



Access Controller Deployment Guidelines

This document describes the different options to deploy a Bountiful WiFi Access Controller (AC) and Access Points (APs) into an existing network.

General Deployment Guidelines

It is good practice to segment the wireless traffic from the rest of the network by isolating the wireless traffic to a dedicated subnet. Compared to a wired network, a shared wireless network has less bandwidth available. Wired LANs support much higher bandwidth and full duplex connectivity. By contrast a wireless network has less bandwidth and it is shared among all devices. Each device that connects to the network generates a certain amount of broadcast and multicast traffic which is propagated to every device on the subnet or LAN. By limiting the number of wired clients on the wireless subnet more bandwidth is preserved for wireless communication.

Recommendation for best performance:

- Limit maximum number of concurrent wireless clients per AP to < 25.

- Place APs well above ground level.

- Place APs away from metal and glass obstructions

- No more than 20% overlap in signal coverage

- Alternate channels using non-overlapping channels 1, 6, 11

- To allow roaming use same SSID and encryption on APs

- Use WPA2 for strongest security

Operational Overview

The APs rely on a Dynamic Host Configuration Protocol (DHCP) Server which also provides the next server IP. The DHCP server provides an IP address and the Next server address (a.k.a. siaddr) for the APs to TFTP boot their image off of the Access Controller. The APs need to be told what their next server's IP address is so they can obtain their boot image and subsequent configuration from the AC. If the APs are not given a next server IP they will reboot and try again.

Default Settings

Web interface:

- Port 80

- User name: admin

- Password: admin

WAN:



DHCP client for dynamic IP address and Domain Name Server address assignments

LAN:

IP address 192.168.101.2 / 24

DHCP server:

DHCP server enabled on LAN interface

Range 192.168.101.100 – 192.168.101.200

Next server: 192.168.101.2

Filename: apimage.bin

Rules:

WAN: allow remote http administration; ping; remote https administration

LAN any protocol, source LAN.net / any port; destination any/any port

Wireless:

Default SSID BountifulWifi

Open network

The AC is managed through a web interface. <http://192.168.101.2>. The default setting also allows the device to be managed via the WAN interface.

Restoring Factory Defaults

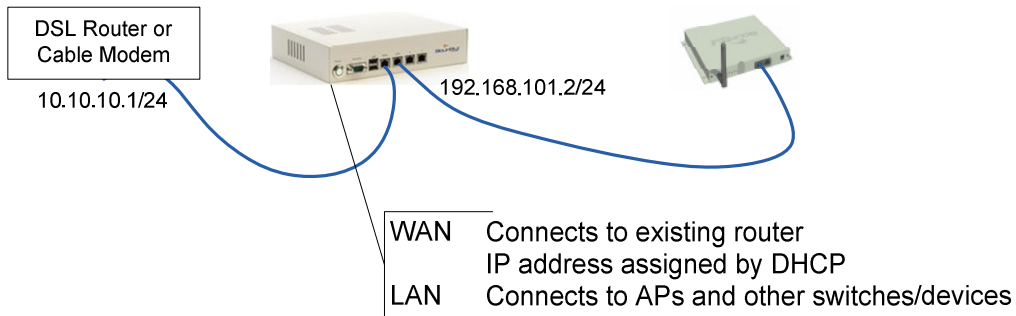
To restore factory defaults apply power to the device with a USB keyboard connected. After 2 minutes. Press 4 followed by the Enter key. y followed by the Enter key.

The device will configure itself to defaults and reboot itself.

Connect a PC to the LAN port with network settings of Obtain an IP address automatically and Obtain DNS server address automatically.

Option 1 AC as main router firewall

With this option the AC acts as a firewall and DHCP server for the wired and WiFi network.



Supports captive portal

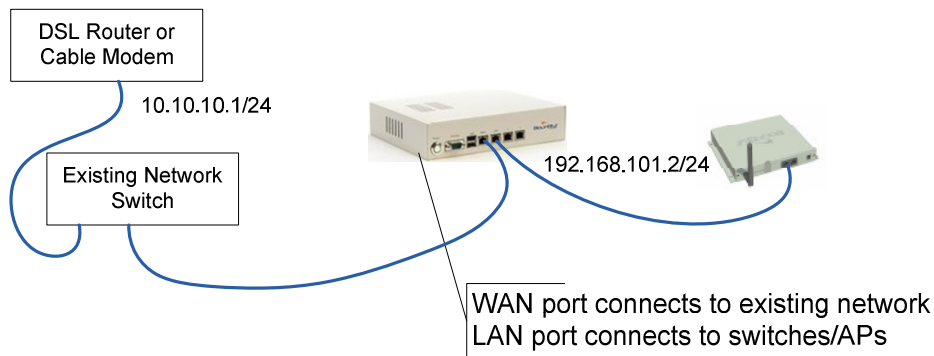
Connect WAN of AC to cable modem or DSL modem/router.

When a static IP for the WAN is configured, it is necessary to configure the Gateway (e.g. 10.10.10.1) as well as DNS server(s). The DNS servers are configured on the General setup page.

Ensure AC's DHCP server is enabled on the LAN interface with a Range and the Next server IP set to the LAN IP address of the AC.

Connect LAN port a switch which connects APs and other wired devices.

Option 2 Separate Local Area Network (LAN) for WiFi



Supports Captive portal

With this option the AC acts as a firewall and DHCP server for the WiFi network. The existing router acts as a firewall for other devices on an existing wired network to which the AC WAN port connects.

Connect WAN port of AC to existing network.

It is recommended if the AC is to be remotely managed to configure a static IP on the WAN interface. (e.g. 10.10.10.2 / 24) and enter a port forwarding rule on the existing router to direct a unique global IP and destination port (e.g. 8080) to the AC's IP address 10.10.10.2 and local port 80. If configuring a static IP for the WAN it is necessary to configure the Gateway (e.g. 10.10.10.1) as well as DNS server(s). The DNS servers are

configured on the General setup page and the IP addresses are provided by the Internet Service Provider.

Configure LAN IP 192.168.101.2 (default)

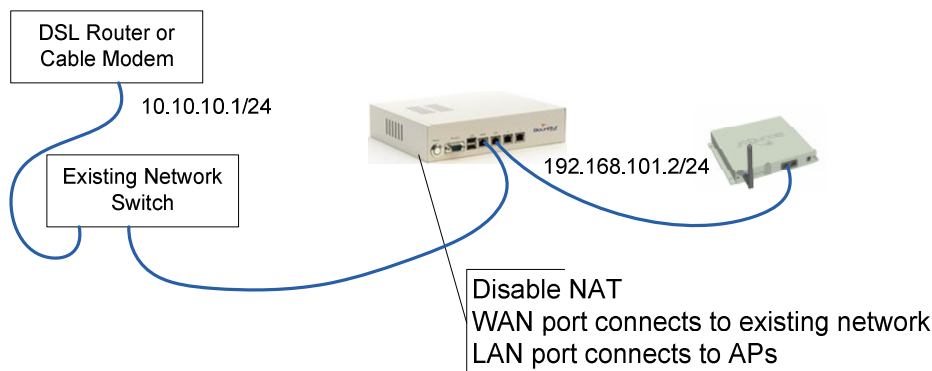
Set DHCP server Enabled on LAN (default)

Configure a range of IP addresses (e.g. 192.168.101.100 – 192.168.101.200 (default)

Next server IP 192.168.101.2 (default) must be configured for APs to boot and be discovered.

The devices connected to the WiFi network will be able to initiate connections to devices on the wired network. However; the devices on the existing network will not be able initiate a connection to the devices on the new WiFi network since the AC is acting as a firewall. NAT port forwarding rules paired with static DHCP mappings can be configured to allow existing devices to initiate connections to specific wireless devices.

Option 3 Separate LAN for WiFi Disabling NAT on WAN interface



Supports Captive portal

Connect WAN port of AC to existing network.

If the AC is to be remotely managed it is recommended to configure a static IP on the WAN interface. (e.g. 10.10.10.2 / 24) and enter a port forwarding rule on the existing router to direct a unique global IP and destination port (e.g. 8080) to the AC's IP address 10.10.10.2 and local port 80. If configuring a static IP for the WAN it is necessary to configure the Gateway (e.g. 10.10.10.1) as well as DNS server(s). The DNS servers are configured on the General setup page and the IP addresses are provided by the Internet Service Provider.

Configure LAN IP 192.168.101.2 (default)

Set DHCP server Enabled on LAN (default)

Configure a range of IP addresses (e.g. 192.168.101.100 – 192.168.101.200 (default)

Next server IP 192.168.101.2 (default) must be configured for APs to boot and be discovered.

When NAT is enabled, the AC translates the traffic on the WAN port. For outgoing traffic each packet's source IP is translated to the WAN IP and a unique source port is selected. This unique entry is placed in a table so the expected reply packet can be translated back to the correct destination. With NAT enabled the WAN IP will be the source IP for all traffic from the AC and the LAN connected clients. When NAT is disabled, the AC no longer translates the IP thus the LAN subnet IPs will be preserved as the traffic exits the WAN interface. Effectively this creates a new subnet of 192.168.101.x/24 on the network. The devices directly connected to the existing 10.10.10.0 / 24 network need to know how to reach this new subnet.

To disable NAT click on NAT under the Firewall menu. Click the Outbound tab. Click Enable advanced outbound NAT check box. Click Save. NAT is now effectively disabled it no longer dynamically creates translation entries. The only translation that would take place would be specific mappings that are entered on this Outbound page.

The default gateway flow of network traffic normally directs traffic toward the internet. When the destination is not on the same subnet the device consults its routing table. A device on the original network will not know how to reach a wireless client behind the AC unless a static route is added. For a windows machine a route can be added on the DOS command window: C:\ route add 192.168.101.0 mask 255.255.255.0 10.10.10.2 this adds a temporary static route. In other words the route will be lost if the system is rebooted. To make a permanent entry to the routing table use the -p option. So to add a persistent static route type:

```
route -p add 192.168.101.0 mask 255.255.255.0 10.10.10.2
```

To display the routing table enter:

```
route print
```

To delete a route enter:

```
route delete 192.168.101.0
```

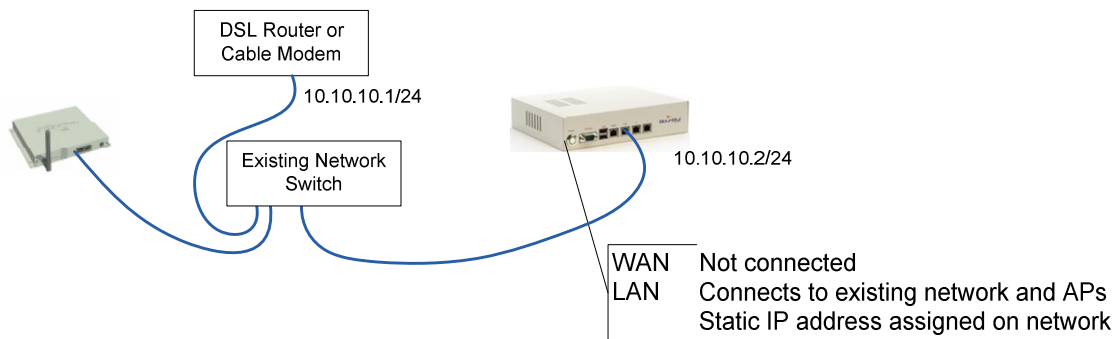
Static routes can be used to inform devices of other networks that are not along the pathway of the default route. For windows Server 2003 option 249 or for Server 2008 option 121 classless-static-routes can be used to inform devices on the network of the route to the new subnet. To configure right-click on 'Scope Options' and choose 'Configure Options...'. On Windows Server 2003 DNS servers, select option 249 'Classless Static Routes' (Option 121 on Windows Server 2008 DNS servers). Click on 'Add Route...', then enter the static route. **Note:** DHCP Option 121 is ignored by DHCP clients prior to Windows Server 2008 and Windows Vista. This may not work if you are using a Windows Server 2008 DNS server to assign networking configuration to these clients.

Windows Vista and Windows Server 2008 DHCP clients use both Option 121 and Option 249.

In order for traffic originating from the internet to be properly directed to the new subnet, a static route must be added to the router or routers between the AC and the internet informing them of how to get to the new subnet. In addition to the static route special consideration may need to be taken on the existing router to allow it to translate IP addresses other than those on the directly connected subnet.

If the WAN is not connected or if DHCP client is disabled and a static IP is configured for the WAN interface the gateway must also be configured on the WAN interface.

Option 4 Connect AC LAN to existing LAN



Captive portal is not supported with this option since internet traffic is not passing through the AC.

When connecting to an existing LAN care must be taken to setup the existing DHCP server to hand out a Next server IP address to the APs. If the existing DHCP server does not support setting the BOOTP Next server IP field then the AC should be used as the DHCP server. . If the AC is acting as the DHCP server then the Gateway field on the DHCP server screen should be set to the existing router's IP address (e.g. 10.10.10.1). This option is available as of 2010_02_11. Ensure that one or more DNS server IP addresses are configured on the General setup and that the DNS forwarder is disabled.

Configure IP address on LAN (e.g. 10.10.10.2)

If the existing DHCP server supports the Next server option for network booting, then ensure that the DHCP server is disabled on LAN interface of the AC

Connect LAN port of AC to existing network

Configure existing DHCP server with next server IP address equal to AC's IP address (e.g. 10.10.10.2) The next server IP is required by the Access Points as they boot and obtain an IP address they also need to know how to reach the AC in order to boot their image and obtain their configuration.

When the Bountiful WiFi AC is not acting as the DHCP server it is necessary to configure the network's DHCP server to hand out the next server IP address of the AC. To configure the **Microsoft Windows Server 2003 DHCP Server** to provide a next server IP address use DHCP options 66 and 67, perform the following:

1. Open the Microsoft DHCP Server management console and select your DHCP server.
2. In the Toolbar, click Action and select Set Predefined Options from the menu.
3. Click Add to add the DHCP options.
4. The Option Type window appears.
5. Enter the Name:
For option 66, enter Boot Server Host Name (AC's IP address 10.10.10.2)
For option 67, enter Bootfile Name (apimage.gz) not critical
6. For the Data Type, select String.
7. For the code, enter 66 or 67 (depending on which option is being set).
8. Enter the description:
For option 66, enter TFTP Boot Server Host Name
For option 67, enter Bootfile Name 9. Click OK.
10. Then enter the Access Controller's LAN IP Address for option 66 or Bootstrap file name for option 67 in the string value.

Example:

For a value in option 66, 10.10.10.2

For a value in option 67: apimage.gz but this is not regarded by the APs they ask for apimage.gz regardless of what is configured on the DHCP server.

11. Click OK.

When the Bountiful Access Controller is not using its WAN port as the Default Gateway it is necessary to setup a dummy static IP on the WAN and set the Default Gateway to the network's existing default router. This allows the AC to reach the network if the user wants to manage the controller via its web interface remotely. Note that an IP forwarding rule would need to be opened in the existing network's firewall router to direct outside traffic to the AC's web interface..

Since the WAN is not connected configure a dummy IP address for the WAN interface so the gateway field can be configured. Use an IP address in the private IP address range:

10.0.0.1 – 10.255.255.254

172.16.0.1 – 172.31.255.254

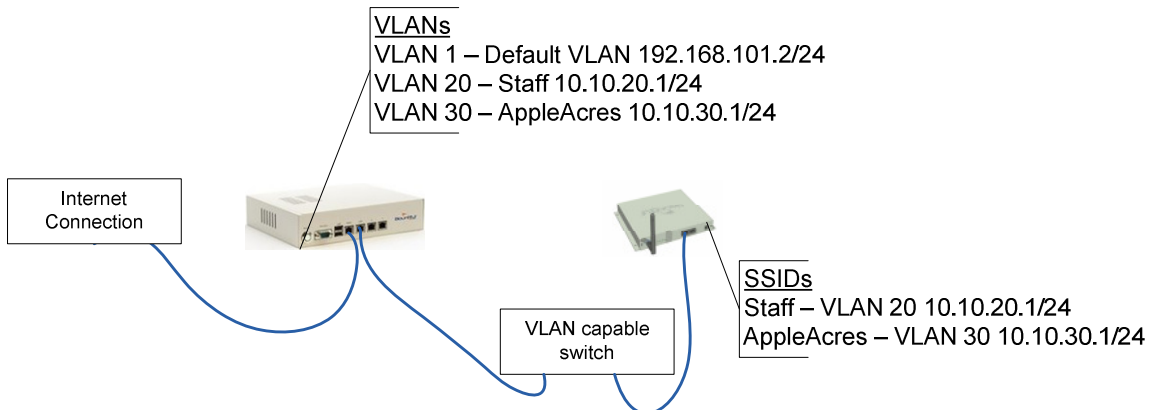
192.168.0.1 – 192.168.255.254

Do not pick an IP address that falls within the same subnet of the LAN or OPT interfaces of the AC. Also it is not recommended to select an IP that ends in 255 as this is reserved for the IP broadcast address for the subnet.

Option 5 Deploying with Virtual LANs (VLANs)

Minimum firmware required on AC is version 2010_02_03.

This option is for experienced network administrators. When Tagging is enabled on the Primary interface (LAN or OPT port) the AC manages the APs over the default VLAN (VLAN tag 1). Select Tagging on the interface when wireless traffic will be passing through the AC to get to the internet. VLAN 1 should have DHCP enabled and the next server IP set. The APs must be provided a DHCP IP address and a next server IP of the AC on VLAN 1. The APs attempt to DHCP BOOTP off of an untagged network then on a tagged network with a VLAN tag of 1. The AC and AP management communication is with TAGGED frames over VLAN 1 on a LAN or OPT port. The WAN port does not support VLAN tagged frames.



The LAN port should be connected to a VLAN capable switch with Tagging enabled and membership in the Default VLAN 1 adding other VLANs as necessary. Remember to create a Rule under the Firewall to allow traffic on vlan 1.

This example shows how VLANs can be used to isolate client traffic; VLAN 20 for the staff and VLAN 30 for tenants of Apple Acres. VLANs can also be used in other network topologies for example where the AC's WAN port is not connected. The APs should connect to Q-trunk tagging ports with membership in the default VLAN as well as the VLANs that are to be used for SSIDs.

When creating additional VLANs on the LAN port be aware that they will be created without Rules defined under the Firewall. To accept and pass traffic on the VLAN interfaces define rules for those interfaces to pass traffic. Rules can be entered such that traffic is not routed between the two VLANs.



Create SSID with VLAN per SSID enabled by selecting a VLAN interface in the dropdown menu on the SSID configuration page.

Once a VLAN per SSID SSID has been created it can be selected under the AP configuration. To see available VLAN SSIDs check the Enable VLAN per SSID on the Edit AP configuration page for the APs.