## Description

APIPA monitor is a watchdog service that monitors network interfaces and resets them if they have an APIPA address or if they are unable to ping the default gateway. It was written to handle a problem we were having with VMs in our virtual environment occasionally losing their IP and falling back to an automatic private IP address (APIPA or the 169.254.x.x range).

## Operation

The service wakes up on a user specified interval (default every 10 seconds), and tests IPV4 enabled interfaces for 169.254 addressing. If an APIPA address is present, the service disables and then re-enables the NIC which clears the problem. For NICS that should have APIPA addresses, including the word “APIPA” anywhere in the NIC interface NAME (right-click, rename network adapter), will prevent APIPA Monitor from processing that interface. The loopback interface and any interface with “Microsoft Failover Cluster Virtual Adapter” in the DESCRIPTION are also skipped. Microsoft’s clustering uses APIPA addressing on the cluster virtual adapter, so not a good idea to reset that every 10 seconds.

A configurable option that is on by default, but may be turned off is APIPA monitor also pings the default gateway every “x” seconds (default 30). The test tries up to 3 times on 2 second intervals to ping the default gateway. The first of the three to succeed results in successful result and terminates the test. If all three pings fail, the gateway test fails. Also configurable, but by default set to 1, is the number of gateway failures that must occur before triggering a NIC reset due to being unable to ping the gateway.

## Optional arguments

**-i nbrSeconds**: Poll interval - how often the service activates. Tests for APIPA on every activation and resets adapter if APIPA address is active. Optional gateway ping test at specified intervals. Default 10 seconds if not specified. Do not set this to less than 10 seconds.

**-g nbrSeconds**: Gateway test interval - how often to run ping tests against the default gateway. Test is a series of 3 pings at 2 sec intervals. If all fail, the test fails. The default is every 30 seconds. SETTING TO ZERO disables gateway ping tests. Note: gateway tests happen when the service activates (polling interval), so the test happens on the first poll activation after the gateway test interval is reached.

**-f nbrFails**: Number of gateway ping tests that are allowed to fail before the adapter is reset due no response from gateway. Default is 1, reset on 1st failure.

**-h nbrSeconds**: Number of seconds to hold-off between adapter resets. This is to prevent back to back resets. Default is 25 secs.

**Example configuration using sc.exe** (mandatory space between binpath= and first quote)

sc config binpath= "\”c:\bin\APIPA Monitor.exe\” -i 10 -g 25 -f 2 -h 45"

You may also test parameter settings by entering arguments on the General tab of the Services window, but those are one time settings and will not persist to the next startup session.

## Install / Uninstall

To install:

* Copy “APIPA Monitor.exe” to the folder where you want it to reside
* Run the EXE with a “-install” switch. You can optionally follow the “-install” switch with desired settings. Example – to install with an APIPA address check every 15 seconds, a gateway failure test every 45 seconds with 2 gateway failures required before an adapter reset, and a reset holdoff value of 90 seconds, use:
  + “APIPA Monitor.exe” -install -i 15 -g 45 -h 90 -f 2

To install with default parameters:

* + “APIPA Monitor.exe” -install
* This installs the service to run as the local system account, with a start type of Automatic (Delayed) and the starts the service.
* Event viewer tracks actions – look for a source of “apipamon” for events.

To uninstall:

* “APIPA Monitor.exe” -uninstall

Reconfigure:

* Use sc.exe as described earlier to change parameters without uninstalling / re-installing, or just uninstall and re-install with new arguments if you prefer.