Visão Geral da Configuração do WPA

Contents

Introduction

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.

Prerequisites

Requirements

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

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

Componentes Utilizados

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

- Pontos de acesso (APs) baseados no software Cisco IOS®
- Software Cisco IOS versão 12.2(15)JA ou posterior**Observação:** de preferência, use a versão mais recente do Cisco IOS Software, mesmo que a WPA seja suportada no Cisco IOS Software Release 12.2(11)JA e posterior. Para obter a versão mais recente do Cisco IOS

Software, consulte Downloads (somente clientes registrados) .
- Uma placa de interface de rede (NIC) compatível com WPA e seu software cliente compatível com 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.

Material de Suporte

Os recursos de segurança em uma rede sem fio, como WEP, são fracos. O grupo industrial da Wi-Fi Alliance (ou WECA) desenvolveu um padrão de segurança provisório de próxima geração para redes sem fio. O padrão oferece defesa contra pontos fracos 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. Depois que o dispositivo cliente e o servidor de autenticação fizerem uma associação EAP/802.1x, o gerenciamento de chaves WPA é negociado entre o AP e o dispositivo cliente compatível com WPA.

Os produtos AP da Cisco também fornecem uma configuração híbrida na qual os clientes EAP baseados em WEP antigos (com gerenciamento legado ou sem chave) trabalham em conjunto com clientes WPA. Essa configuração é chamada de modo de migração. O modo de migração permite uma abordagem em fases para migrar para WPA. Este documento não aborda o modo de migração. Este documento fornece um esboço para uma rede protegida por WPA pura.

Além das preocupações com segurança corporativa ou corporativa, a WPA também oferece uma versão de chave pré-compartilhada (WPA-PSK) destinada ao uso em redes sem fio domésticas ou de pequenos escritórios. O Cisco Aironet Client Utility (ACU) não suporta WPA-PSK. O utilitário Configuração zero sem fio do Microsoft Windows suporta WPA-PSK para a maioria das placas sem fio, assim como estes utilitários:

- Cliente AEGIS da Meetinghouse Communications**Observação:** consulte Anúncio EOS e EOL para a Linha de Produtos AEGIS do Meetinghouse.
- Cliente Odyssey da Funk Software**Observação:** consulte Juniper Networks Customer Support Center .
- Utilitários cliente OEM (Original Equipment Manufaturer, fabricante original de equipamento) de alguns fabricantes

Você pode configurar WPA-PSK quando:

- Você define o modo de criptografia como Cipher Temporal Key Integrity Protocol (TKIP) na guia Encryption Manager (Gerenciador de criptografia).
- Você define o tipo de autenticação, o uso do gerenciamento de chaves autenticado e a chave pré-compartilhada na guia Service Set Identifier (SSID) Manager da GUI.
- Nenhuma configuração é necessária na guia Server Manager.

Para habilitar o WPA-PSK através da interface de linha de comando (CLI), insira estes comandos. Inicie no 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
```

Observação: esta seção fornece somente a configuração que é relevante para WPA-PSK. A configuração nesta seção é apenas para que você compreenda como habilitar o WPA-PSK e não é o foco deste documento. Este documento explica como configurar o WPA.

Conventions

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 pressupõe que você tem uma configuração Light EAP (LEAP), EAP ou Protected EAP (PEAP) que funciona antes de adicionar a configuração para ativar 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 qualquer método de autenticação baseado em EAP/802.1x, você pode questionar quais são as diferenças entre a autenticação Network-EAP e Open 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 dos fabricantes de clientes sem fio define esse campo com o valor 0 (autenticação aberta) e sinaliza seu desejo de fazer a autenticação EAP posteriormente 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 clientes que são:

- Clientes Cisco—Use Network-EAP.
- Clientes de terceiros (que incluem produtos compatíveis com Cisco Compatible Extensions [CCX]) – Use a Open Authentication com o EAP.
- Uma combinação de clientes da Cisco e de terceiros — Escolha a autenticação Network-EAP e Open com EAP.

Configuração de CLI

Este documento utiliza as seguintes configurações:

- Uma configuração de LEAP que existe e funciona
- Software Cisco IOS versão 12.2(15)JA para APs baseados no software Cisco IOS

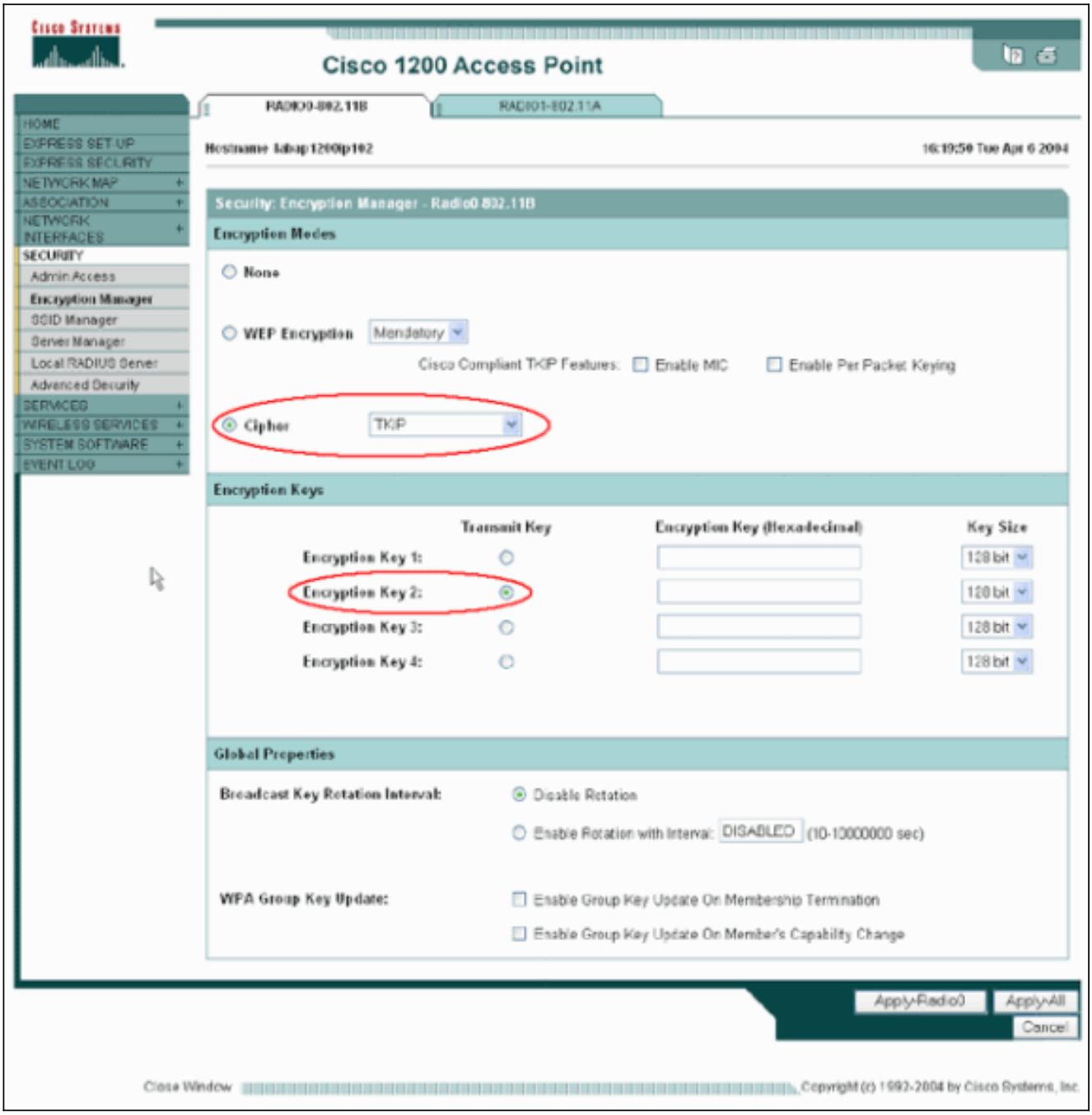
AP

```
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
```

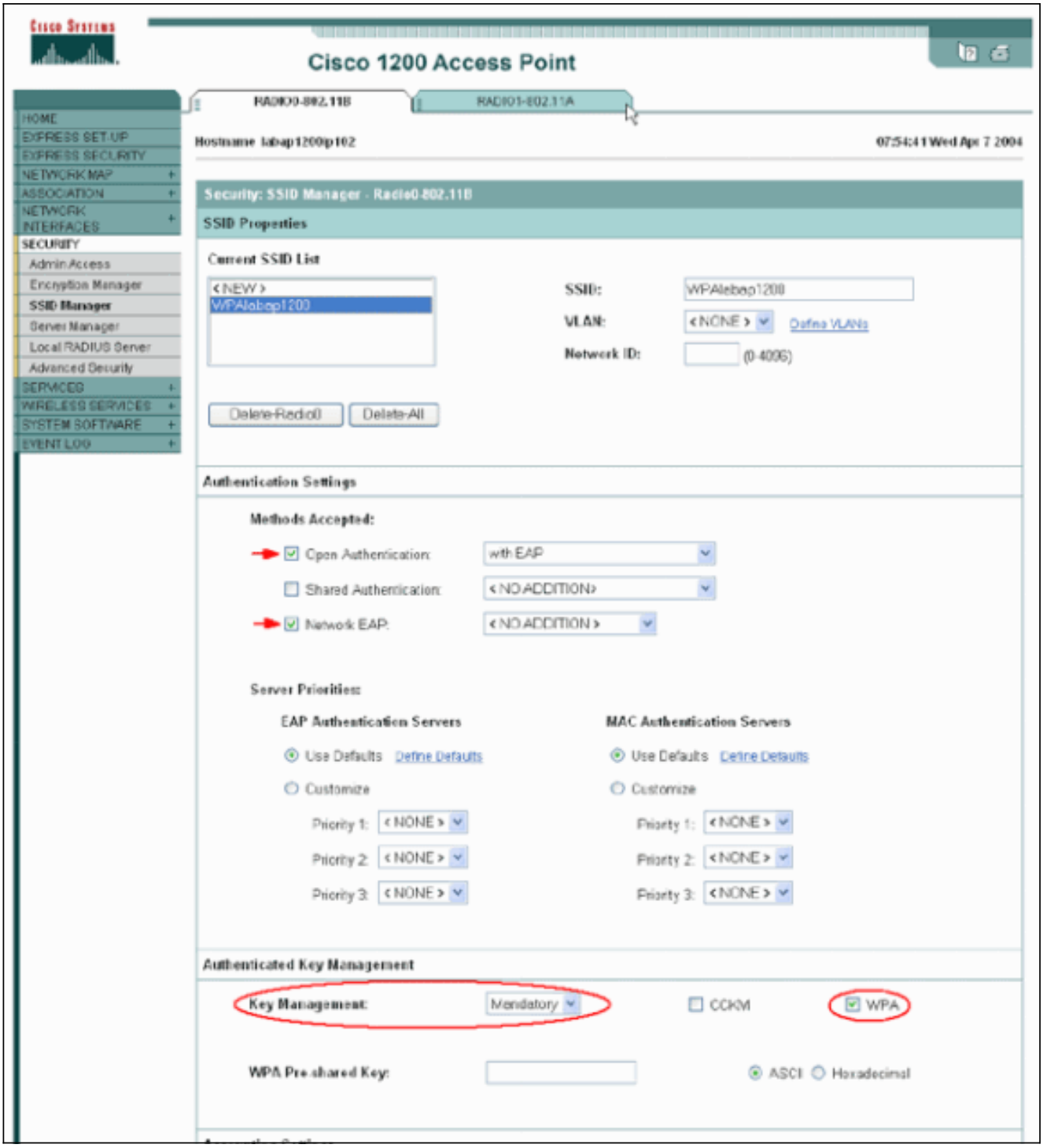
Configuração de GUI

Conclua estes passos para configurar o AP para WPA:

1. Conclua estes passos para configurar o Encryption Manager:Habilitar Cipher para TKIP.Limpe o valor na chave de criptografia 1.Defina a chave de criptografia 2 como a chave de transmissão.Clique em Apply-Radio#.



2. Conclua estes passos para configurar o SSID Manager:Selecione o SSID desejado na Lista de SSID atual.Escolha um método de autenticação apropriado.Baseie esta decisão no tipo de placas cliente que você usa. Consulte a seção EAP de rede ou Autenticação aberta com EAP deste documento para obter mais informações. Se o EAP funcionou antes da adição do WPA, provavelmente não é necessária uma alteração.Conclua estes passos para habilitar o gerenciamento de chaves:Escolha **Obrigatório** no menu suspenso Gerenciamento de chaves.Marque a caixa de seleção WPA.Clique em Apply-Radio#.

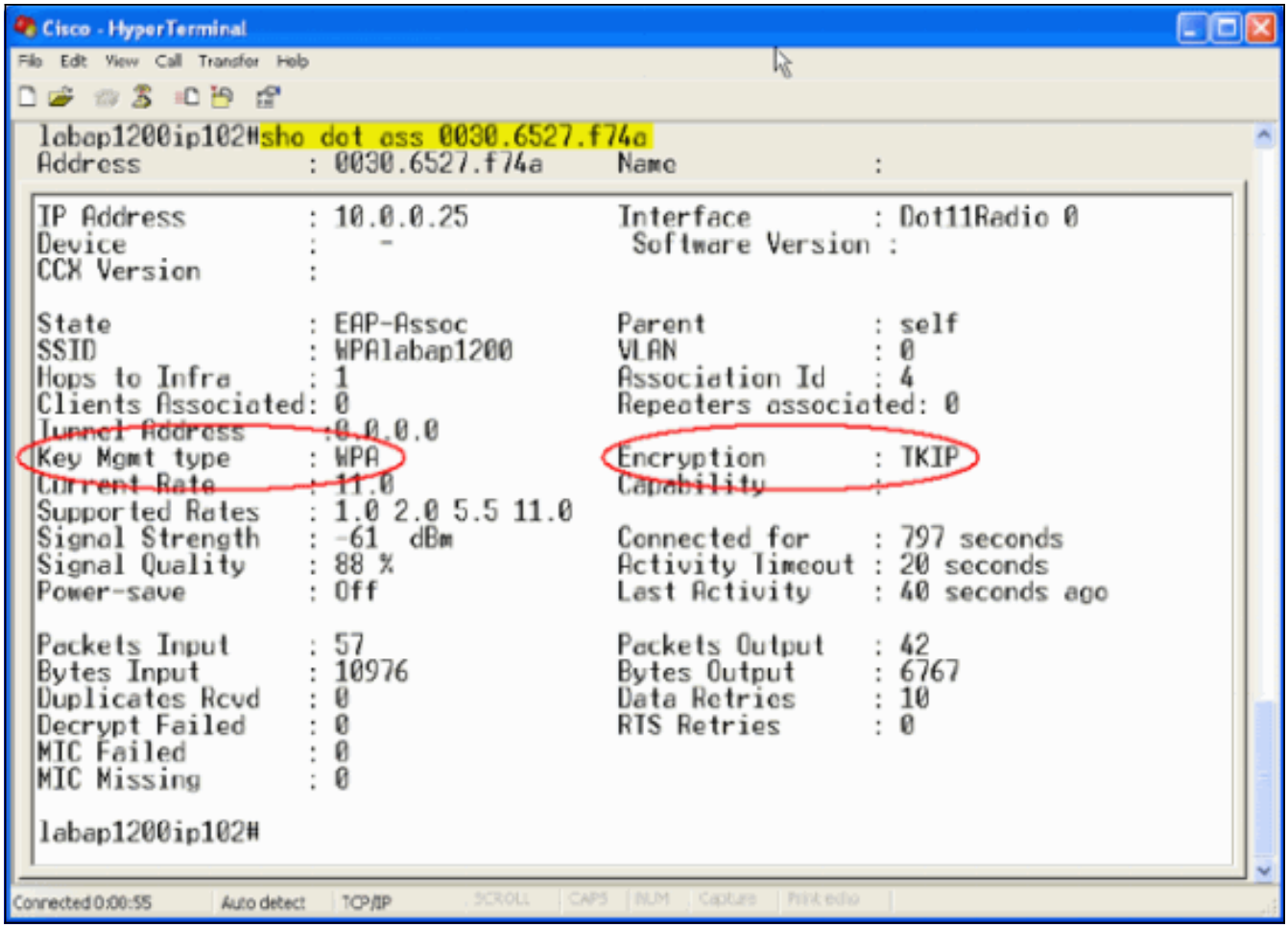


Verificar

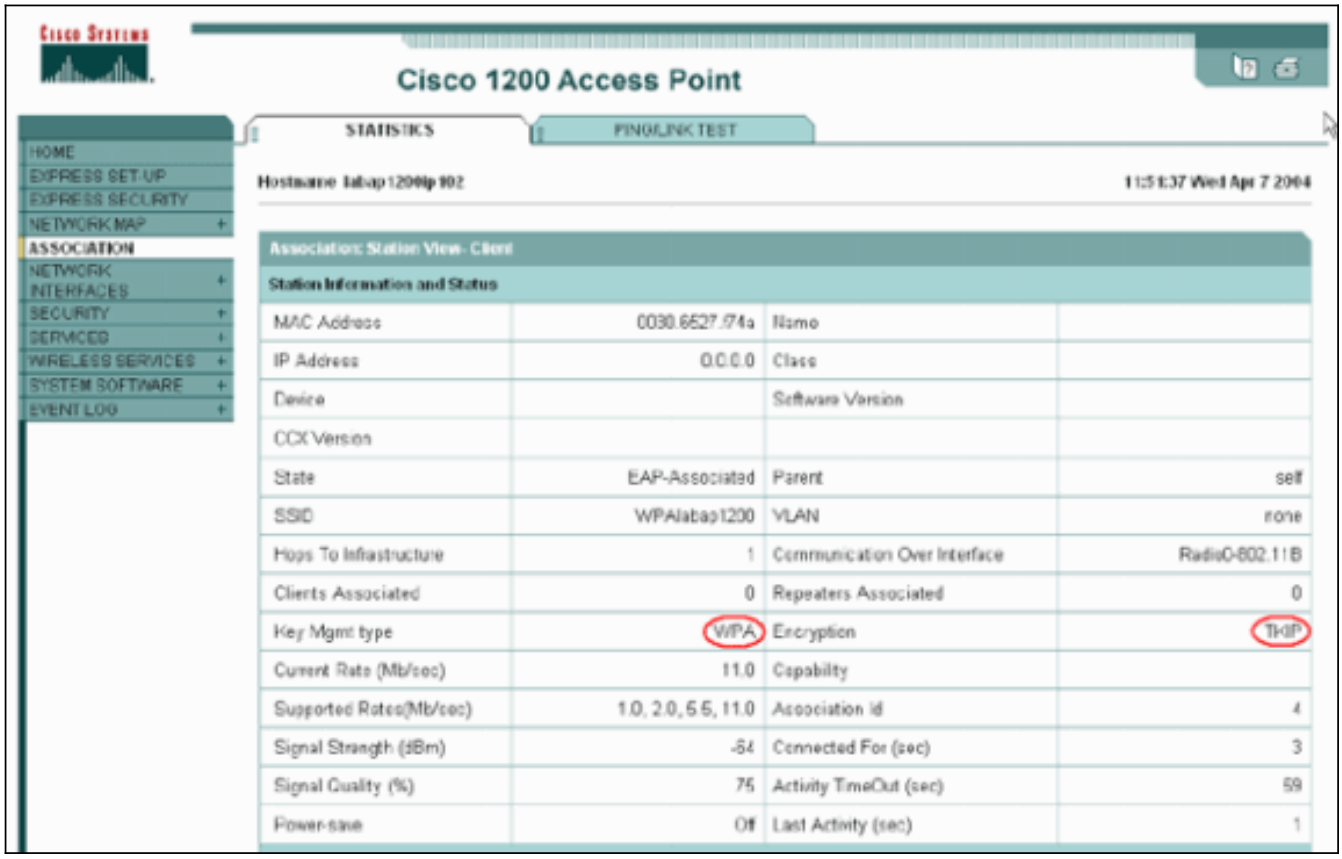
Use esta seção para confirmar se a sua configuração funciona corretamente.

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

- **show dot11 association** *mac_address* —Este comando exibe informações sobre um cliente associado especificamente identificado. Verifique se o cliente negocia o Key Management como **WPA** e Encryption como **TKIP**.



- A entrada da tabela Associação para um cliente específico também deve indicar o Gerenciamento de chaves como **WPA** e Criptografia como **TKIP**. Na tabela Associação, clique em um endereço MAC específico para um cliente para ver os detalhes da associação desse
cliente.



Troubleshoot

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 configuração de LEAP, EAP ou PEAP não tiver sido completamente testada antes da implementação de WPA, você deve concluir estas etapas:Desative temporariamente o modo de criptografia WPA.Reative o EAP apropriado.Confirmar que a autenticação funciona.
2. Verifique se a configuração do cliente corresponde à do AP.Por exemplo, quando o AP estiver configurado para WPA e TKIP, confirme se as configurações correspondem às configurações definidas no cliente.

Comandos de solução de problemas

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

O gerenciamento de chaves WPA envolve um handshake de quatro vias após a conclusão bem-sucedida da autenticação EAP. Você pode ver essas quatro mensagens em depurações. Se o EAP não autenticar o cliente com êxito ou se você não vir as mensagens, faça o seguinte:

1. Desative temporariamente a WPA.
2. Reative o EAP apropriado.
3. Confirmar que a autenticação funciona.

Esta lista descreve as depurações:

- **debug dot11 aaa manager keys** — Esta depuração mostra o handshake que acontece entre o AP e o cliente WPA como a chave transiente (PTK) emparelhada e a chave transiente de grupo (GTK) negociam. Esta depuração foi introduzida no Cisco IOS Software Release 12.2(15)JA.Se nenhuma saída de depuração for exibida, verifique estes itens:O **termo mon do** monitor terminal está ativado (se você usar uma sessão Telnet).As depurações estão habilitadas.O cliente está configurado corretamente para WPA.Se a depuração mostrar que handshakes PTK e/ou GTK foram criados mas não verificados, verifique o software suplicante WPA para obter a configuração correta e a versão atualizada.
- **debug dot11 aaa authenticator state-machine** — Essa depuração mostra os vários estados de negociações pelos quais um cliente passa enquanto associa e autentica. Os nomes de estado indicam esses estados. Esta depuração foi introduzida no Cisco IOS Software Release 12.2(15)JA. A depuração torna obsoleto o comando **debug dot11 aaa dot1x state-machine** no Cisco IOS Software Release 12.2(15)JA e posterior.
- **debug dot11 aaa dot1x state-machine** — Esta depuração mostra os vários estados de negociações pelos quais um cliente passa à medida que associa e autentica. Os nomes de estado indicam esses estados. Nas versões do Cisco IOS Software anteriores ao Cisco IOS Software Release 12.2(15)JA, esta depuração também mostra a negociação de

gerenciamento de chaves WPA.

- **debug dot11 aaa authenticator process** — Essa depuração é mais útil para diagnosticar problemas com comunicações negociadas. As informações detalhadas mostram o que cada participante na negociação envia e mostra a resposta do outro participante. Você também pode usar essa depuração em conjunto com o comando **debug radius authentication**. Esta depuração foi introduzida no Cisco IOS Software Release 12.2(15)JA. A depuração torna obsoleto o comando **debug dot11 aaa dot1x process** no Cisco IOS Software Release 12.2(15)JA e posterior.
- **debug dot11 aaa dot1x process—Esta depuração é útil para diagnosticar problemas com comunicações negociadas.** As informações detalhadas mostram o que cada participante na negociação envia e mostra a resposta do outro participante. Você também pode usar essa depuração em conjunto com o comando **debug radius authentication**. Nas versões do Cisco IOS Software anteriores ao Cisco IOS Software Release 12.2(15)JA, esta depuração mostra a negociação de gerenciamento de chaves WPA.

Informações Relacionadas

- Configurando conjuntos de cifras e o WEP
- Configurando tipos de autenticação
- WPA2 – Wi-Fi Protected Access 2
- Configuração do WPA 2 (Wi-Fi Protected Access 2)
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.