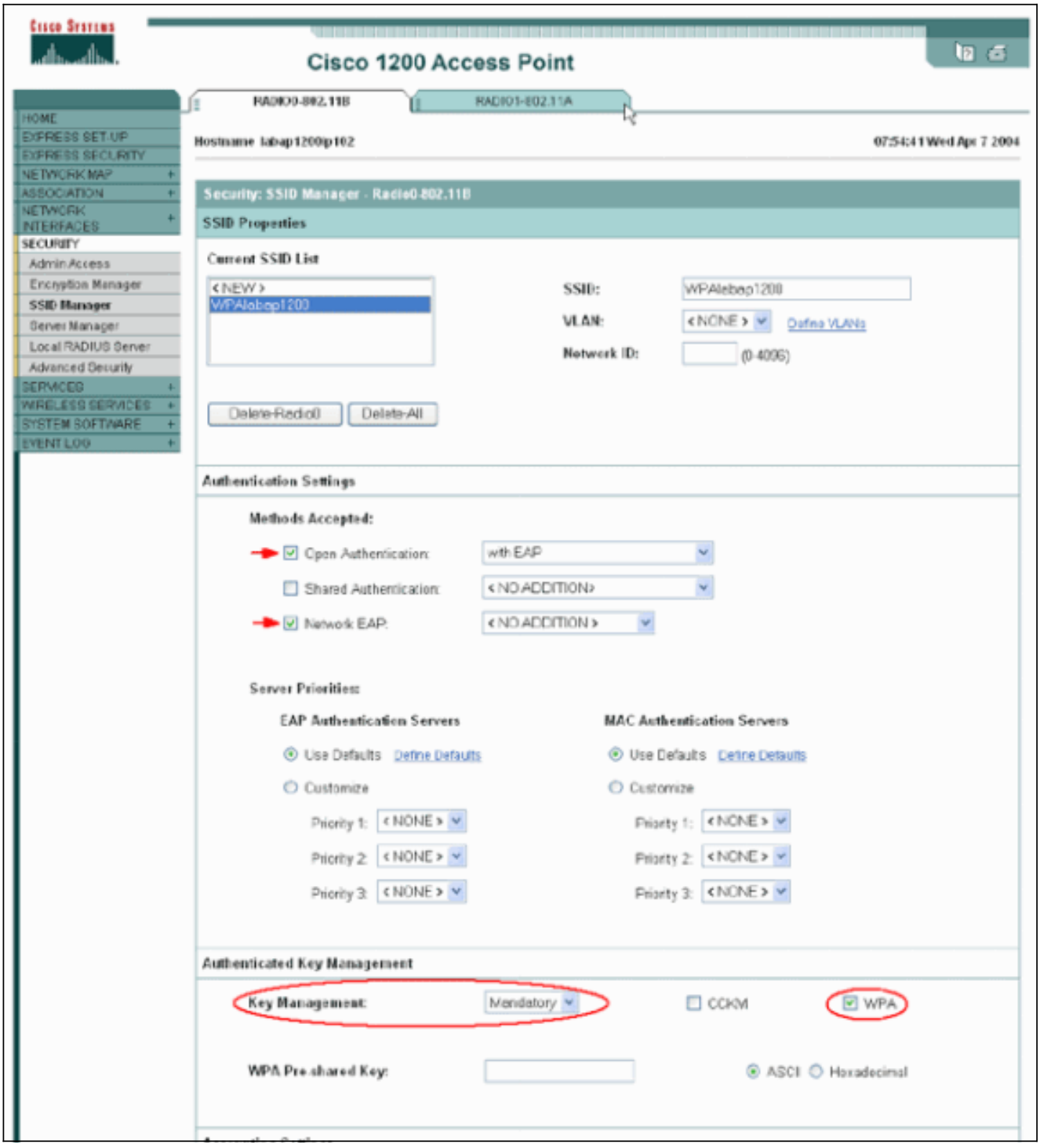
Gehen Sie wie folgt vor, um den Access Point für WPA zu konfigurieren:

1. Führen Sie die folgenden Schritte aus, um den Encryption Manager einzurichten:Aktivieren Sie Cipher für TKIP.Löschen Sie den Wert im Verschlüsselungsschlüssel 1.Legen Sie Verschlüsselungsschlüssel 2 als Übertragungsschlüssel fest.Klicken Sie auf **Apply-Radio#.**



2. Führen Sie die folgenden Schritte aus, um den SSID-Manager einzurichten:Wählen Sie die gewünschte SSID aus der aktuellen SSID-Liste aus.Wählen Sie eine geeignete Authentifizierungsmethode aus.Basieren Sie diese Entscheidung auf dem Typ der Client-Karten, die Sie verwenden. Weitere Informationen finden Sie im Abschnitt Network EAP oder

Open Authentication with EAP dieses Dokuments. Wenn EAP vor dem Hinzufügen von WPA funktionierte, ist eine Änderung wahrscheinlich nicht erforderlich.Gehen Sie wie folgt vor, um die Schlüsselverwaltung zu aktivieren:Wählen Sie **Obligatorisch** aus dem Dropdown-Menü Key Management (Schlüsselverwaltung) aus.Aktivieren Sie das Kontrollkästchen WPA.Klicken Sie auf **Apply-Radio#.**

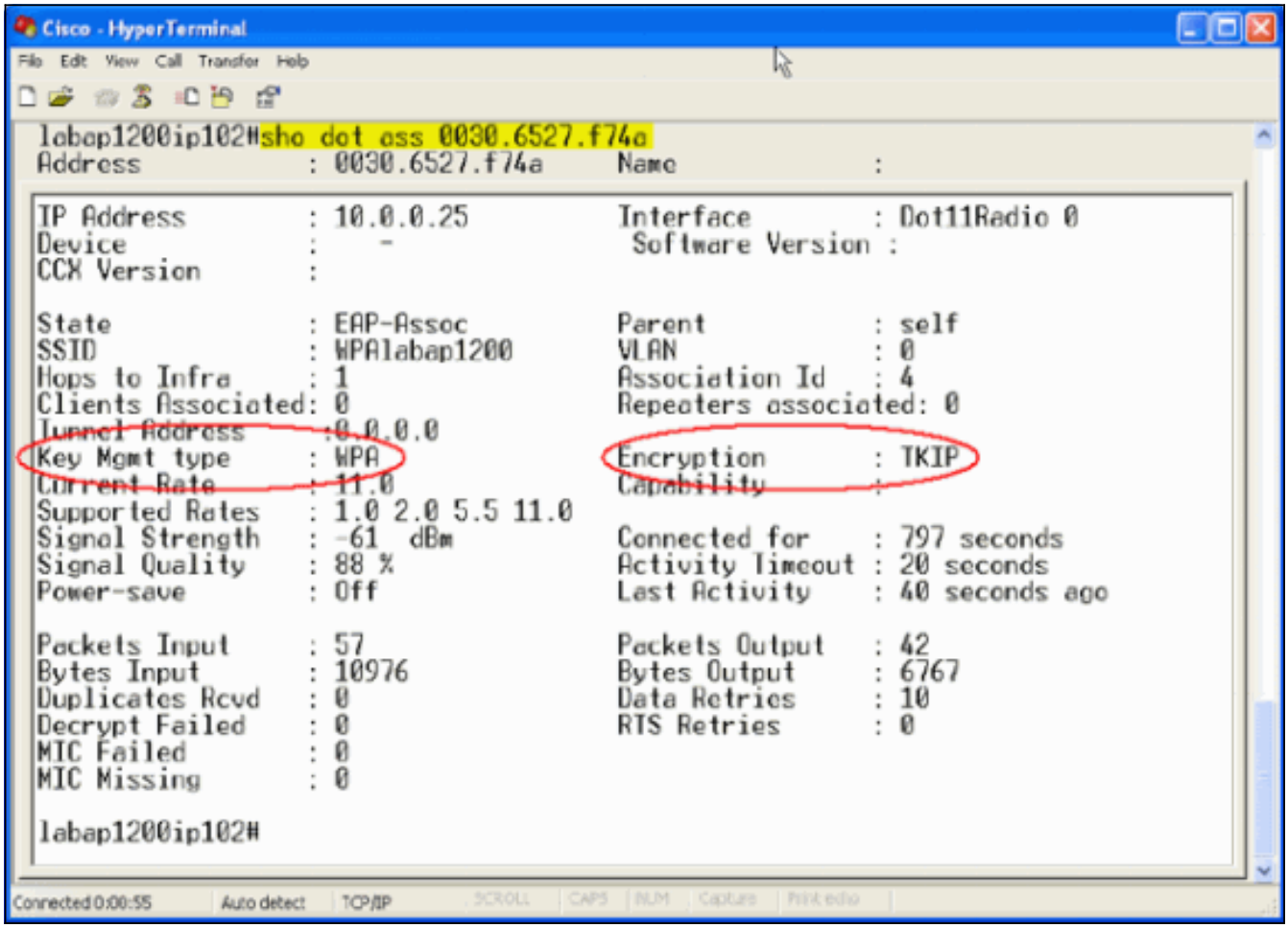


Überprüfung

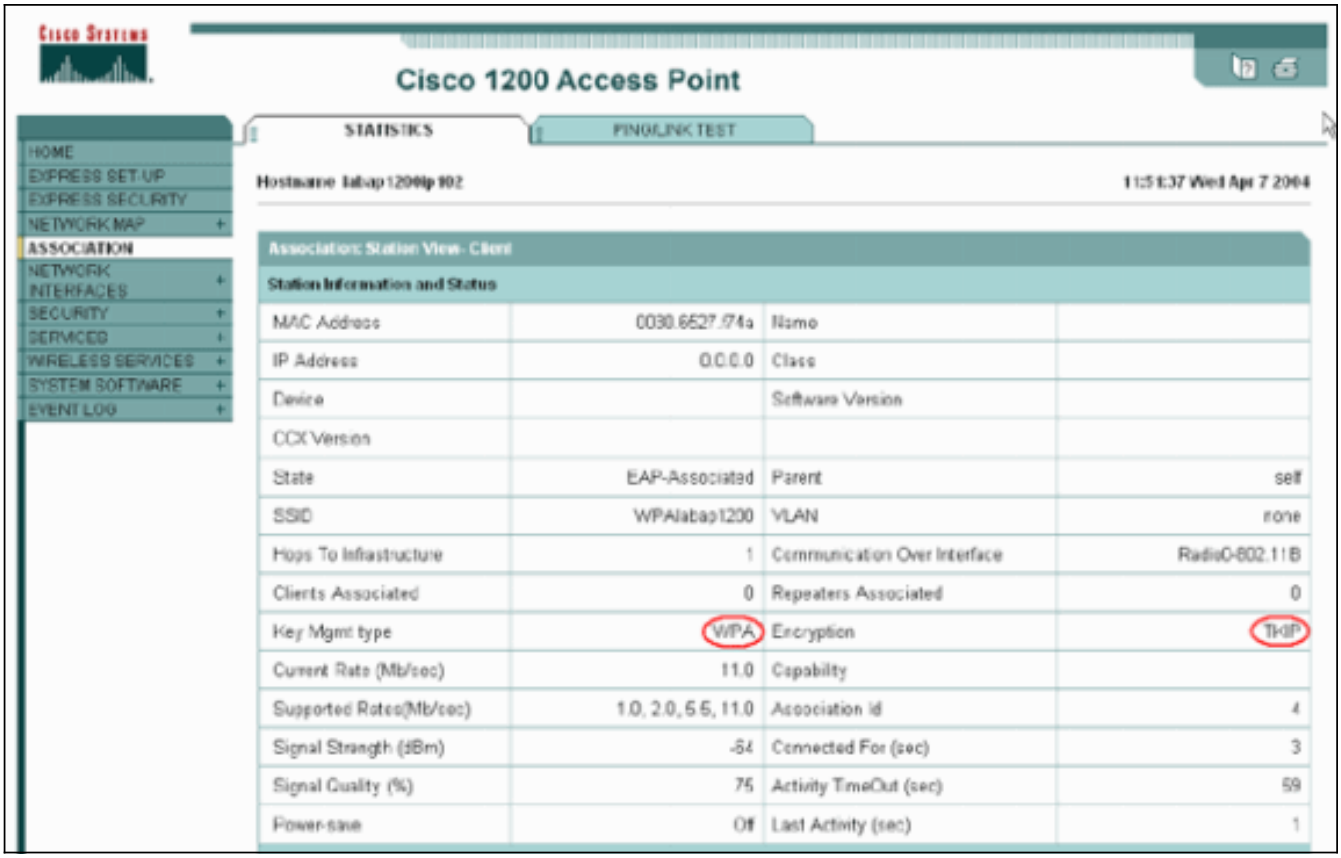
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show dot1 Association *mac_address*: Dieser Befehl** zeigt Informationen über einen speziell identifizierten verknüpften Client an. Überprüfen Sie, ob der Client die Schlüsselverwaltung als **WPA** und Verschlüsselung als **TKIP** aushandelt.



- Der Tabelleneintrag Zuordnungstabelle für einen bestimmten Client muss auch die Schlüsselverwaltung als **WPA** und Verschlüsselung als **TKIP** angeben. Klicken Sie in der Zuordnungstabelle auf eine bestimmte MAC-Adresse für einen Client, um die Details der Zuordnung für diesen Client anzuzeigen.



Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Fehlerbehebungsverfahren

Diese Informationen sind für diese Konfiguration relevant. Gehen Sie wie folgt vor, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen:

1. Wenn diese LEAP-, EAP- oder PEAP-Konfiguration vor der WPA-Implementierung nicht gründlich getestet wurde, müssen Sie die folgenden Schritte ausführen:Deaktivieren Sie vorübergehend den WPA-Verschlüsselungsmodus.Aktivieren Sie den entsprechenden EAP wieder.Bestätigen Sie, dass die Authentifizierung funktioniert.
2. Überprüfen Sie, ob die Konfiguration des Clients mit der des Access Points übereinstimmt.Wenn der Access Point beispielsweise für WPA und TKIP konfiguriert ist, müssen Sie überprüfen, ob die Einstellungen mit den Einstellungen übereinstimmen, die im Client konfiguriert wurden.

Fehlerbehebung bei Befehlen

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Die Verwaltung des WPA-Schlüssels erfolgt in vier Richtungen, nachdem die EAP-Authentifizierung erfolgreich abgeschlossen wurde. Diese vier Meldungen werden im Debuggen angezeigt. Wenn EAP den Client nicht erfolgreich authentifiziert oder die Meldungen nicht angezeigt werden, gehen Sie wie folgt vor:

1. Deaktivieren Sie vorübergehend WPA.
2. Aktivieren Sie den entsprechenden EAP wieder.
3. Bestätigen Sie, dass die Authentifizierung funktioniert.

Diese Liste beschreibt die DebuggingInnen:

- **debug dot11 aaa manager keys** - Dieses Debuggen zeigt den Handshake, der zwischen dem AP und dem WPA-Client als paarweise transient key (PTK) und group transient key (GTK) ausgehandelt wird. Diese Fehlerbehebung wurde in Version 12.2(15)JA der Cisco IOS-Software eingeführt.Wenn keine Debug-Ausgaben angezeigt werden, überprüfen Sie die folgenden Elemente:Der Terminalmonitor-**Begriff mon** ist aktiviert (wenn Sie eine Telnet-Sitzung verwenden).Die DebuggingInnen sind aktiviert.Der Client ist entsprechend für WPA konfiguriert.Zeigt das Debuggen, dass PTK- und/oder GTK-Handshakes erstellt, aber nicht verifiziert wurden, überprüfen Sie die WPA-Supplicant-Software auf die richtige Konfiguration und die aktuelle Version.
- **debug dot11 aaa authentifizierer state-machine** - Dieses Debuggen zeigt die verschiedenen Verhandlungszustände an, die ein Client durchläuft, während er zuordnet und authentifiziert. Diese Zustände werden durch die Zustandsnamen angegeben. Diese Fehlerbehebung wurde in Version 12.2(15)JA der Cisco IOS-Software eingeführt. Der Befehl debug **dot1 aaa dot1x state-machine** in Cisco IOS Software Release 12.2(15)JA und höher wird durch den Befehl debug verdrängt.
- **debug dot11 aaa dot1x state-machine** - Dieses Debugging zeigt die verschiedenen Verhandlungszustände an, die ein Client durchläuft, wenn er eine Verbindung herstellt und sich authentifiziert. Diese Zustände werden durch die Zustandsnamen angegeben. In Cisco IOS-Softwareversionen, die älter als die Cisco IOS-Softwareversion 12.2(15)JA sind, wird in diesem Debugging auch die Aushandlung der WPA-Schlüsselverwaltung angezeigt.
- **debug dot1aaa authentifizierer prozess**: Dieser debug ist am hilfreichsten, um Probleme bei ausgehandelter kommunikation zu diagnostizieren. Die detaillierten Informationen zeigen, was jeder Teilnehmer an der Aushandlung sendet, und zeigen die Antwort des anderen Teilnehmers an. Sie können dieses Debuggen auch zusammen mit dem Befehl **debug radius authentication** verwenden. Diese Fehlerbehebung wurde in Version 12.2(15)JA der Cisco IOS-Software eingeführt. Der Debugger löst den Befehl **debug dot11 aaa dot1x process** in Cisco IOS Software Release 12.2(15)JA und höher aus.
- **debug dot11 aaa dot1x process** - Dieser Debugging ist hilfreich, um Probleme bei ausgehandelter Kommunikation zu diagnostizieren. Die detaillierten Informationen zeigen, was jeder Teilnehmer an der Aushandlung sendet, und zeigen die Antwort des anderen Teilnehmers an. Sie können dieses Debuggen auch zusammen mit dem Befehl **debug radius authentication** verwenden. In Cisco IOS-Softwareversionen, die älter als die Cisco IOS-Softwareversion 12.2(15)JA sind, zeigt dieses Debuggen die Aushandlung der WPA-Schlüsselverwaltung.

Zugehörige Informationen

- Konfigurieren von Cipher-Suiten und WEP
- Konfigurieren von Authentifizierungstypen
- WPA2 - Wi-Fi Protected Access 2
- Konfiguration von Wi-Fi Protected Access 2 (WPA 2)
- Technischer Support und Dokumentation für Cisco Systeme