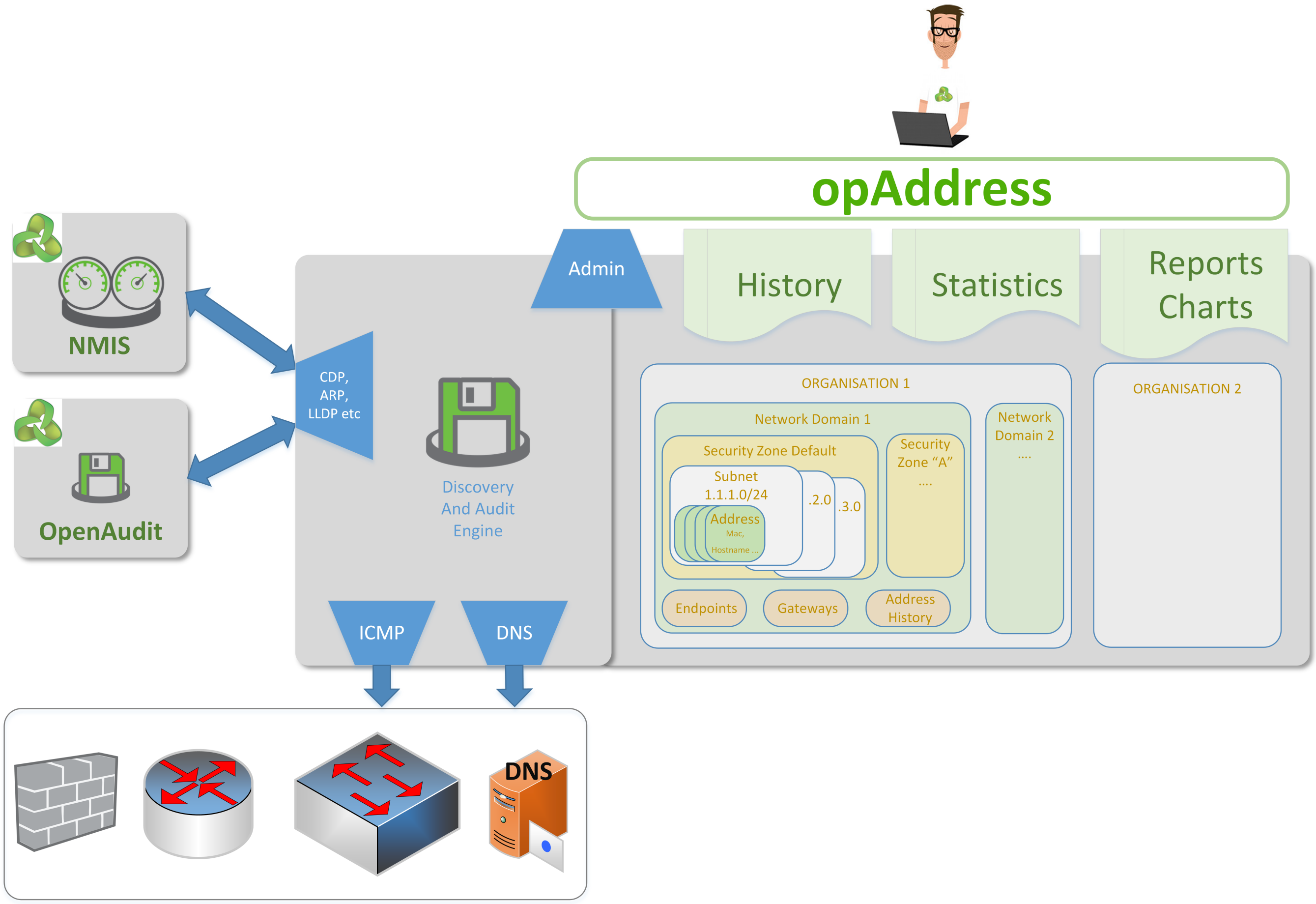
How opAddress discovers information



Summary of opAddress information collection

opAddress is designed to collect and build your IP address management information dynamically with little manual input required. It does this by importing information about your network and networked devices from NMIS and/or Open-Audit Enterprise on a daily basis. It makes use of the interface information from these devices (IP address, mask etc) to build a list of known subnets and known IP addresses and known hosts, gateways etc.

The administrator or users can also manually add subnets or edit discovered subnets to complete the picture.

The complete list of subnets allows opAddress to scan your networks every thirty minutes. A list of all possible IP addresses is created from the subnet information and once added to the address table these addresses are then pinged (ICMP) to see what IPs are in use/live, this scan/ping also enables opAddress to retrieve "fresh" MAC address information from your router's ARP tables via NMIS and SNMP. The MAC address from the ARP tables and NMIS interface information creates a table of Endpoints and these endpoints are dynamically associated with the known addresses. We now have a dynamic picture of the addresses, which are/not currently in use (reachbale or unreachable) and we know which endpoint (MAC / host) is using them and we also have a history of addresses used by each endpoint (if the endpoint changes address e.g. a laptop moving between office LANs or to and from WiFi areas).

The final part of the network scan action is to do a DNS lookup for any live IP addresses found. We do a PTR (reverse) Record lookup to find a DNS name from an IP address. Obviously for this to work your DNS services needs to have PTR records recorded. This uses the servers native DNS services to complete this action so DNS needs to be configure on your OS and it needs to be able to access suitable DNS services in your organisation. If you have windows servers providing DHCP services in your organisation then they should provide dynamic PTR records for DHCP leases which is very useful, so make sure your server can access these DNS resources.

Daily Information Imported from OAE and NMIS

- Interface listing for each host
  - IP address
  - Subnet Mask
  - interface details such as type and speed

    - Subnet information which is inferred from the above - when/if the subnet is scanned this also generates an IP address for every possible IP in the subnet
    - Device name
    - Location information
    - Gateways - if the device has two or more interfaces and has location information it is added as a gateway for it's subnets.
    - **NOTES**
        - The time and frequency of the import is controlled through cron (/etc/cron.d/opaddress) the default being at 01:11 and 01:21.
        - OpenAudit must be Enterprise edition as we make use of the API feature for import
        - Gateways are only added if they have a location
        - NMIS import is only known to work with localhost not remote hosts (it may operate for opHA enabled servers but not currently tested ver1.0.5
    - **NOTES for opAddress 2.0.0**
        - Open-AudIT **must** have a query with the name opAddress in order for opAddress to import Open-AudIT information. This query will be built in to Open-AudIT as at the next release after May 2021. If you do not have this query, but do have opAddress 2.0.0 and want to import Open-AudIT data, please see opAddress 2.0 -> Open-AudIT 4.x Query for importing.

30 minute interval subnet_scan process

- Every IP address in every known subnet is pinged
    - This is done in batches of 50 addresses to limit impact
    - The kick of the batch process is what creates "Addresses" in the address table if they do not already exist.
    - At the end of each scan batch the ARP tables of the gateways for that subnet are queried for MAC addresses and these MACs are created as endpoints
- If a live IP is found
    - The address "Operational Status" is changed to "reachable"
    - The address "Administrative Status" is changed - what it changes to is configurable in opCommon.nmis / 'opaddress_default_address_state'. I recommend changing this to "allocated" from the default undef/"unkonwn"
    - The address is associated with an endpoint / MAC address found from the ARP entry / endpoint table
- At the end of the subnet_scan the DNS lookups are completed for the live IPs to attempt to find a name.
- **NOTES**
    - The subnet will only be scanned if it's "admin status" is "allocated" or "unallocated"
        - auto added subnets default to Allocated
        - manually added subnets default to unknown or rather the dropdown when adding subnets manually defaults to unknown.
        - If you do not want an automatically added subnet to be scanned then change the admin status to something such as delegated or unmanaged.
    - An IP address will NOT be pinged if the address has had it's "administrative status" changed to "unmanaged", "delegated" or "reserved"

Manually Entered data

- You can manually add or modify all classes of information - addresses, subnets, gateways etc.
- Subnets are the primary information one would manually add (typically those not found by import from OAE and NMIS).
    - You must at this time enter the subnet in CIDR notation (x.x.x.x/y) for both the NAME field and the Subnet field.
    - You should change the subnets administrative status from "unknown" to "allocated" or "unallocated" if you would like it to be scanned; else if you do not want it scanned change it to "delegated" or "unmanaged" or leave it as "unknown"
    - The adding of a subnet will not create it's addresses in the address table, the addresses in the address table are only added once this subnet is scanned, or if the addresses are added manually.
- You can manually add gateways, with a list of the subnets they cover
- You can add IP address information manually
- You can Bulk edit address information
    - A good example is to denote DHCP ranges, one would bulk edit the address range and change the "type" from "static" to "dynamic" to denote DHCP.