WPA 구성 개요

목차

소개

이 문서에서는 Wi-Fi Alliance 멤버가 사용하는 임시 보안 표준인 WPA(Wi-Fi Protected Access)의 샘플 구성을 제공합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 무선 네트워크 및 무선 보안 문제에 대한 철저한 지식
- EAP(Extensible Authentication Protocol) 보안 방법에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 기반 액세스 포인트(AP)
- Cisco IOS Software 릴리스 12.2(15)JA 이상**참고:** Cisco IOS Software 릴리스 12.2(11)JA 이상에서 WPA가 지원되는 경우에도 최신 Cisco IOS 소프트웨어 릴리스를 사용하십시오.최신 Cisco IOS Software 릴리스를 얻으려면 다운로드(등록된 고객만 해당)를 참조하십시오.

- WPA 호환 네트워크 인터페이스 카드(NIC) 및 WPA 호환 클라이언트 소프트웨어

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 이론

WEP와 같은 무선 네트워크의 보안 기능은 취약합니다.Wi-Fi Alliance(또는 WECA) 산업 그룹은 무선 네트워크에 대한 차세대 임시 보안 표준을 고안했습니다.이 표준은 IEEE 조직이 802.11i 표준을 비준할 때까지 약점에 대한 방어를 제공합니다.

이 새로운 구성표는 현재 EAP/802.1x 인증 및 동적 키 관리를 기반으로 하며 더 강력한 암호 암호화를 추가합니다.클라이언트 장치와 인증 서버가 EAP/802.1x 연결을 만든 후 WPA 키 관리는 AP와 WPA 호환 클라이언트 장치 간에 협상됩니다.

Cisco AP 제품은 레거시 WEP 기반 EAP 클라이언트(레거시 또는 키 관리 없음)가 모두 WPA 클라이언트와 함께 작동하는 하이브리드 구성을 제공합니다.이 컨피그레이션을 마이그레이션 모드라고 합니다.마이그레이션 모드를 사용하면 단계별 접근 방식으로 WPA로 마이그레이션할 수 있습니다.이 문서에서는 마이그레이션 모드를 다루지 않습니다.이 문서에서는 순수 WPA 보안 네트워크에 대한 개요를 제공합니다.

WPA는 기업 또는 기업 수준의 보안 문제 외에도 소규모 사무실, 홈 오피스(SOHO) 또는 홈 무선 네트워크에서 사용할 수 있는 WPA-PSK(Pre-Shared Key Version)도 제공합니다.Cisco Aironet Client Utility(ACU)는 WPA-PSK를 지원하지 않습니다.Microsoft Windows의 Wireless Zero Configuration 유틸리티는 다음 유틸리티와 마찬가지로 대부분의 무선 카드에 대해 WPA-PSK를 지원합니다.

- Meetinghouse Communications의 AEGIS 클라이언트**참고:** Meetinghouse AEGIS 제품 라인에 대한 EOS 및 EOL 발표를 참조하십시오.
- Funk Software의 Odyssey 클라이언트**참고:** Juniper Networks 고객 지원 센터를 참조하십시오.
- 일부 제조업체의 OEM(Original Equipment Manufacturer) 클라이언트 유틸리티

다음과 같은 경우 WPA-PSK를 구성할 수 있습니다.

- 암호화 관리자 탭에서 암호화 모드를 TKIP(Cipher Temporal Key Integrity Protocol)로 정의합니다.
- GUI의 SSID(Service Set Identifier) Manager 탭에서 인증 유형, 인증된 키 관리 사용 및 사전 공유 키를 정의합니다.
- Server Manager 탭에는 구성이 필요하지 않습니다.

CLI(Command Line Interface)를 통해 WPA-PSK를 활성화하려면 다음 명령을 입력합니다.컨피그레이션 모드에서 시작:

```
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
```

참고: 이 섹션에서는 WPA-PSK와 관련된 구성만 제공합니다.이 섹션의 컨피그레이션은 WPA-PSK를 활성화하는 방법에 대한 이해를 제공하기 위한 것이며 이 문서의 초점이 아닙니다.이 문서에서는 WPA를 구성하는 방법에 대해 설명합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

구성

WPA는 현재 EAP/802.1x 방법을 기반으로 합니다.이 문서에서는 WPA에 참여하기 위해 구성을 추가하기 전에 작동하는 LEAP(Light EAP), EAP 또는 PEAP(Protected EAP) 컨피그레이션이 있다고 가정합니다.

이 섹션에서는 이 문서에 설명된 기능을 구성하기 위한 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 EAP 또는 EAP를 통한 개방 인증

EAP/802.1x 기반 인증 방법에서는 네트워크 EAP와 EAP를 통한 개방 인증 간의 차이점이 무엇인지 질문할 수 있습니다.이러한 항목은 관리 및 연결 패킷의 헤더에 있는 인증 알고리즘 필드의 값을 참조합니다.대부분의 무선 클라이언트 제조업체는 이 필드를 값 0(Open 인증)으로 설정한 다음 연결 프로세스의 뒷부분에서 EAP 인증을 수행하고자 한다는 신호를 보냅니다.Cisco는 네트워크 EAP 플래그와의 연결 시작에서 값을 다르게 설정합니다.

네트워크에 다음과 같은 클라이언트가 있는지 여부를 나타내는 인증 방법을 사용합니다.

- Cisco 클라이언트 - 네트워크 EAP를 사용합니다.
- 타사 클라이언트(CCX[Cisco Compatible Extensions] 호환 제품 포함) - EAP를 통해 개방형 인증을 사용합니다.
- Cisco 및 타사 클라이언트의 조합 - Network-EAP 및 Open authentication with EAP를 모두 선택합니다.

CLI 컨피그레이션

이 문서에서는 다음 구성을 사용합니다.

- 존재하고 작동하는 LEAP 컨피그레이션
- Cisco IOS 소프트웨어 기반 AP용 Cisco IOS 소프트웨어 릴리스 12.2(15)JA

AP

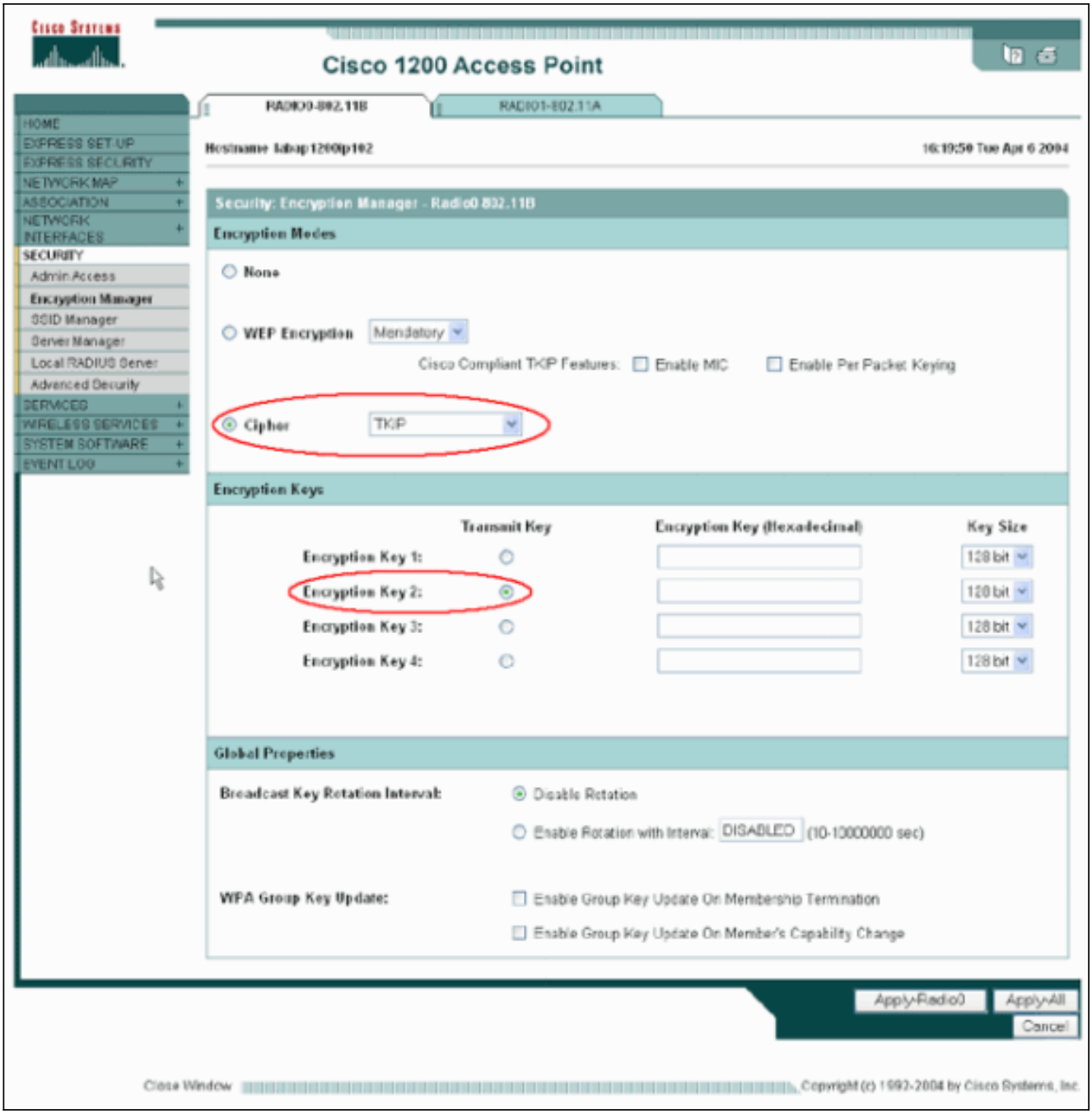
```
ap1#show running-config
 Building configuration...
 .
 .
 .
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
```

```
.
.
.
!
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 컨피그레이션

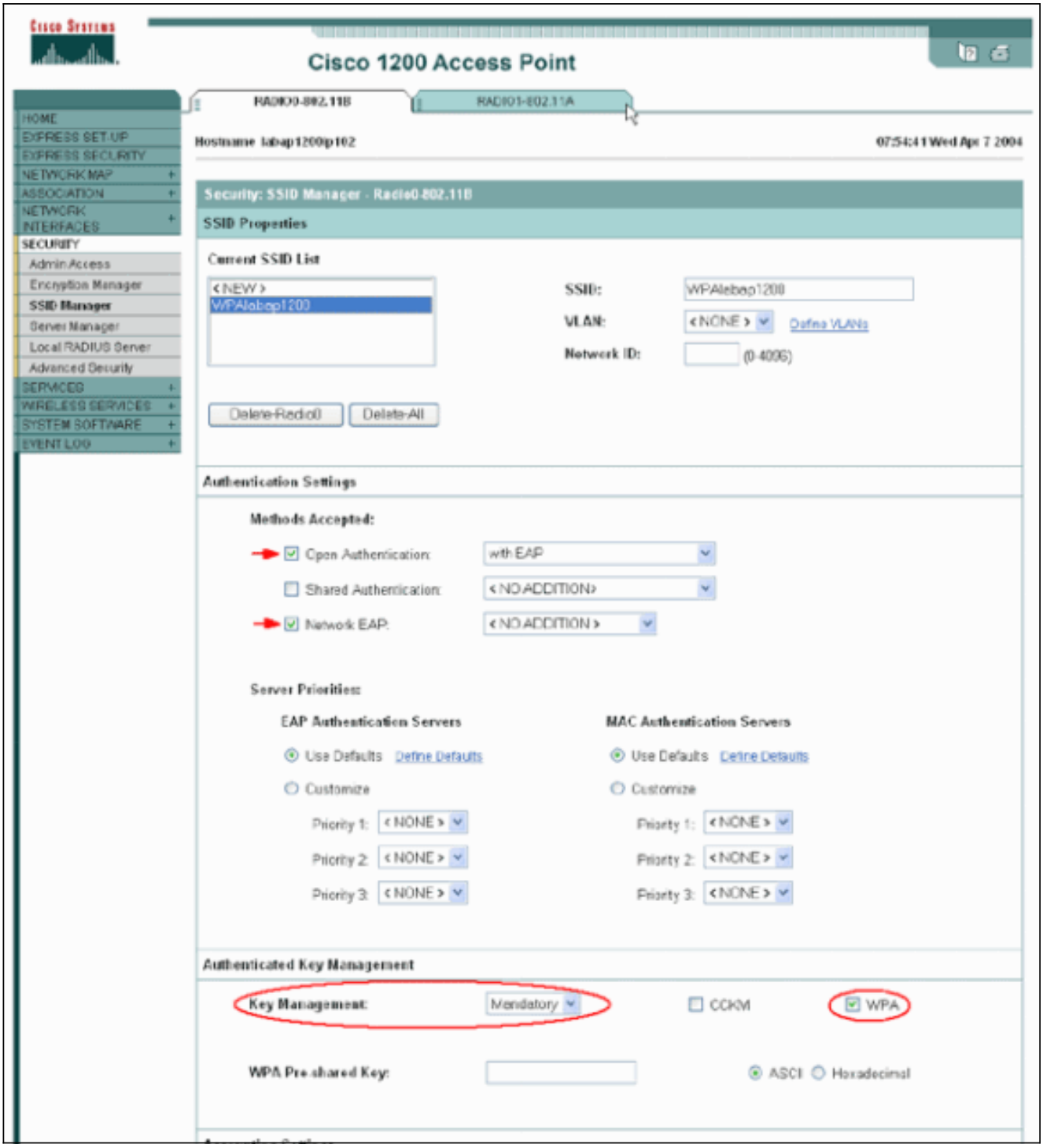
WPA용 AP를 구성하려면 다음 단계를 완료하십시오.

1. 암호화 관리자를 설정하려면 다음 단계를 완료합니다.TKIP에 대해 암호를 활성화합니다.암호화 키 1의 값을 지웁니다.암호화 키 2를 전송 키로 설정합니다.Apply-Radio*#를 클릭합니다*
   .



2. SSID 관리자를 설정하려면 다음 단계를 완료합니다.현재 SSID 목록에서 원하는 SSID를 선택합니다.적절한 인증 방법을 선택합니다.이 결정은 사용하는 클라이언트 카드 유형에 따라 결정됩니다.자세한 내용은 이 문서의 [네트워크 EAP 또는 EAP를 통한 인증](#) 열기 섹션을 참조하십시오.WPA를 추가하기 전에 EAP가 작동했다면 변경할 필요가 없을 수 있습니다.키 관리를 활성화하려면 다음 단계를 완료하십시오.Key Management 드롭다운 메뉴에서 Mandatory를 선택합니다.WPA 확인란을 선택합니다.Apply-**Radio#*를 클릭합니다***

.

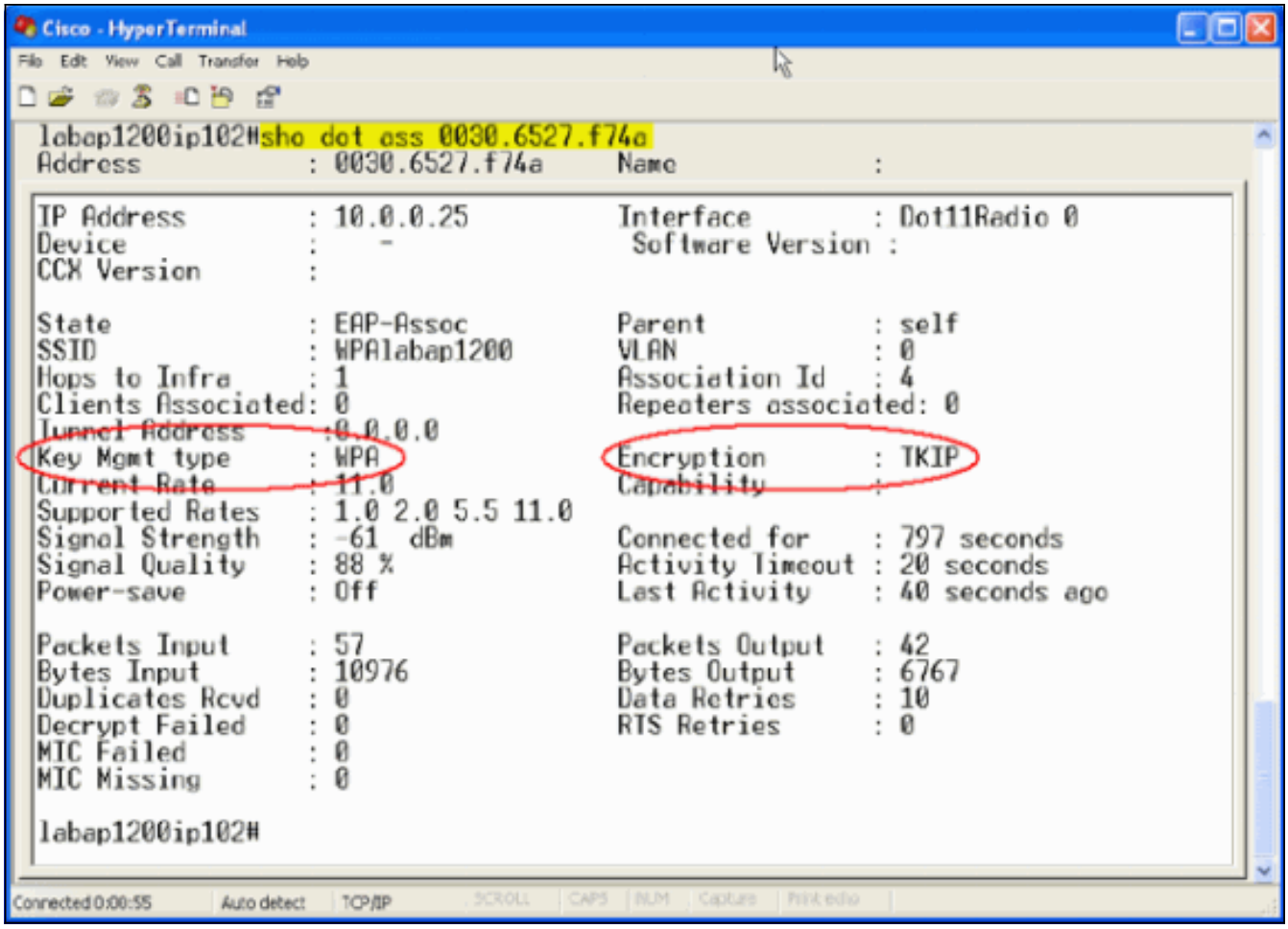


다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

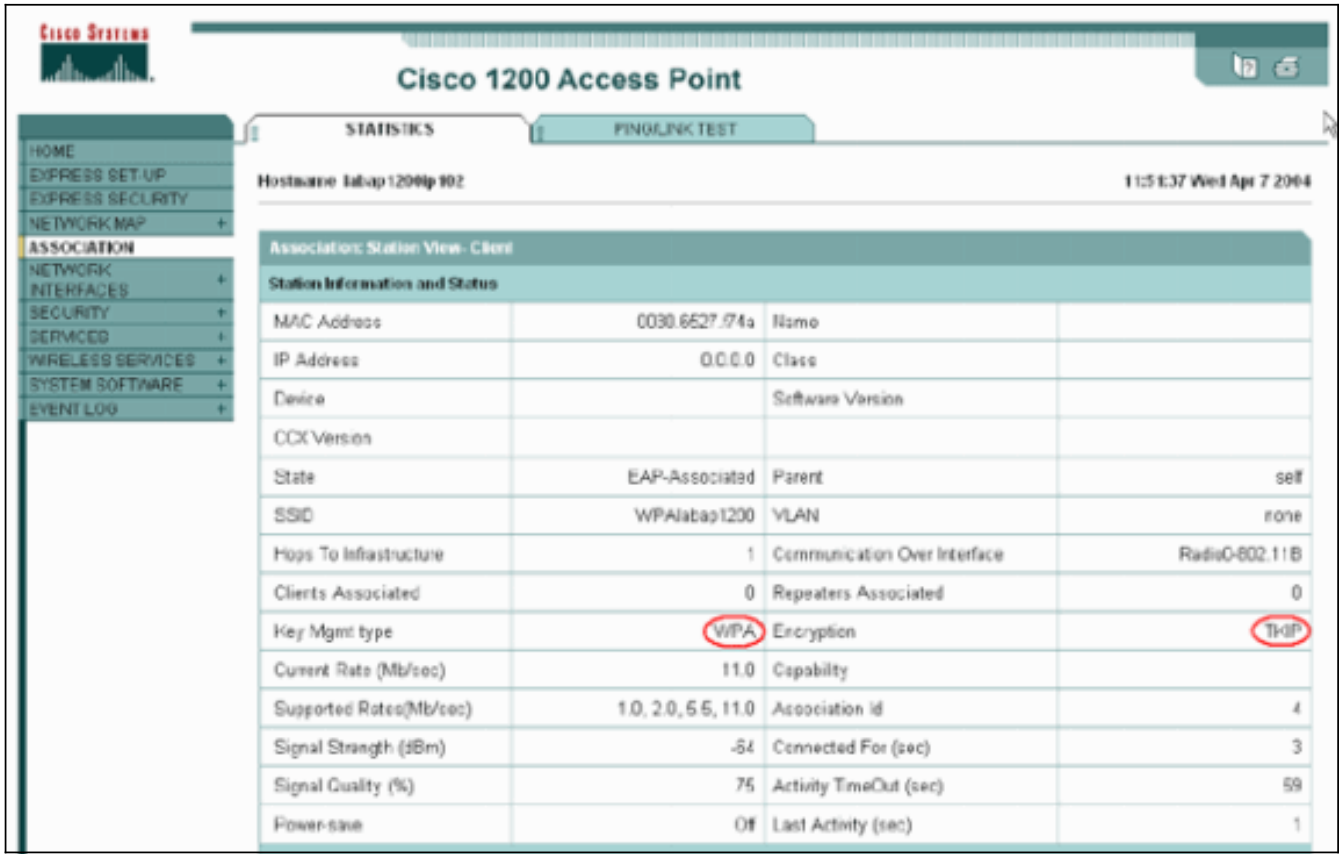
Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show dot11 association** *mac_address*—이 명령은 특별히 식별된 연결된 클라이언트에 대한 정보를 표시합니다.클라이언트가 키 관리를 WPA로, **TKIP**로, 암호화를 **협상하는지 확인합니다**
  .



- 특정 클라이언트에 대한 연결 테이블 항목도 키 관리를 WPA로, **암호화**를 TKIP로 나타내야 합니다.Association(연결) 테이블에서 클라이언트의 특정 MAC 주소를 클릭하여 해당 클라이언트에 대한 연결 세부 정보를 확인합니다

.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 절차

이 정보는 이 컨피그레이션과 관련이 있습니다.컨피그레이션 문제를 해결하려면 다음 단계를 완료하십시오.

1. WPA 구현 전에 이 LEAP, EAP 또는 PEAP 컨피그레이션이 완전히 테스트되지 않은 경우 다음 단계를 완료해야 합니다.WPA 암호화 모드를 일시적으로 비활성화합니다.적절한 EAP를 다시 활성화합니다.인증이 작동하는지 확인합니다.
2. 클라이언트 컨피그레이션이 AP와 일치하는지 확인합니다.예를 들어 WPA와 TKIP에 대해 AP가 구성된 경우 설정이 클라이언트에 구성된 설정과 일치하는지 확인합니다.

문제 해결 명령

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

WPA 키 관리에는 EAP 인증이 성공적으로 완료된 후 4방향 핸드셰이크가 포함됩니다.이 네 개의 메시지를 디버그에 표시할 수 있습니다.EAP가 클라이언트를 성공적으로 인증하지 않거나 메시지가 표시되지 않으면 다음 단계를 완료합니다.

1. WPA를 일시적으로 비활성화합니다.
2. 적절한 EAP를 다시 활성화합니다.
3. 인증이 작동하는지 확인합니다.

이 목록에서는 디버그에 대해 설명합니다.

- **debug dot11 aaa manager keys** - 이 디버그는 AP와 WPA 클라이언트 사이에 PTK(pairwise transient key) 및 GTK(group transient key) 협상 중 발생하는 핸드셰이크를 표시합니다.이 디버그는 Cisco IOS Software 릴리스 12.2(15)JA에서 도입되었습니다.디버그 출력이 표시되지 않으면 다음 항목을 확인하십시오.터미널 모니터 **용어 월**이 활성화됩니다(텔넷 세션을 사용하는 경우).디버그가 활성화됩니다.클라이언트는 WPA에 맞게 구성됩니다.디버그에 PTK 및/또는 GTK 핸드셰이크가 작성되었지만 확인되지 않은 것으로 표시되면 WPA 신청자 소프트웨어에서 올바른 컨피그레이션 및 최신 버전을 확인하십시오.
- **debug dot11 aaa authenticator state-machine** - 이 디버그는 클라이언트가 연결하고 인증하면서 거치는 다양한 협상 상태를 표시합니다.상태 이름은 이러한 상태를 나타냅니다.이 디버그는 Cisco IOS Software 릴리스 12.2(15)JA에서 도입되었습니다.디버그는 Cisco IOS Software 릴리스 12.2(15)JA 이상에서 **debug dot11 aaa dot1x state-machine** 명령을 사용하지 않습니다.
- **debug dot11 aaa dot1x state-machine**—이 디버그는 클라이언트가 연결하고 인증하면서 거치는 다양한 협상 상태를 표시합니다.상태 이름은 이러한 상태를 나타냅니다.Cisco IOS Software Release 12.2(15)JA 이전 버전의 Cisco IOS Software 릴리스에서는 이 디버그도 WPA 키 관리 협상을 보여줍니다.
- **debug dot11 aaa authenticator process** - 이 디버그는 협상된 통신 문제를 진단하는 데 가장 유용합니다.세부 정보는 협상의 각 참가자가 보내는 내용을 표시하고 다른 참가자의 응답을 표시합니다.이 디버그를 debug radius **authentication** 명령과 함께 사용할 수도 있습니다.이 디버그는 Cisco IOS Software 릴리스 12.2(15)JA에서 도입되었습니다.디버그는 Cisco IOS Software 릴리스 12.2(15)JA 이상에서 **debug dot11 aaa dot1x process** 명령을 사용하지 않습니다.

- **debug dot11 aaa dot1x process** - 이 디버그는 협상된 통신 문제를 진단하는 데 유용합니다.세부 정보는 협상의 각 참가자가 보내는 내용을 표시하고 다른 참가자의 응답을 표시합니다.이 디버그를 debug radius **authentication** 명령과 함께 사용할 수도 있습니다.Cisco IOS Software Release 12.2(15)JA 이전 버전의 Cisco IOS Software에서 이 디버그는 WPA 키 관리 협상을 보여줍니다.

관련 정보

- 암호 그룹 및 WEP 구성
- 인증 유형 구성
- WPA2 - Wi-Fi 보호 액세스 2
- WPA 2(Wi-Fi Protected Access 2) 구성
- 기술 지원 및 문서 – Cisco Systems