Device Detection and Merging

https://campus.barracuda.com/doc/98217262/

Occasionally you may notice devices listed in Barracuda RMM with only partial information (eg. only an IP address,) a device which gets re-detected even after being excluded, or you may have two devices whose records unexpectedly merge. This article explains how device detection and merging function within Barracuda RMM.

Device Discovery

Below is a simplified description of how Barracuda RMM performs device discovery:

- The Onsite Manager sends out ICMP (Ping) requests to every IP address in its scan range
- Devices that are configured to respond to ICMP requests send responses back
- The Onsite Manager attempts to verify the device's identity against its database of known devices using ARP and DNS records
    - If an IP responds to ICMP but has no ARP or DNS entry, at this point all that is known is the ICMP response
- The Onsite Manager attempts to connect to every device via its configured SNMP, SSH, and WMI credentials
    - If an IP corresponds to ICMP, has no ARP or DNS and does not respond to SNMP, SSH, or SMI, at this point all that is known is its ICMP response
    - If the IP responded to a monitoring protocol, that protocol is used to collect additional basic information so that the device can be positively identified

ICMP Information

The information acquired by pinging a device is somewhat limited, for example:

```
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

The bytes value is configurable when sending the ping, so this does not provide valuable information,

and the IP address is also known since that is where the request was sent. The new information that is gained in this fashion is the Time To Live (TTL), which is supplied by the device.

TTL is a numerical counter on a packer that is decremented every time that it completes a 'hop' from one network device to another. TTL's ensure that if a packet is misrouted into an infinite loop, it will not keep looping forever, building up load on the network. Devices on small or simple networks will typically keep the original TTL of the packet for the full trip, while a trip across a large or complex network will normally decrement a few times.

By convention, Windows devices will respond with a TTL of 128, while non-Windows devices will respond with something different, often 48, 52, or 64. This provides enough information to be able to recognize if a device is likely running a version of Windows or something else. Unfortunately, because other TTL values are often shared between different manufacturers and device types, it is not possible to effectively narrow the 'not Windows' group down further without additional information.

ARP Information

ARP data will give us the MAC address, which includes information about the manufacturer of the network card. This information allows certain devices that don't have monitoring protocols enabled to be tentatively identified. The IEEE has a standard list of registered manufacturers' MAC prefixes found here which can be used to identify the manufacturer of the device through the ARP record. Since many manufacturers are specialized in a particular type of device, this can also be used to guess the device's role as well.

Many modern devices (eg. most current versions of iOS or Android) have security features that disable ARP by default or spoof their MAC address, making them impossible to identify in this manner.

Merging Records

If the Onsite Manager (OM) detects a device that appears to be a duplicate, it will merge the records. Normally this should occur seamlessly as devices change IPs etc. however in circumstances when there is either insufficient information available (eg. only ARP and/or ICMP) or incorrect information (eg. stale forward or reverse lookup records on your DNS server) strange behaviors may occur.

The best solution for cases in which devices are duplicating or being redetected constantly is to enable a monitoring protocol on the device. If the device is WMI, SSH or SNMP enabled, the Onsite Manager should be able to retrieve sufficient information to correctly identify the device.

If that is not possible for some reason, doing anything that provides additional information will aid the OM in identifying the device. Configuring a static IP address for the device and adding DNS records for

it, or enabling ARP on the device so its MAC address and manufacturer can be detected will provide additional information in order to identify the device.

Stale DNS records can lead the OM to believe that two different devices share the same DNS name, which may cause devices to be incorrectly merged. Cleaning up the DNS records will usually rectify this situation. Barracuda RMM recommends configuring DNS scavenging to be run over the same period as the DHCP leases on a network, so if DHCP is leasing IP addresses for 7 days, DNS scavenging should run once every 7 days to keep stale records from piling up.

In some circumstances, you may need to delete a merged device out of Barracuda RMM before the two devices are correctly identified as being separate.