Peer-to-Peer Client Support

Information About Peer-to-Peer Client Support

Peer-to-peer client support can be applied to individual WLANs, with each client inheriting the peer-to-peer blocking setting of the WLAN to which it is associated. The peer-to-Peer Client Support feature provides a granular control over how traffic is directed. For example, you can choose to have traffic bridged locally within a device, dropped by a device, or forwarded to the upstream VLAN.

Peer-to-peer blocking is supported for clients that are associated with local and central switching WLANs.

Restrictions

- Peer-to-peer blocking does not apply to multicast traffic.

- Peer-to-peer blocking is not enabled by default.

- In FlexConnect, peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all the FlexConnect APs that broadcast the SSID.

- FlexConnect central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect local switching. This is treated as peer-to-peer drop and client packets are dropped.

  FlexConnect central switching clients supports peer-to-peer blocking for clients associated with different APs. However, for FlexConnect local switching, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.

Configure Peer-to-Peer Client Support

Follow the procedure given below to configure Peer-to-Peer Client Support:

Procedure

	Command or Action	**Purpose**
Step 1	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 2	**wlan** *profile-name* **Example:** Device(config)# wlan wlan1	Enters WLAN configuration submode. The *profile-name* is the profile name of the configured WLAN.
Step 3	**peer-blocking** [**allow-private-group** |**drop** | **forward-upstream**] **Example:** Device(config-wlan)# **peer-blocking drop**	Configures peer to peer blocking parameters. The keywords are as follows: • **allow-private-group**—Enables peer-to-peer blocking on the Allow Private Group action. • **drop**—Enables peer-to-peer blocking on the drop action. • **forward-upstream**—No action is taken and forwards packets to the upstream. **Note** The **forward-upstream** option is not supported for Flex local switching. Traffic is dropped even if this option is configured. Also, peer to peer blocking for local switching SSIDs are available only for the clients on the same AP.
Step 4	**end** **Example:** Device(config)# end	Returns to privileged EXEC mode.
Step 5	**show wlan id** *wlan-id* **Example:** Device# show wlan id 12	Displays the details of the selected WLAN.