Single Point Setup

This chapter describes how to configure Single Point Setup over multiple WAP devices. It includes the following topics:

Single Point Setup Overview

Single Point Setup provides a centralized method to administer and control wireless services across multiple devices. You use Single Point Setup to create a single group, or cluster, of wireless devices. After the WAP devices are clustered, you can view, deploy, configure, and secure the wireless network as a single entity. After a wireless cluster is created, Single Point Setup also facilitates channel planning across your wireless services to reduce radio interference and maximize bandwidth on the wireless network.

When you first set up your WAP device, you can use the Setup Wizard to configure Single Point Setup or join an existing Single Point Setup. If you prefer not to use the Setup Wizard, you can use the web-based configuration utility.

Managing Single Point Setup Across Access Points

Single Point Setup creates a dynamic, configuration-aware cluster, or group, of WAP devices in the same subnet of a network. A cluster supports a group of up to 16 configured WAP581 devices, but no other non-WAP581 models in the same cluster.

Note Ensure that the PID is exactly the same in order for the device to cluster. For example: The WAP581-C-K9 will not cluster with the WAP581-E-K9 or any other WAP.

Single Point Setup allows the management of more than one cluster in the same subnet or network; however, they are managed as single independent entities. The following table shows the wireless service limits of a Single Point Setup:

Table 1: Single Point Setup Wireless Service Limits

Group/Cluster Type	WAP Devices per Single Point Setup	Number of Active Clients per Single Point Setup	Maximum Number of Clients (Active and Idle)
Cisco WAP581	16	960 for the WAP581 with a dual radio	2048 for the WAP581 with a dual radio

A cluster can propagate configuration information, such as VAP settings, the QoS queue parameters, and the radio parameters. When you configure Single Point Setup on a device, settings from that device (whether they are manually set or set by default) are propagated to other devices as they join the cluster.

To form a cluster, make sure the following prerequisites or conditions are met:

Step 1 Plan your Single Point Setup cluster. Be sure that two or more WAP devices that you want to cluster are the same model. For example, Cisco WAP581 devices can only cluster with other Cisco WAP581 devices.

Note It is strongly recommended to run the same firmware version on all clustered WAP devices. Firmware can be upgraded from the Dominant AP (Cluster Controller). See Access Points for more information.

Step 2 Set up the WAP devices that will be clustered on the same IP subnet and verify that they are interconnected and accessible across the switched LAN network.

Step 3 Enable Single Point Setup on all WAP devices. See Access Points for more information.

Step 4 Verify that all WAP devices reference the same Single Point Setup name. See Access Points for more information.

Single Point Setup Negotiation

When a AP is enabled and configured for Single Point Setup, it begins sending periodic advertisements every 10 seconds to announce its presence. If there are other WAP devices that match the criteria for the cluster, arbitration begins to determine which WAP device will distribute the master configuration to the rest of the members of the cluster.

The following rules apply to Single Point Setup cluster formation and arbitration:

- For existing Single Point Setup clusters, whenever the administrator updates the configuration of any member of the cluster, the configuration change is propagated to all members of the cluster, and the configured WAP device assumes control of the cluster.
- When two separate Single Point Setup clusters join into a single cluster, then the latest modified cluster wins arbitration of the configuration and overwrites and updates the configuration of all clustered WAP devices.
- If a WAP device in a cluster does not receive advertisements from a WAP device for more than 60 seconds (for example, if the device loses connectivity to other devices in the cluster), the device is removed from the cluster.
- If a WAP device in Single Point Setup mode loses connectivity, it is not immediately dropped from the cluster. If it regains connectivity and rejoins the cluster without having been dropped, and configuration changes were made to that device during the lost connectivity period, the changes are propagated to the other cluster members when connectivity resumes.

- If a WAP device in a cluster loses connectivity, is dropped, later rejoins the cluster, and configuration changes were made in the during the lost connectivity period, the changes are propagated to the device when it rejoins. If there are configuration changes in both the disconnected device and the cluster, then the device with the greatest number of changes and, secondarily, the most recent change, will be selected to propagate its configuration to the cluster. (That is, if WAP1 has more changes, but WAP2 has the most recent change, WAP1 is selected. If they have an equal number of changes, but WAP2 has the most recent change, then WAP2 is selected.)

Operation of a Device Dropped From a Single Point Setup

When a WAP device that was previously a member of a cluster becomes disconnected from the cluster, the following guidelines apply:

- The loss of contact with the cluster prevents the WAP device from receiving the latest operational configuration settings. The disconnection results in a halt to proper seamless wireless service across the production network.
- The WAP device continues to function with the wireless parameters that it last received from the cluster.
- The wireless clients associated with the non-clustered WAP device continue to associate with the device with no interruption of the wireless connection. In other words, the loss of contact with the cluster does not necessarily prevent the wireless clients associated with that WAP device from continued access to network resources.
- If the loss of contact with the cluster is due to a physical or logical disconnection with the LAN infrastructure, the network services out to the wireless clients may be impacted depending on the nature of the failure.

Configuration Parameters Propagated and Not Propagated to Single Point Setup Access Points

The following table summarizes the configurations that are shared and propagated among all clustered WAP devices:

Table 2: Configuration Parameters Propagated and Not Propagated

Common Configuration Settings and Parameters that are Propagated in Single Point Setup	
Access Control	Password Complexity
Client QoS	User Accounts
Email Alert	QoS
HTTP/HTTPs Service (Except SSL Certificate Configuration)	Radio Settings Including TSPEC Settings (Some exceptions)
Log Settings	Rogue AP Detection
Client Filter	Scheduler
Management Access Control	SNMP and SNMPv3

Common Configuration Settings and Parameters that are Propagated in Single Point Setup	
Networks	WPA-PSK Complexity
Time Settings	Cisco Umbrella (Except Device Tag)
LLDP (Except POE Priority Configuration)	PnP (Plug and Play)
Radio Configuration Settings and Parameters that are Propagated in Single Point Setup	
Wireless Network Mode	
Fragmentation Threshold	
RTS Threshold	
Rate Sets	
Channel	
Protection	
Fixed Multicast Rate	
Broadcast or Multicast Rate Limiting	
Wireless Band Selection	
Short Guard Interval Supported	
Radio Configuration Settings and Parameters that are Not Propagated in Single Point Setup	
Channel	
Beacon Interval	
DTIM Period	
Maximum Stations	
Transmit Power	
Other Configuration Settings and Parameters that are Not Propagated in Single Point Setup	
Utilization Threshold	Port Settings
Bonjour	VLAN and IPv4
IPv6 Address	Bridge
IPv6 Tunnel	Packet Capture

Access Points

The **Access Points** page allows you to enable or disable Single Point Setup on a WAP device, view the cluster members, and configure the location and cluster name for a member. You can also click the IP address of a member to configure and view data on that device.

Configuring the WAP Device for Single Point Setup

To configure the location and name of an individual Single Point Setup cluster member:

Step 1 Select **Single Point Setup** > **Access Points**.

The Single Point Setup is disabled on the WAP device by default. Check the **Enable** checkbox to enable this feature.

Step 2 Configure the following parameters for each individual member of a Single Point Setup cluster:

- **AP Location**—Enter a description of where the WAP device is physically located, for example, Reception. The location field is optional. The valid range can be between 1 to 64 characters which includes alphanumeric and special characters.
- **AP Priority**—Enter the priority of the cluster for Dominant AP (Cluster Controller) election. The higher number indicates the higher preference for this AP to become the Dominant AP. In case of tie, lowest MAC address becomes dominant. The range can be between 0 to 255. The default value is 0.
- **Cluster Name to Join**—Enter the name of the cluster for the WAP device to join, for example Reception_Cluster. The cluster name is not sent to other WAP devices. You must configure the same name on each device that is a member. The cluster name must be unique for each Single Point Setup that you configure on the network. The default is ciscosb-cluster. The valid range is 1 to 64 alphanumeric and special characters.
- **Cluster IP Protocol**—Choose the IP version that the WAP devices in the cluster use to communicate with other members of the cluster. The default is IPv4.
- If you choose IPv6, Single Point Setup can use the link local address, auto-configured IPv6 global address, and statically configured IPv6 global address. When using IPv6, ensure that all WAP devices in the cluster either use link-local addresses only or use global addresses only.

  Single Point Setup works only with the WAP devices using the same type of IP addressing. It does not work with a group of the WAP devices where some have IPv4 addresses and some have IPv6 addresses.

The WAP device begins searching for other WAP devices in the subnet that are configured with the same cluster name and IP Protocol. A potential cluster member sends the advertisements every 10 seconds to announce its presence.

Step 3 Configure the Cluster Management Address:

Cluster Management Address—In order to access the cluster with a single IP. The Cluster can be configured with an option of Cluster IPv4 address. This is part of the global configuration of the cluster in section. It has to be statically configured by the Cluster Administrator. The Cluster IP management address should be part of the same subnet as the clustered AP management IP addresses. The Cluster IP address is configured as secondary IP address to the management interface of the Dominant AP. The Dominant AP user interface is accessible using the Cluster IP address. When the Cluster IP address is set as secondary IP address on the Dominant IP, it sends Gratuitous ARPs on the management VLAN so that the mapping between the new IP address and the MAC-address is established in the subnet. The Cluster IP address configuration is shared among all the clustered APs.

Step 4 Click **Apply**.

Step 5 Repeat these steps on additional WAP devices that you want to join the Single Point Setup.

Firmware Management

Cluster provides a centralized cluster firmware upgrade feature that allows all the APs in the cluster to be upgraded from the Dominant AP (Cluster Controller). The Cluster firmware upgrade can be performed only from the Dominant AP.

On the cluster firmware upgrade page the WAP devices detected are listed in a table and the following information is shown:

- **Location**—Description of where the access point is physically located.
- **IP Address**—The IP address for the access point.
- **MAC Address**—Media Access Control (MAC) address of the access point. The address is the MAC address for the bridge (br0), and is the address by which the WAP device is known externally to other networks.
- **Current Firmware Version**—The current running firmware version for the access point.
- **Firmware-transfer-status**—Shows whether the firmware download and validation in cluster member is None/Started/Downloaded/Success/Fail/Abort_admin/Abort_local/Dap_resigned.
- **Firmware-transfer-progress-bar**—Shows the progress bar for firmware download.

To select the cluster member for upgrade:

1. Select **Single Point Setup** > **Firmware Management** in the navigation pane.
2. Select the check box of the AP to be upgraded.
3. Click **Apply**.

To get the latest cluster firmware upgrade status:

Click **Refresh**.

To upgrade the firmware on a cluster member using **TFTP**:

1. Select **TFTP** for **Transfer Method**.
2. Enter a name (1 to 256 characters) for the image file in the **Source File Name** field, including the path to the directory that contains the image to upload.

   For example, to upload the ap_upgrade.tar image located in the /share/builds/ap directory, enter: /share/builds/ap/ap_upgrade.tar

   The firmware upgrade file supplied must be a tar file. Do not attempt to use bin files or files of other formats for the upgrade; these types of files do not work.

   The filename cannot contain the following items: spaces, <, >, |, \, : , (,), &, ; , #, ? , *, and two or more successive periods.
3. Enter the **TFTP Server IPv4 Address** and click **Start-Upgrade**.

To upgrade using HTTP:

1. Select **HTTP** for **Transfer Method**.
2. If you know the name and path to the new file, enter it in the **New Firmware Image** field.

   Otherwise, click the Browse button and locate the firmware image file on your network.

   The firmware upgrade file supplied must be a tar file. Do not attempt to use bin files or files of other formats for the upgrade; these types of files do not work.
3. Click **Start-Upgrade** to apply the new firmware image.

Note **Overall Upgrade Status** shows the combined upgrade status (**Not Initialized/In Progress/ Completed/Fail/Abort_admin/ None**) of all the cluster members.

To stop the cluster member upgrade from Dominant AP:

Click **Stop-Upgrade**.

Channel Management

Use the **Channel Management** page to manage the channel for the WAP devices in a Single Point Setup cluster.

When the channel management is enabled, the WAP device automatically assigns the radio channels used by the WAP devices in a Single Point Setup cluster. The automatic channel assignment reduces mutual interference (or interference with other WAP devices outside of its cluster) and maximizes the Wi-Fi bandwidth to help maintain efficient communication over the wireless network.

The **Automatic Channel Assignment** feature is enabled by default. The state of channel management (enabled or disabled) is propagated to the other devices in the Single Point Setup cluster.

Configuring Advanced Settings

The Advanced area enables you to customize and schedule the channel plan for the Single Point Setup.

By default, channels are automatically reassigned once every hour, but only if the interference can be reduced by 25 percent or more. The channels are reassigned even if the network is busy.

The default settings are designed to satisfy most scenarios where you would need to implement the channel management.

You can change the advanced settings by configuring the following settings:

- **Change Channel Threshold**—The minimum percentage of interference reduction that a proposed plan must achieve in order to be applied. The default is 75 percent. Choose the percentages ranging from 5 percent to 75 percent. Using this setting lets you set a threshold gain in efficiency for channel reassignment so that the network is not continually disrupted for minimal gains in efficiency.

  For example, if the channel interference must be reduced by 75 percent and the proposed channel assignments will only reduce the interference by 30 percent, then the channels will not be reassigned.

However, if you reset the minimal channel interference benefit to 25 percent and click **Apply**, the proposed channel plan will be implemented and the channels will be reassigned as needed.

- **Reassess Channel Assignment Every**—The schedule for automated updates. A range of intervals is provided, from 30 minutes to six months. The default is one hour, meaning that the channel usage is reassessed and the resulting channel plan is applied every hour.

  If you change these settings, click **Apply**. The changes are saved to the active configuration and the Startup Configuration.

  When the Automatic Channel Assignment is enabled, the page shows the Channel Assignations table.

Channel Assignment Table

The **Channel Assignment Table** shows a list of all WAP devices in the Single Point Setup cluster by IP address.

The table provides the following details on the channel assignments:

- **AP Location**—The physical location of the WAP device.
- **MAC Address**—The MAC address of the radio.
- **IP Address**—The IP address for the WAP device.
- **Radio Band**—The band on which the WAP device is broadcasting.
- **Up/Down**—Shows the status of the wireless radio in the WAP device. Some WAP devices may have more than one wireless radio; each radio is displayed on a separate line in the table. The radio status is up (operational) or down (not operational).
- **Current Channel**—The radio channel on which the WAP device is currently broadcasting.
- **Lock Current Channel**—When selected for a WAP device, the automated channel management plans do not reassign the WAP device to a different channel as a part of the optimization strategy. Instead, the WAP devices with locked channels are factored in as requirements for the plan.
- **Proposed Channel (xx Hours Ago)**—which is the radio channel to which this WAP device would be reassigned if the channel plan is applied.

Click **Apply** to update the locked setting. The locked devices show the same channel for the Current Channel Assignment table and the Proposed Channel Assignment table. The locked devices keep their current channels.

The proposed channels that are to be assigned to each WAP device when the next update occurs. The locked channels are not reassigned—the optimization of channel distribution among the devices takes into account that the locked devices must remain on their current channels. The WAP devices that are not locked may be assigned to different channels than what they were previously using, depending on the results of the plan.

Refresh the page to see the new channel assignment table.