Wireless Mesh

Why Wireless mesh?

The access point of a WiFi network is usually connected to the WiFi Controller through Ethernet wiring. A wireless mesh eliminates the need for Ethernet wiring by connecting WiFi access points to the controller by radio. This is useful where installation of Ethernet wiring is impractical.

Below shows a wireless mesh topology.

Overview of Wireless Mesh

- The FortiAP-221B is connected to the network by Ethernet is called the Mesh Root node.
- The root node can be a FortiAP unit or built-in AP of a FortiWiFi unit.
- AP that serve only regular WiFi clients are called Leaf nodes, in this its FortiAP-220B.
- Leaf AP’s carry mesh SSID to other Leaf AP in the topology using a dedicated radio for eg, the 5GHz radio could carry only the mesh SSID (backhaul SSID) while the 2.4GHz radio carries one or more SSIDs that serve users.

Network:

- Network between FortiGate/FortiWiFi is 10.10.2.0/24 with dhcp enabled.
- Network for internet users is 10.0.0.0/24 with dhcp enabled configured on WiFi controller.

Firmware requirements:

All FortiAP units that will be part of the wireless mesh network must be running FAP firmware version 5.0 build 003. FortiWiFi or FortiGate unit used as the WiFi controller must be running FortiOS 5.0.
Configuration of meshed WiFi network:

Setting up Full Mesh Wireless on FortiGate Unit using two FortiAP Units.

- Configure the mesh SSID, go to WiFi Controller > WiFi Network > SSID.
- Edit the default mesh SSID fmesh.root and change the SSID from the default to something unique. Note that the traffic mode is set to mesh downlink. Enter a new pre-shared key.
- Create another SSID for clients access and use tunnel

<table>
<thead>
<tr>
<th>Name</th>
<th>Mesh_Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>WiFi SSID</td>
</tr>
<tr>
<td>Traffic Mode</td>
<td>Mesh Downlink</td>
</tr>
</tbody>
</table>

### WiFi Settings

- **SSID**: fmesh.root
- **Security Mode**: WPA/WPA2-Personal
- **Data Encryption**: AES
- **Pre-shared Key**: (8 - 63 characters)

- **Comments**: Write a comment...
- **Administrative Status**: Up

Go to WiFi Controller > WiFi Network > Custom AP Profile and create a new AP profile, or edit the profile created earlier, and enter the follow settings: Select the correct platform, in this example we are using the FAP 221B.

- Select Radio 1 and set mode Access Point and use default Band and Channel settings. Enable your SSID and the mesh SSID from the list of available SSIDs.
- Select Radio 2 and set mode Access Point and use default Band and Channel settings.
- Enable your SSID and the mesh SSID from the list of available SSIDs. Click OK.
If this is a new profile you will need to apply this to your custom AP profile in your managed AP. Go to WiFi Controller > Managed Access Points > Managed FortiAP and select your device and select edit. In the wireless settings change the AP profile from automatic to your new profile and select apply and ok to save your changes.

This change will cause the access point daemons on the AP to restart.
<table>
<thead>
<tr>
<th><strong>Serial Number</strong></th>
<th>FP221B3X12008432</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Comments</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Managed AP Status**
- **Status**: Online
- **Connected Via**: Ethernet (10.10.2.4)
- **Base MAC Address**: 00:09:0f:7c:6c:30
- **Join Time**: 11/25/14 11:00
- **Clients**: 1
- **FortiAP OS Version**: FP221B-v5.0-build032 [A recommended update is available]
- **State**: Authorized [Deauthorize] [Restart]

**Wireless Settings**

**AP Profile**: myap [Change]

**Radio 1**
- **Mode**: Access Point
- **Band**: 802.11an_5G
- **Channel**: 36, 40, 44, 48, 149, 153, 157, 161, 165

**Radio 2**
- **Mode**: Access Point
- **Band**: 802.11bgn_2.4G
- **Channel**: 1, 6, 11
The FortiAP units that will serve as branch/leaf nodes must be preconfigured as follows.

- Connect to the FortiAP unit web-based manager on its default Ethernet interface IP address 192.168.1.2
- In the connectivity section enter the IP address of your AP network as follows:

<table>
<thead>
<tr>
<th>Address Mode</th>
<th>Static</th>
<th>DHCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VLAN ID</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Local IP Address</td>
<td>10.10.2.4</td>
<td></td>
</tr>
<tr>
<td>Local Network Mask</td>
<td>255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>Gateway IP</td>
<td>10.10.2.10</td>
<td></td>
</tr>
<tr>
<td>Administrative Access</td>
<td>□ HTTP</td>
<td>□ TELNET</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Uplink</th>
<th>Ethernet</th>
<th>Mesh</th>
<th>Ethernet with mesh backup support</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>AC Discovery Type</th>
<th>Auto</th>
<th>Static</th>
<th>DHCP</th>
<th>DNS</th>
<th>Broadcast</th>
<th>Multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC Control Port</td>
<td>5246</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC IP Address 1</td>
<td>10.10.2.10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC IP Address 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC IP Address 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC Host Name 1</td>
<td>_capwap-control._udp.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC Host Name 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC Host Name 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC Discovery Multicast Address</td>
<td>224.0.1.140</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC Discovery DHCP Option Code</td>
<td>138</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Start your second AP. You may need to work in pairs for this lab, in that case you have to de-authorizes one AP and then you have to authorizes the second AP The second AP will use the automatic profile which is fine for this lab.
- Configure the second AP to use the wireless mesh as an uplink. From the FortiAP GUI, go to Connectivity and select mesh and enter the mesh SSID and pre-shared key. This change will cause the access point daemons on the AP to restart.
You should observe that the second AP connects as a leaf device.

**Note:** It might take some time for the state icon to become green however if you feel it is taking too long you can reboot the AP to expedite the process.

- You have now created the full mesh. If you would like to test that clients on the leaf AP can reach the wireless controller modify the AP profile associated with your root AP and remove your wireless client SSID so that it is only being announced on the leaf AP.
Debug commands:

Using the wireless controller debug of the FortiGate, try the following commands.

Use the following command to see the status of the FortiAPs:
`diagnose wireless-controller wlac -c wtp`

FWF60C3G12006306 # diagnose wireless-controller wlac -c wtp

------------------------------------- WTP 1 -------------------------------------
WTP vd            : root
vfid             : 0
id               : FAP22B3U12009906
mgmt_vlanid      : 0
region code      : C
regcode status   : invalid
refcnt           : 3 own(1) wtpprof(1) ws(1)
plain_ctl        : disabled
deleted          : no
admin            : enable
wtp-mode         : normal
wtp-profile      : resv-dflt-FAP22B3U12009906
name             :
location         :
ip-frag-prevent  : TCP_MSS
tun-mtu          : 0,0
active sw ver    : FAP22B-v5.0-build032
local IPv4 addr  : 10.10.2.6
board mac        : 00:09:0f:a1:94:3e
join_time        : Tue Nov 25 11:01:38 2014
mesh-uplink      : mesh
mesh hop count   : 1
parent wtp id    : FP221B3X12008432
connection state : Connected
image download progress: 0
last failure     : 0 -- N/A
last failure param: 
last failure time: N/A
station info     : 0/0
geo              : World (0)
Radio 1          : AP
country name     : CN
country code     : 156
radio_type       : 11N_5G
channel list     : 36 40 44 48 149 153 157 161 165
darrp            : disabled
txpower          : 100% (23 dBm)
beacon_intv      : 100
rts_threshold    : 2346
frag_threshold   : 2346
ap scan : disable
ap scan passive : disabled
sta scan : disabled
WIDS profile : ---
  wlan 0 : Mesh_WiFi
  wlan 1 : leafSSID
max vaps : 8
base bssid : 00:09:0f:a1:94:40
oper chan : 149
station info : 0/0
Radio 2 : AP
country name : CN
country code : 156
radio_type : 11N
channel list : 1 6 11
darrp : disabled
txpower : 100% (27 dBm)
beacon_intv : 100
rts_threshold : 2346
frag_threshold : 2346
ap scan : disable
ap scan passive : disabled
sta scan : disabled
WIDS profile : ---
  wlan 0 : Mesh_WiFi
  wlan 1 : leafSSID
max vaps : 8
base bssid : 00:09:0f:a1:94:47
oper chan : 1
station info : 0/0
Radio 3 : Not Exist

---------------------------------------------------------------WTP  2---------------------------------------------------------------
WTP vd : root
  vfid : 0
  id : FP221B3X12008432
mgmt_vlanid : 0
region code : A
regcode status : valid
refcnt : 3 own(1) wtpprof(1) ws(1)
plain_ctl : disabled
deleted : no
admin : enable
wtp-mode : normal
wtp-profile : myap
name :
location : N/A
ip-frag-prevent : TCP_MSS
tun-mtu : 0,0
active sw ver : FP221B-v5.0-build032
local IPv4 addr : 10.10.2.4
board mac : 00:09:0f:7c:6c:30
join_time : Tue Nov 25 11:00:15 2014
mesh-uplink : ethernet
mesh hop count : 0
parent wtp id :
connection state : Connected
image download progress: 0
last failure : 10 -- JOIN REQ from unmanaged WTP is denied
last failure param: N/A
last failure time: Tue Nov 25 10:30:07 2014
station info : 1/0
geo : World (0)
Radio 1 : AP
country name : US
country code : 841
radio_type : 11N_5G
channel list : 36 40 44 48 149 153 157 161 165
darrp : disabled
taxpower : 100% (23 dBm)
beacon_intv : 100
rts_threshold : 2346
frag_threshold : 2346
ap scan : disable
ap scan passive : disabled
sta scan : disabled
WIDS profile : ---
  wlan 0 : Mesh_Link
  wlan 1 : leaf_SSID
max vaps : 8
base bssid : 00:09:0f:7c:6c:31
oper chan : 36
station info : 0/0
Radio 2 : AP
country name : US
country code : 841
radio_type : 11N
channel list : 1 6 11
darrp : disabled
taxpower : 100% (27 dBm)
beacon_intv : 100
rts_threshold : 2346
frag_threshold : 2346
ap scan : disable
ap scan passive : disabled
sta scan : disabled
WIDS profile : ---
  wlan 0 : Mesh_Link
  wlan 1 : leaf_SSID
max vaps : 8
base bssid : 00:09:0f:7c:6c:38
oper chan : 1
station info : 1/0
Radio 3 : Not Exist
----------------------------------WTP 3----------------------------------
WTP vd : root
   vfid : 0
id : FWF60C-WIFI0
mgmt_vlanid : 0
region code : ALL
regcode status : valid
refcnt : 3 own(1) wtpprof(1) ws(1)
plain_ctl : disabled
deleted : no
admin : enable
wtp-mode : normal
wtp-profile : resv-dflt-FWF60C-WIFI0
name :
location :
ip-frag-prevent : TCP_MSS
tun-mtu : 0,0
active sw ver : FWF60C-v5.0-build292
local IPv4 addr : 127.0.0.1
board mac : 00:09:0f:00:00:01
join_time : Mon Nov 24 12:37:52 2014
mesh-uplink : ethernet
mesh hop count : 0
parent wtp id :
connection state : Connected
image download progress: 0
last failure : 0 -- N/A
last failure param: 
last failure time: N/A
station info : 0/0
geo : World (0)
Radio 1 : AP
country name : US
country code : N/A
radio_type : 11N
channel list : 1 6 11
darrp : disabled
txpower : 100% (27 dBm)
beacon_intv : 100
rts_threshold : 2346
frag_threshold : 2346
ap scan : disable
ap scan passive : disabled
sta scan : disabled
WIDS profile : ---
max vaps : 8
base bssid : 00:0e:8e:41:2e:69
oper chan : 1
station info : 0/0
Radio 2 : Not Exist
Radio 3 : Not Exist
--------------------------------------Total 3 WTPs--------------------------------------
Use the following command to list the configured wireless LANs:

diagnose wireless-controller wlac -c wlan

FWF60C3G12006306 # diagnose wireless-controller wlac -c wlan

WLAN (001/003) vdom,name: root, Mesh_Link
  vlanid : 0 (auto vlan intf disabled)
  sw name :
  ip, mac : 0.0.0.0, 00:ff:b1:aa:12:39
  status : up
  refcnt, deleted : 3 own(1) wtpprof(2)
  mesh backhaul : enabled
  local bridging : disabled
  local switching : disabled
  dynamic vlan : disabled
  auth type : 0
  mac type : 0xffffffff
  tunnel type : 0xffffffff
  fast roaming : 0x1
  bc suppression : dhcp arp
  suppress ssid : 0
  ssid : fmesh.root
  security : 7
  radius mac auth : disabled
  radius mac auth srv:
  auth : 0
  key :
  keyindex : 1
  password : fmeshroot
  radius_server :
  usergroup : 0
  intra privacy : disabled
  station info : 1/0
  kern sock : 23
  mf acl cfg : disabled, allow, 0 entries
  sta list 0000 72:09:0f:a1:94:47 ws (0-10.10.2.4:5246) 1 0
WTP 0001 0, FP221B3X12008432
  ---- 0-10.10.2.4:5246 (12 - CWAS_RUN)

WLAN (002/003) vdom,name: root, Mesh_WiFi
  vlanid : 0 (auto vlan intf disabled)
  sw name :
  ip, mac : 10.0.0.1, 00:ff:d7:12:eb:8f
  status : down
  refcnt, deleted : 3 own(1) wtpprof(2)
  mesh backhaul : disabled
  local bridging : disabled
  local switching : enabled
  dynamic vlan : disabled
  auth type : 0
  mac type : 0xffffffff
  tunnel type : 0xffffffff
fast roaming : 0x1
bc suppression : dhcp arp
suppress ssid : 0
ssid : fortinet.mesh.root
security : 7
radius mac auth : disabled
radius mac auth svr:
  auth : 0
  key :
  keyindex : 1
  password : fortinet
  radius_server :
usergroup : 0
  intra privacy : disabled
  station info : 0/0
  kern sock : 8
  mf acl cfg : disabled, allow, 0 entries
WTP 0002 : 0, FAP2B3U12009906
---- 0-10.10.2.6:5246 (12 - CWAS_RUN)

WLAN (003/003) vdom, name: root, leaf_SSID
vlanid : 0 (auto vlan intf disabled)
sw name :
ip, mac : 10.0.0.1, 00:ff:50:2f:de:4e
status : up
refcnt, deleted : 5 own(1) wtpprof(4)
mesh backhaul : disabled
local bridging : disabled
local switching : enabled
dynamic vlan : disabled
auth type : 0
mac type : 0xffffffff
  tunnel type : 0xffffffff
fast roaming : 0x1
bc suppression : dhcp arp
suppress ssid : 0
ssid : Client_SSID
security : 7
radius mac auth : disabled
radius mac auth svr:
  auth : 0
  key :
  keyindex : 1
  password : fmeshroot
  radius_server :
usergroup : 0
  intra privacy : disabled
  station info : 0/0
  kern sock : 24
  mf acl cfg : disabled, allow, 0 entries
WTP 0003 : 0, FAP2B3U12009906
---- 0-10.10.2.6:5246 (12 - CWAS_RUN)
WTP 0004 : 0, FP221B3X12008432
Use the following command to list the connected wireless stations:

```bash
diagnose wireless-controller wlac -d sta
```

FWF60C3G12006306 # diagnose wireless-controller wlac -d sta

* vf=0 wtp=15 rld=1 wlan=leaf_SSID ip=0.0.0.0 mac=12:09:0f:7c:6c:31 vci= host= user= group=
signal=0 noise=0 idle=23145 bw=0 use=3 chan=36 radio_type=11N_5G security=wpa_wpa2_personal
  encrypt=aes online=yes
* vf=0 wtp=15 rld=2 wlan=leaf_SSID ip=0.0.0.0 mac=12:09:0f:7c:6c:38 vci= host= user= group=
signal=0 noise=0 idle=23145 bw=0 use=3 chan=1 radio_type=11N security=wpa_wpa2_personal
  encrypt=aes online=yes

vf=0 wtp=15 rld=2 wlan=leaf_SSID ip=10.0.0.3 mac=00:26:c7:99:33:86 vci=MSFT 5.0 host=Yogesh-
PC user= group= signal=-43 noise=-95 idle=1 bw=0 use=3 chan=1 radio_type=11N
  security=wpa2_only_personal encrypt=aes online=yes
* vf=0 wtp=16 rld=2 wlan=leaf_SSID ip=0.0.0.0 mac=12:09:0f:a1:94:47 vci= host= user= group=
signal=0 noise=0 idle=23061 bw=0 use=3 chan=1 radio_type=11N security=wpa_wpa2_personal
  encrypt=aes online=yes
* vf=0 wtp=15 rld=1 wlan=leaf_SSID ip=0.0.0.0 mac=12:09:0f:7c:6c:31 vci= host= user= group=
signal=0 noise=0 idle=22187 bw=0 use=3 chan=36 radio_type=11N_5G security=wpa_wpa2_personal
  encrypt=aes online=yes
* vf=0 wtp=15 rld=2 wlan=Mesh_Link ip=0.0.0.0 mac=00:09:0f:7c:6c:38 vci= host= user= group=
signal=0 noise=0 idle=22187 bw=0 use=3 chan=1 radio_type=11N security=wpa_wpa2_personal
  encrypt=aes online=yes

* vf=0 wtp=16 rld=2 wlan=Mesh_WiFi ip=0.0.0.0 mac=00:09:0f:a1:94:25 vci= host= user= group=
signal=0 noise=0 idle=23062 bw=0 use=3 chan=1 radio_type=11N security=wpa_wpa2_personal
  encrypt=aes online=yes
* vf=0 wtp=16 rld=1 wlan=Mesh_WiFi ip=0.0.0.0 mac=00:09:0f:a1:94:40 vci= host= user= group=
signal=0 noise=0 idle=23062 bw=0 use=3 chan=149 radio_type=11N_5G
  security=wpa_wpa2_personal encrypt=aes online=yes
Using the debug of the FortiAP, try the following commands.

**View the status of the Wireless clients:**

Go to WiFi Controller > Monitors > Wireless Health to view the list of all connected internet users.

![AP Status]

![Active Clients For FP221B3X12008432 (2.4 GHz Band)]

In the FortiAP CLI, you can check the **main ip** field in the output from the commands

```
cw_diag -c mesh
```

**FAP22B3U12009906 # cw_diag -c mesh**

```
Sys Cfg AP addr mode: static
stp mode : 0
dflt ip : 10.10.2.6
dflt mask: 255.255.255.0
dflt gw : 10.10.2.10

Mesh Cfg Uplink : Mesh Uplink
AP SSID : fmesh.root
AP BSSID : 00:00:00:00:00:00
```
**Troubleshooting Guide of Wireless Mesh:**

Use the following command to list the Authentication process and client connection:

diagnose debug application wpad 4
diagnose debug enable
Use the following command to list specific client process by filtering it with mac-address:

```
diagnose wireless-controller wlc sta_filter <client-mac> 1
diagnose debug enable
```

To turn it off use following commands:

```
diagnose wireless-controller wlc sta_filter <client-mac> 0
diagnose debug reset
```
IMPA: For specific mac-address filtering you have to use the same debug commands with grep and the name of the mac-address