Autenticação de EAP com servidor RADIUS

Índice

Introdução

Este documento fornece uma configuração de exemplo de um Access point baseado IOS® de Cisco para a autenticação do Extensible Authentication Protocol (EAP) dos usuários Wireless contra um base de dados alcançado por um servidor Radius.

Devido ao papel passivo que o Access point joga em EAP (pacotes wireless das pontes do cliente nos pacotes prendidos destinados ao Authentication Server, e vice-versa), esta configuração é usada com virtualmente todos os métodos de EAP. Estes métodos incluem (mas não são limitados a) o PULO, EAP protegido (PEAP) - versão 2 do protocolo de autenticação de cumprimento do MS-desafio (RACHADURA), a placa de token PEAP-genérica (GTC), a Autenticação Flexível de EAP através do Tunelamento seguro (RÁPIDO), a Segurança da camada do EAP-transporte (TLS), e TLS EAP-em túnel (TTL). Você deve apropriadamente configurar o Authentication Server para cada um destes métodos de EAP.

Este capas de documento como configurar o Access Point (AP) e o servidor Radius, que é Cisco Secure ACS no exemplo de configuração neste documento.

Pré-requisitos

Requisitos

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

- Você é familiar com o Cisco IOS GUI ou CLI.
- Você é familiar com os conceitos atrás da autenticação de EAP.

Componentes Utilizados

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

- Produtos do Cisco Aironet AP que executa o Cisco IOS.
- Suposição de somente um LAN virtual (VLAN) na rede.
- Um produto do servidor de autenticação RADIUS que integre com sucesso em uma base de dados de usuário.Estes são os Authentication Server apoiados para o PULO de Cisco e EAP-FAST:Cisco Secure Access Control Server (ACS)Cisco Access Registrar (CAR)Funk Steel Belted RADIUSInterlink MeritEstes são os Authentication Server apoiados para a versão 2 de Microsoft PEAP-MS-CHAP e o PEAP-GTC:Internet Authentication Service de Microsoft (IAS)Cisco Secure ACSFunk Steel Belted RADIUSInterlink MeritTodo o Authentication Server adicional Microsoft pode autorizar.**Nota:** O GTC ou as senhas de uma vez exigem os serviços adicionais que exigem o software adicional em ambos o lado do cliente e servidor, assim como o hardware ou os geradores de token de software.Consulte o fabricante do suplicante do cliente para os detalhes em que os Authentication Server são apoiados com seu Produtos para o EAP-TLS, o EAP-TTLS e os outros métodos de EAP.

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.

Convenções

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

Configurar

Esta configuração descreve como configurar a autenticação de EAP em um AP baseado IO. No exemplo neste documento, o PULO é usado como um método de autenticação de EAP com servidor Radius.

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

Como a maioria dos algoritmos de autenticação baseados em senha, o LEAP Cisco é vulnerável a ataques de dicionários. Esse não é um novo ataque ou uma nova vulnerabilidade do Cisco LEAP. A criação de uma política de senha elaborada é a maioria de maneira eficaz abrandar ataques do dicionário. Isto inclui o uso das senhas elaboradas e da expiração periódica de senhas. Refira o ataque do dicionário no PULO de Cisco para obter mais informação sobre ataques do dicionário e como impedi-los.

Este documento usa esta configuração para o GUI e o CLI:

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do AP é 10.0.0.106.

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius (ACS) é 10.0.0.3.

EAP de rede ou autenticação aberta com EAP

Em todo o EAP/802.1x baseado método de autenticação, você pode questionar o que as diferenças estão entre a rede EAP e a autenticação aberta com EAP. Estes artigos referem os valores no campo do algoritmo de autenticação nos cabeçalhos de gerenciamento e nos pacotes de associação. A maioria de fabricantes do grupo dos clientes Wireless este campo no valor 0 (autenticação aberta), sinalizam então um 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.

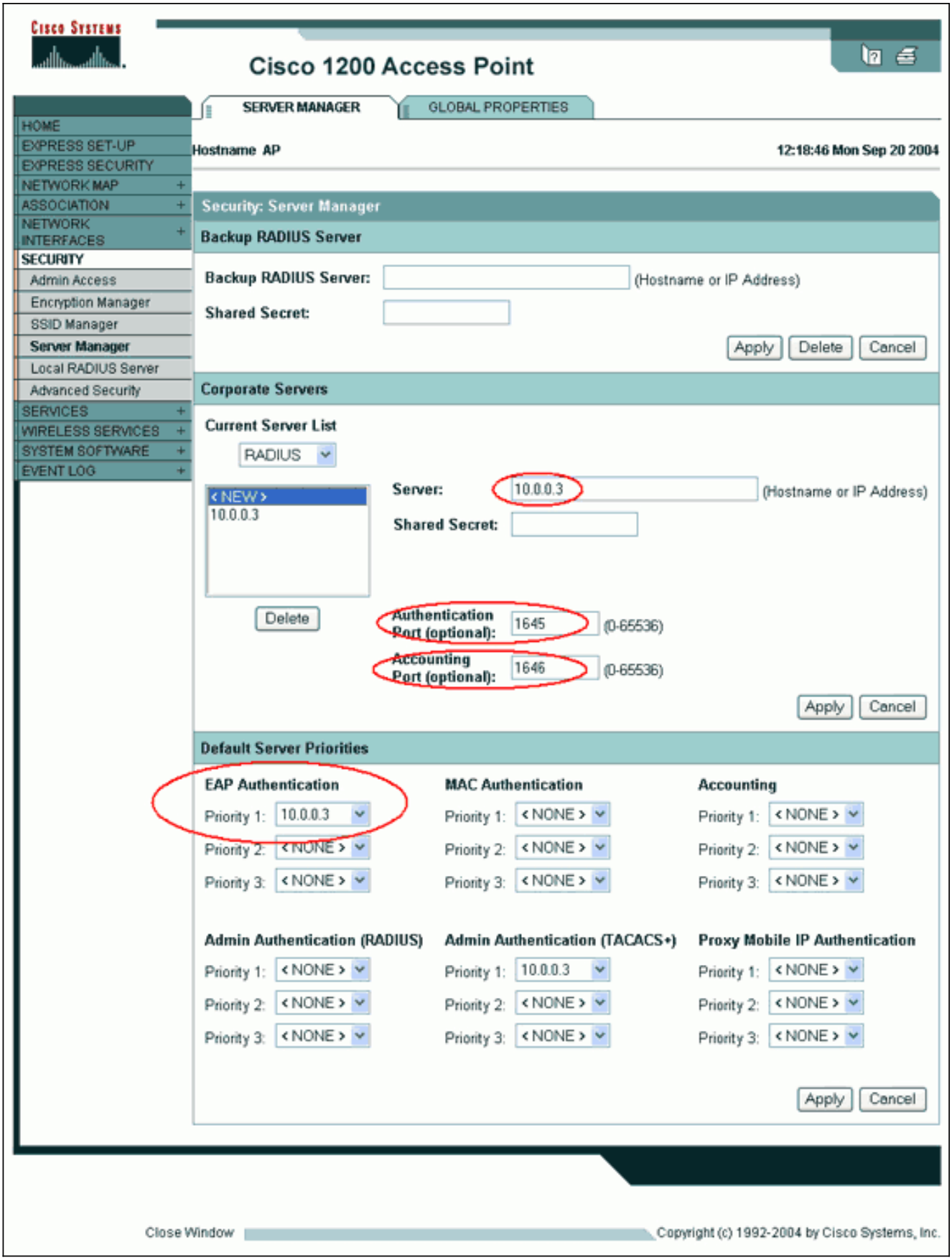
Se sua rede possui clientes que são:

- Clientes Cisco — Use a Rede EAP.
- Clientes da terceira parte (inclua produtos em conformidade com CCX) — Use aberto com EAP.
- Uma combinação de ambo o Cisco e clientes da terceira parte — escolha a Rede EAP e abra-a com EAP.

Defina o Authentication Server

A primeira etapa na configuração EAP é definir o Authentication Server e estabelecer um relacionamento com ela.

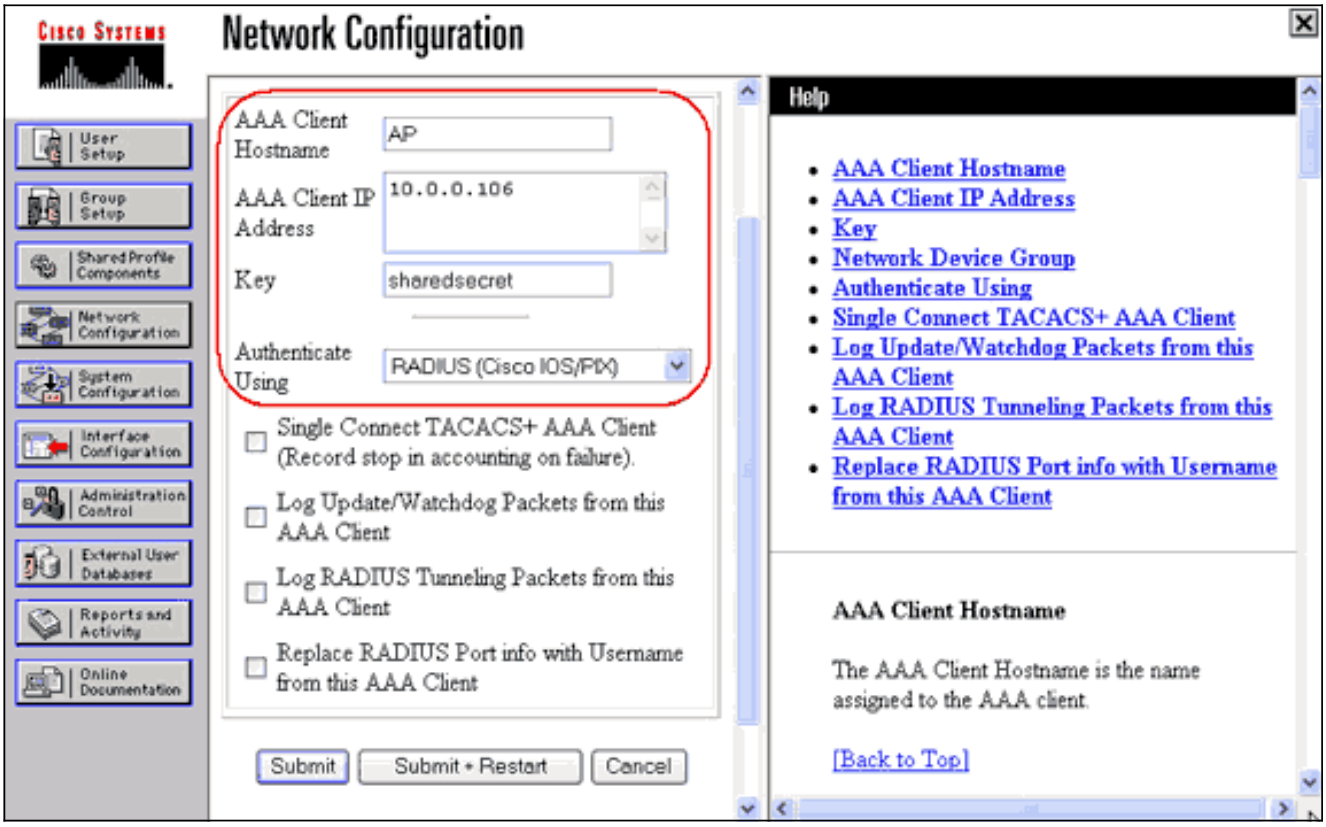
1. Na aba do gerenciador do servidor do Access point (sob o item de menu da **Segurança > do gerenciador do servidor**), termine estas etapas:Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do Authentication Server ao campo do server.Especifique o segredo compartilhado e as portas.O clique **aplica-se** a fim criar a definição e povoar as listas suspensas.Ajuste o tipo campo da autenticação de EAP da prioridade 1 ao endereço IP do servidor sob prioridades do server do padrão.Clique em
   Apply.



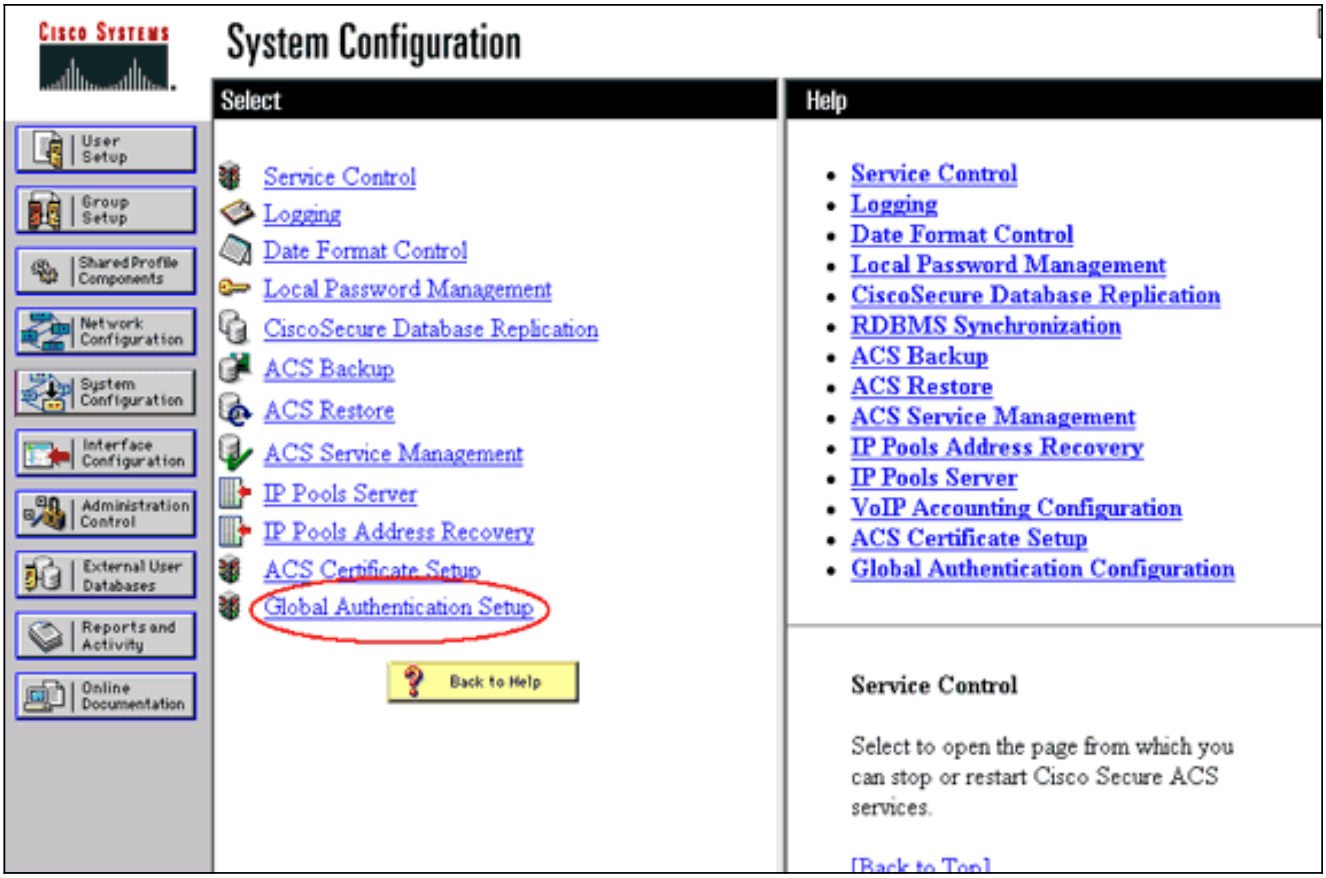
Você pode igualmente emitir estes comandos do CLI:`AP#configure terminal Enter configuration commands, one per line. End with CNTL/Z. AP(config)#aaa group server radius rad_eap AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646 AP(config-sg-radius)#exit AP(config)#aaa new-model AP(config)#aaa authentication login eap_methods group rad_eap AP(config)#radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key labap1200ip102 AP(config)#end AP#write memory`

2. O Access point deve ser configurado no Authentication Server como um cliente de AAA.Por exemplo, no Cisco Secure ACS, isto acontece na página da configuração de rede onde o

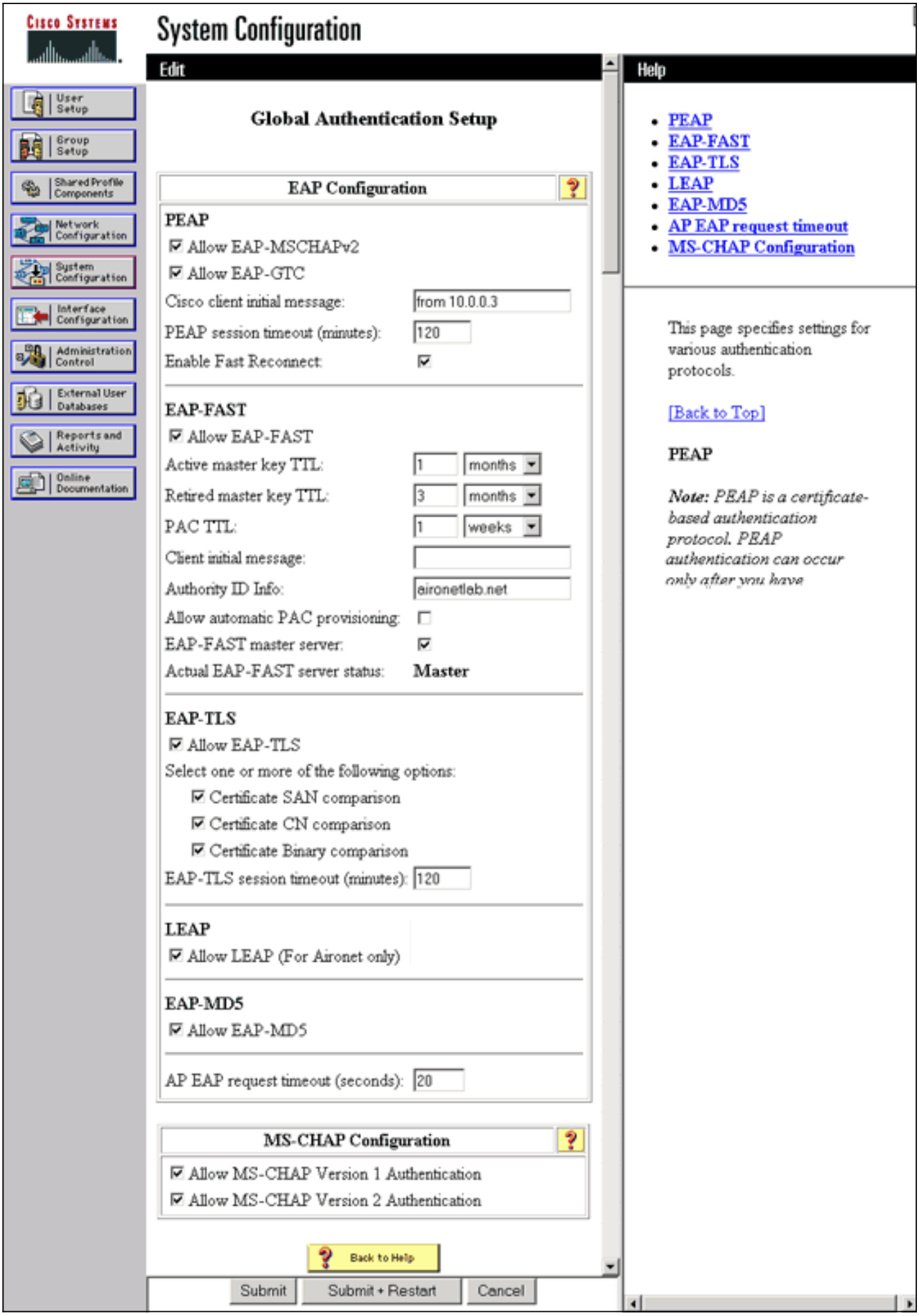
nome do Access point, o endereço IP de Um ou Mais Servidores Cisco ICM NT, o segredo compartilhado e o método de autenticação (Cisco Aironet do RAIO ou RAIO Cisco IOS/PIX) são definidos. Refira a documentação do fabricante para outros Authentication Server NON-ACS.



Assegure-se de que o Authentication Server esteja configurado para executar o método de autenticação de EAP desejado. Por exemplo, para um Cisco Secure ACS que PULA, configurar a autenticação de leap na configuração de sistema - página de instalação da autenticação global. Clique a **configuração de sistema**, a seguir clique a **instalação da autenticação global**. Refira a documentação do fabricante para outros Authentication Server NON-ACS ou outros métodos de
EAP.



Esta imagem mostra o Cisco Secure ACS configurado para o PEAP, EAP-FAST, o EAP-TLS, o PULO e o EAP-
MD5.

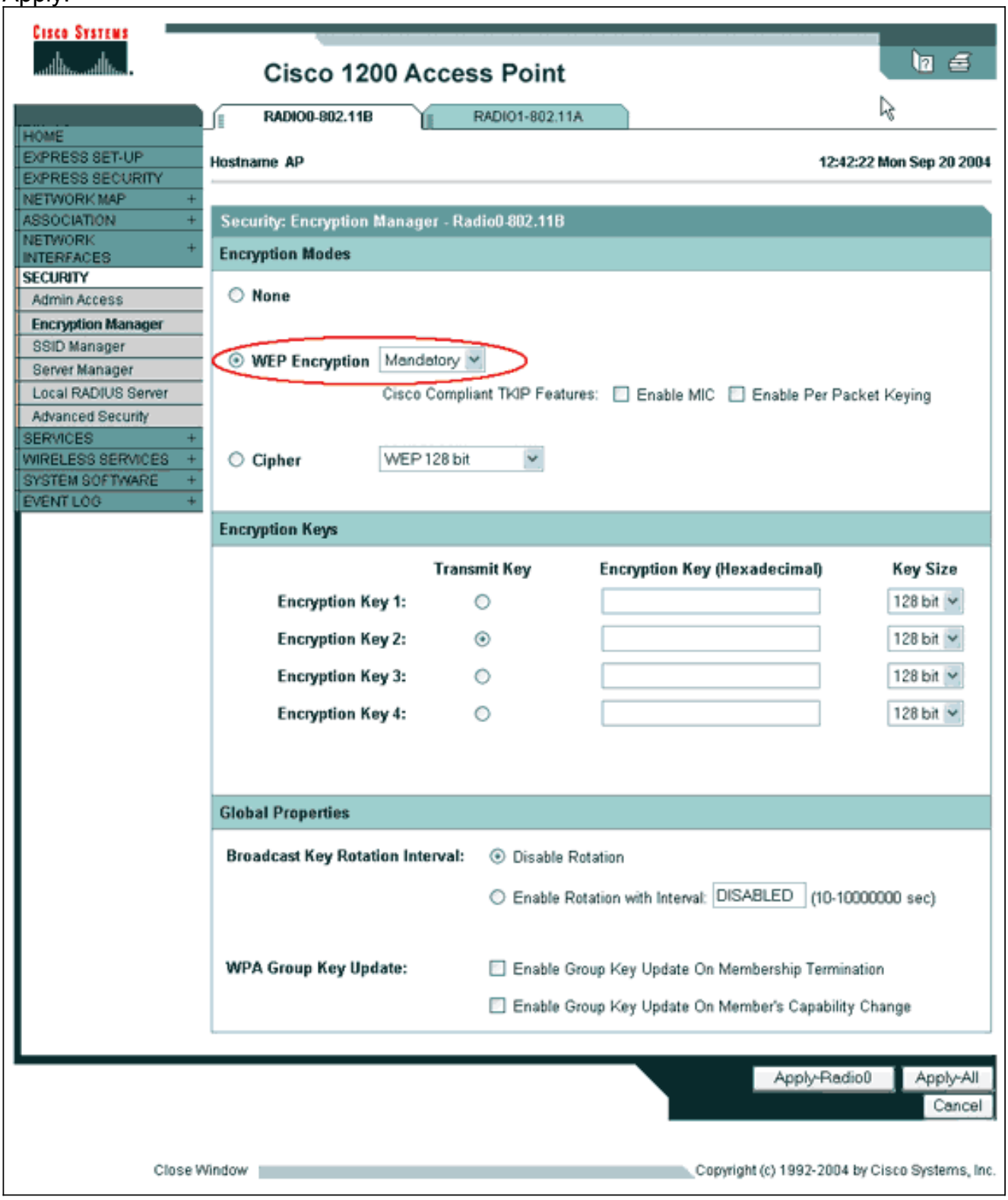


[Defina métodos de authenticação do cliente]

Uma vez que o Access point sabe onde enviar pedidos da authenticação do cliente, a configura para aceitar aqueles métodos.

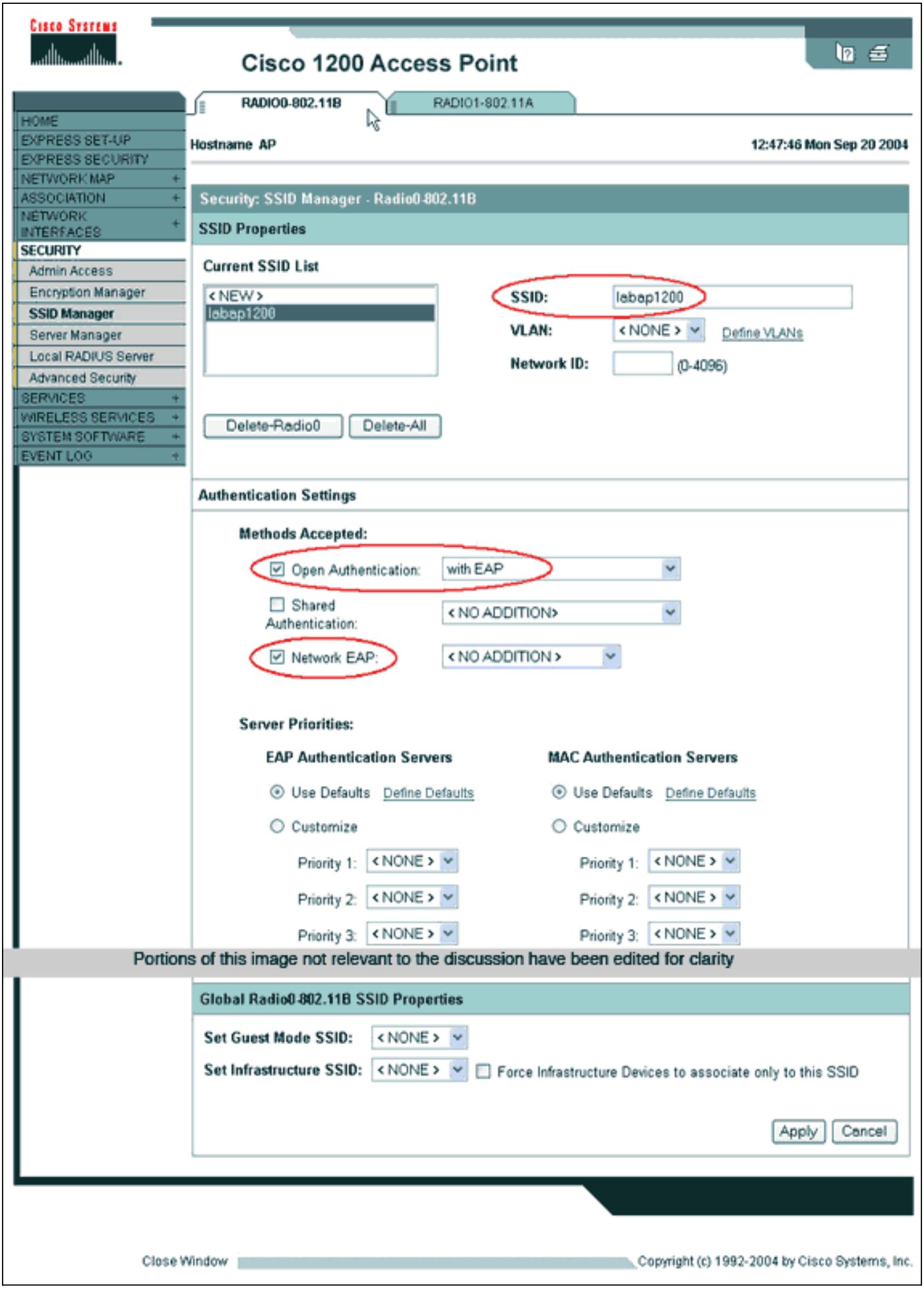
Nota: Estas instruções são para uma instalação baseada em WEP. Para o WPA (que usa cifras em vez do WEP), refira a visão geral de configuração de WPA.

1. Na aba do gerenciador de criptografia do Access point (sob o item de menu da **Segurança > do gerenciador de criptografia**), termine estas etapas:Especifique que você quer usar a **criptografia de WEP**.Especifique que o WEP é **imperativo**.Verifique que o tamanho chave está ajustado ao **128-bits**.Clique em
   Apply.



Você pode igualmente emitir estes comandos do CLI:`AP#configure terminal Enter configuration commands, one per line. End with CNTL/Z. AP(config)#interface dot11radio 0 AP(config-if)#encryption mode wep mandatory AP(config-if)#end AP#write memory`

2. Termine estas etapas na aba do gerenciador de SSID do Access point (sob o item de menu da **Segurança > do gerenciador de SSID**):Selecione o SSID desejado.Sob os “métodos de autenticação aceitados,” verifique a caixa etiquetada **aberta** e use a lista suspensa para escolher **com EAP**.Verifique a caixa etiquetada **Rede EAP** se você tem cartões do cliente Cisco. Veja a discussão na rede EAP ou a autenticação aberta com seção EAP.Clique em Apply.



Você pode igualmente emitir estes comandos do CLI:

```
AP#configure terminal Enter configuration commands, one per line. End with CNTL/Z.
AP(config)#interface dot11radio 0 AP(config-if)#ssid labap1200 AP(config-if-ssid)#authentication
open eap eap_methods AP(config-if-ssid)#authentication network-eap eap_methods AP(config-if-
ssid)#end AP#write memory
```

Uma vez que você confirma a funcionalidade básica com uma configuração de EAP básica, você pode adicionar recursos adicionais e gerenciamento chave mais tarde. Mergulhe umas funções mais complexas sobre bases funcionais a fim facilitar a pesquisa de defeitos.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **mostre o grupo de servidores todo do raio** — Indica uma lista de todos os grupos de servidores configurados do RAIO no AP.

Troubleshooting

Procedimento de solução de problemas

Termine estas etapas a fim pesquisar defeitos sua configuração.

1. Na utilidade ou no software do lado do cliente, crie um perfil ou uma conexão nova com o mesmo ou os parâmetros similares a fim assegurar-se de que nada se torne corrompido na configuração do cliente.
2. A fim eliminar a possibilidade de edições RF que impedem a autenticação bem sucedida, temporariamente autenticação do desabilitação segundo as indicações destas etapas:Do CLI, use os comandos no authentication open eap eap_methods, no authentication network-eap eap_methods e authentication open.Do GUI, na página do gerenciador de SSID, a **Rede EAP da un-**verificação, verifica **aberto**, e ajusta a lista suspensa de volta a **nenhuma adição**.Se o cliente associa com sucesso, a seguir o RF não contribui ao problema de associação.
3. Verifique que as senhas secundárias compartilhadas estão sincronizadas entre o Access point e o Authentication Server. Se não, você pode receber este Mensagem de Erro:`Invalid message authenticator in EAP request`Do CLI, verifique a linha `<shared_secret> chave da acct-porta x da autêntico-porta x do host de servidor RADIUS x.x.x.x.`Do GUI, na página do gerenciador do servidor, reenter o segredo compartilhado para o server apropriado na caixa etiquetada “segredo compartilhado.”A entrada secreta compartilhada para o Access point no servidor Radius deve conter a mesma senha secundária compartilhada que aquelas mencionaram previamente.
4. Remova todos os grupos de usuário do servidor RADIUS. Às vezes os conflitos podem ocorrer entre os grupos de usuário definidos pelo servidor Radius, e os grupos de usuário no domínio subjacente. Verifique os logs do servidor Radius para ver se há falhas de tentativa, e as razões que aquelas tentativas falharam.

Comandos de solução de problemas

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Debugar autenticações fornece uma quantidade significativa de detalhe sobre como recolher e para interpretar a saída de debuga relacionado ao EAP.

Nota: Antes que você emita **comandos debug**, refira a informação importante em comandos Debug.

- **debugar a estado-máquina do autenticador aaa do dot11** — Os indicadores major divisões (ou estados) da negociação entre o cliente e o Authentication Server. Está aqui uma saída de uma **autenticação bem sucedida**:
```
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending
identity request to 0040.96ac.dd05
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client:
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96ac.dd05 (client) *Mar 1 02:37:46.931:
dot11_auth_dot1x_send_id_req_to_client: Client 0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CLIENT_REPLY)
for 0040.96ac.dd05 *Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server: Sending
client 0040.96ac.dd05 data (User Name) to server *Mar 1 02:37:46.938:
dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds *Mar 1
02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_REPLY) for
0040.96ac.dd05 *Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client: Forwarding
server message(Challenge) to client 0040.96ac.dd05 *Mar 1 02:37:47.018:
dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 20 seconds *Mar 1
02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CL IENT_REPLY) for
0040.96ac.dd05 *Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server: Sending client
0040.96ac.dd05 data(User Credentials) to server ------------------Lines Omitted for
simplicity------------------ *Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds *Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm:
Executing Action (SERVER_WAIT,SE RVER_PASS) for 0040.96ac.dd05 *Mar 1 02:37:47.041:
dot11_auth_dot1x_send_response_to_client: Forwarding server message(Pass Message) to client
0040.96ac.dd05 *Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 30 seconds *Mar 1 02:37:47.043: %DOT11-6-ASSOC: Interface Dot11Radio0,
Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays associated to the
access point)
```
Nota: Nos Cisco IOS Software Release antes de 12.2(15)JA, a sintaxe deste **comando debug** é **debuga a estado-máquina do dot1x aaa do dot11**.
- **debugar o processo do autenticador aaa do dot11** — Indica as entradas individuais de diálogo da negociação entre o cliente e o Authentication Server.**Nota:** Nos Cisco IOS Software Release antes de 12.2(15)JA, a sintaxe deste comando debug é **debuga o processo do dot1x aaa do dot11**.
- **debugar a autenticação RADIUS** — Indica as negociações de RADIUS entre o server e o cliente, ambo, é construído uma ponte sobre pelo AP. Esta é uma saída para a **autenticação falha**:
```
*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi]
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 02:34:55.087: RADIUS: 32 [2]
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106 *Mar 1 02:34:55.087:
RADIUS/ENCODE(00000031): acct_session_id: 47 *Mar 1 02:34:55.087: RADIUS(00000031): Config
NAS IP: 10.0.0.106 *Mar 1 02:34:55.087: RADIUS(00000031): sending *Mar 1 02:34:55.087:
```

```
RADIUS(00000031): Send Access-Request to 10.0.0.3 :164 5 id 1645/61, len 130 *Mar 1
02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E - 56 77 A4 7E D3 C2 26 EB *Mar 1
02:34:55.088: RADIUS: User-Name [1] 8 "wirels" *Mar 1 02:34:55.088: RADIUS: Framed-MTU [12]
6 1400 *Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0" *Mar 1
02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05" *Mar 1 02:34:55.088:
RADIUS: Service-Type [6] 6 Login [1] *Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80]
18 *Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5 4A AB 88
[s?Y??QS?XM???J??] *Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13 *Mar 1 02:34:55.089:
RADIUS: NAS-Port-Id [87] 5 "299" *Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6
10.0.0.106 *Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap" *Mar 1 02:34:55.093:
RADIUS: Received from id 1645/61 10.0.0.3 :1645, Access-Challenge, len 79 *Mar 1
02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 - 84 87 49 9B B4 77 B8 973 -----
----------------------Lines Omitted---------------------------------- *Mar 1 02:34:55.117:
RADIUS(00000031): Config NAS IP: 10.0.0.106 *Mar 1 02:34:55.118: RADIUS/ENCODE(00000031):
acct_session_id: 47 *Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106 *Mar 1
02:34:55.118: RADIUS(00000031): sending *Mar 1 02:34:55.118: RADIUS(00000031): Send Access-
Request to 10.0.0.3 :164 5 id 1645/62, len 168 *Mar 1 02:34:55.118: RADIUS: authenticator 49
AE 42 83 C0 E9 9A A7 - 07 0F 4E 7C F4 C7 1F 24 *Mar 1 02:34:55.118: RADIUS: User-Name [1] 8
"wirels" *Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400 ----------------------------
---Lines Omitted---------------------- *Mar 1 02:34:55.124: RADIUS: Received from id
1645/62 10.0.0.3 :1645, Access-Reject, len 56 *Mar 1 02:34:55.124: RADIUS: authenticator A6
13 99 32 2A 9D A6 25 - AD 01 26 11 9A F6 01 37 *Mar 1 02:34:55.125: RADIUS: EAP-Message [79]
6 *Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????] *Mar 1 02:34:55.125: RADIUS: Reply-Message
[18] 12 *Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D [Rejected??] *Mar 1
02:34:55.125: RADIUS: Message-Authenticato[80] 18 *Mar 1 02:34:55.126: RADIUS(00000031):
Received from id 1645/62 *Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total
4 bytes *Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes *Mar
1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station 0040.96ac.dd05 Authentication failed
```

- **debugar a autenticação aaa** — Indica as negociações AAA de autenticação entre o dispositivo do cliente e o Authentication Server.

Informações Relacionadas

- Debugar autenticações
- Configurando tipos de autenticação
- Autenticação de leap em um servidor Radius local
- Configuração de servidores RADIUS e TACACS+
- Configurando o Cisco Secure ACS for Windows v3.2 com autenticação da máquina PEAP-MS-CHAPv2
- Cisco Secure ACS for Windows v3.2 com autenticação da máquina do EAP-TLS
- Configurando o PEAP/EAP no Microsoft IAS
- Pesquisando defeitos o Microsoft IAS como um servidor Radius
- Cliente de autenticação do 802.1X de Microsoft
- Suporte Técnico e Documentação - Cisco Systems