

[Show](#)

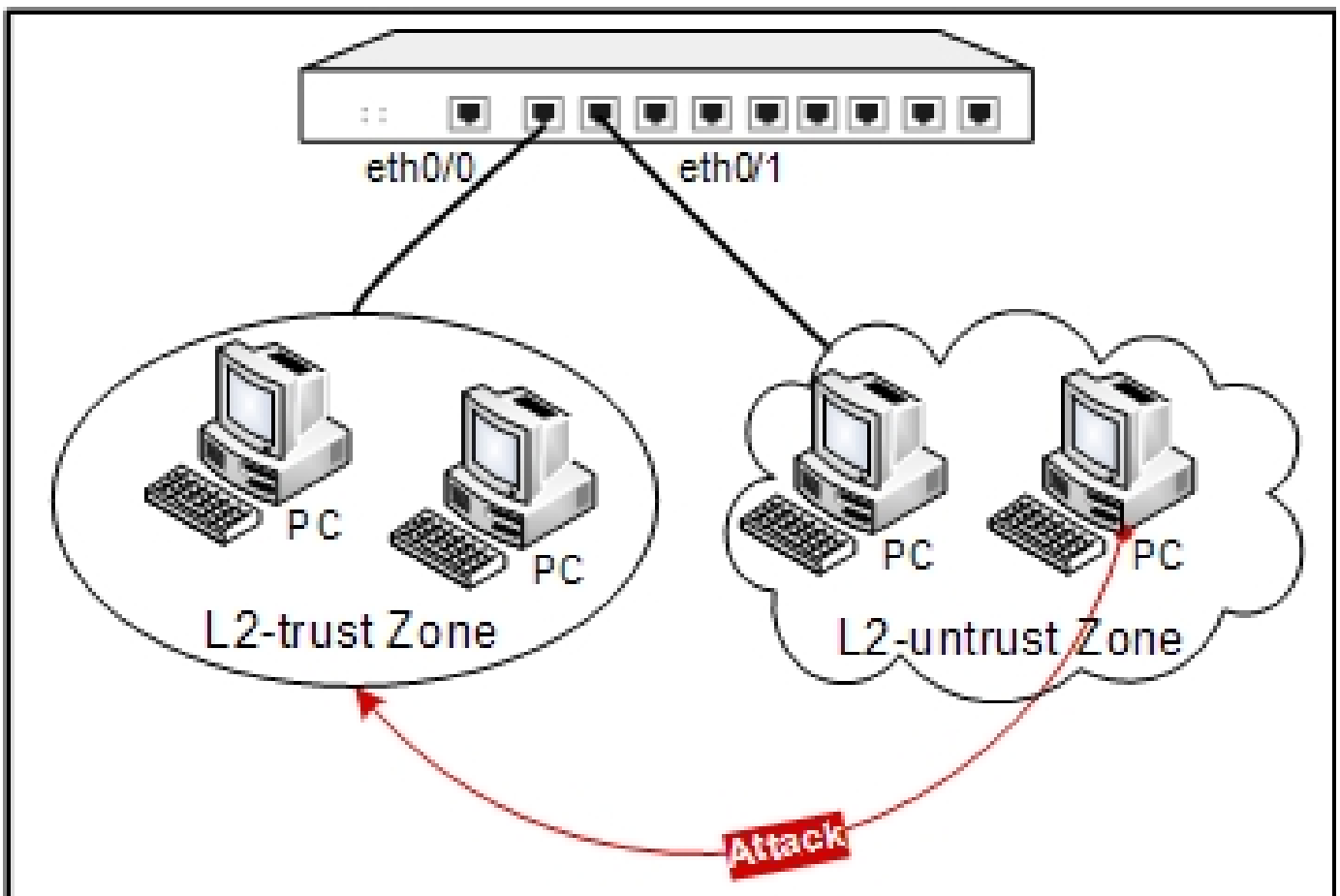
[Root](#) > [Configure](#) > [Security](#) > [Attack Defense](#) > [AD Example](#) > AD Example 2

## Layer 2 IP Address Spoof Defense Configuration Example

This section describes a Layer 2 IP address spoof defense configuration example.


Ethernet 0/0 is bound to the l2-trust zone, and ethernet 0/1 is bound to the l2-untrust zone.

The defense networking topology is shown as follows:



Take the following steps:

**Step 1:** Create an address book.

1. Select **Objects > Address Book** from the menu bar.
2. In the Address Book dialog, click **New**. In the Address Entry Configuration dialog, configure the options as below:
  - **Name:** l2-ip-spoof
  - Select **IP/netmask** from the **Member** drop-down list
  - Type **192.168.1.0** and **24** into the **IP address** and **Netmask** box respectively, and then click **Add**.
6. Click **OK** to return to the Address Book dialog.
7. Click  to close the dialog.

**Step 2:** Configure ethernet0/0 and ethernet0/1.

1. On the Navigation pane, click **Configure > Network > Network** to visit the Network page.
2. Select **ethernet0/0** from the interface list, and click **Edit**. In the Interface Configuration dialog, configure

the options as below:

- **Name:** ethernet0/0
- **Binding zone:** Layer 2 zone
- **Zone:** Select **I2-trust** from the drop-down list.

3. Click **OK** to save the changes and return to the main page.

4. Select **ethernet0/1** from the interface list, and click **Edit**. In the Interface Configuration dialog, configure the options as follows:

- **Name:** ethernet0/1
- **Binding zone:** Layer 2 zone
- **Zone:** Select **I2-untrust** from the drop-down list.

5. Click **OK** to save the changes and return to the main page.

### **Step 3:** Configure a policy rule.

1. On the Navigation pane, click **Configure > Security > Policy** to visit the Policy page.

2. Click **New**. On the **Basic** tab in the Policy Configuration dialog, configure the options as below:

- **Src zone:** l2-untrust
- **Dst zone:** l2-trust
- **Src address:** Any
- **Dst address:** Any
- **Service:** Any
- **Action:** Permit

3. Click **OK** to save the settings and return to the main page.

**Step 4:** Enable Layer 2 IP address spoof defense for the l2-untrust zone.

1. On the Navigation pane, click **Configure > Security > Attack Defense** to visit the Attack Defense page.
2. Select **l2-untrust** from the **Zone** drop-down list.
3. In the Scan/spoof defense section, select the **IP address spoof** check box to enable IP address spoof defense.
4. Click **OK** to save the changes.

**Step 5:** Craft an IP or ARP packet on a PC in the l2-untrust zone, set the source IP address to 192.168.1.100, and send it to ethernet0/1. The device will detect an IP address

spoof or ARP attack, and then give an alarm and drop the packet.