Visão Geral da Configuração do WPA

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Material de Suporte
Convenções
Configurar
EAP de rede ou autenticação aberta com EAP
Configuração de CLI
Configuração de GUI
Verificar
Troubleshooting
Procedimento de solução de problemas
Comandos de solução de problemas
Informações Relacionadas

Introdução

Este documento fornece uma configuração de exemplo para WPA (Wi-Fi Protected Access), o padrão de segurança temporário usado pelos membros da Wi-Fi Alliance.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento completo da rede Wireless e problemas de segurança Wireless
- Conhecimento de métodos de segurança do Extensible Authentication Protocol (EAP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Access point com base no software de Cisco IOS® (AP)
- Cisco IOS Software Release 12.2(15)JA ou Mais Recente**Nota:** Preferivelmente, use o Cisco IOS Software Release o mais atrasado, mesmo que o WPA seja apoiado no Cisco IOS Software Release 12.2(11)JA e Mais Recente. A fim obter o Cisco IOS Software Release o

mais atrasado, refira transferências (clientes registrados somente).
- Um Network Interface Cards WPA-complacente (NIC) e seu software do cliente WPA-complacente

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Material de Suporte

Os recursos de segurança em uma rede sem fio, como WEP, são fracos. O grupo industrial de Alliance do Wi-fi (ou WECA) planejou uma próxima geração, padrão de segurança provisório para redes Wireless. O padrão fornece a defesa contra fraquezas até que a organização IEEE ratifique o padrão 802.11i.

O novo esquema é construído sobre a autenticação e gerenciamento dinâmico de chave EAP/802.1x atual, e acrescenta uma criptografia de cifra mais forte. Após o dispositivo do cliente e o Authentication Server faça uma associação do EAP/802.1x, o gerenciamento chave WPA é negociado entre o AP e o dispositivo do cliente WPA-complacente.

O Produtos de Cisco AP igualmente prevê uma configuração híbrida em que ambos os clientes EAP baseado em WEP do legado (com legado ou nenhum gerenciamento chave) trabalham conjuntamente com clientes de WPA. Esta configuração é referida como o modo de migração. O modo de migração permite uma aproximação posta em fase migrar ao WPA. Este documento não cobre o modo de migração. Este documento fornece um esboço para uma rede WPA-fixada pura.

Além do que interesses de segurança da empresa ou do nível corporativo, o WPA igualmente fornece uma versão da chave pré-compartilhada (WPA-PSK) que seja pretendida para o uso no escritório pequeno, escritório home (SOHO) ou nas redes Wireless home. O utilitário de cliente do Cisco Aironet (ACU) não apoia o WPA-PSK. O utilitário de configuração do Sem fio zero de Microsoft Windows apoia o WPA-PSK para a maioria de placas Wireless, como fazem estas utilidades:

- Aegis cliente dos Meetinghouse Communications**Nota:** Refira o EOS e o anúncio de EoL para a linha de produto da ÉGIDE de Meetinghouse.
- Cliente Odyssey do software Funk**Nota:** Refira o centro de suporte de cliente de Juniper Networks .
- Utilitários de cliente do Original Equipment Manufacturer (OEM) de alguns fabricantes

Você pode configurar o WPA-PSK quando:

- Você define o modo de criptografia como o Temporal Key Integrity Protocol (TKIP) da cifra na aba do gerenciador de criptografia.
- Você define o tipo do autenticação, o uso do gerenciamento chave autenticado, e a chave pré-compartilhada no guia do gerenciador do Service Set Identifier (SSID) do GUI.
- Nenhuma configuração é necessária na guia Server Manager.

A fim permitir o WPA-PSK através do comando line interface(cli), incorpore estes comandos. Parta do modo de configuração:

```
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: Esta seção fornece somente a configuração que é relevante ao WPA-PSK. A configuração nesta seção é dar-lhe somente uma compreensão em como permitir o WPA-PSK e não é o foco deste documento. Este documento explica como configurar o WPA.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

O WPA é construído a partir dos métodos de EAP/802.1x atuais. Este documento supõe que você tem uma luz EAP (PULO), EAP, ou a configuração protegida EAP (PEAP) que trabalha antes que você adicione a configuração a fim contratar o WPA.

Esta seção apresenta as informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

EAP de rede ou autenticação aberta com EAP

Em todo o método de autenticação EAP/802.1x-based, você pode questionar o que as diferenças estão entre a Rede EAP e a autenticação aberta com EAP. Esses itens se referem a valores no campo Authentication Algorithm (Algoritmo de autenticação) nos cabeçalhos dos pacotes de gerenciamento e associação. A maioria de fabricantes do grupo dos clientes Wireless este campo no valor 0 (autenticação aberta), e sinalizam então seu desejo fazer mais tarde a autenticação de EAP no processo de associação. A Cisco define o valor de maneira diferente, desde o início da associação com o flag Network EAP.

Use o método de autenticação que esta lista indica se sua rede tem os clientes que são:

- Clientes Cisco — Use a Rede EAP.
- Clientes da terceira (que incluem extensões compatível Cisco que o [CCX] - produtos em conformidade) — usa a autenticação aberta com EAP.
- Uma combinação de ambo o Cisco e clientes da terceira — escolha a Rede EAP e a autenticação aberta com EAP.

Configuração de CLI

Este documento utiliza as seguintes configurações:

- Uma configuração leap que exista e trabalhe
- Cisco IOS Software Release 12.2(15)JA para o Cisco IOS AP com base no software

AP

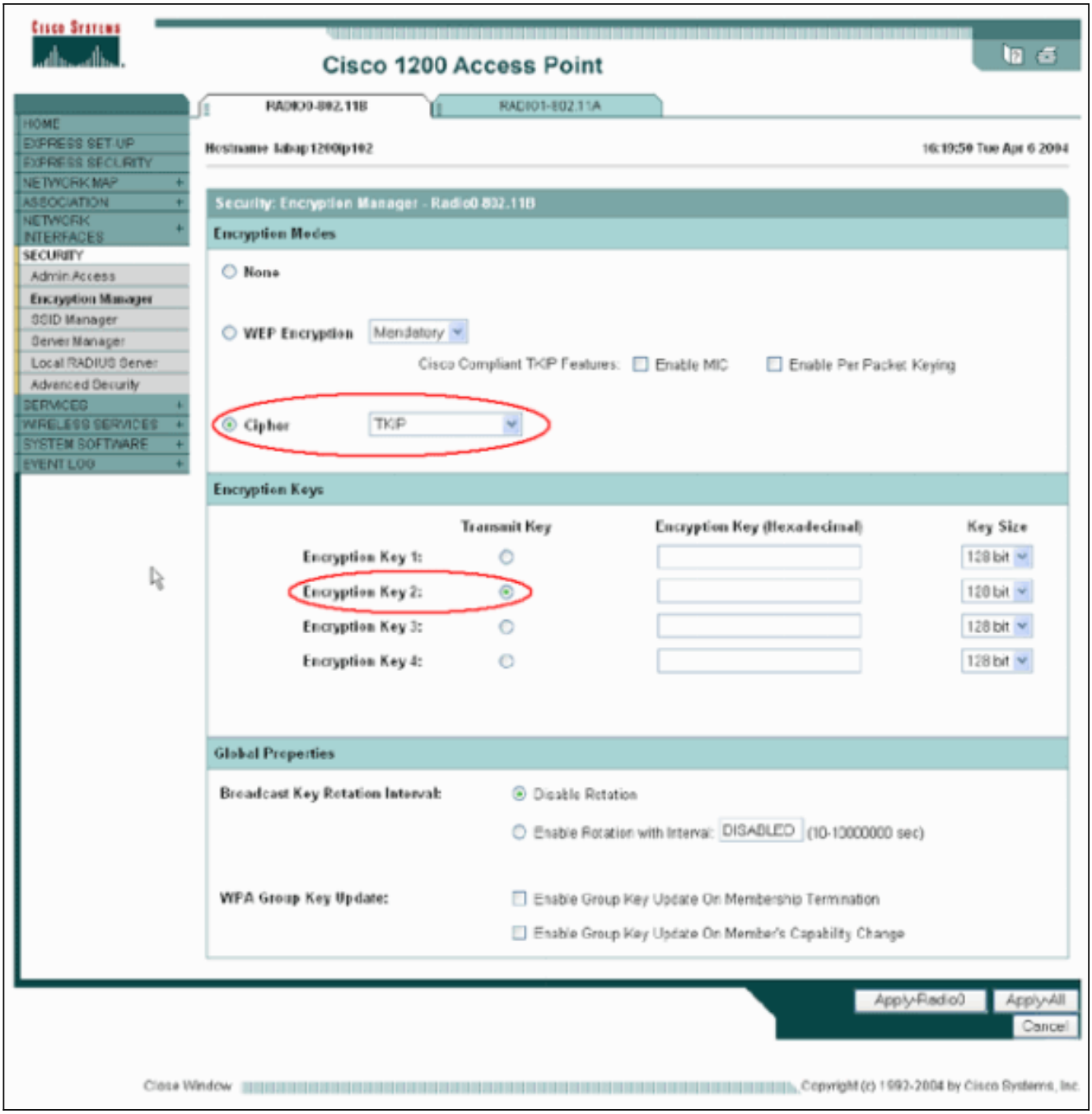
```
ap1#show running-config Building configuration... . . .
aaa new-model ! aaa group server radius rad_eap server
192.168.2.100 auth-port 1645 acct-port 1646 . . aaa
authentication login eap_methods group rad_eap . . . !
bridge irb ! interface Dot11Radio0 no ip address no ip
```

```
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
```

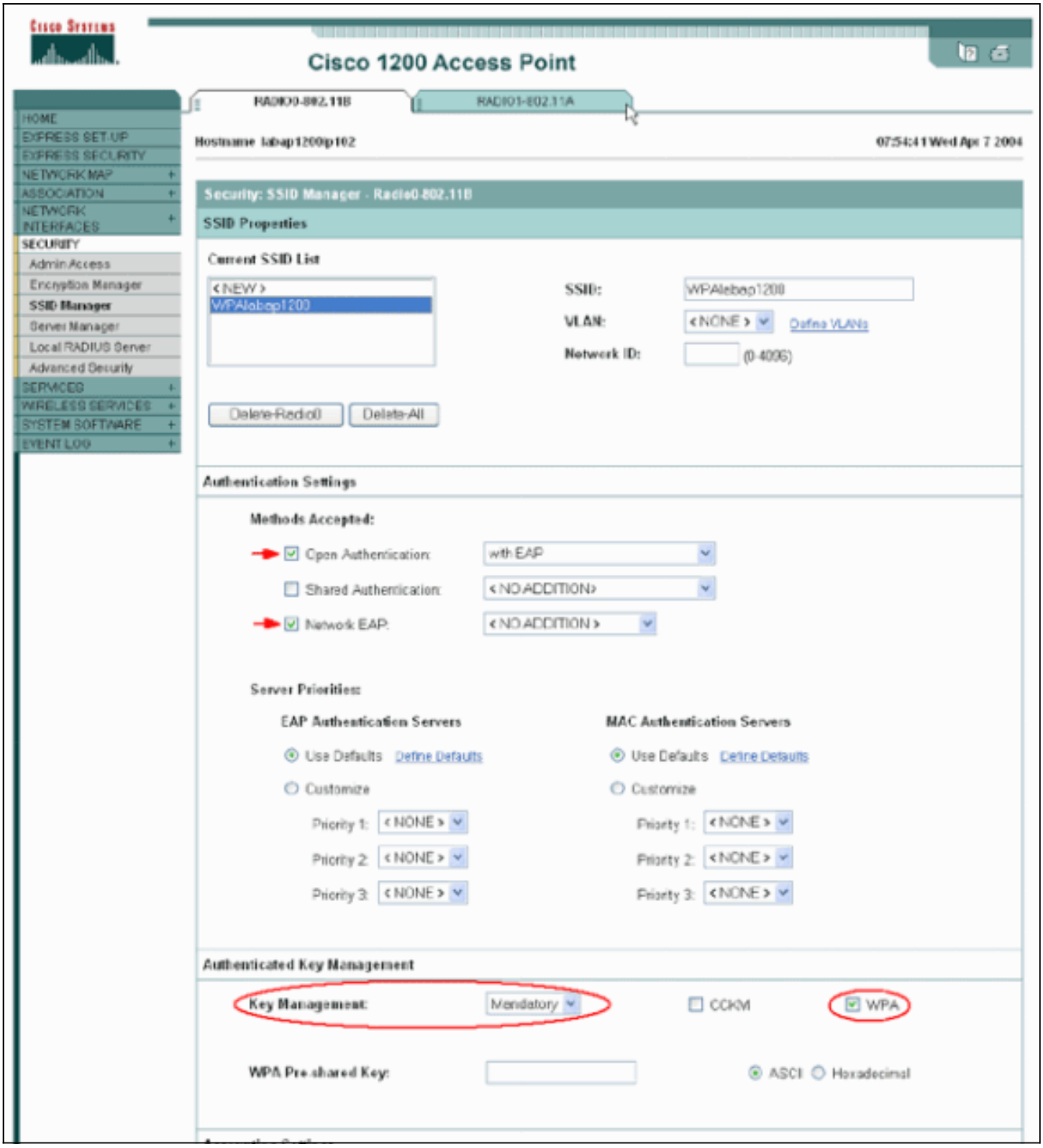
Configuração de GUI

Termine estas etapas a fim configurar o AP para o WPA:

1. Termine estas etapas a fim estabelecer o gerenciador de criptografia:Habilitar Cipher para TKIP.Cancele o valor na chave de criptografia 1.Ajuste a chave de criptografia 2 como a chave transmissora.Clique o Aplicar-**rádio**
   #.



2. Termine estas etapas a fim estabelecer o gerenciador de SSID:Selecione o SSID desejado da lista atual SSID.Escolha um método de autenticação apropriado.Baseie esta decisão no tipo de cartões do cliente que você usa. Veja a rede EAP ou a autenticação aberta com seção EAP deste documento para mais informação. Se o EAP trabalhou antes da adição de WPA, uma mudança não é provavelmente necessária.Termine estas etapas a fim permitir o gerenciamento chave:Escolha **imperativo do** menu suspenso do gerenciamento chave.Verifique a caixa de verificação WPA.Clique o Aplicar-**rádio #**.

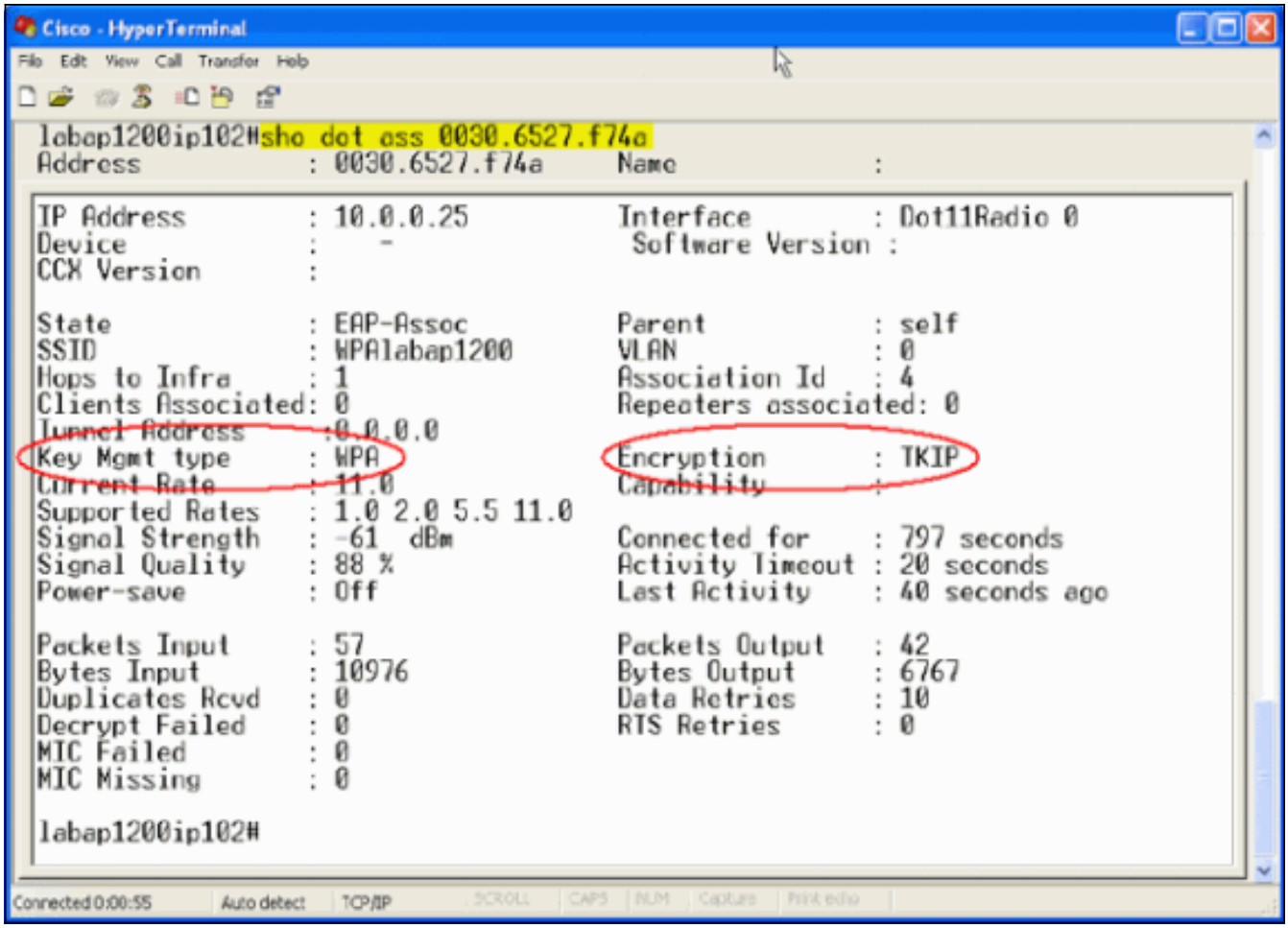


Verificar

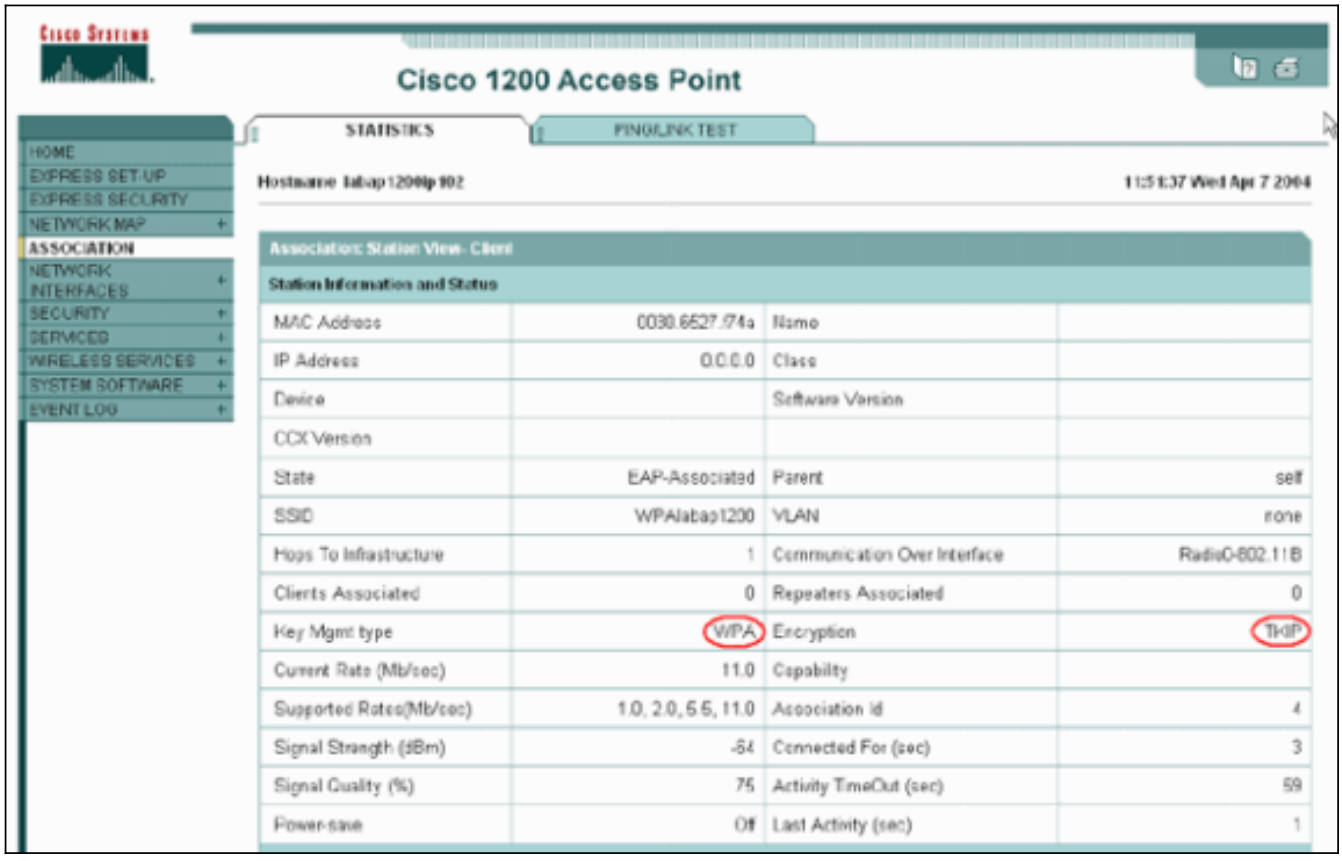
Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre o** *mac_address da* **associação do dot11** — Este comando indica a informação sobre um cliente associado especificamente identificado. Verifique que o cliente negocia o gerenciamento chave como o **WPA** e a criptografia como o **TKIP**.



- A entrada de tabela da associação para um cliente específico deve igualmente indicar o gerenciamento chave como o **WPA** e a criptografia como o **TKIP**. Na tabela de associação, clique um endereço MAC particular para um cliente a fim ver os detalhes da associação para esse
cliente.



Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Procedimento de solução de problemas

Essas informações são relevantes para esta configuração. Execute estes passos para fazer troubleshoot da sua configuração:

1. Se esta PULO, EAP, ou configuração de PEAP não foram testados completamente antes da implementação WPA, você deve terminar estas etapas:Desabilite temporariamente o modo de criptografia WPA.Reenable o EAP apropriado.Confirme que a autenticação trabalha.
2. Verifique que a configuração do cliente combina aquela do AP.Por exemplo, quando o AP é configurado para o WPA e o TKIP, confirme que os ajustes combinam os ajustes que são configurados no cliente.

Comandos de solução de problemas

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

O gerenciamento chave WPA envolve um aperto de mão de quatro vias depois que a autenticação de EAP termina com sucesso. Você pode ver que estas quatro mensagens debugam dentro. Se o EAP não autentica com sucesso o cliente ou se você não vê as mensagens, termine estas etapas:

1. Desabilite temporariamente o WPA.
2. Reenable o EAP apropriado.
3. Confirme que a autenticação trabalha.

Esta lista descreve debuga:

- **debugar chaves do gerente aaa do dot11** — Isto debuga mostras o aperto de mão que acontece entre o AP e o cliente de WPA como a chave por pares transiente (PTK) e a chave transiente do grupo (GTK) negocia. Isto debuga foi introduzido no Cisco IOS Software Release 12.2(15)JA.Se nenhum resultado do debug aparece, verifique estes artigos:**O termo** terminal **segunda-feira do** monitor é permitido (se você usa uma sessão de Telnet).Debuga são permitidos.O cliente é configurado apropriadamente para o WPA.Se debugar mostra que o PTK e/ou os handshakes de GTK estão construídos mas não verificados, verifique o software suplicante de WPA para ver se há a configuração correta e a versão atualizada.
- **debugar a estado-máquina do autenticador aaa do dot11** — Isto debuga mostras os vários estados de negociações que um cliente vai completamente enquanto associam e autenticam. Os nomes do estado indicam estes estados. Isto debuga foi introduzido no Cisco IOS Software Release 12.2(15)JA. Os obsoletes debugar o **comando debug dot11 aaa dot1x state-machine no** Cisco IOS Software Release 12.2(15)JA e Mais Recente.
- **debugar a estado-máquina do dot1x aaa do dot11** — Isto debuga mostras os vários estados de negociações que um cliente vai completamente enquanto associam e autenticam. Os nomes do estado indicam estes estados. Nos Cisco IOS Software Release que estão mais

adiantados do que o Cisco IOS Software Release 12.2(15)JA, isto debuga igualmente mostra a negociação do gerenciamento chave WPA.

- **debugar o processo do autenticador aaa do dot11** — Isto debuga é o mais útil diagnosticar problemas com comunicações negociadas. A informação detalhada mostra o que cada participante na negociação envia e mostra a resposta do outro participante. Você pode igualmente usar este debuga conjuntamente com o **comando debug radius authentication**. Isto debuga foi introduzido no Cisco IOS Software Release 12.2(15)JA. Os obsoletes debugar o **comando debug dot11 aaa dot1x process no** Cisco IOS Software Release 12.2(15)JA e Mais Recente.
- debug dot11 aaa dot1x process—Esta depuração é útil para diagnosticar problemas com comunicações negociadas. A informação detalhada mostra o que cada participante na negociação envia e mostra a resposta do outro participante. Você pode igualmente usar este debuga conjuntamente com o **comando debug radius authentication**. Nos Cisco IOS Software Release que estão mais adiantados do que o Cisco IOS Software Release 12.2(15)JA, isto debuga mostras a negociação do gerenciamento chave WPA.

Informações Relacionadas

- Configurando conjuntos de cifras e o WEP
- Configurando tipos de autenticação
- WPA2 - Acesso protegido por wi-fi 2
- Configuração do acesso protegido por wi-fi 2 (WPA2)
- Suporte Técnico e Documentação - Cisco Systems