Configurar o Access point de pouco peso como um suplicante do 802.1x

Índice

Introdução

Este documento descreve como configurar um Access point de pouco peso como um suplicante do 802.1x para autenticar contra um servidor Radius.

Pré-requisitos

Requisitos

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

- Cisco Aironet 1130, 1240, ou Access point do 1250 Series
- WLC que executa a versão 5.1 IOS®
- Cisco Catalyst 3560 Series Switch com Cisco IOS Release 12.2(35)SE5
- Cisco Catalyst 3750 Series Switch com Cisco IOS Release 12.2(40)SE
- Cisco Catalyst 4500 Series Switch com Cisco IOS Release 12.2(40)SG
- Cisco Catalyst 6500 Series Switch com Supervisor Engine 32 que executa o Cisco IOS Release 12.2(33)SXH

Componentes Utilizados

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.

Informações de Apoio

Os regaços têm os Certificados X.509 instalados fábrica, assinados por uma chave privada, que são queimados no dispositivo na altura da fabricação. Os regaços usam este certificado para autenticar com o WLC no processo da junta. Para mais informação, refira a fixação do plano do controle LWAPP dos controladores de distribuição do Wireless LAN do Cisco 440X Series do documento. Este método descreve uma outra maneira de autenticar regaços. Com versão 5.1 WLC, você pode configurar a autenticação do 802.1x entre um Access point do Cisco Aironet e um switch Cisco. O Access point atua como o suplicante do 802.1x e é autenticado pelo interruptor contra um servidor Radius (ACS) esse os usos EAP-FAST com abastecimento anônimo PAC. Uma vez que é configurado para a autenticação do 802.1x, o interruptor não permite que nenhum tráfego a não ser o tráfego do 802.1x passe através da porta até que o dispositivo conectado à porta autentique com sucesso. Um Access point pode ser autenticado ou antes que se junte a um WLC ou depois que se juntou a um WLC, neste caso você configura o 802.1x no interruptor depois que o REGAÇO se junta ao WLC.

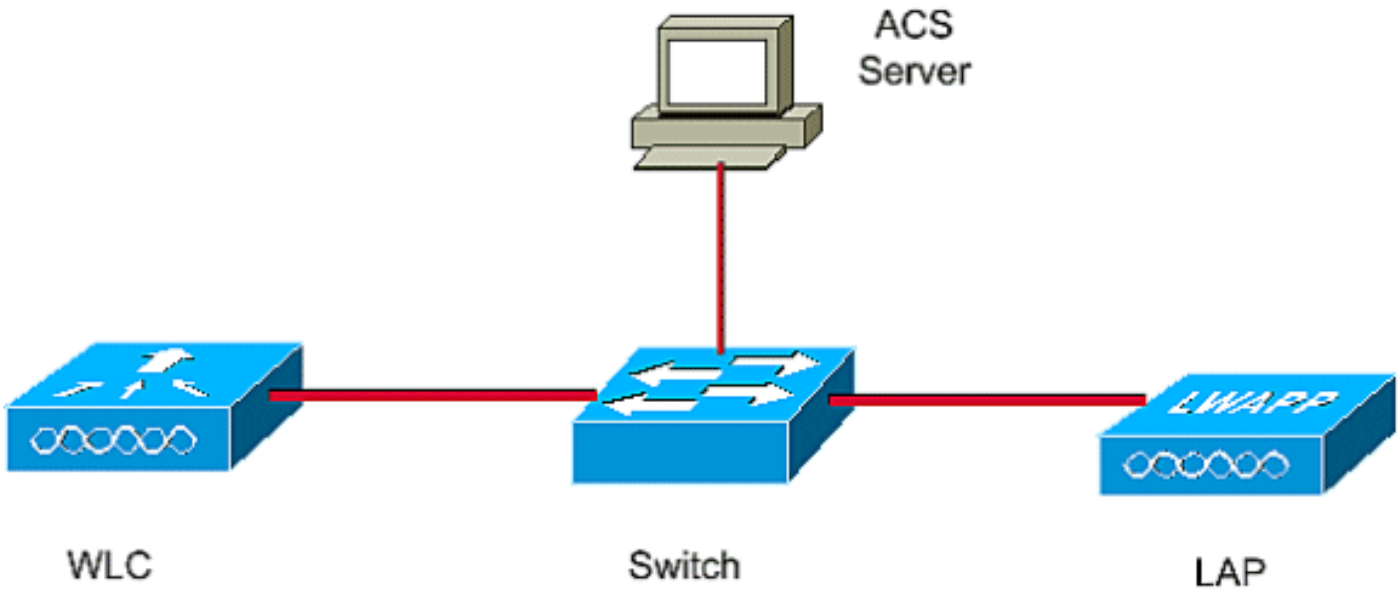
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a ferramenta Command Lookup Tool (apenas para clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento usa estes endereços IP de Um ou Mais Servidores Cisco ICM NT:

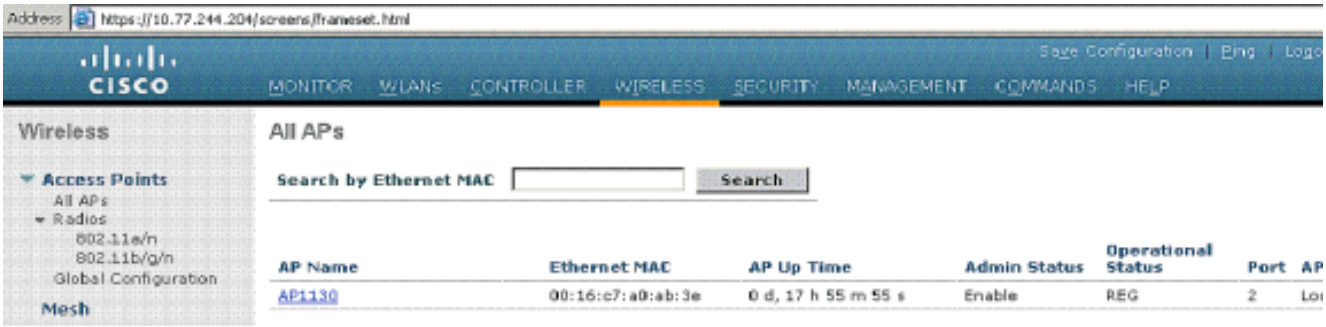
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do interruptor é 10.77.244.210
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor ACS é 10.77.244.196
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC é 10.77.244.204

Configurar o REGAÇO

Nesta seção, você é presentado com a informação para configurar o REGAÇO como um suplicante do 802.1x.

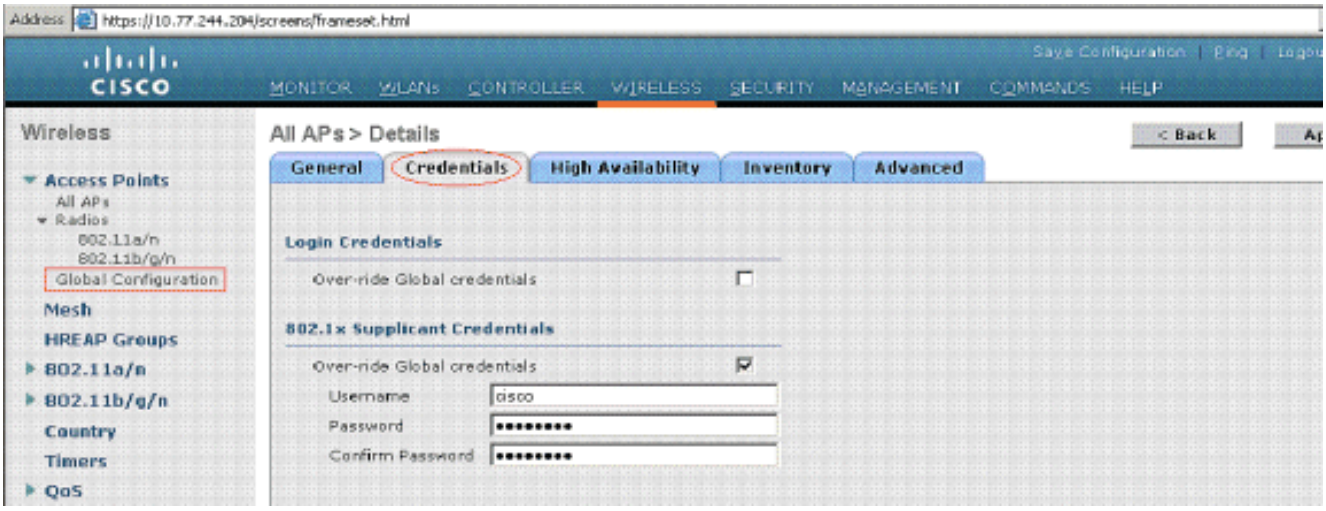
Conclua estes passos:

1. Certifique-se de que o Access point está carregado com uma imagem de recuperação de pouco peso.
2. Conecte o REGAÇO ao interruptor.
3. O REGAÇO atravessa o processo da junta e registra-se com o WLC. Isto pode ser verificado do menu wireless do WLC segundo as indicações de figura 1.**Figura 1**



4. Clique o **Access point**, e clique a aba das **credenciais**.
5. Sob as credenciais do suplicante do 802.1x que dirigem, verifique a caixa **global das credenciais da ultrapassagem** para ajustar o nome de usuário e senha do 802.1x para este Access point. Você pode igualmente ajustar o nome de usuário e senha na terra comum a

todos os Access point que se juntam a um WLC com o menu da configuração global. Figura 2 mostra como ajustar as credenciais do 802.1x para um Access point.**Figura 2**



Nota: Você pode igualmente ajustar o nome de usuário e senha do 802.1x para um Access point com o comando CLI que WLC a **configuração ap dot1xuser adiciona o <password> Cisco_AP da senha do <user> username (nome AP)**.

6. O clique **aplica-se** para comprometer suas mudanças.
7. **Configuração da salvaguarda do** clique para salvar as credenciais.**Nota:** Uma vez que salvar, estas credenciais são retidas através das repartições WLC e AP. Mudam somente quando o REGAÇO se junta a um WLC novo. O REGAÇO supõe o nome de usuário e senha que foi configurado no WLC novo.
8. Se o Access point não se juntou a um WLC ainda, você deve consolar no REGAÇO para ajustar as credenciais e para usar este comando CLI no modo enable:`LAP#lwapp ap dot1x username <username> password <password>` **Nota:** Este comando está disponível somente para os Access point que executam a imagem de recuperação 5.1.

Configurar o interruptor

O interruptor atua como um autenticador para o REGAÇO e autentica o REGAÇO contra um servidor Radius. Se o interruptor não tem o software complacente, promova o interruptor. No interruptor CLI, incorpore estes comandos permitir a autenticação do 802.1x em uma porta de switch:

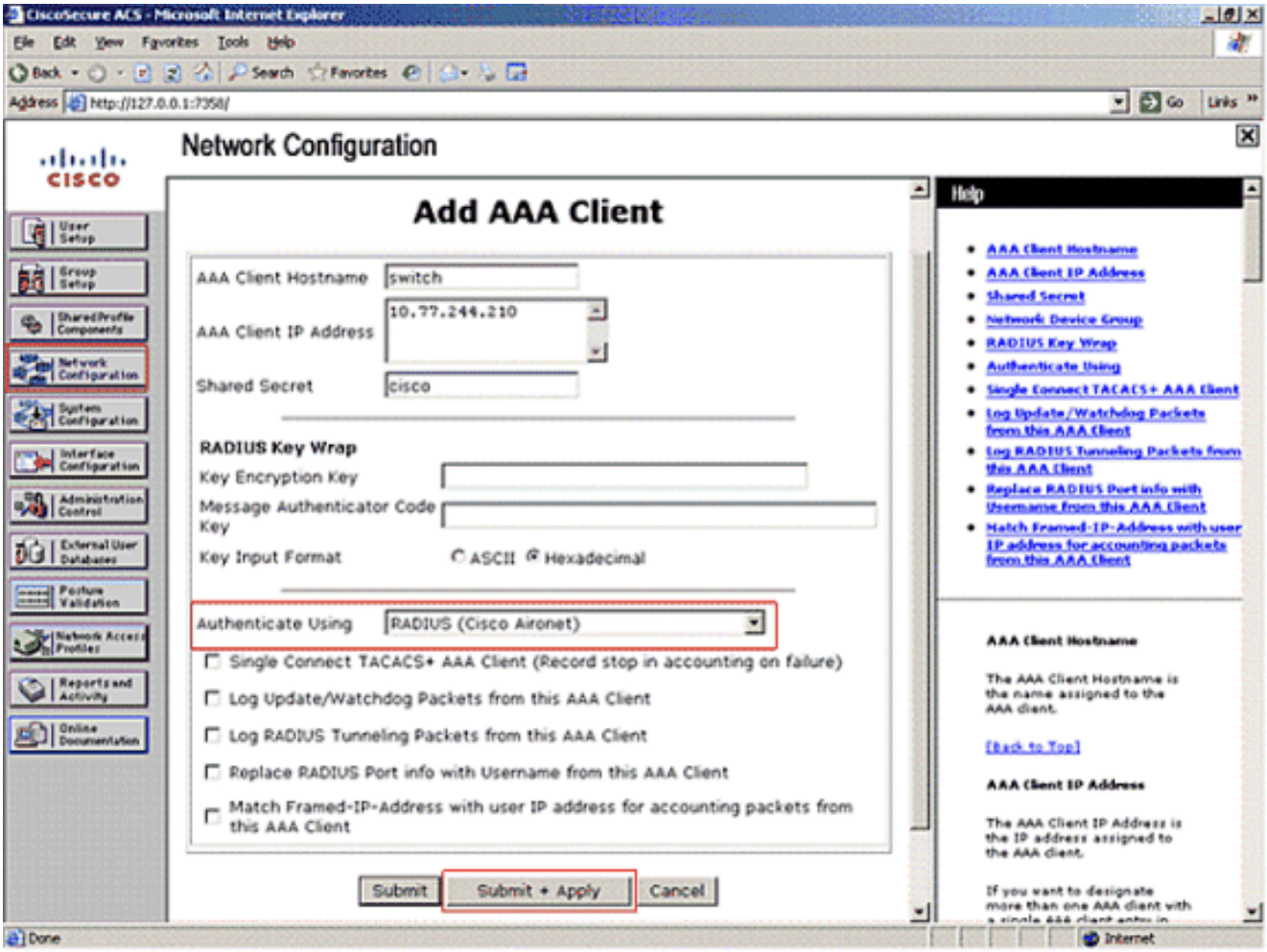
```
switch#configure terminal                    switch(config)dot1x system-auth-control
switch(config)aaa new-model                    switch(config)aaa authentication dot1x default
group radius                    switch(config)radius server host 10.77.244.196 key cisco!---
configures the radius server with shared secret switch(config)interface gigabitEthernet 1/0/43!-
-- 43 is the port number on which the access point is connected. switch(config-if)switchport
mode access switch(config-if)dot1x pae authenticator!--- configures dot1x authentication
switch(config-if)dot1x port-control auto!--- With this command switch initiates the 802.1x
authentication.
```

Configurar o servidor Radius

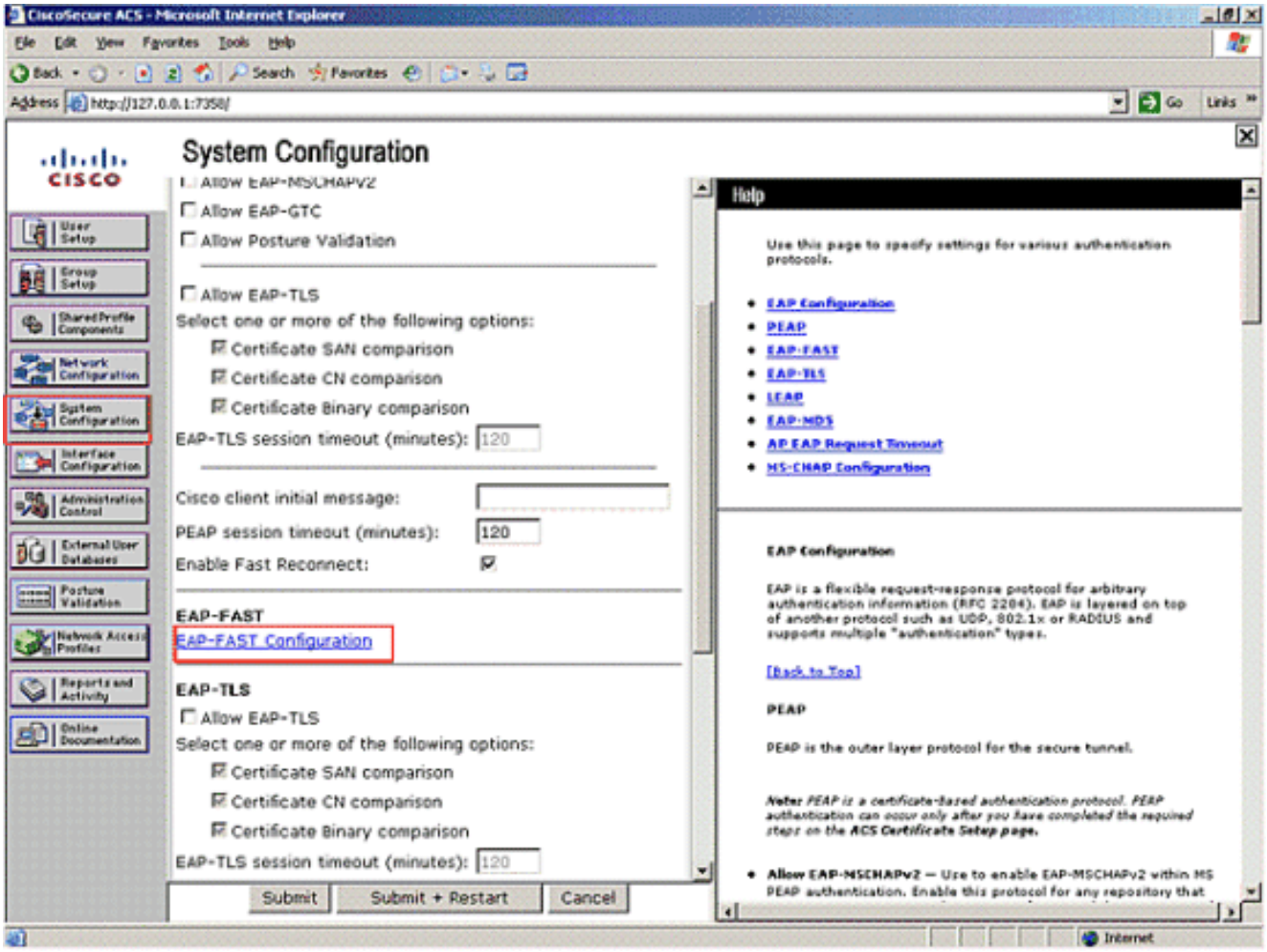
O REGAÇO é autenticado com EAP-FAST. Certifique-se de que o servidor Radius você usa apoios este método de EAP. Neste exemplo, o servidor ACS é usado para a autenticação. Termine estas etapas no servidor ACS:

1. Lance a tela ACS admin.

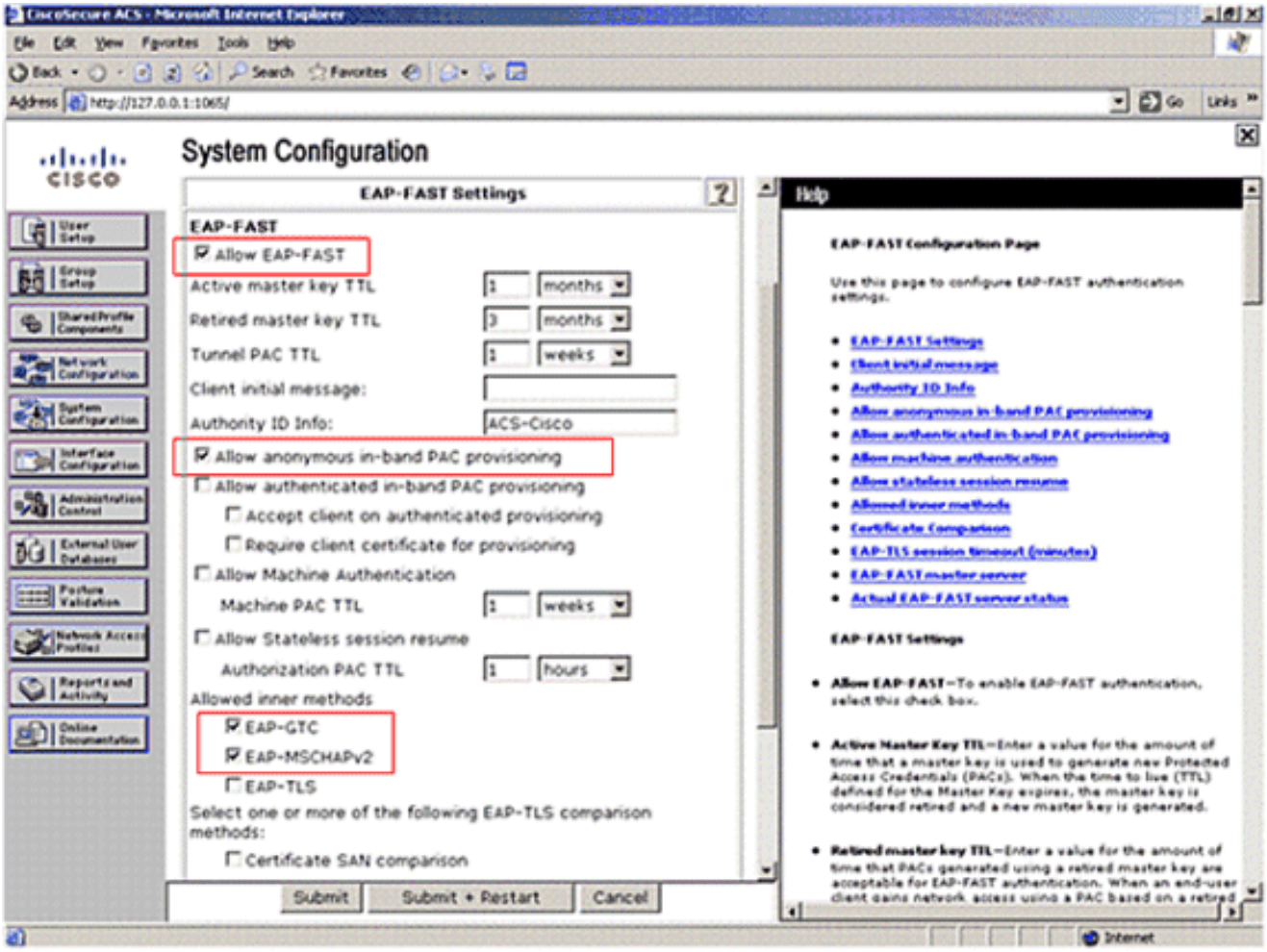
2. Configurar o nome de usuário e senha do REGAÇO no base de dados ACS. A fim adicionar uma conta de usuário no ACS, refira a seção de gerenciamento de usuário do Guia do Usuário do documento para o Serviço de controle de acesso Cisco Secure 4.2.
3. Configurar o interruptor como um cliente de AAA ao servidor ACS. Na tela ACS admin, clique o menu da **configuração de rede**.
4. Sob a seção do **cliente de AAA**, o clique **adiciona a entrada nova**. Incorpore estes parâmetros:Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do interruptor ao campo do *endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA*.Incorpore o segredo compartilhado do interruptor. Este deve ser exatamente o mesmo no interruptor e no servidor ACS.Escolha um **protocolo de raio na** *autenticação usando o* campo. À revelia, é TACACS+.**Nota:** Verifique o servidor ACS para ver se há uma descrição dos protocolos de raio.Consulte a figura 3.**Figura 3**



5. O clique **submete-se + aplica-se** para salvar o cliente de AAA.
6. EAP-FAST tem que ser permitido no servidor Radius. Clique o menu da **configuração de sistema no** lado esquerdo. Clique a opção da **instalação da autenticação global**.**Figura 4**



7. **Configuração EAP-FAST do** clique segundo as indicações de figura 4.
8. Nos ajustes EAP-FAST pagine, verifique a caixa **EAP-FAST reservar**. O REGAÇO usa EAP-FAST com abastecimento anônimo PAC. Verifique a caixa **anônima do abastecimento da em-faixa PAC reservar**. Para mais informação, refira a autenticação EAP-FAST do documento com exemplo de configuração dos controladores e do servidor de raio externo do Wireless LAN.**Figura 5**



9. Certifique-se de que o **EAP-GTC** e o **EAP-MSCHAPv2** estão verificados abaixo *permitem métodos internos*. Figure que 5 mostra uma configuração de exemplo das etapas 8 e 9.

Verificar

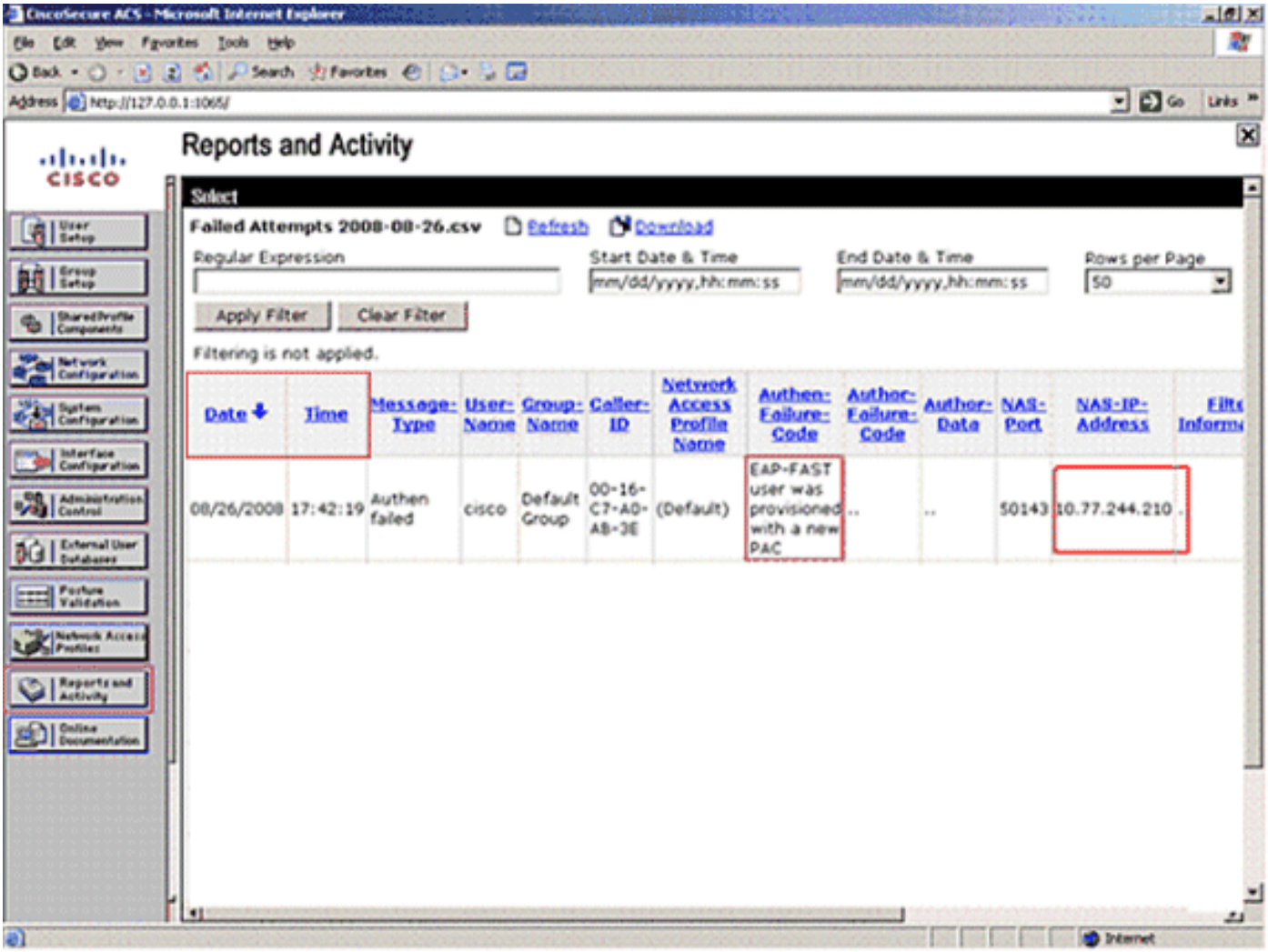
Use esta seção para confirmar se a sua configuração funciona corretamente.

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.

Uma vez que o 802.1x é permitido na porta de switch, todo o tráfego a não ser que o tráfego do 802.1x seja obstruído através da porta. O REGAÇO, que é registrado já ao WLC, obtém dissociado. Somente depois que uma autenticação bem sucedida do 802.1x é o outro tráfego permitido passar completamente. O registro bem-sucedido do REGAÇO ao WLC depois que o 802.1x é permitido no interruptor indica que a autenticação do REGAÇO é bem sucedida.

Você pode igualmente verificar este do ACS. Da tela principal ACS, clique o menu dos **relatórios e da autenticação**. Clique a opção das **falhas de tentativa**. Se a autenticação é bem sucedida, você encontra que uma *falha de mensagem da autenticação* com o *usuário EAP-FAST do* código *era fornecida com um PAC novo com endereço IP de Um ou Mais Servidores Cisco ICM NT do interruptor no* campo do Nas-ip-address segundo as indicações da figura 6. Você pode igualmente confirmar com a data e hora da autenticação.

Figura 6



Troubleshooting

Use esta seção para resolver problemas de configuração.

1. Use o **comando ping** e a verificação se o servidor ACS é alcançável do interruptor.
2. Certifique-se de que o interruptor está configurado como um cliente de AAA no servidor ACS.
3. Assegure-se de que o segredo compartilhado seja o mesmo entre o interruptor e o servidor ACS.
4. Verifique se EAP-FAST é permitido no servidor ACS.
5. Verifique para ver se há a conformidade do software nos dispositivos.
6. Verifique se as credenciais do 802.1x são configuradas para o REGAÇO e são mesmas no servidor ACS.**Nota:** O nome de usuário e senha é diferenciando maiúsculas e minúsculas.

Comandos para Troubleshooting

Há atualmente uns comandos no debug disponíveis para esta característica.

Informações Relacionadas

- Controlando Pontos de Acesso Lightweight

- Configurando a autenticação com base na porta do IEEE 802.1X
- Suporte Técnico e Documentação - Cisco Systems