Diagnostics:

1. Connect the laptop to the Mako’s LAN 2 port, open a web browser and type in the default gateway of LAN 2.
2. The default gateway can be obtained through checking the ISP router’s settings or performing `ipconfig` commands (`ifconfig` for Mac, or similar for different platforms).
3. In order to use the CMS Diagnostic tools, you must have a Mako appliance selected.
4. From the CMS, the Diagnostics toolset is found under: Reports > Diagnostics
5. A recommended procedure for diagnosing connection problems is:
   a. Check the CMS Home page ‘Network Status’ widget for the Mako’s status.
   b. Check MakoScope for the Mako’s connectivity status to the network.
   c. Check ‘Current Connections’ for service statuses.
   d. Check ‘VPN Setup’ for tunnel statuses and logs.
   e. Check ‘ARP Table Listing’ for IP-to-MAC mapping.

Read this guide fully for details.
Mako Status

The first and simplest diagnostic the Mako System Central Management System (CMS) offers is the Network Status Widget.

Once we have logged into the CMS, and selected a site to troubleshoot, we are presented with the Home screen, which includes the ‘Network Status’ widget. This widget provides a quick snapshot of the current state of the Mako device, and shows us whether this is online and what state each interface is in.

We can see this particular device is currently ‘Online’ in our CMS, and it has seven active interfaces/networks attached to it:

**LAN 1 - 4**

These are the local networks used for POS, local office networks, Wi-Fi system on-site.

**Ethernet**

This is the primary cable connection to the Internet used by the Mako.

**xDSL**

This connection covers most forms of Internet connection over a telephone line, whether is ADSL, VDSL or fiber optic.

**3G**

This is the cellular network on the device, and may read 4G/LTE, depending on the cellular technology involved. This is used as a backup internet connection, in the event there is an outage with the primary broadband connection then the Mako device will begin to operate on this cellular connection.
In the event that one of these interfaces/networks were to go down, we would see this on the status widget as a disconnected symbol would appear, rather than the blue tick.

This network status display shows a normally-functioning, non-Wi-Fi Mako, where two LANs are connected and operating, two are unused, that it’s connected to the Internet via Ethernet, and that there is no SIM card present in the device.

The above Network Status shows a ‘perfect storm’: it indicates this two-LAN, Wi-Fi-enabled Mako is completely offline with no SIM card inserted.
The Diagnostics Toolset

Reports > Diagnostics

The Diagnostics page contains 31 tools at your disposal. This document outlines the top four commonly used ones.

 관한 Connections

Current Connections shows all of the current inbound and outbound connections being processed by the Mako.

<table>
<thead>
<tr>
<th>Connection Types</th>
<th>Current Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>19101 (1)</td>
<td></td>
</tr>
<tr>
<td>19303 (1)</td>
<td></td>
</tr>
<tr>
<td>IPSec NAT Traversal (UDP-4500) (2)</td>
<td></td>
</tr>
<tr>
<td>Web Traffic (6)</td>
<td></td>
</tr>
<tr>
<td>TCP-8000 (1)</td>
<td></td>
</tr>
<tr>
<td>TCP-8083 (1)</td>
<td></td>
</tr>
<tr>
<td>TCP-9000 (1)</td>
<td></td>
</tr>
</tbody>
</table>

View all items (1)

Note: Some lines did not match the correct format and were excluded. Click on the Advanced link to see all the lines.

Place the mouse over the name of a service for a more technical description.

<table>
<thead>
<tr>
<th>Service</th>
<th>State</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Traffic</td>
<td>Closing</td>
<td>192.168.0.121</td>
<td>202.37.170.30</td>
<td>Outbound</td>
</tr>
<tr>
<td>IPSec NAT Traversal (UDP-4500)</td>
<td></td>
<td>192.168.0.121</td>
<td>157.130.213.30</td>
<td>Outbound</td>
</tr>
<tr>
<td>TCP-19101</td>
<td>Active</td>
<td>Allocated by System</td>
<td>10.0.21.10</td>
<td>Outbound</td>
</tr>
<tr>
<td>Web Traffic</td>
<td>Active</td>
<td>192.168.0.121</td>
<td>202.37.170.30</td>
<td>Outbound</td>
</tr>
<tr>
<td>IPSec NAT Traversal (UDP-4500)</td>
<td></td>
<td>192.168.0.121</td>
<td>157.130.151.106</td>
<td>Outbound</td>
</tr>
<tr>
<td>TCP-19303</td>
<td>Active</td>
<td>Allocated by System</td>
<td>10.0.21.10</td>
<td>Outbound</td>
</tr>
<tr>
<td>TCP-35353</td>
<td>Active</td>
<td>209.116.176.177</td>
<td>184.225.20.19</td>
<td>Outbound</td>
</tr>
<tr>
<td>TCP-8083</td>
<td>Closing</td>
<td>Allocated by System</td>
<td>10.0.47.10</td>
<td>Outbound</td>
</tr>
<tr>
<td>Web Traffic</td>
<td>Closing</td>
<td>192.168.0.121</td>
<td>202.37.170.30</td>
<td>Outbound</td>
</tr>
<tr>
<td>TCP-90000</td>
<td>Closing</td>
<td>192.168.0.121</td>
<td>209.116.176.169</td>
<td>Outbound</td>
</tr>
<tr>
<td>TCP-9000</td>
<td>Closing</td>
<td>192.168.0.121</td>
<td>209.116.176.169</td>
<td>Outbound</td>
</tr>
<tr>
<td>Web Traffic</td>
<td>Closing</td>
<td>192.168.0.121</td>
<td>213.129.74.200</td>
<td>Outbound</td>
</tr>
</tbody>
</table>

Underlined in Red are the active POS connections, currently being processed by the Mako device. This tells us that the POS is connected, and is processing traffic to a network via IP address 10.0.21.10.

Underlined in Blue is are the active VPN or IPSec connections on the Mako device, which tells us that the Mako is currently connected to a network via its IPSec VPN connection.
If you can see this VPN traffic, The Mako’s connection is working.
If you cannot see the POS traffic, either:
- The POS system is not processing its traffic, or;
- The POS system is not connecting through the Mako correctly.
The latter indicates an issue with the local POS systems (the registers or the local switch they are connected to) and would need to be checked accordingly.

🔗 MakoScope

MakoScope is the Mako System’s most-used diagnostic tool. By browsing to the IP address of your Mako, you can get real time information on its status.
From your internal network, type the IP address of your Mako ( e.g. http://192.168.1.254 ) into a browser.

Connectivity information

The text for the connectivity information is colour coded, **green for active (on)** and **red for disabled/disconnected (off)**. This applies to the DSL, PPP and LAN information.

**PPP Status**
If it is red then this could be an indication that:
- Your username and password are not being accepted by your ISP;
- The Mako is still booting;
- PPP can not yet authenticate because the DSL WAN is not up.

**LAN Status**
eth1 is the status of LAN 1 and eth2 is that status of LAN 2, etc. This displays red when no Ethernet connection is detected and green when the Ethernet port is successfully connected to a switch/hub or a PC. It also displays the status of the DHCP server and the port speed in Mb/s.
### Mako_ID

This is a unique identifier used to differentiate between each Mako. In the example above, the MakoID is more formally entered as 30:1A:28:00:EF:6E. While this number is taken from the MAC address of current Makos, it’s important to understand that a MakoID is NOT a MAC Address.

### Software_ID

This is the version of firmware that is currently installed and running on the Mako. The Software ID is broken down by date [yyyymmdd] - F[irmware version]version number ([Internal Bamboo build version], [Internal version build])

### Failover Status

The current failover status on the Mako, including whether the Mako is using its primary connection (eth0) or secondary 3G (ppp1) connection. In the example above, the Secondary WAN or 3G (ppp1) is being used by the Mako, so it’s in cellular failover. An appliance not in failover is usually operating over eth0.

### Last Mako Server Contacted

The most recent time the Mako made contact with the CMS. Currently the time stamp for this should be within 2 minutes of interrogating MakoScope (because Makos poll the CMS every 2mins for reports/configuration etc.). If it has exceeded 2 minutes this would indicate the Mako is having issues communicating with our servers, due to an interrupted Internet connection or no power to the Mako.

### Last User Change

The last configuration change made on the Mako through the CMS. In the example above an IPSec modification was made, indicating a VPN tunnel was created, modified or deleted. Other common changes include Guardian, User Info updates or Firewall changes.
Firewall status
Shows whether the firewall is Active or Disabled on the Mako.

Mako Guardian Status
Shows whether Mako Guardian (Mako’s WAC filter) is Active or Inactive.

Temperature
The current CPU temperature of the Mako. In the example above the temperature is 40.1°C (40.1 Degrees Celsius). Normal operating temperatures for the Makos are anywhere from 40°C to 55°C. If an appliance exceeds 60°C, this could indicate an issue with the Mako, its internal fans or an exceptionally hot environment.

<table>
<thead>
<tr>
<th>PPP</th>
<th>User '&quot;', Address 184.225.56.145/32</th>
</tr>
</thead>
<tbody>
<tr>
<td>CELLULAR</td>
<td>-- Using EV-DO Rev A signal 77% (-65dBm)</td>
</tr>
</tbody>
</table>

Active WAN interface (PPP)
If it is red then this could be an indication that:

- Your username and password are not being accepted by your ISP;
- The Mako is still booting;
- The DSL link is not up. The WAN’s cable may be disconnected or faulty, or there’s an issue with the router/modem the Mako sits behind.

For DSL connections Receive and send are the maximum ADSL speeds in Kbps.
In the example above, the first line shows us the Active WAN is operating over a PPP connection. This appliance has failed over: the user/password is unreportable. The current IP address/subnet of the primary connection allocated by a cellular provider is 184.225.56.145/32.

-- Double-hyphens indicate continuing info from the line above, so the CELLULAR line shows that PPP is being used over a cellular WAN. The green text indicates a successful cellular connection. This Mako is receiving good signal strength.

Bridge (not pictured)
This will only be visible when the Mako is in PPPoE mode and indicates the VPI VCI virtual circuit ID.
INTERNET

These two lines indicate the status of the Makos primary WAN interface (connected via WAN port on the Mako). It shows the Mako has received an IP Address of 192.168.137.2/24 from the upstream modem/router that the Mako receives its WAN connection from. The second line gives us the current speed of this connection, which is currently connected at 100Mb/s. If this was red it would indicate the WAN cable or has been unplugged from the Mako.

LAN interfaces (2-n)

This section shows us the two or more LAN connections for the selected appliance, and their current states. In this example above you can see that LAN 1 is operating.

In a PCI configuration LAN 1 typically connects to a switch/hub which has all of the Point Of Sale (POS) devices connected to it. The first line gives the interface name (LAN 1) and also the IP address being used. The LAN1 IP Address/subnet has been set to 192.168.1.254/24. This would mean all devices connected to LAN 1 would be using an IP address such as 192.168.1.x, where ‘x’ is a unique value on each device.

The second line for LAN 1 shows us the Mako property used to identify the interface, in this case it is eth1 (this is only used by Mako Support and Development teams). We can also see the speed of this connection, in this example it is currently connected at 100Mb/s.

LAN 2 is disabled, but is set to use 192.168.21.254/24. The second line shows us the state of the connection and its connection speed, as it is disconnected this will show 10Mb/s by default. If it was connected this would increase to 100Mb/s on a normal connection.

Information logs

The rest of MakoScope shows additional informational logs and messages related to the Mako. These are always changing and will show different information depending on its state or activity. These are typically used by Mako Support and Development teams to troubleshoot any issues being experienced on the appliance.
VPN Connection Overview

Mako appliances operate with devices outside of its protected network by creating Virtual Private Network (VPN) connections, usually to allow the passage of POS and payment data.

Many VPN networks operate using the IPSec protocol, one of the most common and secure methods of configuring a remote network connection, and each Mako has a VPN would be configured to transfer all payment and POS data/traffic in a secure method to the destination network.

Other VPN networks operate using Mako’s VPN Cloud technology. VPN Cloud allows the use of certificate-based authentication for secure transactions, creating faster, more flexible network design options with better network performance metrics.

First Aid: IPSec VPNS

The first diagnostic we perform on a site that is having issues with the POS systems is to check the current VPN connection state to ensure this is connected successfully.

In the CMS:

Reports > Diagnostics > VPN Setup

This will then display all of the current VPNs configured on the Mako device.
VPN connection logs

Below is a screenshot of a site's VPN logs, showing that it has successfully connected to a network. The important log here is the ‘IPSec SA established tunnel mode’, usually found as the last line in these VPN logs.

This state confirms the VPN is online and successfully connected.
VPN Cloud Connections

This diagnostic lists the end points connected to the VPN Cloud. No difference is made between a headpoint (a Mako serving as a concentrator for a VPN Cloud) and an endpoint (a Mako connected to a cloud, but not acting as a concentrator for it). This diagnostic’s main use is to identify which VPN clouds the selected Mako connects to and it’s status.

Note

VPN Cloud Routing Table tells you the LAN, weight and status of the VPN tunnels, and might be handy if you’re already looking at the Diagnostic toolset. But you generally get better, more detailed information on a VPN Cloud’s setup from:

Management > Company > [Company name] > VPN Cloud
**ARP Table Listing**

The Address Resolution Protocol (ARP) is a protocol that turns IP Addresses into physical Ethernet (or MAC) addresses.

![Mako Current arp table](image)

Diagnostically, there are a couple of uses for this tool:

- **Checking for physical connection from a device, such as a server, to the Mako.** A common network check is a Ping to a server, for example, but if Ping traffic has been disabled a Ping is inconclusive. If connected, the ARP Table Listing will display the server’s IP and MAC address (unless a name for the device has been assigned through a DHCP Lease). If the server is powered off or disconnected, there will be no ARP listing for it.

- **Matching IP traffic with MAC addresses.** If you only have either the IP address or the MAC address, this table reveals the other half.

- The Create Lease button is a shortcut to:

  Configure > Network > **DHCP Leases**