How ICMP Network Discovery Works

https://campus.barracuda.com/doc/98217214/

ICMP sweep intervals (Device Availability) are based on the Network Discovery interval, which you can find by navigating to:

Configuration > **Site Management** > **Site Name** > **Network Discovery**

Here you will find the following discovery settings:

ICMP Sweep Interval

The ICMP sweep interval, is that which the Onsite Manager will do a ping sweep across the IP ranges configured in the scan settings. By default, this is set to 5 minutes. This does not mean that our software starts a scan every 5 minutes, but rather that it will wait 5 minutes between scans.

For a large network where a scan may take several minutes to complete, the scans themselves may actually be several minutes apart. In extreme cases like this, it may be recommended to scan only the required IP addresses or ranges rather than entire subnets when it can be avoided. Scanning over slower connections such as VPN's or MPLS links can also cause longer scan times due to bandwidth limitations. Avast recommends using separate OMs for separate physical locations.

TCP Probe

If ping/probe requests time out on a device, it will be logged against the device availability monitor (if one is applied to the device in question), each time a scan occurs. Due to the non-guaranteed delivery of the ICMP protocol used for the pings, up to three more pings are attempted at 2.5, 5. and 7.5 second timeout intervals.

Starting from Barracuda RMM v10 SP2, when all pings time out on a previously available device, a TCP probe is attempted at carefully selected ports whereby any response, including rejection (RST packet), is counted as the device being available on the network. This TCP probe, therefore, helps to prevent false device down alerts. Additionally, TCP probing that is specific for printers with so-called 'deep sleep' mode, can be implemented and enabled if particular printer models are being monitored, such as OKI MC561.

If no response is received from any of these mechanisms, then the Device Availability monitor triggers

an alert, if one is applied. Based on these parameters, having an Alert triggered for a Device Offline after 2 minutes may not be feasible as it is likely less time than the combined Scan Interval + time taken for the scan. TCP probing can be disabled through configuration settings

The time that the device went down between network scans will factor into the time between scans. For example, if a device went down immediately after a scan completed, it will be 5 minutes until the next scan. The next scan may take 1-2 minutes (high estimate) to complete, and the device has now been down for 6-7 minutes in order to trigger the device down. This is the worst case scenario.

Alerting

The alert configuration has no effect on the data points that determine the device's availability. By the time that you receive the alert, the device may have already been offline for 7-8 minutes, which will be reported in the alert. Avast software then checks the alert configuration and sends an alert if the time the device has been down is equal to or greater than the alert threshold.

Alerting at 5 minutes will usually come within 2-3 minutes of the actual time the device has been down. Note that this only applies to the availability of devices already monitored by the system, not device discovery. There is a much slower background process of pinging to detect newly discovered devices whose monitoring would then begin, if they satisfy the auto-inclusion rules.

Scan Time

Avast software does not complete real-time scanning however, you can lower the Device Discovery setting as low as 1 minute in order to come close. However, by changing the setting to 1 minute, you will be flooding your network with ping requests which may pose other problems for example firewalls or network hardware such as routers or switches may detect this as an attack, such as a ping Denial of Service (DoS) attack.

Our Ping Sweep occurs at the rate of roughly one per millisecond, namely pausing for 50ms after each 50 are fired. Staring with MW v10 SP3, this delay will be made tunable, to account for more stringent DoS detection prevention systems.

You can monitor the `C:\Program Files (x86)\Level Platforms\Onsite Manager\Logs\TraceExpertSystem.txt` log for the following events if you want to determine exactly how long your network scan takes to complete, in order to fine-tune your scan interval vs. alert threshold configuration for your environment. However, keep in mind the risks of lowering the

discovery scan setting.

```
2013/11/06 11:27:19 [9] INFO LPI.Discovery.DataCollection.ScanManager -
Scanning device statuses for all devices
.........
2013/11/06 11:27:20 [9] INFO LPI.ExpertSystem.ActionManagers.ActionNwkScan -
Scanning completely done - time taken: 14 secs.
```