Wireless Bridge

This chapter describes how to configure the **Wireless Bridge** settings. It contains the following topics:

- Wireless Bridge, on page 1
- Configuring WDS Bridge, on page 2
- WPA/PSK on WDS Links, on page 2
- WorkGroup Bridge, on page 3

Wireless Bridge

The Wireless Distribution System (WDS) allows you to connect multiple WAP devices. With WDS, the WAP devices communicate with one another wirelessly. This provides a seamless experience for roaming the clients and managing multiple wireless networks. You can configure the WAP device in point-to-point or point-to-multipoint bridge mode based on the number of links to connect.

In the point-to-point mode, the WAP device accepts client associations and communicates with the wireless clients. The WAP device forwards all traffic meant for the other network over the tunnel that is established between the access points. The bridge does not add to the hop count. It functions as a simple OSI Layer 2 network device.

In the point-to-multipoint bridge mode, one WAP device acts as the common link between multiple access points. In this mode, the central WAP device accepts the client associations and communicates with the clients. All other access points associate only with the central WAP device that forwards the packets to the appropriate wireless bridge for routing purposes.

The WAP device can also act as a repeater. In this mode, the WAP device serves as a connection between two WAP devices that may be too far apart to be within cell range. When acting as a repeater, the WAP device does not have a wired connection to the LAN and repeats signals by using the wireless connection. No special configuration is required for the WAP device to function as a repeater, and there are no repeater mode settings. The wireless clients can still connect to an WAP device that is operating as a repeater.

Before you configure WDS on the WAP device, note these guidelines:

- All Cisco WAP devices participating in a WDS link must have the following identical settings:
  - Radio
  - IEEE 802.11 Mode
  - Channel Bandwidth

- Channel (Auto is not recommended)

When operating bridging in the 802.11n 2.4 GHz band, set the Channel Bandwidth to 20 MHz, rather than the default 20/40 MHz. In the 2.4 GHz, 20/40 MHz band, the operating bandwidth can change from 40 MHz to 20 MHz if any 20 MHz WAP devices are detected in the area. The mismatched channel bandwidth can cause the link to disconnect.

- When using WDS, be sure to configure WDS on both WAP devices participating in the WDS link.
- You can have only one WDS link between any pair of WAP devices. That is, a remote MAC address may appear only once on the WDS page for a particular WAP device.

Configuring WDS Bridge

To configure a WDS bridge:

Step 1 Select **Wireless Bridge**.

Step 2 Click **WDS** as the Wireless Bridge mode.

Step 3 Check **Enable** to enable a WDS port in the WDS Settings.

Step 4 Configure the remaining parameters:

- **Radio** — Specifies the Radio ID (Radio 1 (2.4 GHz) or Radio 2 (5GHz).
- **Local MAC Address** — Specifies the physical or MAC address of the current or local WAP device to which data is transmitted from.
- **Remote MAC Address** — Specifies the MAC address of the destination WAP device. You can find the MAC address on the Monitor> Dashboard> Wireless page.
- **Encryption** — Select the type of encryption to use on the WDS link (**None or WPA Personal**).

  If you are not concerned about the security issues on the WDS link, you may decide not to set any type of encryption. Alternatively, if you have security concerns, you can choose the WPA Personal. In WPA Personal mode, the WAP device uses WPA2-PSK with CCMP (AES) encryption over the WDS link. See WPA/PSK on WDS Links, on page 2 for more information about encryption options.

Step 5 Repeat these steps for up to four WDS interfaces.

Step 6 Click **Apply**.

Step 7 Replicate this procedure on devices connecting to the bridge.

Note You can verify if the bridge link is up by accessing the **Monitor** > **Dashboard** > **Wireless** page. In the Interface Status table, the WDS(x) status should state **Up**.

WPA/PSK on WDS Links

These additional fields appear when you select WPA/PSK as the encryption type:

- **WDS ID** — Enter an appropriate name for the new WDS link that you have created. It is important that the same WDS ID is also entered at the other end of the WDS link. If this WDS ID is not the same for both WAP devices on the WDS link, they will not be able to communicate and exchange data.

  The WDS ID can be any alphanumeric combination within a range of 2-32 characters.

- **Key** — Enter a unique shared key for the WDS bridge. This unique shared key must also be entered for the WAP device at the other end of the WDS link. If this key is not the same for both WAPs, they will not be able to communicate and exchange data.

  The WPA-PSK key is a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include uppercase and lowercase alphabetic letters, the numeric digits, and special symbols such as @ and #.

WorkGroup Bridge

The Work Group Bridge feature enables the WAP device to extend the accessibility of a remote network. In the Work Group Bridge mode, the WAP device acts as a wireless station (STA) on the wireless LAN. It can bridge traffic between a remote wired network or associated wireless clients and the wireless LAN that is connected using the Work Group Bridge mode.

The Work Group Bridge feature enables support for STA-mode and AP-mode operation simultaneously. The WAP device can operate in one Basic Service Set (BSS) as an STA device while operating on another BSS as a WAP device. When the Work Group Bridge mode is enabled, the WAP device supports only one BSS for wireless clients that associate with it, and another BSS with which the WAP device associates as a wireless client.

We recommend that you use the Work Group Bridge mode only when the WDS bridge feature cannot be operational with a peer WAP device. WDS is a better solution and is preferred over the Work Group Bridge solution. Use WDS if you are bridging the Cisco WAP150 and Cisco WAP361 devices. If you are not, then consider the Work Group Bridge. When the Work Group Bridge feature is enabled, the VAP configurations are not applied; only the Work Group Bridge configuration is applied.

Note The WDS feature does not work when the Work Group Bridge mode is enabled on the WAP device.

In Work Group Bridge mode, the BSS managed by the WAP device while operating in WAP device mode is referred to as the access point interface, and associated STAs as the downstream STAs. The BSS managed by the other WAP device (that is, the one to which the WAP device associates as an STA) is referred to as the infrastructure client interface, and the other WAP device is referred as the upstream AP.

The devices connected to the wired interface of the WAP device, as well as the downstream stations associated with the access point interface of the device, can access the network connected by the infrastructure client interface. To allow the bridging of packets, the VLAN configuration for the access point interface and the wired interface must match that of the infrastructure client interface.

The Work Group Bridge mode can be used as a range extender to enable BSS to provide access to remote or hard-to-reach networks. A single radio can be configured to forward packets from associated STAs to another WAP device in the same ESS, without using WDS.

Before you configure **Work Group Bridge** on the WAP device, note these guidelines:

- All WAP devices participating in Work Group Bridge must have the following identical settings:

- Radio
- IEEE 802.11 Mode
- Channel Bandwidth
- Channel (Auto is not recommended)

See Radio (Basic Settings) for information on configuring these settings.

- Work Group Bridge mode currently supports only IPv4 traffic.
- Work Group Bridge mode is not supported across a Single Point Setup.

To configure Work Group Bridge mode:

Step 1 Select **Wireless Bridge**.

Step 2 Click **WorkGroup**.

Step 3 Select the WGB Port to which the configuration parameters will be applied.

Step 4 Click **edit** to configure the following parameters for the Infrastructure Client Interface (Uplink / Downlink):

Table 1: Infrastructure Client Interface (Uplink / Downlink)

WGB Port	Uplink	Downlink
Enabled	Check the check box to enable the Infrastructure Client Interface.	Check the check box to enable the Infrastructure Client Interface.
Radio	Specifies the Radio Id (Radio 1 (2.4 GHz) or Radio 2 (5GHz)).	Specifies the Radio Id (Radio 1 (2.4 GHz) or Radio 2 (5GHz)).
SSID	Specifies the current SSID of the BSS. **Note** There is an arrow next to SSID for SSID Scanning. This feature is disabled by default, and is enabled only if AP Detection is enabled in Rogue AP Detection (which is also disabled by default).	The SSID for the Access Point Interface cannot be the same as the Infrastructure Client SSID.
Encryption	The type of security to use for authenticating as a client station on the upstream WAP device. It can be one of the following: • **None** • **WPA Personal** • **WPA Enterprise**	The type of security to use for authenticating. The options are: • **None** • **WPA Personal**
Connection Status	Indicates whether the WAP is connected to the upstream WAP device.	Not Applicable (N/A)

WGB Port	Uplink	Downlink
VLAN ID	Specifies the VLAN associated with the BSS.	Configure the Access Point Interface with the same VLAN ID as advertised on the Infrastructure Client Interface.
Note The Infrastructure Client Interface will be associated with the upstream WAP device with the configured credentials. The WAP device may obtain its IP address from a DHCP server on the upstream link. Alternatively, you can assign a static IP address.		
SSID Broadcast	Specifies if the broadcast of the SSID is available, enabled or disabled.	Check if you want the downstream SSID to be broadcast. SSID Broadcast is enabled by default.
Client Filter	Not Applicable (N/A)	Choose one of the following options: • Disabled—The set of clients in the APs BSS that can access the upstream network is not restricted to the clients specified in a MAC address list. • Local—The set of clients in the APs BSS that can access the upstream network is restricted to the clients specified in a locally defined MAC address list. • RADIUS—The set of clients in the APs BSS that can access the upstream network is restricted to the clients specified in a MAC address list on a RADIUS server.
Note If you choose Local or RADIUS, see Client Filter for instructions on creating the Client filter list.		

Step 5 Click **Apply**. The associated downstream clients now have connectivity to the upstream network.