



Configuring Link Aggregation

- [Link Aggregation, on page 1](#)
- [Restrictions on Link Aggregation, on page 1](#)
- [Configuring Link Aggregation \(GUI\), on page 3](#)
- [Configuring Link Aggregation \(CLI\), on page 4](#)
- [Verifying Link Aggregation Settings \(CLI\), on page 4](#)
- [Configuring Neighbor Devices to Support Link Aggregation, on page 4](#)
- [Choosing Between Link Aggregation and Multiple AP-Manager Interfaces, on page 5](#)

Link Aggregation

Link aggregation (LAG) is a partial implementation of the 802.3ad port aggregation standard. It bundles all of the controller's distribution system ports into a single 802.3ad port channel. This reduces the number of IP addresses required to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

LAG simplifies controller configuration because you no longer require to configure primary and secondary ports for each interface. If any of the controller ports fail, traffic is automatically migrated to one of the other ports. As long as at least one controller port is functioning, the system continues to operate, access points remain connected to the network, and wireless clients continue to send and receive data.

You can use fast restart for any LAG changes.

Controller does not send CDP advertisements on a LAG interface.



Note LAG is supported across switches.

This section contains the following subsections:

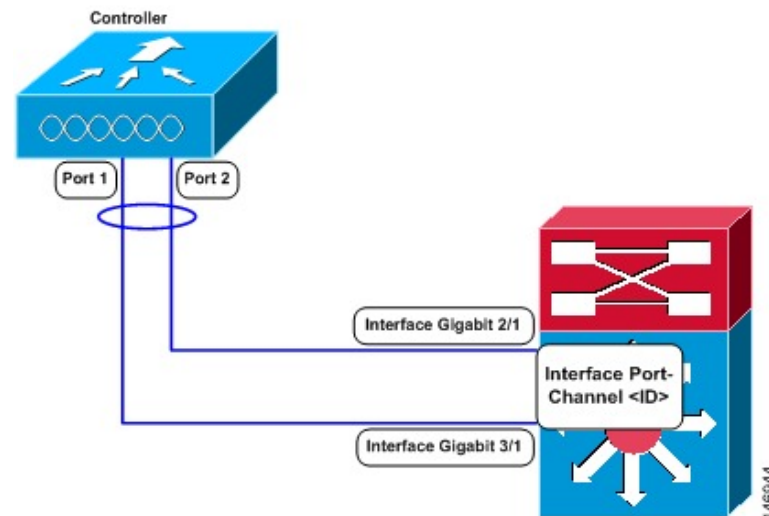
Restrictions on Link Aggregation

- You can bundle all eight ports on a Cisco 5508 Controller into a single link.
- Terminating on two different modules within a single Catalyst 6500 series switch provides redundancy and ensures that connectivity between the switch and the controller is maintained when one module fails.

The controller's port 1 is connected to Gigabit interface 3/1, and the controller's port 2 is connected to Gigabit interface 2/1 on the Catalyst 6500 series switch. Both switch ports are assigned to the same channel group.

- The controller relies on the switch for the load balancing decisions on traffic that come from the network, with “source-destination IP” as the typically recommended option. It is important to select a correct balancing configuration on the switch side, as some variations might have an impact on controller performance or cause packet drops on some scenarios, where traffic from different ports is split across different data planes internally.
- When using Link aggregation (LAG) make sure all ports of the controller have the same Layer 2 configuration on the switch side. For example, avoid filtering some VLANs in one port, and not the others.
- LAG requires the EtherChannel to be configured for 'mode on' on both the controller and the Catalyst switch.
- Once the EtherChannel is configured as on at both ends of the link, the Catalyst switch should not be configured for either Link Aggregation Control Protocol (LACP) or Cisco proprietary Port Aggregation Protocol (PAgP) but be set unconditionally to LAG. Because no channel negotiation is done between the controller and the switch, the controller does not answer to negotiation frames and the LAG is not formed if a dynamic form of LAG is set on the switch. Additionally, LACP and PAgP are not supported on the controller.
- If the recommended load-balancing method cannot be configured on the Catalyst switch, then configure the LAG connection as a single member link or disable LAG on the controller.

Figure 1: Link Aggregation with the Catalyst 6500 Series Neighbor Switch



- You cannot configure the controller's ports into separate LAG groups. Only one LAG group is supported per controller.
- When you enable LAG or make any changes to the LAG configuration, you must immediately reboot the controller.
- When you enable LAG, you can configure only one AP-manager interface because only one logical port is needed.

- When you enable LAG, all dynamic AP-manager interfaces and untagged interfaces are deleted, and all WLANs are disabled and mapped to the management interface. Also, the management, static AP-manager, and VLAN-tagged dynamic interfaces are moved to the LAG port.
- Multiple untagged interfaces to the same port are not allowed.
- When you enable LAG, all ports participate in LAG by default. You must configure LAG for all of the connected ports in the neighbor switch.
- When you enable LAG, if any single link goes down, traffic migrates to the other links.
- When you enable LAG, only one functional physical port is needed for the controller to pass client traffic.
- When you enable LAG, access points remain connected to the controller until you reboot the controller, which is needed to activate the LAG mode change, and data service for users continues uninterrupted.
- When you enable LAG, you eliminate the need to configure primary and secondary ports for each interface.
- When you enable LAG, the controller sends packets out on the same port on which it received them. If a CAPWAP packet from an access point enters the controller on physical port 1, the controller removes the CAPWAP wrapper, processes the packet, and forwards it to the network on physical port 1. This may not be the case if you disable LAG.
- When you disable LAG, the management, static AP-manager, and dynamic interfaces are moved to port 1.
- When you disable LAG, you must configure primary and secondary ports for all interfaces.
- When you enable LAG on Cisco 2504 WLC to which the direct-connect access point is associated, the direct connect access point is disconnected since LAG enabling is still in the transition state. You must reboot the controller immediately after enabling LAG.
- In Cisco 8510 WLCs, when more than 1000 APs join the controller, flapping occurs. To avoid this, we recommend that you do not add more than 1000 APs on a single Cisco Catalyst switch for CAPWAP IPv6.
- If you have configured a port-channel on the switch and you have not configured the AP for LAG, the AP moves to standalone mode.
- We recommend that you configure LAG with HA-SSO in disabled state. Therefore, you must enable LAG before placing the controllers in HA-SSO pair or schedule a maintenance window to break the HA-SSO (requires controller reboot) and then enable LAG and re enable HA-SSO thereafter (incurs multiple controller reboots in the process).

Configuring Link Aggregation (GUI)

-
- Step 1** Choose **Controller > General** to open the **General** page.
 - Step 2** Set the **LAG Mode on next reboot** parameter to **Enabled**.
 - Step 3** Save the configuration.
 - Step 4** Reboot the controller.
-

Configuring Link Aggregation (CLI)

Step 1 Enter the **config lag enable** command to enable LAG.

Note Enter the **config lag disable** command if you want to disable LAG.

Step 2 Enter the **save config** command to save your settings.

Step 3 Reboot controller.

Verifying Link Aggregation Settings (CLI)

Verify your LAG settings by entering this command:

show lag summary

Information similar to the following appears:

```
LAG Enabled
```

Configuring Neighbor Devices to Support Link Aggregation

The controller's neighbor devices must also be properly configured to support LAG.

- Each neighbor port to which the controller is connected should be configured as follows:

```
interface GigabitEthernet <interface id>
  switchport
  channel-group <id> mode on
  no shutdown
```

- The port channel on the neighbor switch should be configured as follows:

```
interface port-channel <id>
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk native vlan <native vlan id>
  switchport trunk allowed vlan <allowed vlans>
  switchport mode trunk
  no shutdown
```

Choosing Between Link Aggregation and Multiple AP-Manager Interfaces

controllers have no restrictions on the number of access points per port, but we recommend that you use link aggregation (LAG) or multiple AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load.

The following factors should help you decide which method to use if your controller is set for Layer 3 operation:

- With LAG, all of the controller ports need to connect to the same neighbor switch. If the neighbor switch goes down, the controller loses connectivity.
- With multiple AP-manager interfaces, you can connect your ports to different neighbor devices. If one of the neighbor switches goes down, the controller still has connectivity. However, using multiple AP-manager interfaces presents certain challenges when port redundancy is a concern.

