Overzicht van WAP-configuratie

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor Wi-Fi Protected Access (WAP), de tussentijdse beveiligingsstandaard die leden van Wi-Fi Alliance gebruiken.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Grondig kennis van draadloze netwerken en draadloze beveiligingsproblemen
- Kennis van uitgebreide verificatieprotocollen (EAP)-beveiligingsmethoden

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS® op software gebaseerde access points (AP's)
- Cisco IOS-softwarerelease 12.2(15)JA of hoger**Opmerking:** Gebruik bij voorkeur de nieuwste Cisco IOS-softwarerelease, ook al wordt WAP ondersteund in Cisco IOS-softwarerelease 12.2(11)JA en hoger. Raadpleeg voor het verkrijgen van de nieuwste Cisco IOS-

softwarerelease downloads (alleen geregistreerde klanten).
- Een WAP-conforme netwerkinterfacekaart (NIC) en zijn WAP-conforme clientsoftware

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

De veiligheidseigenschappen in een draadloos netwerk, zoals EVN, zijn zwak. De WiFi Alliance (of WECA) industriegroep heeft een volgende generatie, voorlopige veiligheidsnorm voor draadloze netwerken ontworpen. De standaard biedt bescherming tegen zwakheden totdat de IEEE-organisatie de 802.11i-standaard ratificeert.

Dit nieuwe scheme bouwt voort op de huidige EAP/802.1x-authenticatie en dynamisch sleutelbeheer, en voegt een sterkere encryptie toe. Nadat het clientapparaat en de authenticatieserver een EAP/802.1x associatie maken, wordt het beheer van de WAP-toets tussen de AP en het WAP-conforme clientapparaat overeengekomen.

Cisco AP-producten voorzien ook in een hybride configuratie waarin zowel op erfelijke hefboomwerking gebaseerde MAP-klanten (met erfenis of geen zeer belangrijk beheer) in combinatie met de cliënten van WAP werken. Deze configuratie wordt migratiemodus genoemd. De migratiemodus staat een gefaseerde benadering toe om naar WAP te migreren. Dit document heeft geen betrekking op de migratiemodus. Dit document biedt een overzicht van een zuiver WAP-beveiligd netwerk.

Naast de veiligheidsproblemen op bedrijfsniveau biedt WAP ook een pre-Shared Key versie (WAP-PSK) die is bedoeld voor gebruik in kleine kantoor-, startkantoor- (SOHO) of draadloze thuisnetwerken. Cisco Aironet Client Utility (ACU) biedt geen ondersteuning voor WAP-PSK. Het Wireless Zero Configuration-hulpprogramma van Microsoft Windows ondersteunt WAP-PSK voor de meeste draadloze kaarten, evenals deze hulpprogramma's:

- AEGIS-client voor Meetings-huiscommunicatie**Opmerking:** Raadpleeg EOS- en End-of-life aankondigingen voor de Meetinghouse AEGIS-productlijn.
- Odyssey client vanaf Funk Software**Opmerking:** Raadpleeg het Customer Support Center van Juniper Networks.
- Originele apparatuurfabrikant (OEM) clientadaptertools van sommige fabrikanten

U kunt WAP-PSK configureren wanneer:

- U definieert de encryptiemodus als CIP-protocol (Central Key Integrity Protocol) op het tabblad Encryption Manager.
- U definieert het verificatietype, het gebruik van geauthentiseerd belangrijk beheer en de vooraf gedeelde sleutel in het tabblad Service Set Identifier (SSID) Manager van de GUI.
- Er is geen configuratie vereist op het tabblad Server Manager.

Voer deze opdrachten in om WAP-PSK via de opdrachtregel-interface (CLI) in. Begin vanuit de configuratie-modus:

```
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
```

Opmerking: deze sectie verschaft alleen de configuratie die relevant is voor WAP-PSK. De configuratie in deze sectie geeft u alleen een begrip van hoe u WAP-PSK kunt inschakelen en is niet de focus van dit document. Dit document legt uit hoe u WAP moet configureren.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

WAP bouwt voort op de huidige EAP/802.1x-methoden. In dit document wordt ervan uitgegaan dat u een EAP-configuratie (Light EAP), EAP (Protected EAP) of PEAP-configuratie hebt die werkt voordat u de configuratie toevoegt om met WAP te werken.

In deze sectie wordt de informatie gepresenteerd om de functies te configureren die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

PPP-verificatie of open verificatie met EAP

Bij elke op MAP/802.1x gebaseerde authenticatiemethode kun je je afvragen wat de verschillen zijn tussen netwerk-EAP en Open authenticatie met MAP. Deze items verwijzen naar waarden in het veld Verificatiealgoritme in de kopregels van beheer- en associatiepakketten. De meeste fabrikanten van draadloze klanten stelden dit veld op waarde 0 (Open authenticatie) en geven vervolgens aan dat zij later in het associatieproces de MAP-authenticatie willen doen. Cisco stelt de waarde anders in vanaf het begin van de associatie met de MAP-vlag.

Gebruik de authenticatiemethode die in deze lijst aangeeft of het netwerk klanten heeft die:

- Cisco client-Gebruik netwerk-EAP.
- Clients van derden (die Cisco-compatibele Uitbreidingen [CCX]-conforme producten omvatten)—Gebruik Open verificatie met MAP.
- Een combinatie van zowel Cisco als klanten van derden — Kies zowel netwerk-EAP als Open authenticatie met EAP.

CLI-configuratie

Dit document gebruikt deze configuraties:

- Een LEAP-configuratie die bestaat en werkt
- Cisco IOS-softwarerelease 12.2(15)JA voor Cisco IOS-softwarerelease 12.2(15)JA

AP
ap1#**show running-config**

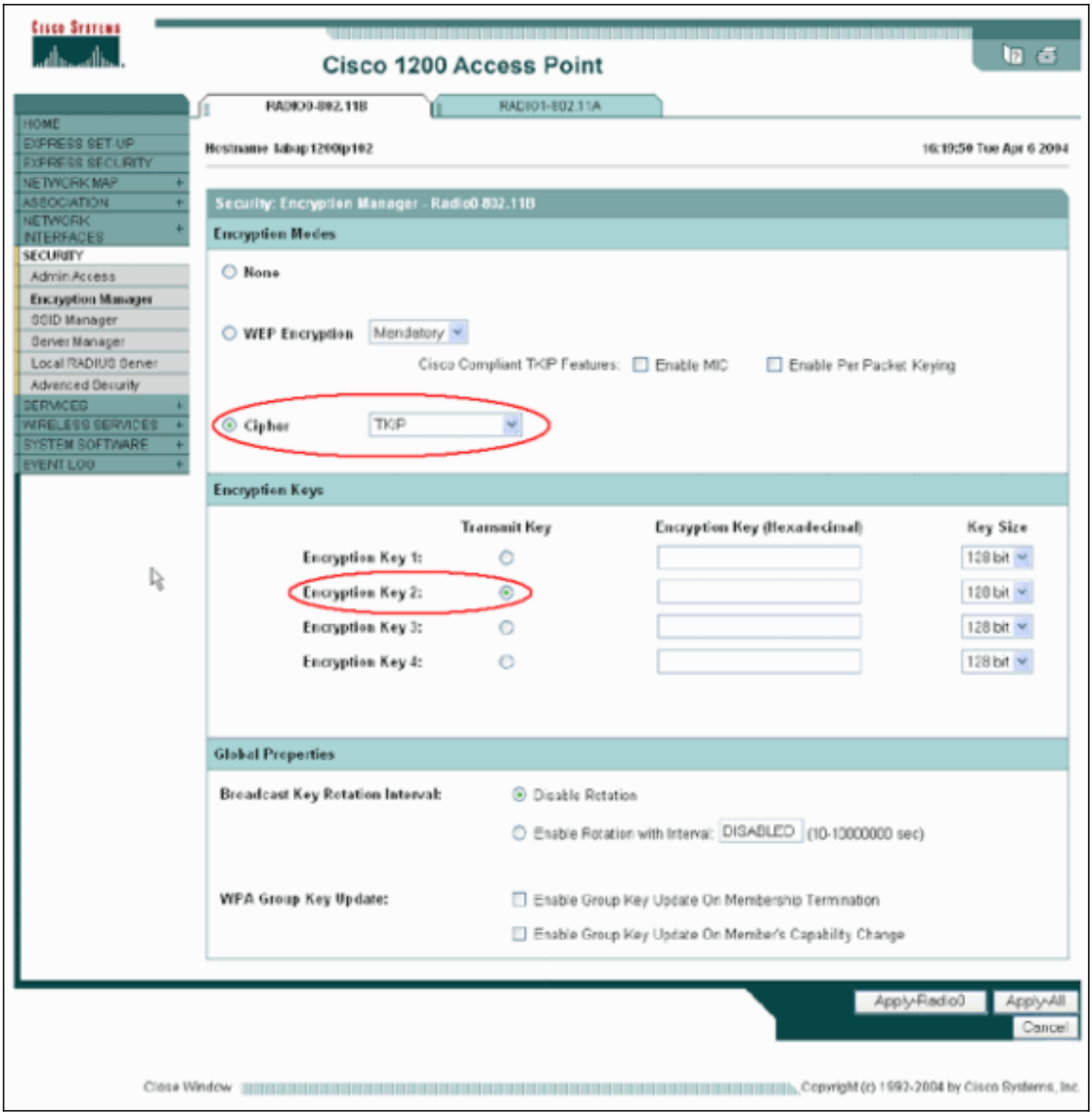
```
 Building configuration...
 .
 .
 .
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip
!--- 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-configuratie

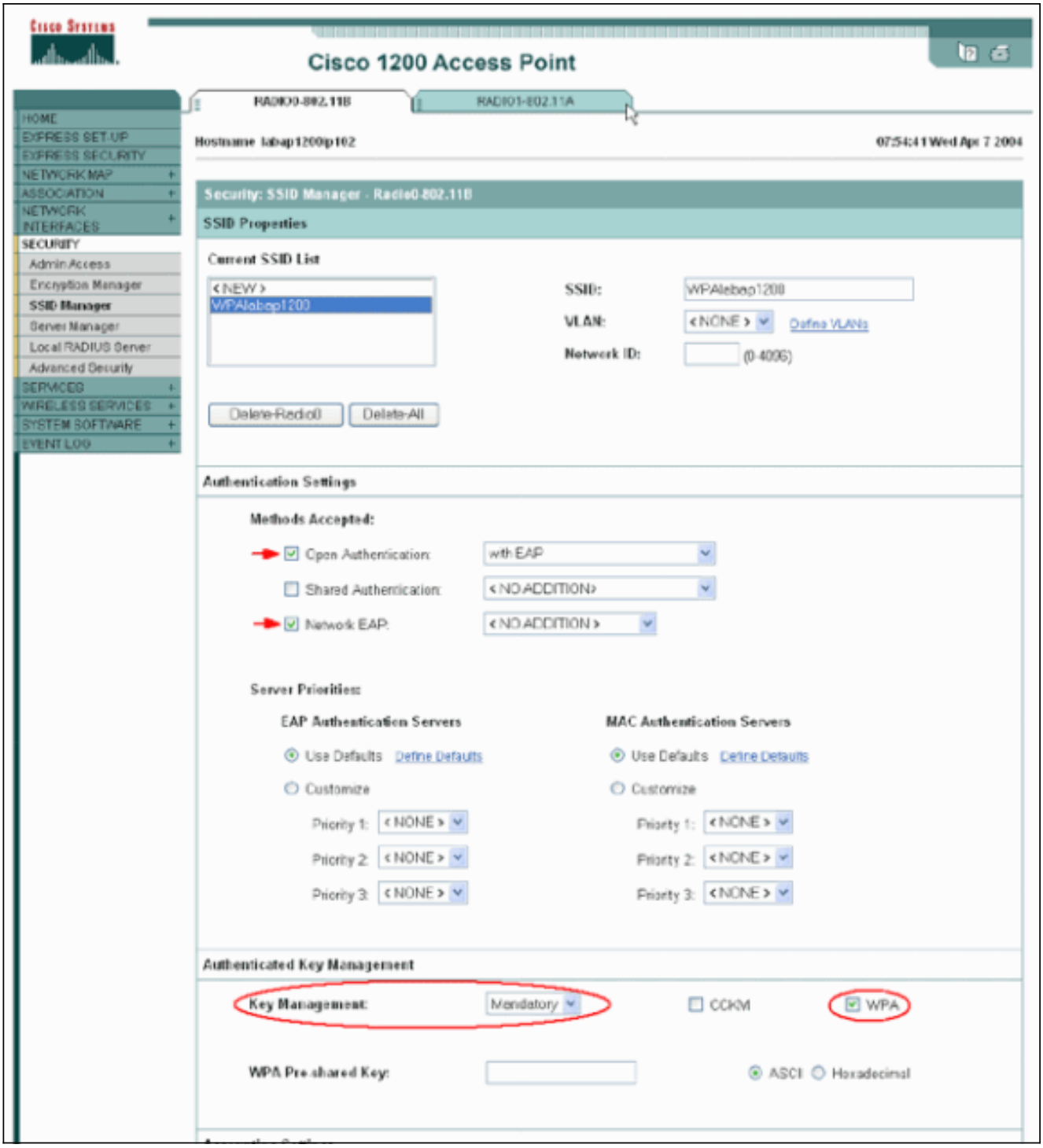
Voltooi deze stappen om AP voor WAP te configureren:

1. Voltooi deze stappen om de Encryptiebeheer in te stellen:Cipher inschakelen voor

TKIP.Schakel de waarde uit in Encryption Key 1.Stel encryptie-sleutel 2 in als de transmissiesleutel.Klik op **Toepassen-radio#**.



2. Voltooi deze stappen om de SSID Manager in te stellen:Selecteer de gewenste SSID in de huidige SSID-lijst.Kies een geschikte authenticatiemethode.Baseer deze beslissing op het type clientkaarten dat u gebruikt. Zie het gedeelte netwerk EAP of Open Verificatie met EAP van dit document voor meer informatie. Indien EAP werkte vóór de toevoeging van WAP, is een verandering waarschijnlijk niet nodig.Voltooi deze stappen om het sleutelbeheer mogelijk te maken:Kies de optie Verplicht in het vervolgkeuzemenu Key Management.Controleer het dialoogvenster WAP.Klik op **Toepassen-radio#**.

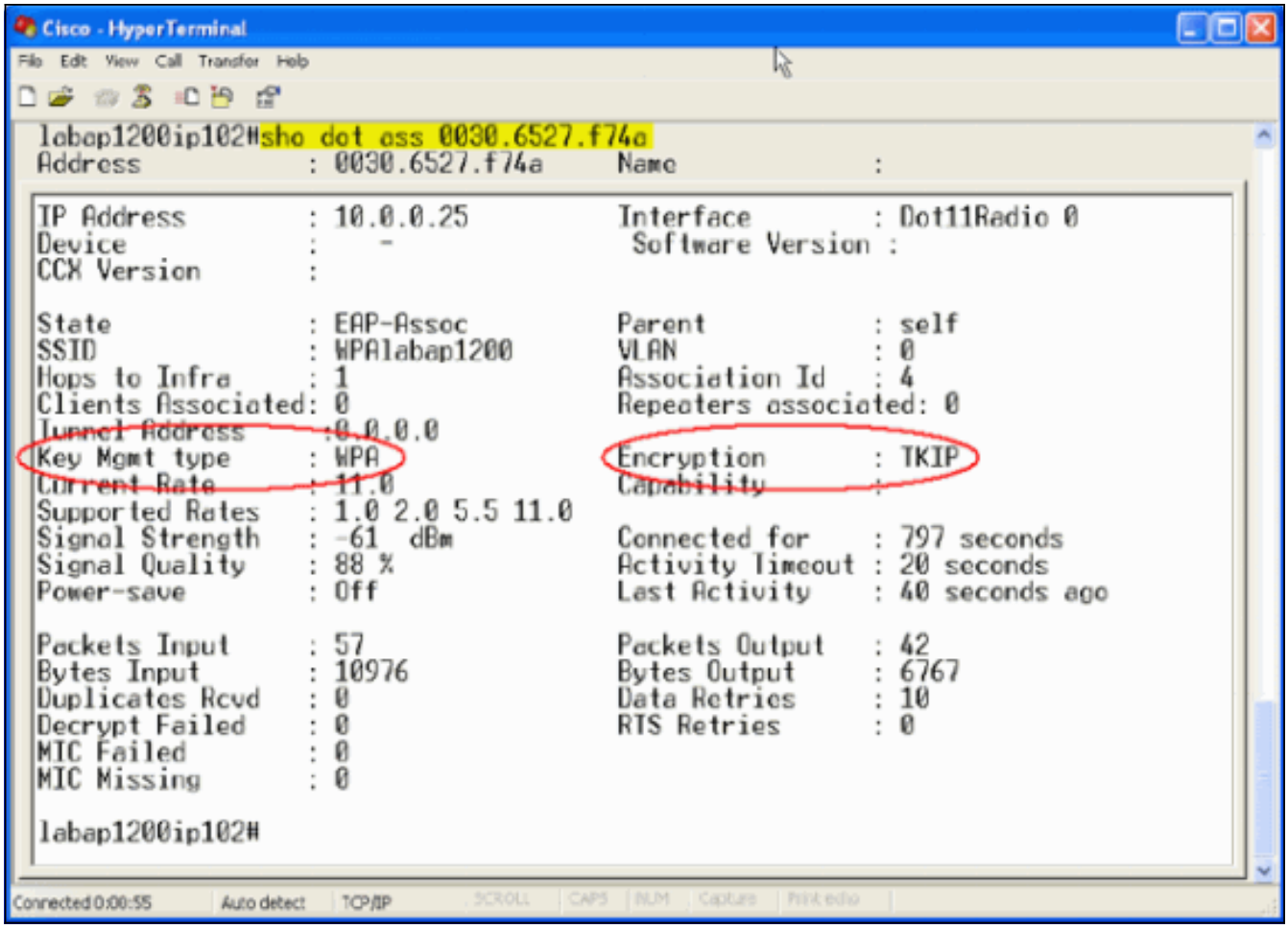


Verifiëren

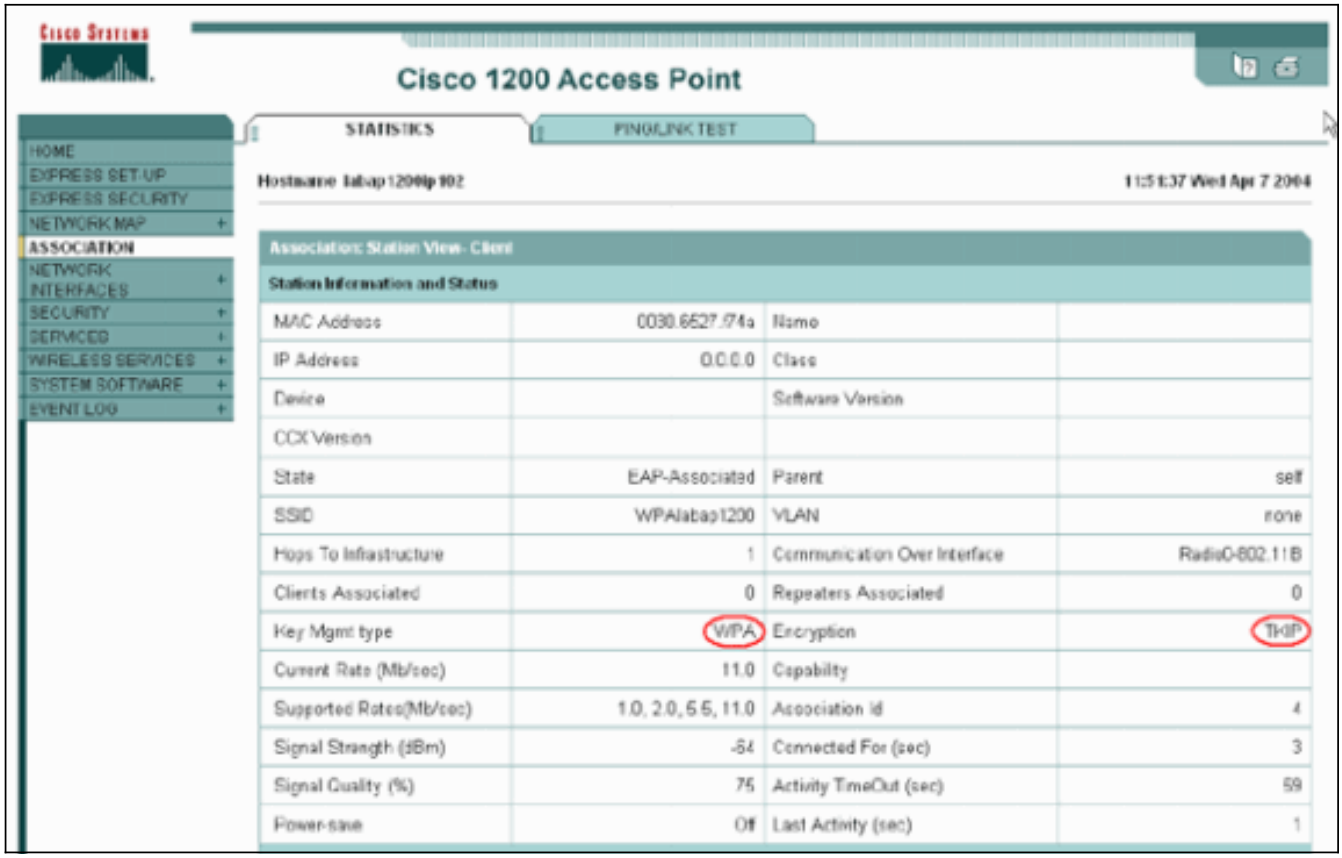
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toon dot11 associatie** *mac_address* - Deze opdracht geeft informatie weer over een specifiek geïdentificeerde verbonden client. Controleer dat de client onderhandelt over Key Management als **WAP** en Encryption als **TKIP**.



- De ingang van de Associatietabel voor een bepaalde client moet ook zeer belangrijk beheer als **WAP** en encryptie als **TKIP** aangeven. In de Associatietabel, klik op een bepaald MAC-adres voor een client om de details van de associatie voor die client te zien.



Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Procedure voor probleemoplossing

Deze informatie is relevant voor deze configuratie. Voltooi deze stappen om een oplossing voor uw configuratie te vinden:

1. Als deze configuratie van LEAP, EAP of PEAP niet grondig is getest vóór de implementatie van WAP, moet u deze stappen voltooien:Schakel tijdelijk de WAP-encryptie uit.Reinbaarheid van het juiste MAP.Bevestig dat de authenticatie werkt.
2. Controleer dat de configuratie van de client overeenkomt met die van de AP.Bijvoorbeeld, wanneer AP voor WAP en TKIP wordt gevormd, bevestig dat de instellingen overeenkomen met de instellingen die in de client worden gevormd.

Opdrachten voor probleemoplossing

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

Het zeer belangrijke beheer van WAP omvat een viervoudige handdruk nadat de MAP-verificatie met succes is voltooid. Je ziet deze vier berichten in debugs. Als EAP de client niet echt heeft geauthentiseerd of als de berichten niet worden weergegeven, moet u deze stappen uitvoeren:

1. Schakel tijdelijk WAP uit.
2. Reinbaarheid van het juiste MAP.
3. Bevestig dat de authenticatie werkt.

In deze lijst worden de specificaties beschreven:

- **debug dot11 a Manager keys**—Dit debug toont de handdruk die tussen AP en de client van WAP gebeurt terwijl parwise transient key (PTK) en group transient key (GTK) onderhandelen. Dit debug werd geïntroduceerd in Cisco IOS-softwarerelease 12.2(15)JA.Als er geen debug-uitvoer verschijnt, controleert u deze items:De terminal monitor **term mon** is geactiveerd (als u een Telnet sessie gebruikt).De uitwerpselen zijn ingeschakeld.De client is correct ingesteld voor WAP.Als het debug aantoont dat handtekeningen van PTK en/of GTK gebouwd maar niet geverifieerd zijn, controleer dan de van de Levering software van de WAP voor de juiste configuratie en de bijgewerkte versie.
- **debug dot11 a staat-machine**-Dit debug toont de verschillende staten van onderhandelingen die een client doorvoert zoals deze associeert en authentiek verklaart. De staatsnamen geven deze staten aan. Dit debug werd geïntroduceerd in Cisco IOS-softwarerelease 12.2(15)JA. Het debug ruimt de opdracht **debug dot11 a dot1x staatsmachine op** in Cisco IOS-softwarerelease 12.2(15)JA en hoger.
- **debug dot11 aaa dot1x state-machine**-This debug toont de verschillende staten van onderhandelingen die een cliënt door gaat zoals het associeert en authentiek verklaart. De staatsnamen geven deze staten aan. In Cisco IOS-softwarereleases die eerder zijn dan Cisco IOS-softwarerelease 12.2(15)JA, toont dit debug ook de onderhandeling over het WAP-beheer.

- **debug dot11 a authenticator proces** - Dit debug is vooral handig om problemen met onderhandelde communicatie te diagnosticeren. De gedetailleerde informatie laat zien wat elke deelnemer aan de onderhandelingen stuurt en toont de reactie van de andere deelnemer. U kunt dit debug ook gebruiken in combinatie met de opdracht **Straalverificatie** uitvoeren. Dit debug werd geïntroduceerd in Cisco IOS-softwarerelease 12.2(15)JA. Het debug vervalt de opdracht **debug dot11 a dot1x-proces** in Cisco IOS-softwarerelease 12.2(15)JA en hoger.
- **debug dot11 a dot1x proces**—Dit debug is behulpzaam om problemen bij het onderhandelen van communicatie te diagnosticeren. De gedetailleerde informatie laat zien wat elke deelnemer aan de onderhandelingen stuurt en toont de reactie van de andere deelnemer. U kunt dit debug ook gebruiken in combinatie met de opdracht **Straalverificatie** uitvoeren. In Cisco IOS-softwarereleases die eerder zijn dan Cisco IOS-softwarerelease 12.2(15)JA, toont dit debug de onderhandeling over het WAP-hoofdbeheer.

Gerelateerde informatie

- Cipuites en EFN configureren
- Verificatietypen configureren
- WAP2 - Wi-Fi beschermde toegang 2
- Configuratie van Wi-Fi beschermde Access 2 (WAP 2)
- Technische ondersteuning en documentatie – Cisco Systems