Unified Wireless Network: Resolução de Problemas de Clientes

Índice

Introdução

O ambiente do Radio Frequency (RF) é complexo e dinâmico. Os vários fatores precisam de ser considerados para criar um bom ambiente Wireless. Este documento explica diversos problemas que podem ser encontrados ao se conectar a um cliente wireless em um ambiente Cisco Unified Wireless, assim como as etapas a serem realizadas para resolver problemas e solucionar essas questões.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Solução do Cisco Unified Wireless
- Configurações básicas dos controladores de LAN do Cisco Wireless (WLC) GUI

Componentes Utilizados

Este documento é aplicável a todos os dispositivos que participam no ambiente unificado Cisco mas não é restringido à versão de software e hardware específica.

Convenções

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

Informações de Apoio

Em Cisco o ambiente unificado, o WLC supõe um papel central. Controla a rede Wireless inteira. O Lightweight Access Points (regaços), que servem os clientes Wireless, registra-se ao WLC e transfere-se a configuração completa do WLC. A etapa inicial é verificar se o REGAÇO é registrado ao WLC. Clique o menu wireless de WLC GUI, e verifique se o REGAÇO é alistado na página.

Problemas de configuração

Para uma conexão Wireless bem sucedida, é essencial que a configuração no WLC está feita corretamente. Esta seção descreve alguns o mais geralmente - dos problemas de configuração considerados.

Má combinação SSID

O cliente usa seu SSID para identificar e associar à rede Wireless, assim que assegure-se de que o SSID esteja configurado identicamente no WLC e no cliente. A fim verificar o SSID configurado no WLC, clique a página **WLAN**. Clique o *WLAN* apropriado, e verifique o *SSID* configurado sob o *tab geral*.

Nota: *O SSID* é diferenciando maiúsculas e minúsculas. Pôde ajudar o cliente Wireless a associar ao WLAN se você suprime e recreia do WLAN.

Má combinação da Segurança

As configurações de segurança devem combinar entre o WLC e o cliente. Se o tipo do autenticação é WEP estático, verifique se a chave de criptografia apropriada/deslocamento predeterminado chave no WLC combina aquela do cliente. Se o tipo do autenticação é 802.1x ou WPA, assegure a isso a harmonia do tamanho do tipo do autenticação/chave de criptografia entre o cliente e o WLC. Para obter mais informações sobre de como configurar o WLC e o cliente para

várias soluções da Segurança, refira a autenticação em exemplos de configuração dos controladores do Wireless LAN.

Nota: Mergulhe 2 soluções da Segurança, tais como o WPA ou o 802.1x, não possa ser usado para um WLAN configurado com soluções da Segurança da camada 3, tais como a autenticação da Web ou a transmissão. Para obter mais informações sobre da Segurança compatível as soluções referem a matriz de compatibilidade da Segurança da camada 2 e da camada 3 do controlador do Wireless LAN.

WLAN deficiente

Para uma conexão Wireless bem sucedida, o WLAN correspondente deve ser ativo no WLC. À revelia, o estado do WLAN não é permitido no WLC. A fim ativar o WLAN, clique o menu **WLAN no** WLC. Uma lista de WLANs configuradas na WLC é exibida. Clique o WLAN que é configurado com o SSID a que o cliente quer associar. Sob o tab geral do os **WLAN > editam a** página, verificam a caixa do estado.

Taxas de dados Unsupported

Para um padrão particular, 802.11b/g ou 802.11a, você pode opcionalmente ajustar determinadas taxas de dados como imperativo e outras taxas de dados como apoiadas ou desabilitadas no WLC. Para uma associação bem sucedida, um cliente Wireless deve apoiar as taxas de dados que são configuradas como imperativas no WLC. A fim verificar as taxas de dados configuradas no WLC, clicar o menu **wireless no** WLC GUI, e verificar as taxas de dados configuradas sob **802.11b/g/n > rede ou 802.11a/n > opção de rede** que aparece no lado esquerdo da página. Verifique a página de suporte do vendedor do cliente para determinar isto. Se você promove o driver de cliente, pode ajudar o cliente a apoiar as taxas de dados obrigatórios.

Nota: Para a melhor Conectividade, ajuste a mais baixa taxa de dados a **imperativo no** WLC e outras taxas de dados ao **apoiado**.

Clientes deficientes

No WLC, há uma opção para desabilitar manualmente os clientes. Esta característica ajuda a impedir que os clientes desonestos tentem alcançar a rede. Verifique se o MAC address do cliente que é incapaz de associar é encontrado nos clientes deficientes alista, e, em caso afirmativo, removem-no. Você pode encontrar a lista de clientes deficientes quando você clica a **opção de clientes deficiente** sob o **menu Segurança no** GUI.

Nota: Os clientes podem ser negados a associação à rede se não habitam pelas políticas da exclusão do cliente do padrão configuradas no WLC. Para obter mais informações sobre da política da exclusão do cliente, refira a seção configurando das políticas da exclusão do cliente do manual de configuração do controlador de LAN do Cisco Wireless, a liberação 4.2.

Transmita por rádio preâmbulos

O preâmbulo de rádio (chamado às vezes um encabeçamento) é uma seção dos dados na cabeça de um pacote, que contenha a informação que os dispositivos Wireless precisam quando enviam e recebem pacotes.

Alguns clientes não apoiam o **preâmbulo curto**, assim que não podem conectar ao WLAN que tem

o **preâmbulo curto** permitido. Os preâmbulos curtos melhoram o desempenho da taxa de transferência de dados, assim que são permitidos à revelia no WLC. Para desabilitar o preâmbulo curto, clique o menu **Wireless da** GUI da WLC. Em seguida, clique no menu de rede **802.11b/g >** no lado esquerdo. *Desmarcar a* caixa **curto do preâmbulo**.

Características de Cisco Properietary - Edições com clientes da terceira parte

Se os dispositivos do cliente que são incapazes de conectar à rede são dispositivos que não é da Cisco, desabilitar alguns dos recursos proprietários de Cisco conduz a uma conexão bem sucedida. Para uma lista de características que os suportes ao cliente, contactam o vendedor do dispositivo do cliente da terceira.

Estes são alguns dos recursos proprietários importantes:

- Aironet IE - O Aironet IE contém informações como o nome do ponto de acesso, a carga, número de clientes associados e assim por diante enviadas pelo ponto de acesso nas respostas de sinalização e sonsagem da WLAN. Os clientes CCX usam essas informações para escolher o melhor ponto de acesso para se associarem.
- **MFP** — A proteção do quadro do Gerenciamento é uma característica introduzida para assegurar a integridade dos quadros do Gerenciamento, tais como a de-autenticação, a desassociação, as balizas, e as pontas de prova onde o Access point protege os quadros do Gerenciamento que transmite quando adiciona um elemento de informação do Message Integrity Check (MIC IE) a cada quadro. Toda a tentativa feita pelos intrusos para copiar, altera-se, ou a repetição o quadro invalida o MIC, que causa algum Access point de recepção, que for configurado para detectar quadros MFP, para relatar a discrepância.Esses recursos são habilitados por padrão para qualquer WLAN criada na WLC. Para desabilitar esses recursos, clique o menu WLAN na WLC. Uma lista de WLANs configuradas na WLC é exibida. Clique na WLAN em que o cliente deseja se associar. Na guia Advanced da página WLANs > Edit, desmarque as caixas correspondentes ao Aironet IE e MFP.
- **Preâmbulos de rádio** — O preâmbulo de rádio (chamado às vezes um encabeçamento) é uma seção dos dados na cabeça de um pacote que contenha a informação que o dispositivo Wireless e os dispositivos do cliente precisam de enviar e receber pacotes. Você pode ajustar o preâmbulo de rádio a longo ou a curto segundo que ajuste é apoiado no cliente Wireless.
- **Transformação da encapsulation do Ethernet** — Quando o dispositivo Wireless recebe os pacotes de dados que não são 802.3 pacotes, o dispositivo Wireless deve usar um método da transformação do encapsulamento para formatar os pacotes a 802.3. Estão aqui os dois métodos da transformação:802.1H: Este método fornece o desempenho ideal para produtos Wireless do Cisco Aironet. 802.1H é a configuração padrão.RFC1042: Use este ajuste para assegurar a Interoperabilidade com equipamento não-Cisco do Aironet wireless. O RFC1042 não fornece as vantagens da Interoperabilidade de 802.1H, mas é usado por outros fabricantes do equipamento Wireless.
- **intervalo do aperto de mão do wpa** — Alguns vendedores precisam uns intervalos mais longos do aperto de mão do wpa. Você pode usar o **comando timeout do aperto de mão do wpa do dot11** a fim mudar o intervalo do aperto de mão do wpa.
- **ssid** — Alguns vendedores exigem o ssid ser transmissão. A fim transmitir o ssid, permita o *modo de convidado* sob a configuração do ssid.

Edições do endereço IP de Um ou Mais Servidores Cisco ICM

NT

Os clientes Wireless precisam endereços IP válidos de comunicar-se com o resto da rede.

O controlador comporta-se como um roteador com um endereço IP auxiliar. Isto é, preenche o endereço IP de Gateway e os unicasts ele ao servidor DHCP através da interface dinâmica em que o cliente é instalado. Esteja assim ciente que a espião DHCP no Switches, à revelia, obstruirá estes pacotes DHCP em portas não-confiável.

Quando a oferta do DHCP retorna ao controlador, ele altera o endereço IP do servidor DHCP para o seu endereço IP virtual. A razão que faz esta é porque quando Windows vagueia entre AP, a primeira coisa faz é tentativa para contactar o servidor DHCP e para renovar seu endereço.

Com o endereço do servidor DHCP de 1.1.1.1 (que é o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual típico em um controlador), o controlador pode interceptar esse pacote e falsificar para fora Windows. Isso é igualmente porque o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual é o mesmo em todos os controladores. Se um laptop com o Windows mover para um AP em um outro controlador, ele tentará contatar a interface virtual no controlador. Devido ao evento da mobilidade e à transferência do contexto, o controlador novo a que o cliente do Windows vagueou já tem toda a informação para falsificar para fora outra vez Windows.

Se você quer usar o servidor DHCP interno, tudo que você tem que fazer está posto o endereço IP de gerenciamento como o servidor DHCP na interface dinâmica você cria para a sub-rede. Depois, atribua essa interface à WLAN. A razão pela qual o controlador precisa de um endereço IP em cada sub-rede é para que ele possa preencher o endereço do gateway DHCP na solicitação do DHCP.

Nós vemos muitos problemas do endereço IP de Um ou Mais Servidores Cisco ICM NT DHCP. Estão aqui as razões e as etapas resolver estas edições:

1. Se o tipo de autenticação configurado é uma de soluções da Segurança da camada 2, tais como o 802.1x ou o WPA, o cliente deve com sucesso autenticar para obter um endereço IP válido. Primeira verificação se o cliente é autenticado com sucesso.**Nota:** Uma exceção é se o cliente está configurado para soluções da Segurança da camada 3, tais como a autenticação da Web, ou o cliente da transmissão da Web está atribuído um endereço IP de Um ou Mais Servidores Cisco ICM NT antes da autenticação.
2. Cada WLAN definido no WLC é traçado a uma interface dinâmica do WLC, que é configurado com um VLAN que pertença a uma sub-rede única. Os clientes que associam a este WLAN são endereços IP atribuídos da sub-rede da relação do VLAN. Verifique se a sub-rede IP e o gateway deste WLAN são definidos no servidor DHCP para que o cliente obtenha um endereço IP de Um ou Mais Servidores Cisco ICM NT nesta sub-rede. Refira a documentação do vendedor apropriado para configurar o servidor DHCP.**Nota:** Como uma condição prévia, a verificação se o servidor DHCP é alcançável do WLC e se o serviço DHCP é girada sobre.
3. Certifique-se de que o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP está definido corretamente na relação do WLC que é traçado ao WLAN. A fim verificar isto, clique o menu do **controlador no** GUI. Clique o menu das **relações no** lado esquerdo, e verifique o campo do **servidor DHCP**. Na mesma página, certifique-se da relação esteja traçada a uma *porta física* que seja ascendente e ativa. A fim pesquisar defeitos problemas relacionados DHCP, para usar os comandos debug dhcp packet enable

e **para debugar o mensagem DHCP permite no** WLC.**Nota:** Você pode igualmente configurar o WLC como um servidor DHCP. Para obter mais informações sobre de como configurar o DHCP separe no WLC, referem a utilização do GUI para configurar a seção DHCP do manual de configuração do controlador de LAN do Cisco Wireless do documento, a liberação 5.0.

4. O proxy DHCP é permitido à revelia no WLC. Unicasts WLC o pacote ao servidor DHCP configurado na relação do WLAN ou no WLAN própria. Se o servidor DHCP não apoia o comportamento do proxy do DHCP Cisco, desabilite o proxy DHCP no WLC. Para obter mais informações sobre de como desabilitar o proxy DHCP no WLC, refira configurar a seção do proxy DHCP do manual de configuração do controlador de LAN do Cisco Wireless, a liberação 5.2.
5. O WLC conecta geralmente à rede ligada com fio através de um interruptor. Verifique se as portas de switch que estão conectadas ao WLC e ao servidor DHCP são configuradas como o tronco e que os VLAN apropriados estão permitidas naquelas portas. Para obter mais informações sobre de como configurar os switch Cisco, refira configurar à porta do switch de Camada 2 que conecta ao WLC como a seção da porta de tronco do convidado WLAN e WLAN interno do documento usando o exemplo de configuração WLC.
6. Não são permitidos aos clientes estáticos associar ao WLAN se o **ADDR DHCP. O campo da atribuição** é permitido para o WLAN. Esta opção necessita que todos os clientes que associam a este WLAN devem obter endereços IP de Um ou Mais Servidores Cisco ICM NT com o DHCP. A fim verificar se esta opção é permitida, clique o menu WLAN no WLC GUI. Uma lista de WLANs configuradas na WLC é exibida. Clique o WLAN apropriado. Vá ao **guia avançada** e encontre o campo da **atribuição de endereço de DHCP**.
7. Alguns servidores DHCP, tais como um Cisco PIX Firewall, não apoiam serviços da transmissão de DHCP. Aceitam somente pacotes DHCP da transmissão, não nenhuns pacotes do unicast de um agente de transmissão de DHCP, assim que assegure-se de que os clientes DHCP estejam conectados diretamente à relação em que o server é permitido.**Nota:** Verifique o documento apropriado do vendedor para ver se há o apoio de transmissão de DHCP.

Problemas com o cliente

Éigualmente importante que as coisas são no lugar no lado do cliente. Execute estas verificações no lado do cliente:

1. Às vezes, o cartão do cliente não é reconhecido pelo computador. Nesse caso, tente o cartão em um entalhe diferente. Se não trabalha, tente-o em um computador diferente. Para obter mais informações sobre das edições dentro da instalação, refira a seção de Troubleshooting do Cisco Aironet 340 do documento, dos 350, e do Guia de Instalação e Configuração dos adaptadores cliente do Wireless LAN CB20A para Windows.**Nota:** Certifique-se de que a placa Wireless é compatível com o sistema operacional que é instalado na máquina. Isto pode ser verificado da folha de dados do cartão do cliente.
2. Verifique se o cliente é instalado corretamente na máquina. O estado do cartão do cliente pode ser verificado da tela do **gerenciador de dispositivo de Windows**. Procure a mensagem que lê, *"este dispositivo está trabalhando corretamente."* Se não é, indica que os direcionadores não estão instalados corretamente. Tente desinstalar o direcionador e

reinstalar os direcionadores na máquina. A fim desinstalar os direcionadores, para clicar com o botão direito o adaptador Wireless da tela do gerenciador de dispositivo e do **desinstalar do** clique. Para obter mais informações sobre de como reinstalar o adaptador cliente, refira a instalação da seção do adaptador cliente do Cisco Aironet 340 do documento, dos 350, e do Guia de Instalação e Configuração dos adaptadores cliente do Wireless LAN CB20A para Windows.**Nota:** Se você usa o ACU para configurar o cartão do cliente, certifique-se de que o rádio não está desabilitado no ACU. Além, verifique se o estado do cartão é permitido sob a **conexão de rede no** Control Panel de Windows.**Nota:** Use somente um software do suplicante para a placa Wireless. Recomenda-se sempre usar vendedor-forneceu o suplicante para o cartão. Como uma opção secundária, você pode usar esse fornecido pelo vendedor PC ou o WZC fornecido por Windows.**Nota:** Termine estas etapas a fim debugar WZC:Use o **traçado ajustado ras do netsh * comando enabled** a fim girar sobre a eliminação de erros WZC.Use o **traçado ajustado ras do netsh *** comando **deficiente** a fim desligar a eliminação de erros WZC.Os logs são escritos a *C:\Windows\tracing*. *eapol.log*, *rastls.log*, e *wzctrace.log* são os logs os mais importantes.**Nota:** Refira diagnósticos wireless e Troubleshooting para mais informação.

3. A configuração no cliente deve combinar aquela do WLC. Isto refere principalmente o SSID e a configuração de segurança no cliente. Se você usa o utilitário Cisco para configurar o cliente, refira a utilização da seção do gerente do perfil do Cisco Aironet 340 do documento, dos 350, e do Guia de Instalação e Configuração dos adaptadores cliente do Wireless LAN CB20A para Windows.
4. Se você é incapaz de transferir dados, mesmo depois um wireless association bem sucedido, tente desabilitar todos adaptadores restantes assim como aqueles do VPN e de adaptadores prendidos. Se há mais de um adaptador Wireless na máquina, desabilite outros adaptadores para evitar conflitos entre eles.
5. Se você encontra problemas de conectividade somente com um único cliente, tente promover os direcionadores e o firmware desse cliente. Se você encontra problemas de conectividade com uma maioria dos clientes e do você para ter ordenado para fora outras edições, escolha promover o WLC.
6. Assegure-se de que os dispositivos, isto é, cliente e o WLC, sejam Wi-fi certificado para evitar todas as questões de interoperabilidade relativas à Segurança e operações.
7. Se você usa uma máquina de Windows, certifique-se de que você instalou todas as correções de programa ou hotfix os mais atrasados da Segurança disponíveis de Microsoft. Se você usa a utilidade do cliente do Windows, certifique-se de que você instalou a correção de programa a mais atrasada disponível de Microsoft.
8. Alguns clientes respondem lentamente à autenticação de EAP. Isto conduz aos intervalos no WLC, e você pode receber este Mensagem de Erro no WLC:

```
Tue Jul 26 16:46:21 2005: 802.1x 'timeoutEvt' Timer expired for station <Mac address of the
client>
```

Em resposta a esta mensagem, aumente os valores de intervalo EAP no WLC para fornecer o tempo suficiente para que o cliente autentique. Use estes comandos ajustar os temporizadores EAP no WLC:

```
config advanced eap identity-request-timeout <1-120 secs>
config advanced eap identity-request-retries <1-20>
 !--- Specifies the amount of time and the maximum number of times the WLC attempts to send an
EAP identity request to wireless clients. config advanced eap request-timeout <1-120>
config advanced eap request-retries <1-20>
 !--- Specifies the amount of time and the maximum number of t imes the WLC attempts to send EAP
```

```
request to the Radius Server . config advanced eap eapol-key-timeout <1-5>
config advanced eap eapol-key-retries <0-4>
 !--- Specifies the amount of time and the maximum number of times the WLC attempts to negotiate
the encryption key.
```

Edições RF

A interferência RF é uma das causas principais para a conexão ruim. A interferência pode ser causada por redes adjacentes do 802.11 ou por outras fontes, tais como os fornos de micro-ondas ou os telefones sem fio que se operam na mesma frequência. A interferência causada por redes adjacentes do 802.11 é de dois tipos:

- **Interferência do co-canal:** Quando os Access point, cuja a área de cobertura sobrepõe, estiverem configurados no mesmo canal ou os canais com frequências de sobreposição, ele causarem problemas de conectividade para clientes na área de cobertura de sobreposição. A fim evitar esta edição, muda o número de canal a um canal desobreposição, ou afasta o Access point mais distante de modo que suas áreas de cobertura não sobreponham. Por exemplo, em 802.11b/g, a rede canaliza 1, 6, e 11 NON-está sobrepondo os canais.
- **Interferência adjacente do canal:** Quando os Access point são colocados demasiado perto entre si ou usam os níveis da potência a rendimento elevado, causa a interferência, mesmo quando os Access point são configurados nos canais desobreposição. Diminua a potência do Access point fixar esta edição.**Nota:** os canais desobreposição são chamados igualmente os canais adjacentes, que explica a *interferência adjacente do canal do* nome.

Use analisadores de espectro para encontrar origens de interferência, tais como os fornos de micro-ondas ou os telefones sem fio que se operam na escala 2.4 gigahertz, ou os dispositivos que se operam na escala gigahertz 5. Remova os origens de interferência uma vez que são identificados. Alternativamente, você pode mudar o padrão em que sua rede de comunicação Wireless se opera, por exemplo, de 802.11b/g a 802.11a para evitar a interferência.

Um outro aspecto importante para uma comunicação eficaz RF é intensidade de sinal. A intensidade de sinal deficiente conduz à conexão intermitente. Os obstáculos, tais como paredes, metais, absorvem e refletem a energia RF, que reduz a intensidade de sinal. Aumente a potência ao nível exigido no Access point fornecer a cobertura adequada. Você pode igualmente usar antenas de ganho elevado para estender a escala e a intensidade de sinal, mas assegura-se de que seja FCC aprovado para se operar com o dispositivo.

Nota: O Signal to Noise Ratio (SNR), que é a diferença entre a intensidade de sinal e o ruído RF (o sinal ou a energia RF de outras fontes que se operam na mesma frequência como a rede Wireless), é um fatora chave para medir a qualidade do link. Um SNR mais alto indica uma boa qualidade do link, que conduza a transferência de dados mais rápida. Um valor mais baixo indica a qualidade ruim, que conduz à conectividade intermitente ou ao desempenho ruim. Os analisadores de pacote wireless/software da análise de site podem mostrar-lhe o SNR e a taxa de transferência em um local particular.

No ambiente unificado Cisco, há um conceito chamado Radio Resource Management (RRM) executado nos WLC. O RRM é um software encaixado no controlador, que atua como um coordenador do acessório RF para fornecer consistentemente o Gerenciamento do tempo real RF de sua rede Wireless. Toma automaticamente de todas as edições mencionadas RF. Para obter mais informações sobre de RRM, refira a seção de gerência de recursos de rádio configurando do manual de configuração do controlador de LAN do Cisco Wireless do documento, a liberação 5.0.

Mensagens de erro

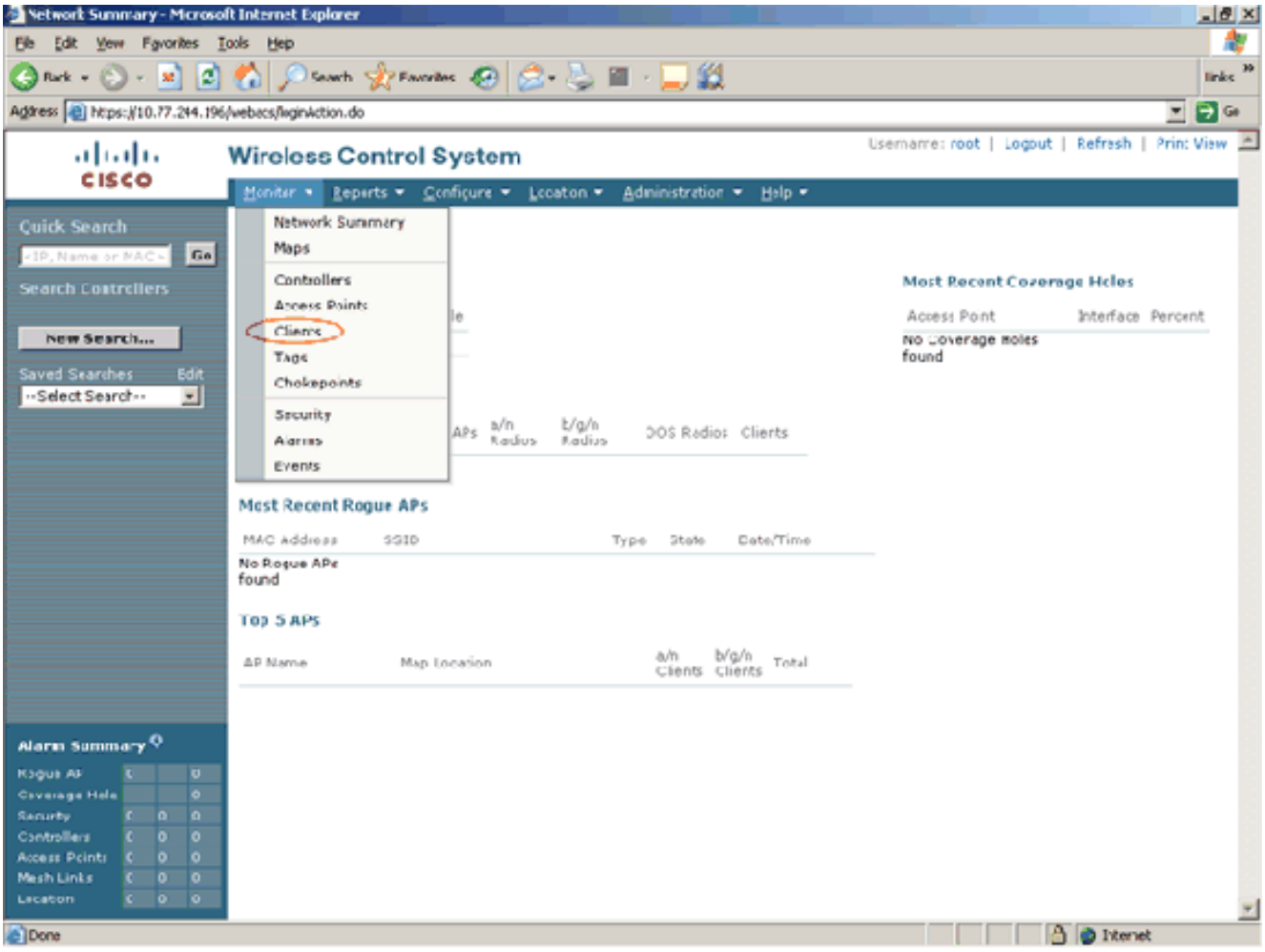
Entre o curso da conectividade de cliente, você pode receber mensagens de erro múltipla, nos lados WLC e de cliente.

- **O cliente é um ou outro incapaz de obter um atraso do endereço IP de Um ou Mais Servidores Cisco ICM NT ou do encontro em obter o endereço IP de Um ou Mais Servidores Cisco ICM NT com o DHCP. O DHCP debugar no controlador indica este:**
  `Sun Nov 9 22:09:05 2008: <mac address of the client> DHCP processing DHCP NAK` *O DHCP NAK* é enviado geralmente pelo servidor DHCP para indicar uma tentativa pelo cliente de obter um endereço IP de Um ou Mais Servidores Cisco ICM NT da sub-rede a que não pertence. Isto ocorre geralmente quando um cliente vagueia de um WLC a outro, onde o mesmo WLAN está atribuído um VLAN diferente.Configurar o proxy DHCP no WLC para fornecer um reparo para este.

Pesquisando defeitos problemas de cliente com WCS

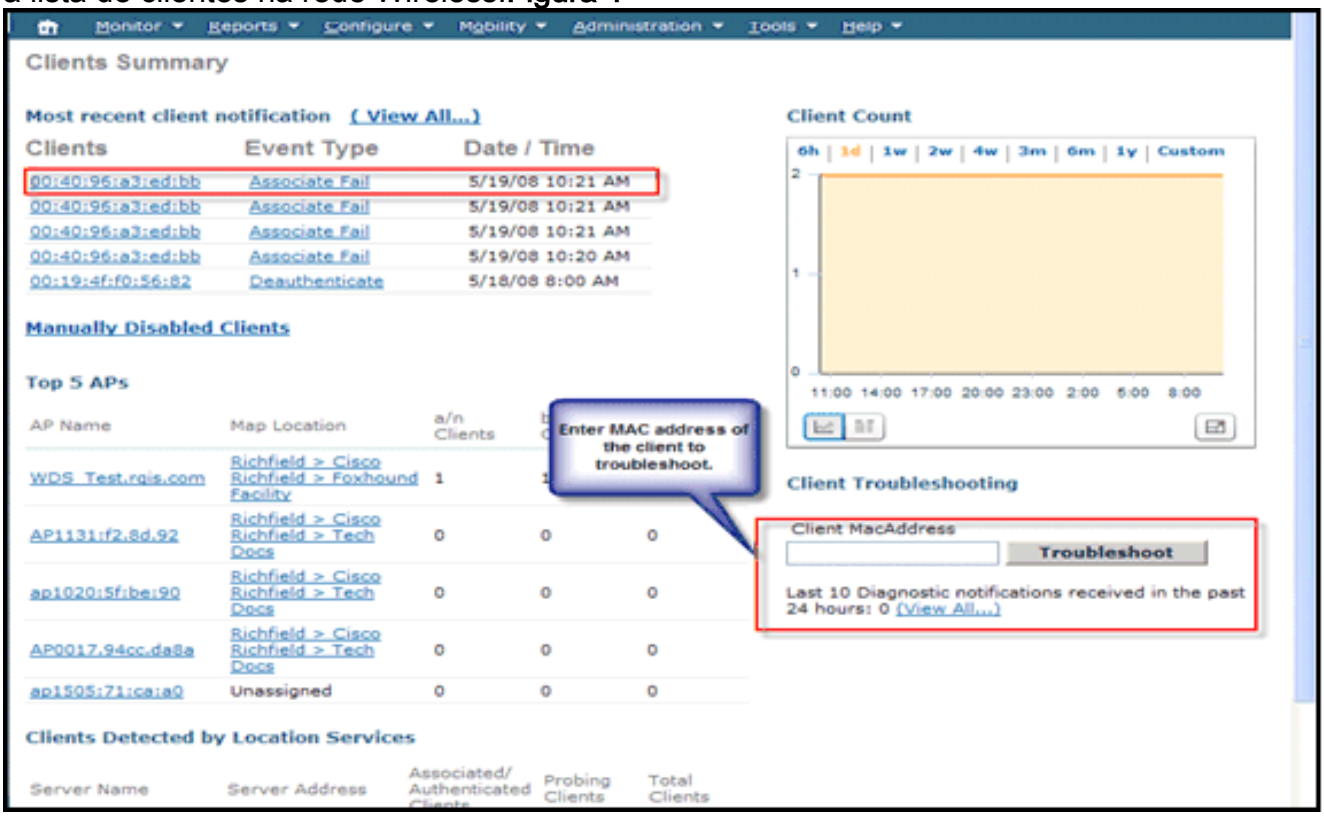
O WCS pode ser usado para pesquisar defeitos edições cliente-relacionadas em um ambiente Wireless. Faz este com a ajuda da ferramenta de Troubleshooting construída no WCS. A fim pesquisar defeitos um cliente com o WCS, necessidade de usuários de executar estas etapas

1. Da página do painel WCS, clique o menu do **monitor** e escolha **clientes da** lista.

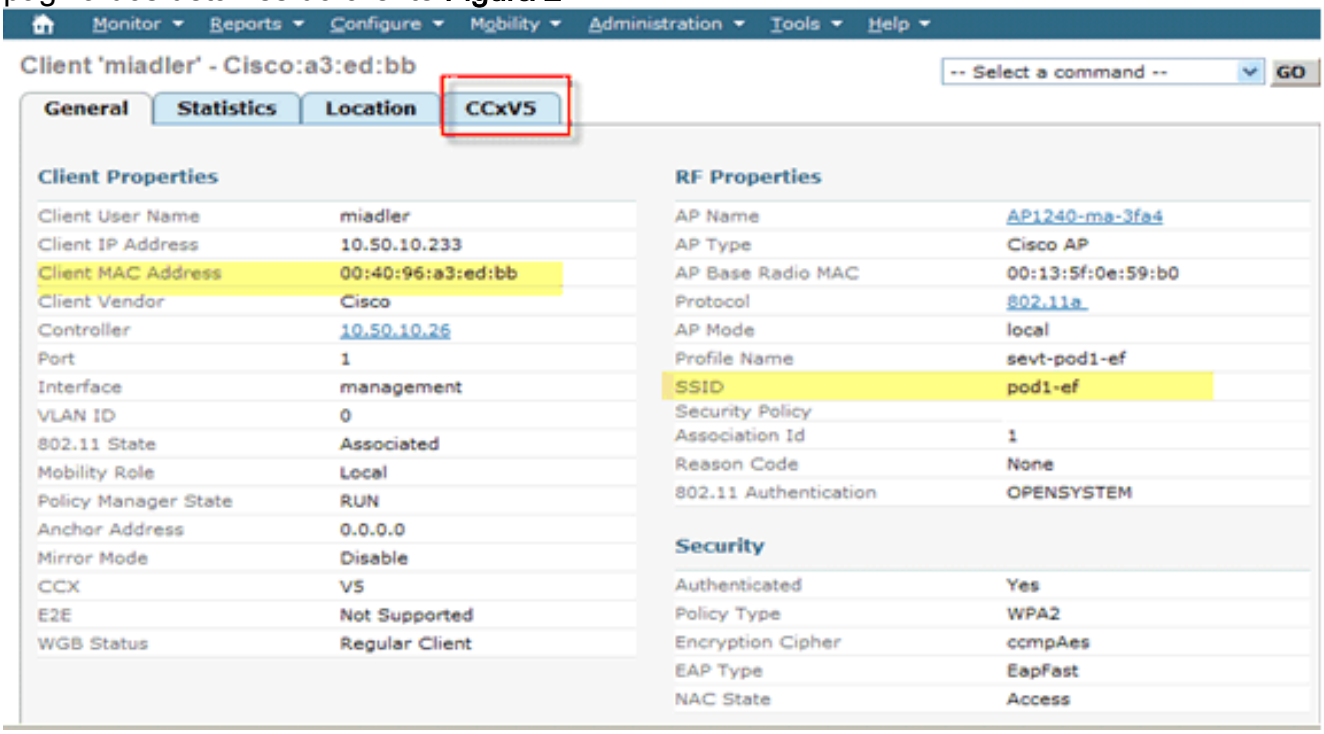


2. Isto traz acima a página de sumário do cliente segundo as indicações de figura 1, que indica

a lista de clientes na rede Wireless.**Figura 1**



3. Clique um cliente para obter detalhes tais como o SSID ou o método de autenticação de um cliente específico. Figura 2 mostra um exemplo deste. A caixa de diálogo da **pesquisa de defeitos no** lado direito inferior da página de sumário do cliente mostrada em figura 1 permite que os usuários entrem no MAC address do dispositivo para pesquisar defeitos. Isto trá-lo à página da ferramenta de Troubleshooting segundo as indicações de figura 3. em cima da identificação e a seleção do cliente a pesquisar defeitos, usuários é presentado com a página dos detalhes do cliente:**Figura 2**



Pesquisando defeitos o WEP

Os clientes Wireless do legado que ainda usam os mecanismos de segurança WEP são

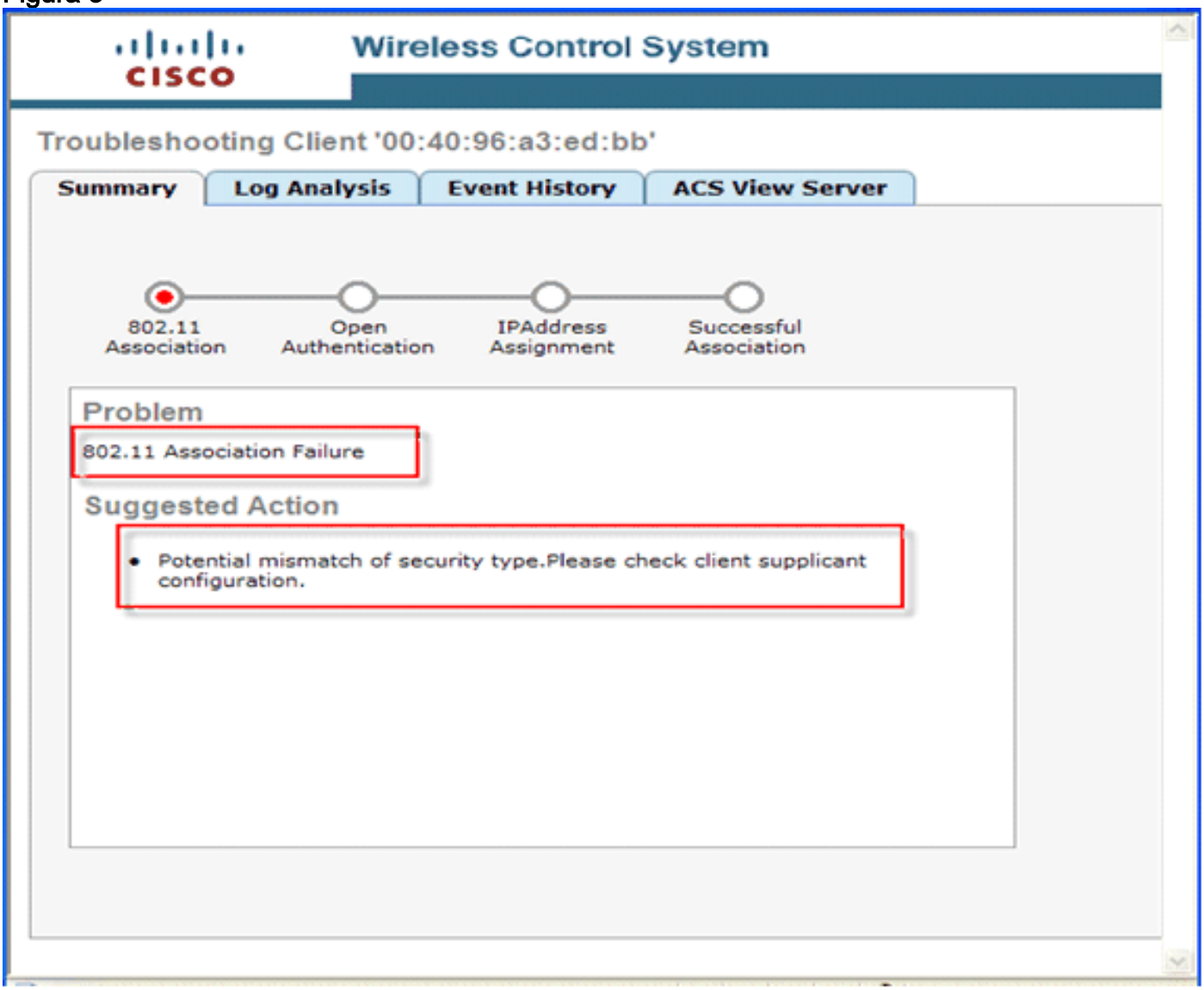
frequentemente duros de pesquisar defeitos. Execute estas verificações no cliente e no AP:

- Comprimento de chave de WEP (e incompatibilidades de chave)
- Deslocamento predeterminado de chave de WEP (e maus combinação da configuração)
- Método de autenticação configurado (abra contra a chave compartilhada)

Má combinação da autenticação

Embora a captação dos pacotes possa ser um processo fastidioso, a ferramenta de Troubleshooting do cliente WCS pode facilmente ajudar a indicar onde o problema existe. Frequentemente, este "TIP" pequeno é o que reduz o tempo de Troubleshooting. Figura 2 mostra a **ferramenta de Troubleshooting WCS**. Como apresentado na figura, a fase problemática é identificada e visualizada, que ajusta a fase para a análise detalhada.

Figura 3



Má combinação do deslocamento predeterminado de chave de WEP

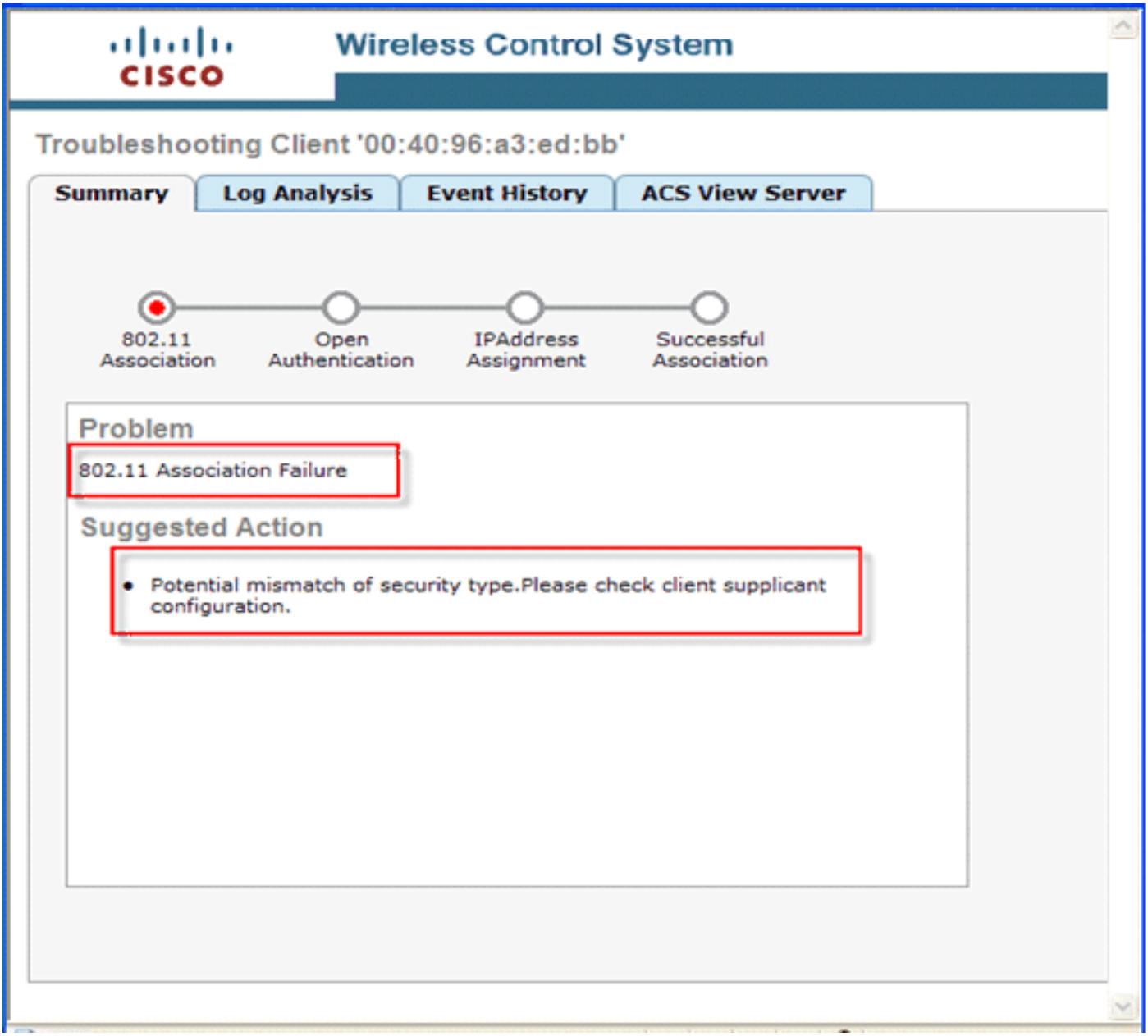
Geralmente, você pode configurar até 4 chaves de WEP no cliente e no AP. Uma das chaves é escolhido como a chave transmissora. Isto deve combinar entre o cliente e o AP. Por exemplo, se a chave 2 é escolhida como a chave transmissora no cliente, isto deve combinar com a chave 2 no AP, mas o AP pode ter uma chave diferente do que a chave transmissora. O outro problema é

frequentemente este: os vendedores do cliente e da infraestrutura interpretam as especificações diferentemente, que causa aplicações diferentes no produto. Um exemplo comum é o uso dos deslocamentos predeterminados chaves de 0 a 3 contra os deslocamentos predeterminados chaves de 1 a 4. Isto pode conduzir à configuração incompatível e a falha na conexão tenta. Nesse ponto, a toda atenção do pagamento à “chave ID” arquivada no pacote descodifica, que diz se aquela é a causa de raiz do problema.

Pesquisando defeitos o WPA-PSK

O Troubleshooting WPA-PSK é similar ao WEP de várias maneiras. A maioria de falhas de tentativa são devido às configurações incorretas na chave. Com a ferramenta de Troubleshooting do cliente WCS, os administradores podem recolher os logs da transação WPA. Os logs, como destacados abaixo, indicador onde o problema potencial pode estar *(configuração incorreta da chave pré-compartilhada no cliente neste exemplo particular)* e é derivado da aba da **análise do log da** ferramenta de Troubleshooting do cliente do WCS. Estabelecer um WLAN com o WPA-PSK como a política de segurança da camada 2 e configura o suplicante do cliente com um PSK incorreto. Estes são logs de chaves desconfigurados PSK nos eventos:

```
<TIMESTAMP> INFO 10.10.10.2
   Controller association request message received.
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client.
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting requires 802 1x authentication.
<TIMESTAMP> INFO 10.10.10.2
   Client moved to associated state successfully.
<TIMESTAMP> ERROR 10.10.10.2
   802.1x authentication message received, static dynamic wep supported.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   EAPOL-key is retransmitted.
<TIMESTAMP> ERROR 10.10.10.2
   Expecting EAPOL key from client but not received yet.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Excluding client as max EAPOL-key re-transmissions reached.
<TIMESTAMP> ERROR 10.10.10.2
   Client 802.1x authentication failure exceeded the limit. <TIMESTAMP> ERROR 10.10.10.2 EAPOL-
key has possible incorrect psk configuration.
```

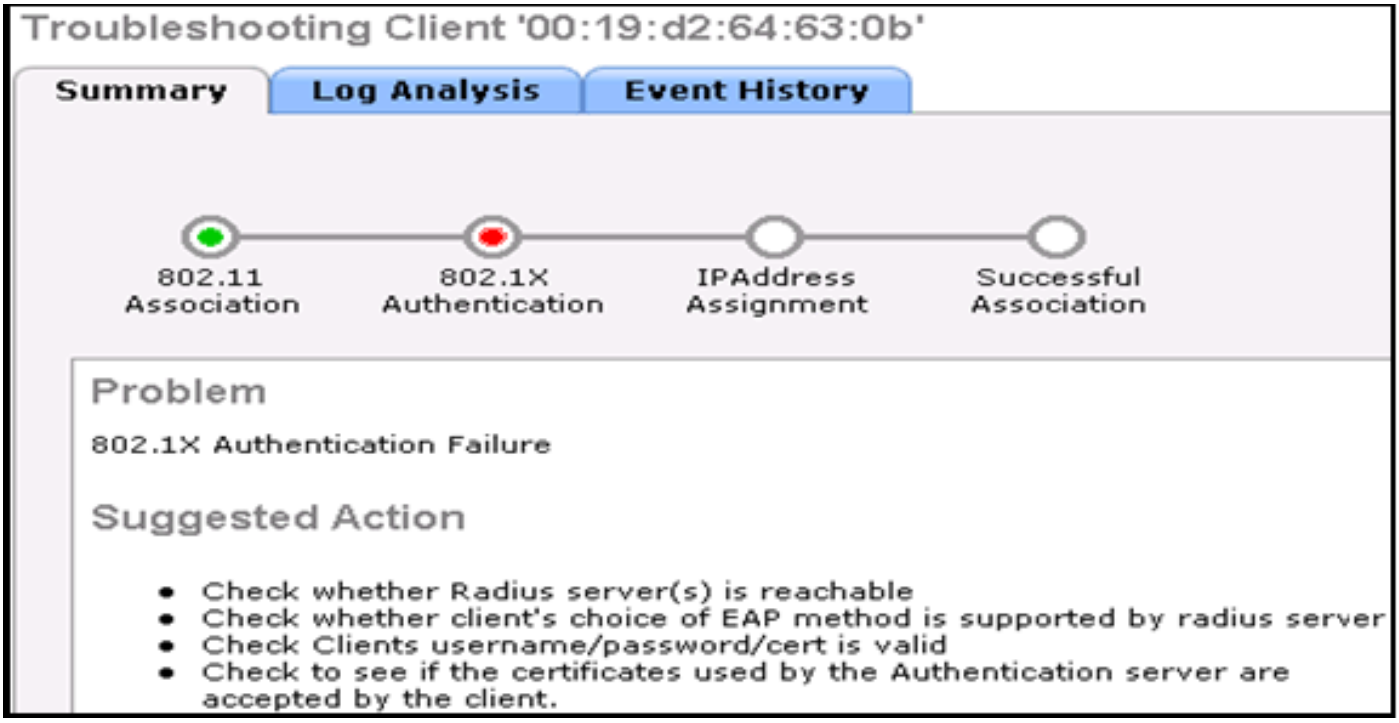


Pesquisando defeitos o 802.1X

Como a adoção WLAN se torna patente, fase dos clientes do legado - para fora; o 802.1x é o sentido para a maioria de disposições futuras. Pode haver uma variedade de edições misconfiguration-relacionadas na corrente (servidor AAA do <> da rede do <> L2/L3 do <> WLC do <> AP do cliente). Aqui supõe-se que as coisas são no lugar entre o WLC e o servidor AAA. As edições que elevaram entre o suplicante (cliente) e o servidor AAA são geralmente estas:

- Tipo errado EAP
- Certificados expirados errados dos credentials/
- Método interno errado EAP

No lado do cliente, altere as credenciais do usuário sob configurações de segurança; por exemplo, incorpore a senha errada e torne a colocar em funcionamento o mesmo teste. A ferramenta de Troubleshooting indica exatamente onde o problema se encontra, assim como a ação sugerida.



Clique a aba da **análise do log na** figura mostrada acima e verifique os logs para ver se há toda a indicação de uma autenticação mal sucedida do 802.1x.

```
<TIMESTAMP> INFO 10.10.10.2
   Received EAP Response from the client.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> INFO 10.10.10.2
   Received Access-Challenge from the RADIUS server for the client
<TIMESTAMP> INFO 10.10.10.2
   Sending EAP request to client from radius server.
<TIMESTAMP> INFO 10.10.10.2
   EAP response from client to AP received.
<TIMESTAMP> INFO 10.10.10.2
   Radius packet received
<TIMESTAMP> ERROR 10.10.10.2 Received Access-Reject from the RADIUS server for the client.
<TIMESTAMP> ERROR 10.10.10.2 Received eap failurefrom the client.
```

Pesquisando defeitos o Web-AUTH

Geralmente, a boa prática de Troubleshooting deve incluir um controle da “do estado do gerente política” do cliente que tem edições. Enquanto se confirma no screen shot WCS abaixo, o cliente na pergunta está colado no estado *WEBAUTH_REQD*. Isto significa que o processo do 802.11 está completo sem nenhuns erros, e estes possíveis problemas podem ocorrer:

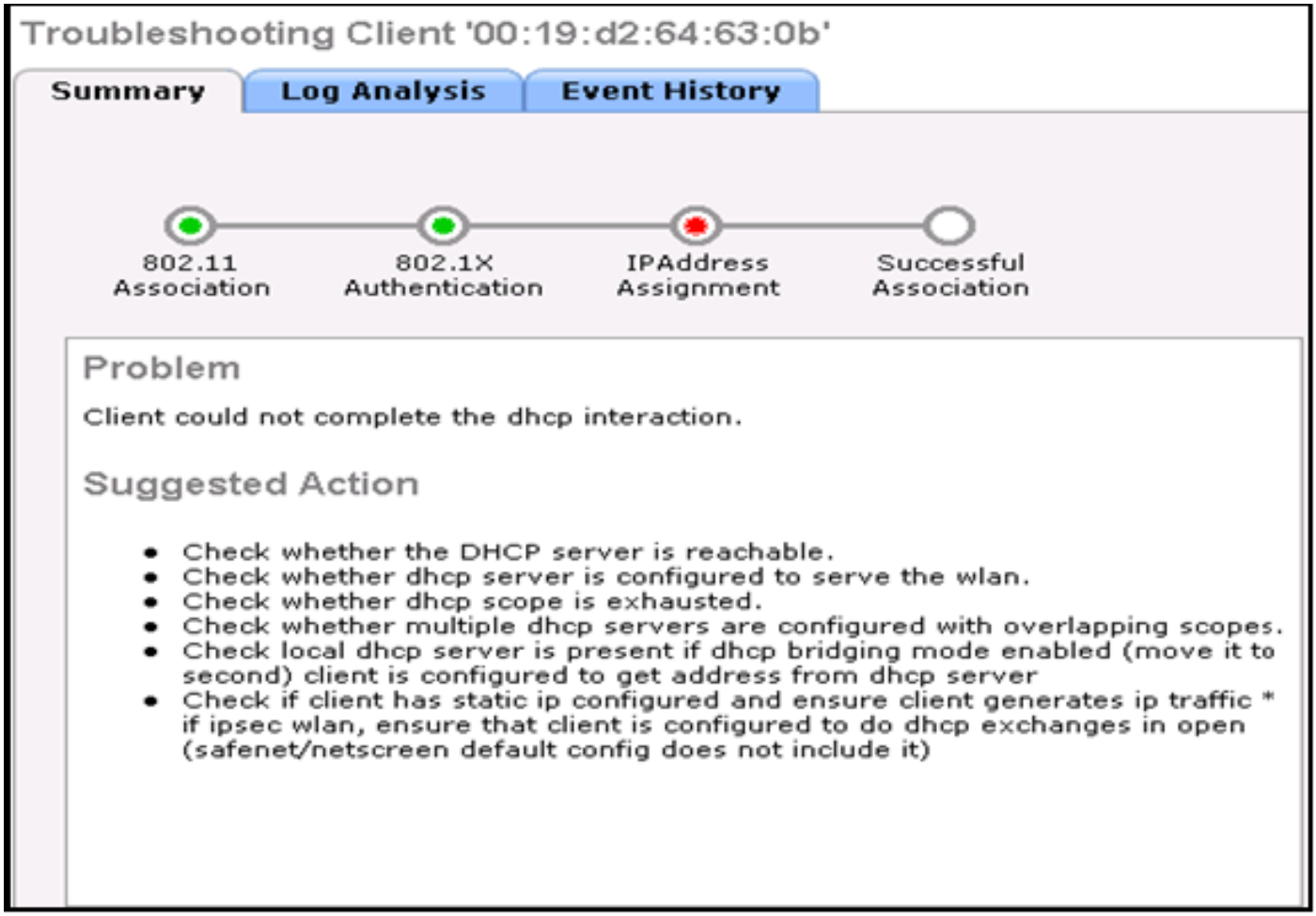
- Nome de usuário incorreto/senha
- Aplicação incorreta ACL (para alcançar o server externo do Web-AUTH, se alguns)
- DNS não configurado corretamente e mais**Nota:** Para obter mais informações sobre da autenticação da Web do Troubleshooting, refira o exemplo de configuração da autenticação da Web do controlador do
  documento.

Os logs recolhidos do WCS indicam que o processo do Web-AUTH não foi bem sucedido. Tal situação pode ser simulada no laboratório se você ajusta a política da camada 3 WLAN ao Web-AUTH e não termina o processo do Web-AUTH nem incorpora credenciais incorretas/inexistentes do início de uma sessão. Verifique a seção sumária da ferramenta de Troubleshooting do cliente para saber onde o problema ocorreu. Você vê que estes entram o WCS:

```
 <TIMESTAMP> INFO 10.10.10.2
   Controller association request message received
<TIMESTAMP> INFO 10.10.10.2
   Received reassociation request from client
<TIMESTAMP> INFO 10.10.10.2
   The wlan to which client is connecting does not require 802 1x authentication
<TIMESTAMP> INFO 10.10.10.2
   Client web authentication is required <TIMESTAMP> INFO 10.10.10.2 Client moved to associated
state successfully <TIMESTAMP> INFO 10.10.10.2 Controller association request message received
```

Pesquisando defeitos o DHCP e o endereçamento de IP

Frequentemente, os dispositivos do cliente são usados em mais de uma rede Wireless. Um exemplo pode ser uso do empregado de um dispositivo corporativo em uma HOME ou em uma rede pública. Um empregado pode ter atribuído um endereço IP estático na rede home. Conecta à rede corporativa com um endereço IP estático previamente atribuído sem o o seu/seu conhecimento. Isto conduz a um problema de conectividade, que possa facilmente ser indicado com o auxílio da série do Troubleshooting do cliente WCS (como indicado abaixo). A maioria das edições neste reino encontra-se no cliente Wireless, mas este pode igualmente apontar para um problema potencial na infraestrutura ligada com fio, tal como um espaço esgotado, o espaço incorreto, a tentativa etc. criar esta encenação quando você atribui um endereço IP estático incorreto no cliente ou muda os parâmetros do escopo de DHCP no interruptor.



Informações Relacionadas

- Manual de configuração do controlador de LAN do Cisco Wireless, liberação 5.1
- Gerência de recursos de rádio sob redes Wireless unificadas
- Suporte Técnico e Documentação - Cisco Systems