Workgroup Bridges with PEAP Authentication Configuration Example

TAC **Document ID: 115736**

Contributed by Surendra BG, Jeal Jimenez, and Carlos Leiton, Cisco TAC Engineers.
Jan 14, 2013

Contents

Introduction

This document describes the enhanced support for Workgroup Bridges (WGBs), which includes:

- Protected Extensible Authentication Protocol (PEAP) support for WGB. An access point configured as a WGB can now associate to a root access point with PEAP.
- Improvements when client WGBs roam.
- Reliability when WGBs fast roam. The unit is allowed an additional retry when it needs to re−associate to the root access point.
- Improvement in the method that WGBs use to select the "best parent" access point. WGBs can share association histories with root access points, which can build and share a list of best root access points among WGBs. This method helps WGBs select the best root access point when they roam.
- VideoStream support on WGBs when used as a client. VideoStream improves the reliability of an IP multicast stream when it converts the multicast frame, over the air, to a unicast frame. VideoStream was not supported for WGB clients in previous releases because a WGB s wired clients cannot be added to the Wireless LAN Controller (WLC) multicast table. In this release, the WGB is added to the WLC multicast table, and the WGB converts the VideoStream unicast frame into an Ethernet multicast frame and sends it out to its wired clients.

  In order to enable VideoStream for WGBs, enter the **configure media−stream wired−client enable** command on the WLC.

Other Document in this Series

- How to Use aIOS WGB with EAP−TLS Authentication in a Cisco Unified Wireless Network
- Workgroup Bridges in a Cisco Unified Wireless Network Configuration Example

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco IOS® Software Release 15.2(2)JA or later.

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.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Configure

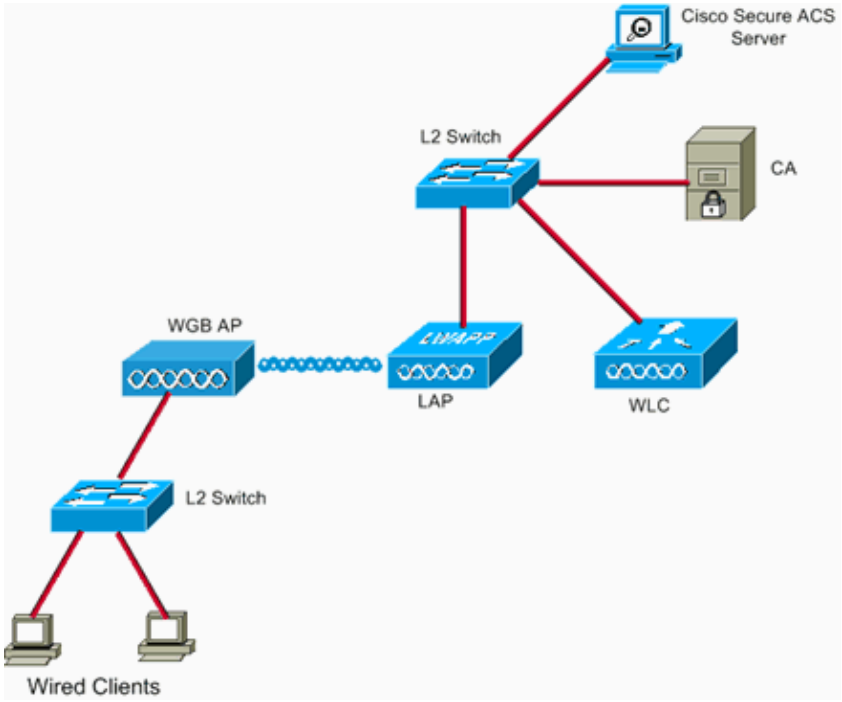
In this section, you are presented with the information to configure a WGB with PEAP along with the Cisco Unified Controller based deployment. In this example, the 1260 Autonomous Access Point is configured as a WGB and connects to the Lightweight Access Point Protocol (LWAPP) network. Use this service set identifier (SSID), **WGB−PEAP**, for the connection to the WLAN and use the PEAP for the authentication of the WGB to the LWAPP network.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses the network setup shown in figure 1:

Figure 1



Workgroup Bridge Configuration

In order to configure the WGB, complete these steps:

1. Set the hostname, domain name, and time of the WGB as required.

   - The hostname must match the username entered for it in ACS as in the previous step:

     ```
     ap#configure terminal
     ap(config)#hostname WGB-Client
     WGB-Client(config)#
     ```

   - The time must be correct for the certifications to work (**clock set** command or configure an SNTP server).

     ```
     WGB-Client#clock set 14:00:00 5 Dec 2011
     ```

2. Configure the trustpoint for the 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
   ```

   Note: The command **subject-name CN=**<*ClientName*> is required. Without it, the Microsoft Certificate Authority (CA) fails to issue the certificate and receives this error message, The request subject name is invalid or too long. 0x80094001 .

   ```
   WGB-Client(config)#revocation-check none
   ```

   Note: The **revocation-check none** command is necessary to avoid the problem described in Cisco bug ID CSCsl07349 (registered customers only) . WGB disassociates/reassociates often and takes a long time to reconnect.

   ```
   WGB-Client(config)#rsakeypair manual-keys 1024
   ```

CA Certificate on the Workgroup Bridge Installation

In order to install the CA certificate on the WGB, complete these steps:

1. Obtain a copy of the CA certificate.
2. Browse to the crtsrv location on your CA server; for example: http://<ca−server−ip−address>/crtsrv
3. Click **Download a CA certificate, certificate chain, or CRL**.
4. From the Choose Encoding method drop−down list, choose **Base 64**.
5. Click **Download CA certificate**.
6. Save the .cer file.
7. Install the CA certificate:

    a. Enter the **crypto pki authenticate CUT−PASTE** command.
    b. Enter the base−64 encoded CA certificate. End with a blank line or the word "quit" on the last line by itself.
    c. Paste the text from the .cer file downloaded in the previous step. The certificate installation will look like this example.

```
-----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
```

After the certificate installation, the AP configuration should look like this example:

```
=~=~=~=~=~=~=~=~=~=~=~= 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 8BAEFDFC 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
```

Verify

Use this section to confirm that your configuration works properly.

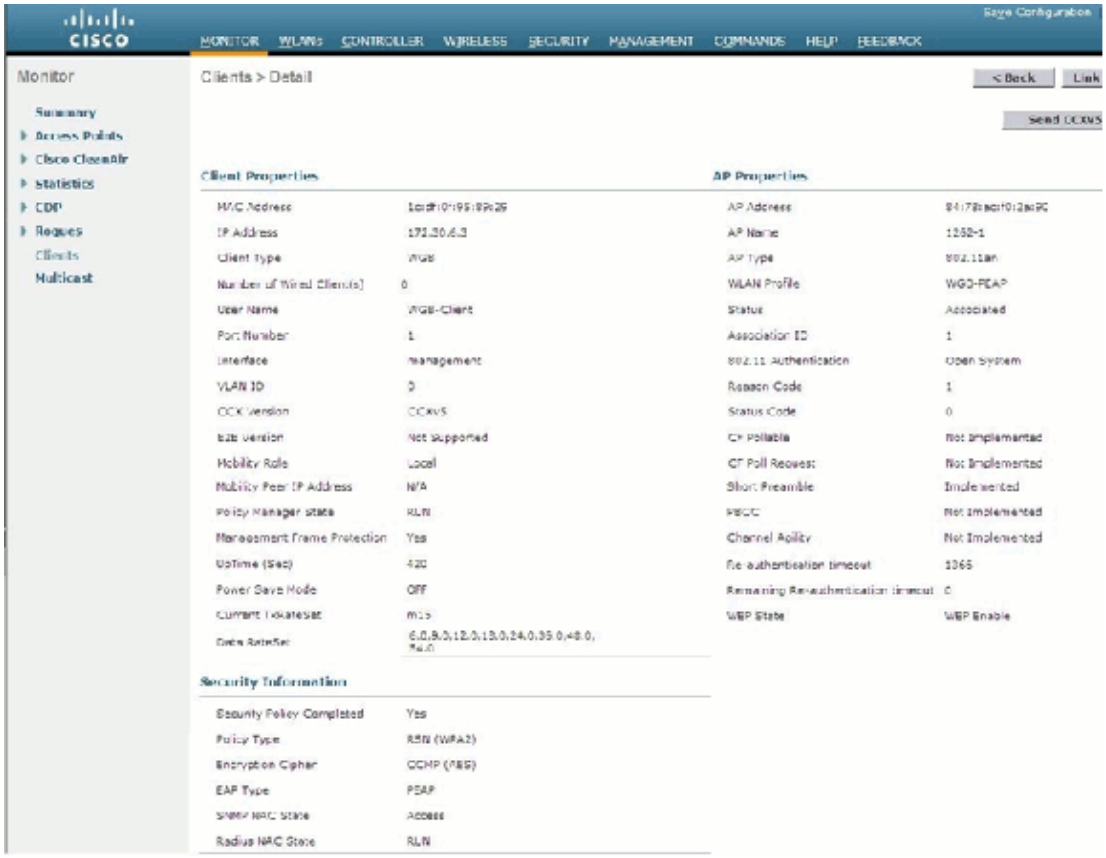
The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

The association on the AP looks like this example:

```
WGB-Client#
WGB-Client#show dot11 associations

802.11 Client Stations on Dot11Radio1:

SSID [WGB-PEAP] :

MAC Address    IP address      Device          Name            Parent          State
8478.acf0.2a9e 172.30.6.253    LWAPP-Parent 1262-1             -               EAP-Assoc

WGB-Client#
WGB-Client#
WGB-Client#
WGB-Client#
WGB-Client#
```

The WGB association from the WLC looks like this example:

The client association looks like this example:



Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Debug the Workgroup Bridge

In order to debug the WGB, enter these commands:

- **debug aaa authentication**
- **debug dot11 supp−sm−dot1x**

Debug the Wireless LAN Controller

In order to debug the WLC, enter the **debug aaa all enable** command.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Jan 14, 2013 Document ID: 115736