

Bridges de grupo de trabalho com exemplo de configuração da autenticação de PEAP

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração do bridge de grupo de trabalho](#)

[Certificado de CA na instalação do bridge de grupo de trabalho](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Debugar o bridge de grupo de trabalho](#)

[Debugar o controlador do Wireless LAN](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve o suporte aprimorado para os bridges de grupo de trabalho (WGB), que inclui:

- Apoio protegido do protocolo extensible authentication (PEAP) para o WGB. Um Access point configurado como um WGB pode agora associar a um ponto de acesso raiz com o PEAP.
- Melhorias quando o cliente WGB vaguear.
- Confiança quando os WGB rápidos vaguearem. A unidade está permitida uma nova tentativa adicional quando precisa de reassociar ao ponto de acesso raiz.
- Melhoria no método que os WGB se usam para selecionar do “o Access point melhor pai”. Os WGB podem compartilhar de histórias da associação com os pontos de acesso raiz, que podem construir e compartilhar de uma lista dos melhores pontos de acesso raiz entre WGB. Este método ajuda WGB seleciona o melhor ponto de acesso raiz quando vagueiam.
- Apoio de VideoStream em WGB quando usado como um cliente. VideoStream melhora a confiança de um córrego do Protocolo IP multicast quando converte o frame de transmissão múltipla, sobre o ar, a um frame de unicast. VideoStream não foi apoiado para clientes WGB em liberações precedentes porque os clientes prendidos de um WGB não podem ser adicionados à tabela do Multicast do controlador do Wireless LAN (WLC). Nesta liberação, o WGB é adicionado à tabela do Multicast WLC, e o WGB converte o frame de unicast de VideoStream em um frame de transmissão múltipla dos Ethernet e envia-o para fora a seus

clientes prendidos. A fim permitir VideoStream para WGB, inscreva o **comando enable do prender-cliente do fluxo de mídia configurar no WLC**.

O outro documento nesta série

- [Como usar o aIOS WGB com autenticação EAP-TLS em uma Cisco Unified Wireless Network](#)
- [Bridges de grupo de trabalho em um exemplo da configuração de rede do Cisco Unified Wireless](#)

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada a liberação em 15.2(2)JA do Cisco IOS ® Software ou em mais tarde.

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

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Configurar

Nesta seção, você é apresentado com a informação para configurar um WGB com o PEAP junto com o desenvolvimento baseado controlador unificado Cisco. Neste exemplo, os 1260 Access point autônomos são configurados como um WGB e conectam à rede de pouco peso do protocolo do Access point (LWAPP). Use este Service Set Identifier (SSID), **WGB-PEAP**, para a conexão ao WLAN e use o PEAP para a autenticação do WGB à rede LWAPP.

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes [registrados](#)).

Diagrama de Rede

Este documento usa a instalação de rede mostrada em figura 1:

Figura 1

Configuração do bridge de grupo de trabalho

A fim configurar o WGB, termine estas etapas:

1. Ajuste o hostname, o Domain Name, e a época do WGB como necessário. O hostname deve combinar o username incorporado para ele no ACS como na [etapa](#) precedente: `ap#configure terminal ap(config)#hostname WGB-Client WGB-Client(config)#` O tempo deve estar correto para que as certificações trabalhem (**comando clock set** ou para configurar um servidor SNTP). `WGB-Client#clock set 14:00:00 5 Dec 2011`
2. Configurar o ponto confiável para CA. `WGB-Client#configure term WGB-Client(config)#crypto pki trustpoint WGB-PEAP WGB-Client(config)#enrollment terminal WGB-Client(config)#subject-name CN=Wireless-CA` **Nota:** O comando `subject-name CN=<ClientName>` é exigido. Sem ele, o Microsoft Certificate Authority (CA) não emite o certificado e recebe esta Mensagem de Erro, "o nome do sujeito do pedido é inválido ou demasiado longo. 0x80094001". `WGB-Client(config)#revocation-check none` **Nota:** O comando `none` da **revogação-verificação** é necessário para evitar o problema descrito na identificação de bug Cisco [CSCsi07349](#) (**clientes registrados somente**). O WGB dissocia-se/reassocia-se frequentemente e toma-se um muito tempo reconectar. `WGB-Client(config)#rsa-keypair manual-keys 1024`

[Certificado de CA na instalação do bridge de grupo de trabalho](#)

A fim instalar o certificado de CA no WGB, termine estas etapas:

1. Obtenha uma cópia do certificado de CA.
2. Consulte ao lugar do crtsrv em seu server de CA; por exemplo: `http:// <ca-server-ip-address>/crtsrv`
3. **Transferência** do clique um **certificado de CA**, um **certificate chain**, ou um **CRL**.
4. Da lista de drop-down do método de codificação da escolha, escolha **Base64**.
5. Clique o **certificado de CA da transferência**.
6. Salvar o arquivo de .cer.
7. Instale o certificado de CA: Entre no **pki cripto autenticam** o comando **CUT-PASTE**. Entre no certificado de CA codificado base-64. Termine com uma linha em branco ou a palavra "parada" na última linha por si só. Cole o texto do arquivo de .cer transferido na etapa precedente. A instalação certificada olhará como este exemplo. `-----BEGIN CERTIFICATE---`

```
--
[ ... ]
-----END CERTIFICATE-----

quit

Certificate has the following attributes:

Fingerprint: 45EC6866 A66B4D8F 2E05960F BC5C1B76

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported
```

Após a instalação certificada, a configuração AP deve olhar como este exemplo:

```
===== PuTTY log 2012.11.07 16:49:51 =====
show run Building configuration... Current configuration : 4822 bytes ! ! Last configuration
change at 16:22:57 UTC Wed Nov 7 2012 ! NVRAM config last updated at 16:23:35 UTC Wed Nov 7 2012
! NVRAM config last updated at 16:23:35 UTC Wed Nov 7 2012 version 15.2 no service pad service
timestamps debug datetime msec service timestamps log datetime msec service password-encryption
! hostname WGB-Client ! logging rate-limit console 9 enable secret 5
```

```

$1$8cu.$a00dIhVntjLuESjgkiK0A. ! no aaa new-model ! ! dot11 syslog ! dot11 ssid WGB-PEAP
authentication open eap PEAP authentication network-eap PEAP authentication key-management wpa
dot1x credentials PEAP dot1x eap profile PEAP infrastructure-ssid ! eap profile PEAP method peap
! crypto pki token default removal timeout 0 ! crypto pki trustpoint WGB-PEAP enrollment
terminal subject-name CN=Wireless-CA revocation-check none rsakeypair WGB 1048 ! ! crypto pki
certificate chain WGB-PEAP certificate ca 5CC74BD9508B78AF4AB5C5F84C32AC2A 3082049E 30820386
A0030201 0202105C C74BD950 8B78AF4A B5C5F84C 32AC2A30 0D06092A 864886F7 0D010105 05003048
31133011 060A0992 268993F2 2C640119 1603636F 6D311B30 19060A09 92268993 F22C6401 19160B43
522D5769 72656C65 73733114 30120603 55040313 0B576972 656C6573 732D4341 301E170D 31323131
30353232 32343034 5A170D31 37313130 35323232 3834385A 30483113 3011060A 09922689 93F22C64
01191603 636F6D31 1B301906 0A099226 8993F22C 64011916 0B43522D 57697265 6C657373 31143012
06035504 03130B57 6972656C 6573732D 43413082 0122300D 06092A86 4886F70D 01010105 00038201
0F003082 010A0282 010100E5 3DEC1126 3EE00F34 9E263E21 BB702E5F EA5833B2 8B3A0FE1 7A6171B1
6D8E96AB 961F3713 49A66832 BC9FFC6D DF4E2795 C83D239A 055A2D9B 0A9E010D 64ABEC56 026F3CD9
B23152F6 39E1B9E0 CEA507D0 D932EE1B AECDCD5D 70A89CC9 118BE425 C827E7E9 167C8181 D0A85178
80C4D812 C376F8F5 0FC03292 F780785A 4DBBC826 4C295A8C 47317AA9 E5FD0016 FCBCB5F7 A6DF7742
62F5AB28 17035E37 D07086F0 86A22531 144C488B 433BA34E DAFFC793 8D847050 F1370F8D F9AFCE9D
635F0907 6F796C6C 82BD0B66 EF034B7F DCD6E012 E265D446 015ACD2C 764015D5 D3B7BAB5 692DF7A2
61D9CF0B 04BA386C C8089018 892F8669 B6C47DEB DCFFFA83 330E9D02 03010001 A3820182 3082017E
30130609 2B060104 01823714 0204061E 04004300 41300B06 03551D0F 04040302 0186300F 0603551D
130101FF 04053003 0101FF30 1D060355 1D0E0416 04148EA5 6E3FC90F 30CDD5FC 4BCA976E 48D0D267
1E313082 01160603 551D1F04 82010D30 82010930 820105A0 820101A0 81FE8681 BB6C6461 703A2F2F
2F434E3D 57697265 6C657373 2D43412C 434E3D63 6973636F 2D333661 37336132 66612C43 4E3D4344
502C434E 3D507562 6C696325 32304B65 79253230 53657276 69636573 2C434E3D 53657276 69636573
2C434E3D 436F6E66 69677572 6174696F 6E2C4443 3D576972 656C6573 732C4443 3D636F6D 3F636572
74696669 63617465 5265766F 63617469 6F6E4C69 73743F62 6173653F 6F626A65 6374436C 6173733D
63524C44 69737472 69627574 696F6E50 6F696E74 863E6874 74703A2F 2F636973 636F2D33 36613733
61326661 2E776972 656C6573 732E636F 6D2F4365 7274456E 726F6C6C 2F576972 656C6573 732D4341
2E63726C 30100609 2B060104 01823715 01040302 0100300D 06092A86 4886F70D 01010505 00038201
01007A3C 9802BFE9 D04CFCCD 4C802F60 9CBF0AE7 77C0D781 92CA1CCE C220349D D8775729 80781349
4C20A518 B9175F44 2F0F6F17 F55CF53E 00042397 CEFB0A98 0DAFB69C 3F6BD9A7 EB87B2F4 3CBF041A
61E6FCD2 F4EE3AB9 460B954A E838436E 5F9F19C4 194E8781 17BA2339 936BA3DB D7747DF5 CFCC6415
1BB63553 63EC86C1 D6544FD6 963FD80E 1135CBA5 3E79E851 AD65F314 CE4E0C04 00EB4BA9 7079512D
DDF1D657 FEF72C2A C7E63CC6 AB9F0305 3ABC79D4 6729BF89 2FB70ACE 52F022D1 F1E069BC 954C3AC1
E18FA04A D2ECE11D E25B2E96 630637D2 B7949B84 099D971A C3B7249C F75C4525 D02A40AB 50E19196
9D1C2853 8BAEFD6C 1CE1945E 1CABC51B AFF5 quit dot1x credentials PEAP username WGB-Client
password 7 13061E010803 pki-trustpoint WGB-PEAP ! username Cisco password 7 123A0C041104 ! !
bridge irb ! ! interface Dot11Radio0 no ip address no ip route-cache shutdown antenna gain 0
station-role root bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 spanning-
disabled bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1
unicast-flooding ! interface Dot11Radio1 no ip address no ip route-cache ! encryption mode
ciphers aes-ccm ! ssid WGB-PEAP ! antenna gain 0 station-role workgroup-bridge bridge-group 1
bridge-group 1 spanning-disabled ! interface GigabitEthernet0 no ip address no ip route-cache
duplex auto speed auto bridge-group 1 bridge-group 1 spanning-disabled ! interface BVI1 ip
address dhcp client-id GigabitEthernet0 no ip route-cache ! ip http server no ip http secure-
server ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag bridge 1
route ip ! ! ! line con 0 line vty 0 4 login local transport input all ! end

```

[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.

A associação no AP olha como este exemplo:

A associação WGB do WLC olha como este exemplo:

A associação de cliente olha como este exemplo:

Troubleshooting

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

Comandos para Troubleshooting

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.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Debugar o bridge de grupo de trabalho

A fim debugar o WGB, incorpore estes comandos:

- **debug aaa authentication**
- **debugar o dot11 supp-sm-dot1x**

Debugar o controlador do Wireless LAN

A fim debugar o WLC, inscreva o **comando debug aaa all enable**.

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)