

Enigma NMS

Distributed Polling Architecture

Enigma NMS has been developed by Queensland based company NETSAS Pty Ltd, ABN# 63 075 696 249, GITC V5.02 accredited, # Q-3900 with the first deployment in Brisbane, Australia in 2006.

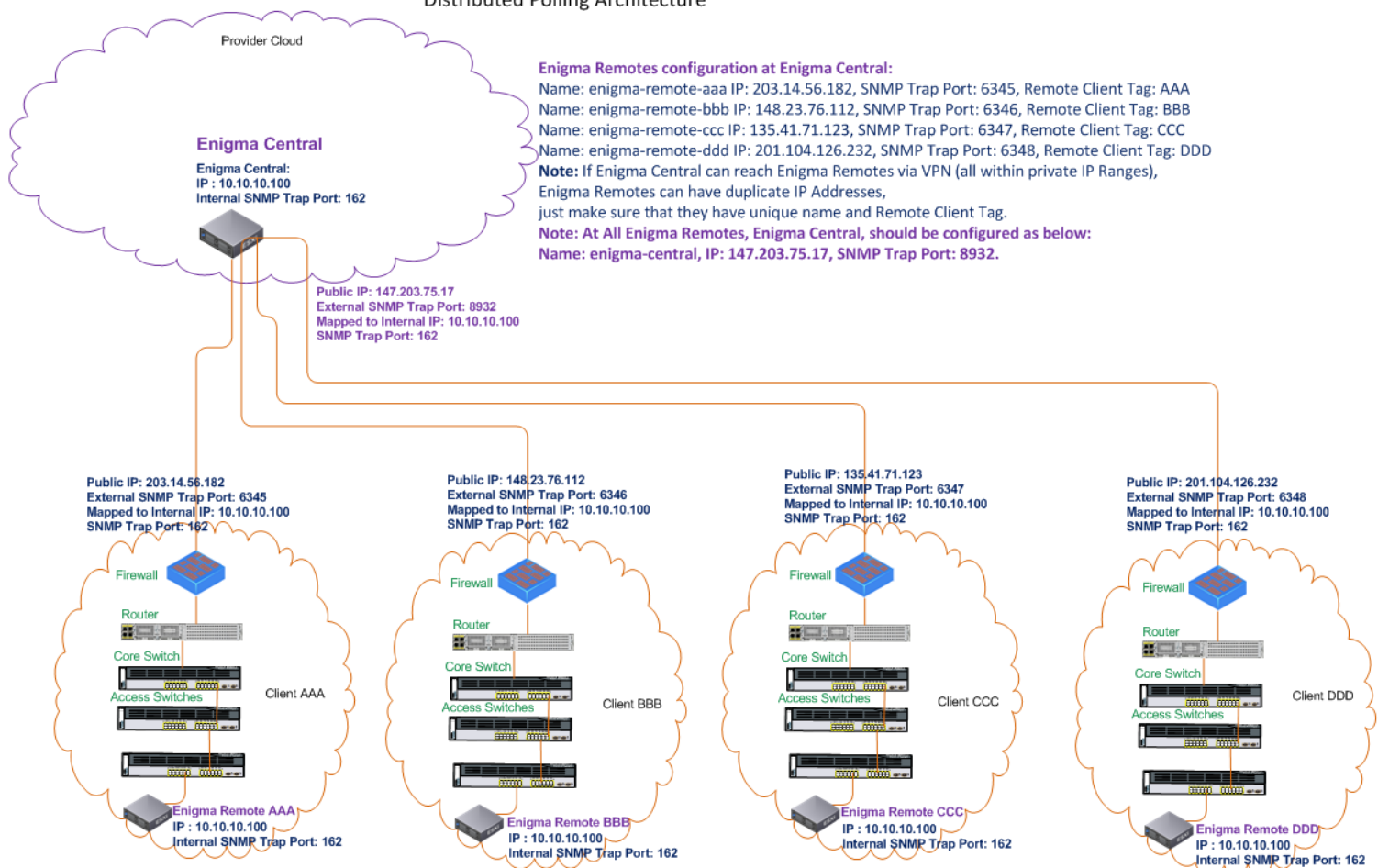
The distributed polling architecture was developed to respond to our clients 'feedback about certain limitations imposed by overlapping private IP Addresses, which may exist in various parts of Enterprise Networking Environments, which belong to the same or different organizations.

Another purpose of creating distributed polling architecture was creating a single pane of glass at the services provider Network Operations Centre (NOC), which would contain network objects from many external clients.

It was suggested that the architectural model would consist of an Enigma Central and Enigma Remote instances of Enigma NMS.

Please see below the conceptual diagram explaining the Distributed Polling Architecture:

Distributed Polling Architecture



A many to many relationship between the Enigma Central and Enigma Remotes exists, where Enigma Central supports multiple Enigma Remotes, and Enigma Remote instances can also have multiple Enigma Centrals to communicate with.

Enigma NMS can function in the following modes:

- **Stand-Alone Mode** –is used as a single instance running on-premises within a customer’s environment, where it undertakes the polling, reporting and dashboard management.
- **Dedicated Central Mode**—Enigma will only receive informational feeds from multiple Enigma Remotes without actively polling any of the local devices.
- **Hybrid mode**—provides the ability to poll locally reachable network nodes and take informational feeds from multiple Enigma Remotes.
- **Remote Mode**—provides the ability to poll locally reachable devices and send this information to the configured Enigma Centrals

The following global System Setting will determine the mode which Enigma NMS will operate:

“System Distributed Mode”, which will have the following values:

- Stand Alone
- Remote
- Central

Please note that global System Setting can be modified by “**admin**” user only.

If Enigma NMS is configured for either Central or Remote mode the relevant prompt will appear in the system Main Page, as per below:

ENIGMA NMS ENIGMA CENTRAL

Version: 79.5.0 System Admin LOGOUT, Mon May 24 14:01:38 2021

This Enigma Server is in: Central Distributed Mode

1 New Node Outages Found!

MY FAVOURITES CUSTOM REPORTS ALARMS TOP STATS NODES INTERFACES CONFIGS TELCO TOOLS CLIENTS FOR MANAGERS SYSTEM

Alarms and Alerts

Performance Dashboard

Node Reports

Interface Reports

Tools you need

Multi Tenant Multi User

Managers Tools

System Configuration

The prompt consists of two hyperlinks, which are underlined in red above.

The central link will take you to the relevant System Setting, and the Distributed mode will take you to the “Distributed Polling Configuration” screen, as per the examples below:

Enigma Central:

ENIGMA NMS ENIGMA CENTRAL

System Admin LOGOUT Mon May 24 14:05:03 2021

MY FAVOURITES CUSTOM REPORTS ALARMS TOP STATS NODES INTERFACES CONFIGS TELCO TOOLS CLIENTS FOR MANAGERS SYSTEM

Viewing the Distributed Mode

This Enigma Server is in: Central Distributed Mode

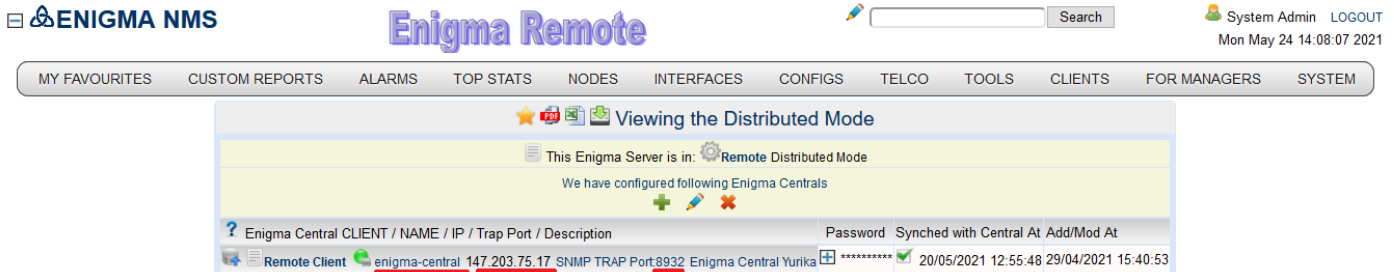
We have configured following Enigma Remotes

Enigma Remote CLIENT / NAME / IP / Description	Password	Remote Client Tag Synched At	Add/Mod At
Remote Client AAA enigma-remote-aaa 203.14.56.182 SNMP TRAP Port:6345 Enigma Remote AAA, IP: 203.14.56.182	*****	AAA N/A	24/05/2021 11:47:27
Remote Client BBB enigma-remote-bbb 148.23.76.112 SNMP TRAP Port:6346 Enigma Remote BBB, IP: 148.23.76.112	*****	BBB N/A	24/05/2021 11:47:13
Remote Client CCC enigma-remote-ccc 135.41.71.123 SNMP TRAP Port:6347 Enigma Remote CCC, IP: 135.41.71.123	*****	CCC N/A	24/05/2021 11:47:53
Remote Client DDD enigma-remote-ddd 201.104.126.232 SNMP TRAP Port:6348 Enigma Remote DDD, IP: 201.104.126.232	*****	DDD N/A	24/05/2021 11:48:15

Please note in above picture, the custom SNMP Trap Ports which are mapped at particular client Firewall to the actual Enigma Remote IP Address and default SNMP Trap Port 162.

In our example we are going to use the same IP Address: 10.10.10.100 for all Enigma Remotes actual IP Addresses.

Enigma Remote:



Enigma Central CLIENT / NAME / IP / Trap Port / Description	Password	Synced with Central At	Add/Mod At
Remote Client enigma-central 147.203.75.17 SNMP TRAP Port:8932 Enigma Central Yurika	*****	20/05/2021 12:55:48	29/04/2021 15:40:53

There are several mandatory requirements for the Distributed Polling Architecture to function correctly; these requirements include:

There are number of mandatory requirements for Distributed Polling Architecture to function properly.

1. The Enigma Central Database must contain node records for all Enigma Remotes.
2. The Enigma Remote Database must contain node records for all Enigma Centrals.
3. The node names for all Enigma Centrals and Enigma Remotes should be identical. If for example on Enigma Central the Enigma Remote node name is "**enigma-remote-aaa**", then on the actual Enigma Remote the server itself should have the same identical name as "**enigma-remote-aaa**", the same applies for the reverse relationship.
4. The relevant passwords configured on Enigma Centrals and Enigma Remotes should also be identical.
5. The Enigma Central configuration contains the field called "**Remote Client Tag**". It has to be unique for all configured Enigma Remotes. Ideally, you may want create relevant client record at Enigma Central and link Enigma Remote to this client. The purpose of this tag is to create unique records for the following imported objects:

- * **clients**
- * **sites**
- * **users**
- * **nodes**

these tags will be appended to the names of relevant objects. Different clients can have sites with identical names, e.g. "Data Centre", code "DC" or "Head Office", code "HO". When these objects are ingested by Enigma Central from two different Enigma Remotes, for the Enigma Remote with Remote Client Tag "**AAA**", they will become "**AAA Data Centre**", code "**AAA_DC**". For the site with the same name, coming from the second Enigma Remote with client tag as "**BBB**", the site "Data Centre", code "DC" will become "**BBB Data Centre**", Code "**BBB_DC**".

Following objects are imported into Enigma Central from all Enigma Remotes:

- **Clients**
- **Users**
- **Sites**
- **Device Types**
- **Model**
- **SLA**
- **Vendor**
- **Node**
- **Node Down and Up Events**

If Enigma Central is located in Provider cloud, the internal IP Address will be in private IP range: e.g. 10.10.10.100. Enigma Central will listen on the default SNMP Trap port: 162. However externally it will be represented by the Public IP Address, in our case as: 147.203.75.17 with external port 8932, being mapped to internal IP and SNMP Trap port as 10.10.10.100 / 162.


In this case the node record for Enigma Central in all Enigma Remotes should be configured as below:
Name: enigma-central, IP: 147.203.75.17, SNMP Trap Port 8932, these are the external Public IP Address of the firewall at Enigma Central WAN ingress point. At the firewall, the outside (Internet) port 8932 will be mapped to internal Enigma Central IP Address: 10.10.10.100 and SNMP Trap Port 162.

The use of Public IP Addresses along with custom SNMP Trap Ports allows bi-directional communications between Enigma Central and Enigma Remotes, in this scenario there is very little will need to be done to make things work. Once relevant configuration is complete on both Enigma Central and Enigma remote and mandatory conditions are met, i.e. identical node names and passwords, at first each pair of Enigma Central and Enigma Remote will synchronize with each other, i.e. they will become aware of each other.

Here is the order of synchronization sequence:

1. Enigma Remote sends request to synch to Enigma Central.
2. When Enigma Central gets this request, it sets the relevant timestamp in the database table.
3. In response Enigma Central sends the request to synch to Enigma Remote.
4. When Enigma Remotes gets this request, it sets the relevant timestamp in the database table.

After the synchronization is complete which takes about 5 to 10 minutes, Enigma Central will send request to Enigma Remote, which will prompt Enigma Remote to send all information about above objects in order to do the initial database population at Enigma Central.

*** Please note:** in order to initiate this request, engineer at Enigma Central needs to click on the icon , near the node name of the relevant Enigma Remote.

* **Please Note:** there could be situation when Enigma Remote clients are unable to create Port mapping on the Internet Firewall between external custom Port and Internal Enigma Remote IP Address and SNMP Trap Port 162.


Following section explains what is going to happen when our Enigma Remote is located behind the firewall without proper port mappings; hence the messages sent by Enigma Central will not be able to be received by Enigma Remote.

If communication between Enigma Central and Enigma Remote is uni-directional, i.e. where Client network infrastructure is protected from the outside world by Firewall and Firewall is under external admin control, which makes it impossible to create required port mappings, so only outbound connections are possible. There are some human intervention will be required.

Here is the order of synchronization sequence:

1. Enigma Remote sends request to synch to Enigma Central.
2. When Enigma Central gets this request, it sets the relevant timestamp in the database table.
3. In response Enigma Central sends the request to synch to Enigma Remote, but because the communication is uni-directional i.e. from Enigma Remote to Enigma Central, this request will never make it to Enigma Remote.
* **Manual action:** The engineer at Enigma Remote will need to manually synchronize with Enigma Central by clicking on the icon ☐ in the “**Synched with Central At**” column of the relevant configuration record for particular Enigma Central.
4. By now the synchronization process between Enigma Central and Enigma Remote is complete.

Due to uni-directional traffic, only from Enigma Remote to Enigma Central, manual action is required:

The engineer at Enigma Remote, when prompted by engineer at Enigma Central, will need to manually initiate sending of all data from Enigma Remote to Enigma Central by clicking on the icon  near the node name of the relevant Enigma Central. This will result in initial Database population at Enigma Central for all relevant objects.

This will need to be done only once and at a time when modification is done at Enigma Central to particular Enigma Remote, which will reset the synchronization timestamps.

When this happens manual intervention is required.

Later on, any changes to all imported objects will trigger relevant messages, which will be sent from Enigma Remote and ingested by Enigma Central.

Please note if you have multiple configured Enigma Centrals this will need to be repeated for each Enigma Central.

Here is the example of Enigma Remote Node records, configured on Enigma Central

Enigma Remote Name	IP Address	SNMP Trap Port	Client Name	Remote Client Tag
enigma-remote-aaa	203.14.56.182	6345	Remote Client AAA	AAA
enigma-remote-bbb	148.23.76.112	6346	Remote Client BBB	BBB
enigma-remote-ccc	135.41.71.123	6347	Remote Client CCC	CCC
enigma-remote-ccc	201.104.126.232	6348	Remote Client DDD	DDD

Enigma Central node record configured on All Enigma Remotes:

Enigma Central Name	IP Address	SNMP Trap Port	Client Name
enigma-remote-aaa	147.203.75.17	8932	Central Client

Note: Please make sure that they have unique names and Remote Client Tags.

Also it is recommended for each Enigma Remote to create its relevant Client Record and link it to the relevant Enigma Remote.