

## Layer 2 Attack Prevention Overview

---

Layer 2 protocols manage data transfer from the source address to the destination address. Attackers can manipulate Layer 2 protocols to perform ARP attacks (such as ARP cache poisoning) and MAC attacks.

The IDP engine does not use security policies to detect Layer 2 attacks, rather all Layer 2 traffic passing through the IDP appliance must conform to properties you configure.

Table 1 provides guidelines for IDP Layer 2 settings.

**Table 1: IDP Layer 2 Settings**

Layer 2 Setting	Guideline
MAC timeout	When the virtual router is in bridge mode, this setting controls how long a MAC entry is maintained in the virtual router. Default: 3600 seconds.
MAC proxy timeout	In bridge mode, the IDP device performs MAC discovery if the target MAC address is not in its MAC table. This setting controls how long the entry is maintained in the virtual router until a reply comes back. Default: 20 seconds.
ARP timeout	When the virtual router is in proxy-ARP mode, this setting controls how long an ARP entry is maintained in the virtual router. If the IDP device does not receive an ARP reply before the timeout expires, the ARP entry times out. Default: 3600 seconds.
ARP proxy timeout	In proxy-ARP mode, the IDP sensor sends out proxy ARPs on all interfaces except the one on which an ARP request was received. This setting indicates how long the original ARP entry is maintained in the virtual router if the IDP device does not receive an ARP reply through that interface. Default: 20 seconds.
ARP attack logging	When selected, the IDP device detects and logs all spoofed ARP requests or replies and other ARP anomalies. Default: Enabled.

**Related Topics** The following related topic is included in the *IDP Administration Guide*:

- Modifying the IDP Device Configuration

---

Published: 2010-01-12