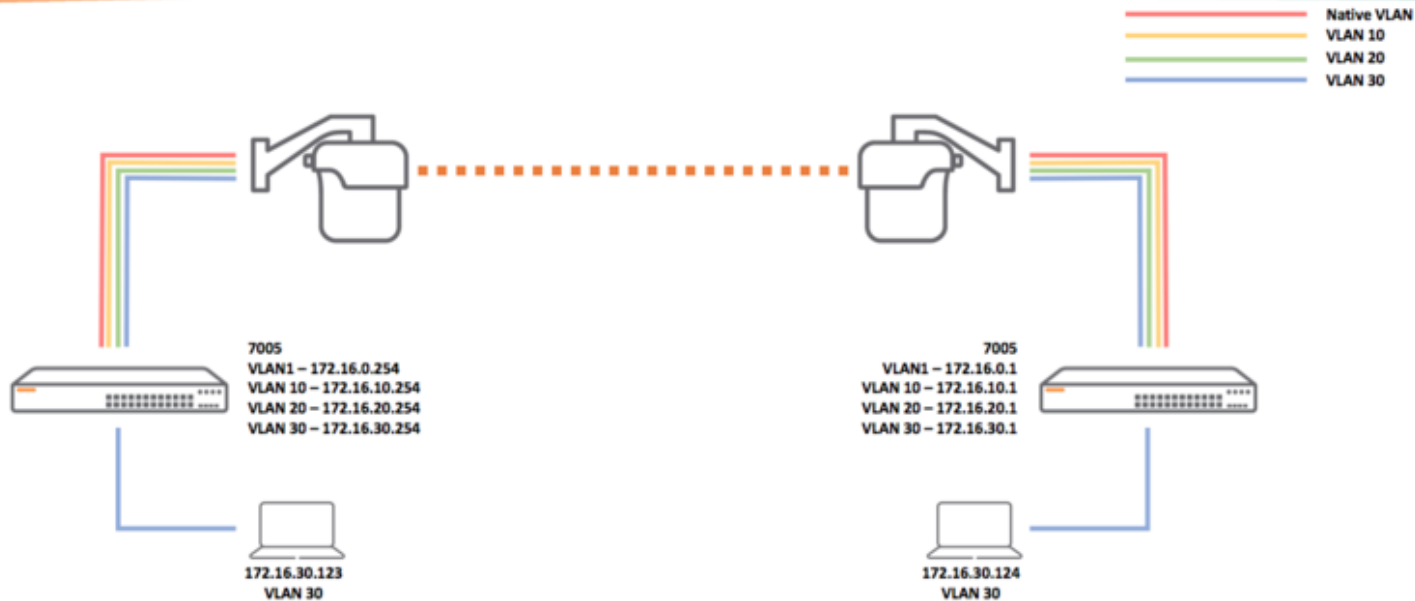


Instant Mesh with Network Bridging - Trunk Port [\[edit\]](#)

When Instant Mesh is desired to provide a PtP link that carries both native, untagged traffic, as well as trunked traffic, the below config guide/stubs will provide proper guidance.

Instant AP – Mesh Bridging

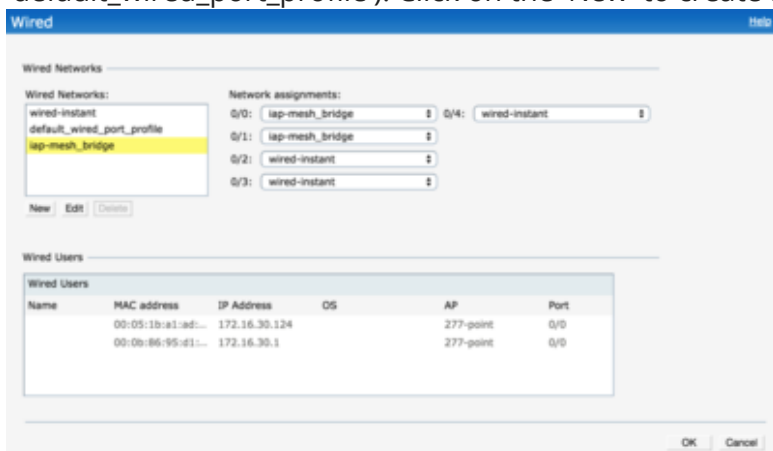


In the diagram above, there are two AP-27x APs providing untagged traffic on VLAN 1, and tagged traffic on VLAN 10, 20, and 30. **Note that in the case where the Instant Mesh Point will be connected to a switch where IP traffic will be seen on boot-up on the wired interface, you must first configure the wired interface of the mesh point to be in Bridge Mode before deployment. Otherwise, the IAP will see wired frames and assign the VC to the wired interface, instead of bringing up the wireless interface first. This is done by editing the IAP Mesh Point from the Main VC window and changing the wired interface to 'Bridge'**

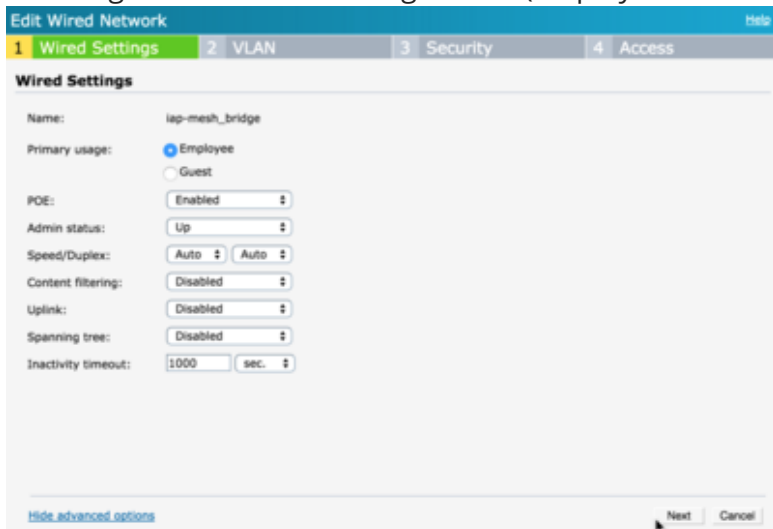
1. From the VC's main dashboard, go to 'More > Wired'



2. From the 'Wired' config window, this shows the two default wired-profiles ('wired-instant' and 'default_wired_port_profile'). Click on the 'New' to create a new bridged profile.



3. Configure the 'Wired Settings' fields (Employee or Guest, etc, etc) and click 'Next'



4. On the VLAN settings, select 'Trunk' and assign Native and Trunk VLANs to carry and click 'Next'

The screenshot shows the 'Edit Wired Network' configuration page with the 'VLAN' tab selected. The 'VLAN Management' section includes the following settings:

- Mode: Trunk
- Client IP assignment: Network assigned
- Native VLAN: 1
- Allowed VLANs: 10,20,30

Below these settings is a 'VLAN Assignment Rules' table, which is currently empty. At the bottom of the table are buttons for 'New', 'Edit', 'Delete', and two arrow buttons. At the bottom of the page are 'Back', 'Next', and 'Cancel' buttons.

5. If there is any MAC or 802.1x settings to be enabled, leave here. Otherwise leave both as disabled and click 'Next'

The screenshot shows the 'Edit Wired Network' configuration page with the 'Security' tab selected. The 'Security' section includes the following settings:

- MAC authentication: Disabled
- 802.1X authentication: Disabled

At the bottom of the page are 'Back', 'Next', and 'Cancel' buttons.

6. Apply any firewall rules to the role assigned to the wired interface, otherwise leave as 'Unrestricted' and click 'Finish'

The screenshot shows the 'Edit Wired Network' configuration page with the 'Access Rules' tab selected. The 'Access Rules' section includes a 'More Control' slider on the left, which is currently set to 'Unrestricted'. The main area displays the text: 'No restrictions on access based on destination or type of traffic'. At the bottom of the page are 'Back', 'Finish', and 'Cancel' buttons.

Once this is complete, you can assign your new Bridge Profile to the IAP's respective wired interfaces for wired

bridging. In the example config, the E0 and E1 ports are all trunk ports carrying tagged VLAN 10, 20, and 30, and are untagged on VLAN 1 (native).

The instant config elements from the CLI will look as follows:

```
wired-port-profile iap-mesh_bridge
  switchport-mode trunk
  allowed-vlan 10,20,30
  native-vlan 1
  no shutdown
  access-rule-name iap-mesh_bridge
  speed auto
  duplex auto
  poe
  type employee
  auth-server InternalServer
  captive-portal disable
  no dot1x

enet0-port-profile iap-mesh_bridge
enet1-port-profile iap-mesh_bridge
```

Once the mesh link is built, you can run the following from the CLI

```
274-portal# show ap mesh link
```

Neighbor list

MAC	Portal	Channel	Age	Hops	Cost	Relation	Fl	
ags	RSSI	Rate	Tx/Rx	A-Req	A-Resp	A-Fail	HT-Details	Cluster ID
94:b4:0f:31:50:70	94:b4:0f:2c:9e:51	157+	0	1	5.00	C	49s	VL
K	82	600/6	1	1	0	VHT-40MHzsgi-3ss	ab43b1cc73de9632d61ff80ab38a265	

Total count: 1, Children: 1

Relation: P = Parent; C = Child; N = Neighbor; B = Blacklisted-neighbor

Flags: R = Recovery-mode; S = Sub-threshold link; D = Reselection backoff; F = Auth-failure; H = High Throughput; V = Very High Throughput, L = Legacy allowed

K = Connected; U = Upgrading; G = Descendant-upgrading; Z = Config pending; Y = Assoc-resp/Auth pending

a = SAE Accepted; b = SAE Blacklisted-neighbour; e = SAE Enabled; u = portal-unreachable; o = opensystem