



Take Today's Network Monitoring Challenges
Head-On

- Constrained by "out-of-the-box" IT operations management solutions?
- Frustrated by the complexity and expense of customized solutions?



Understanding SNMPv3 Engine IDs

December 2015

Understanding SNMP Engine IDs

This is meant to be a general, informative document. If you would like to make suggestions, corrections, or update us on a change that has occurred, please do. Specifications, procedures and recommended practices change over time. It is our intention to have this document be correct and up to date.

Greg Moberg

<gmoberg@logmatrix.com>

Document History:

- 1. June 2014**
- 2. December 2015**

Understanding SNMP Engine IDs

SNMP Engine IDs...

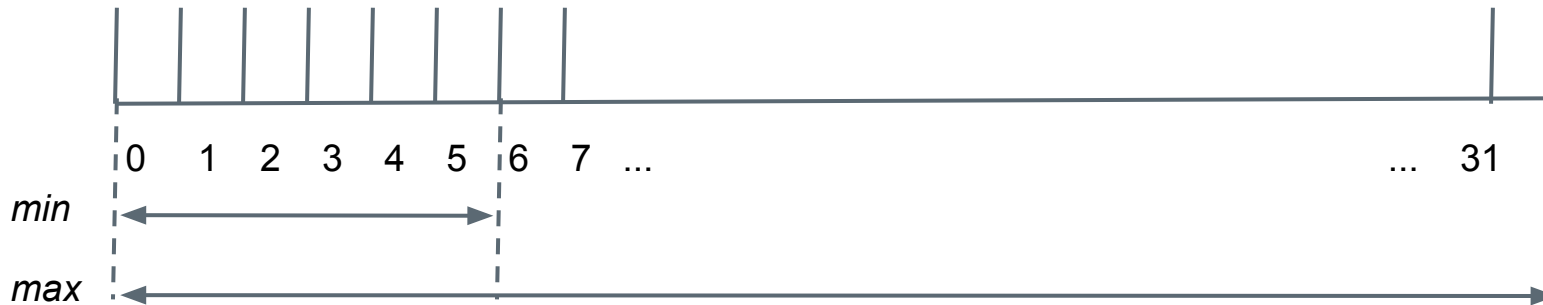
- Are assigned to SNMP Agents and SNMP Management applications that can communicate using SNMPv3.
- Need to be unique across the set of communicating SNMPv3 Agents and Managers.
 - Think of them as how you think of phone numbers. Everyone needs a unique phone number or else multiple people end up answering when a shared phone number is dialed.
- Are often created/viewed/edited on SNMPv3-capable systems via their management interface.
- Can be constructed via a set of formats defined by IETF and IANA. The formats are given in RFC 3411 and RFC 5343. These RFCs allow control of further formats to IANA; however, no additions have been made by IANA.
 - [RFC 3411 / STD 62](#) (Dec 2002)
 - [RFC 5343](#) (Sept 2008)
 - [IANA SnmpEngineID Formats](#)
- Often include Enterprise ID assignments, assigned by IANA.
 - [Enterprise Numbers](#)

Understanding SNMP Engine IDs

Points to consider about SNMP environments...

- SNMP is a *network management service & protocol* that runs on network devices (aka: network nodes). Ex: gateways, servers, workstations, load balancers, printers.
- An SNMP service may take any of several forms (command generator, command responder, and so on) but we can always refer to it as an *SNMP entity*.
- A device may have more than one SNMP entity.
Thus... trying to access an SNMP entity on a device by knowing only the hosting device's information may fall short on being able reach the intended service.
- A device may have more than one IP address, have access to more than one network, and might have addressing onto networks that are not based on IPv4 or IPv6.
Thus... being able to differentiate SNMP entities based only their network address may fall short.
- Each SNMP entity contains one (and only one) *SNMP engine*. This engine is used for sending & receiving messages and controlling access to managed objects.
- Providing each SNMP engine with a 'SNMP Engine ID' allows for a way to uniquely identify the engines apart from each other and therefore the SNMP entities apart from each other (because of the one-to-one relationship of engines to entities).
- Managing the Engine ID assignments of a domain's SNMP Entities is akin to managing a domain's IP addressing and hostname assignments.

The format of SNMP Engine IDs



SNMP Engine IDs are composed of a series of octets (bytes).

They must be at least 5 octets in length and may not be more than 32 octets long.

Each octet can contain a value from 0 up to 255. Hexadecimal: '00'H up to 'FF'H.

There is no standard display format for a SNMP Engine ID.

The raw set of octets is often given. For example: '80000009010A0101C1'H

Delimited versions are far more readable. Example: 80:00:00:09:01:0a:01:01:c1

The format of SNMP Engine IDs



<> For the purposes of providing SNMP Engine ID discovery, the special value

00:00:00:00:06

can be used within SNMPv3 communication but must not be the value assigned to any SNMPv3 system. (RFC5343)

<> An SNMP Engine ID must not be set to all 0s. (RFC3411)

Not valid: 00:00:00:00:00:00:00:00...:00

<> An SNMP Engine ID must not be set to all 255s (hex: 0xff) (RFC3411)

Not valid: ff:ff:ff:ff:ff:ff:ff:ff...:ff

The format of SNMP Engine IDs

<> Method #1: Static size format. (RFC 3411)

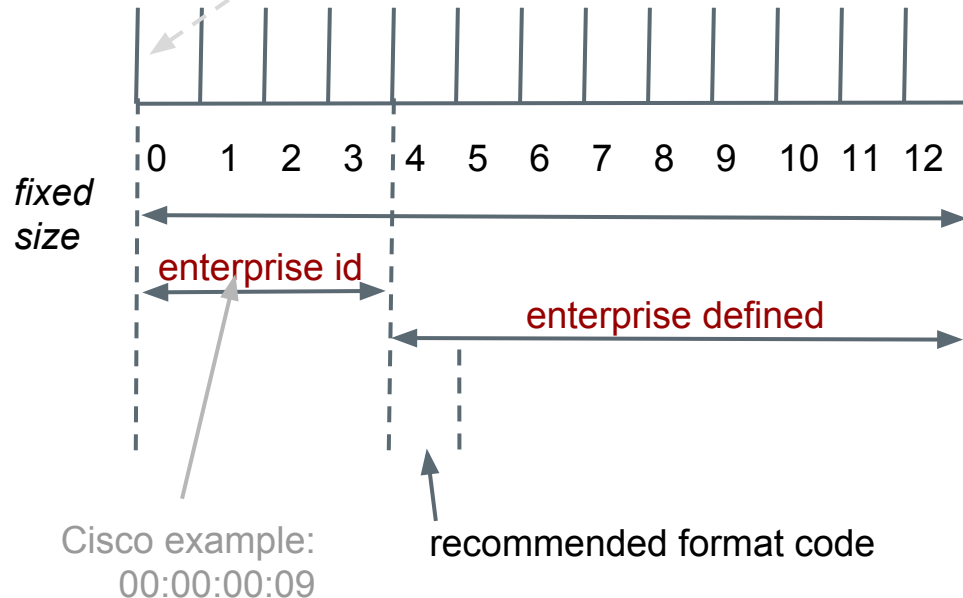
The SNMP Engine ID is always twelve octets in length.

The first bit of the lead octet must be '0'.

The first four octets identify an enterprise. Ex: Cisco is '9', Sprint is '1421', IBM is '2'.

The remaining eight octets are left for the enterprise to specify per their own interests.

It is recommended that if an enterprise has more than one formatting, that the fifth octet be used as the format indicator. The remaining seven octets, then, contain that format's value.



The format of SNMP Engine IDs

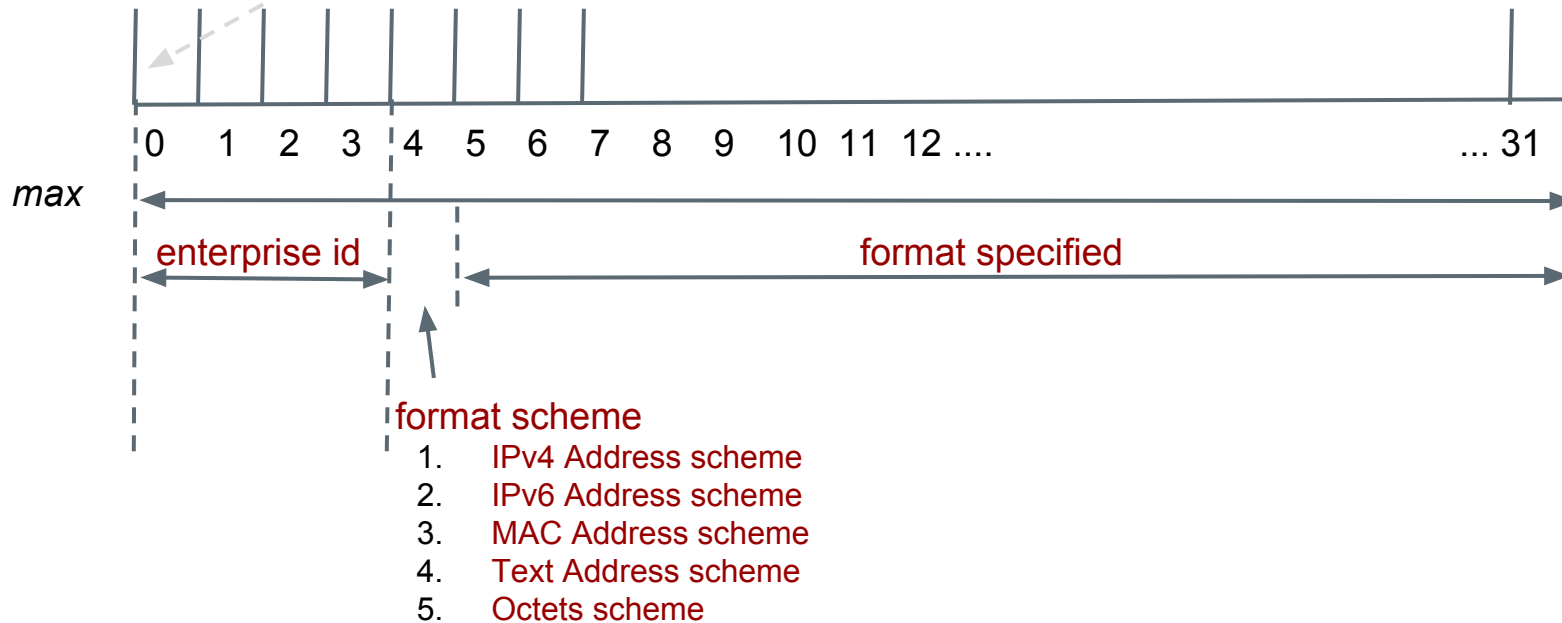
<> Method #2: Variable size format. (RFC 3411)

The SNMP Engine ID can range from 5 up to 32 octets.

The first bit of the leading octet must be '1'.

The first four octets identify an enterprise. Ex: Cisco is '9', Sprint is '1421', IBM is '2'.

The fifth octet specifies a format scheme, which then specifies how the remainder of the SNMP Engine ID is to be allocated.



The format of SNMP Engine IDs

<> Method #2.1: IPv4 Address format scheme. (RFC 3411)

The SNMP Engine ID is always 9 octets in length.

The first bit of the leading octet must be '1'.

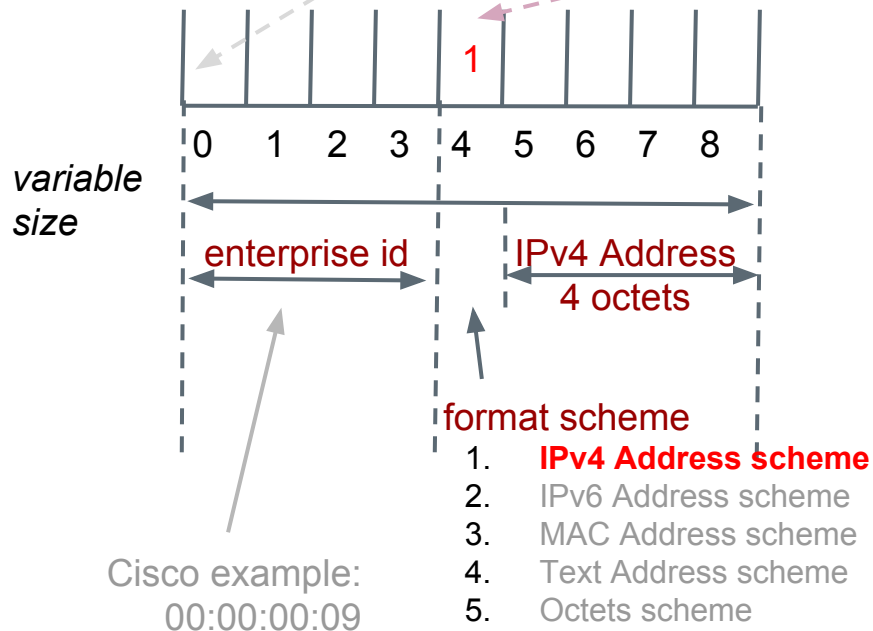
The first four octets identify an enterprise. Ex: Cisco is '9', Sprint is '1421', IBM is '2'.

The fifth octet specifies the IPv4 Address format scheme ('1').

The sixth thru ninth octets specify an IPv4 Address.

<> Example:

A Cisco SNMPv3 Agent is at 10.43.1.235



Enterprise ID

00:00:00:09

Code

1

IPv4 Address

10.43.1.235

0a:2b:01:eb

80:00:00:09:01:0a:2b:01:eb

9 octet length

The format of SNMP Engine IDs

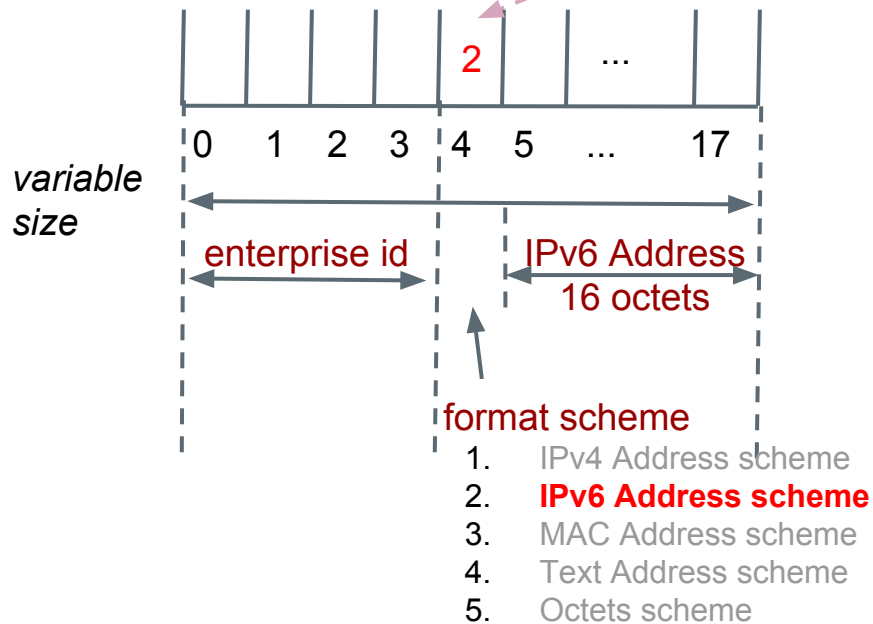
<> Method #2.2: IPv6 Address format scheme. (RFC 3411)

The SNMP Engine ID is always 17 octets in length. The first bit must be '1'.

The first four octets identify an enterprise. Ex: Cisco is '9', Sprint is '1421', IBM is '2'.

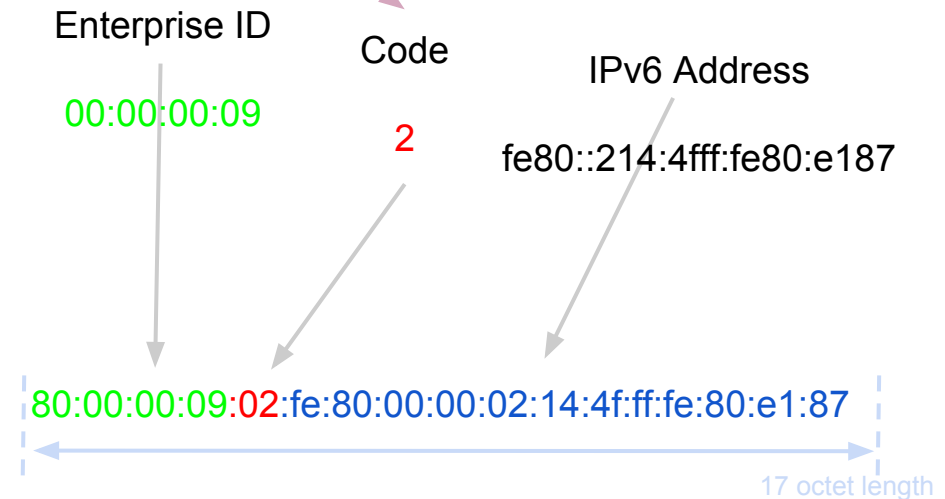
The fifth octet specifies the IPv6 Address format scheme ('2').

The sixth thru ninth octets specify an IPv4 Address.



<> Example:

A Cisco SNMPv3 Agent is at fe80::214:4fff:fe80:e187



The format of SNMP Engine IDs

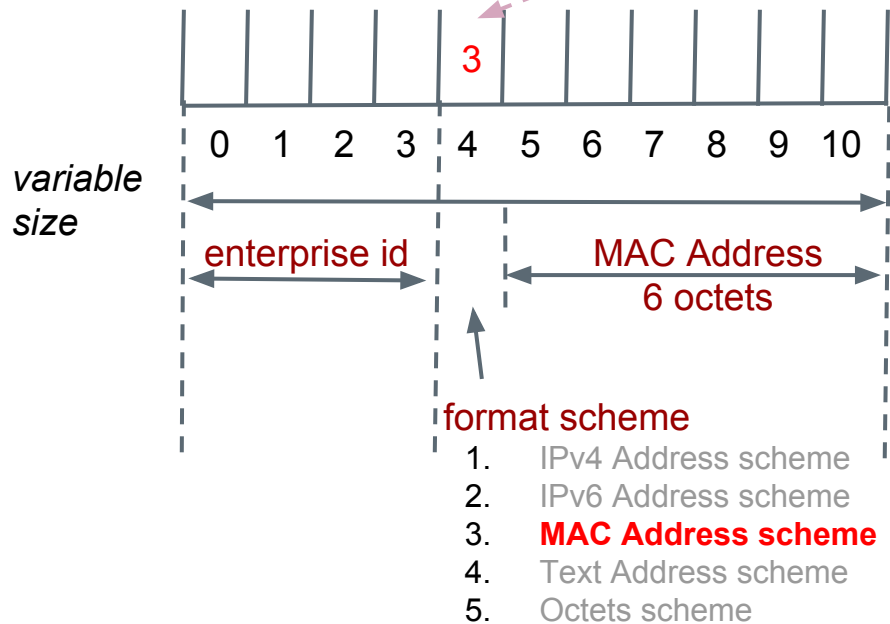
<> Method #2.3: MAC Address format scheme. (RFC 3411)

The SNMP Engine ID is always 11 octets in length. The first bit must be '1'.

The first four octets identify an enterprise. Ex: Cisco is '9', Sprint is '1421', IBM is '2'.

The fifth octet specifies the MAC Address format scheme ('3').

The sixth thru eleventh octets specify a MAC Address.



<> Example:

A Cisco SNMPv3 Agent is at 8:0:27:18:f1:e

Enterprise ID

00:00:00:09

Code

3

MAC Address

8:0:27:18:f1:e

08:00:27:18:f1:0e

80:00:00:09:03:08:00:27:18:f1:0e

11 octet length

The format of SNMP Engine IDs

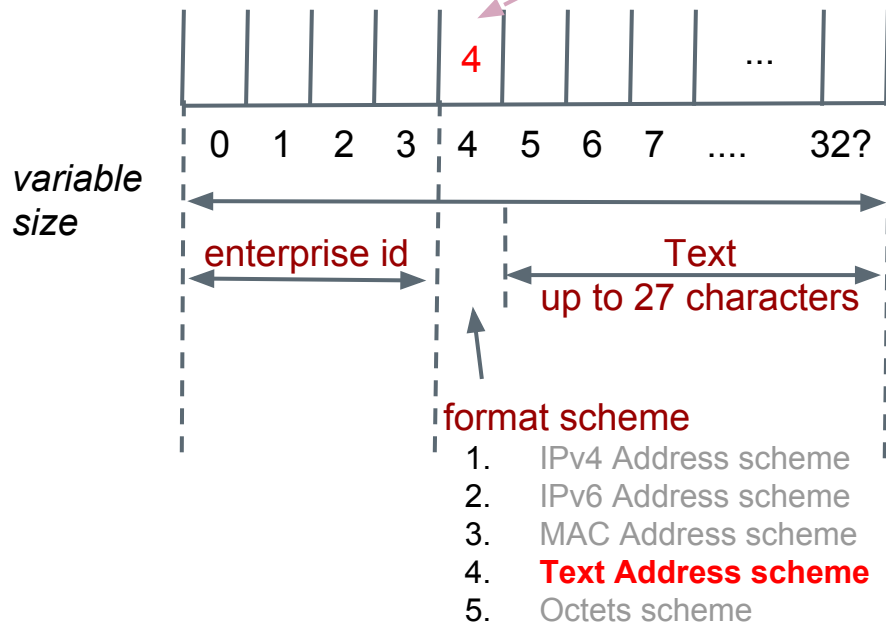
<> Method #2.4: Text format scheme. (RFC 3411)

The SNMP Engine ID can be up to 32 octets in length. The first bit must be '1'.

The first four octets identify an enterprise. Ex: Cisco is '9', Sprint is '1421', IBM is '2'.

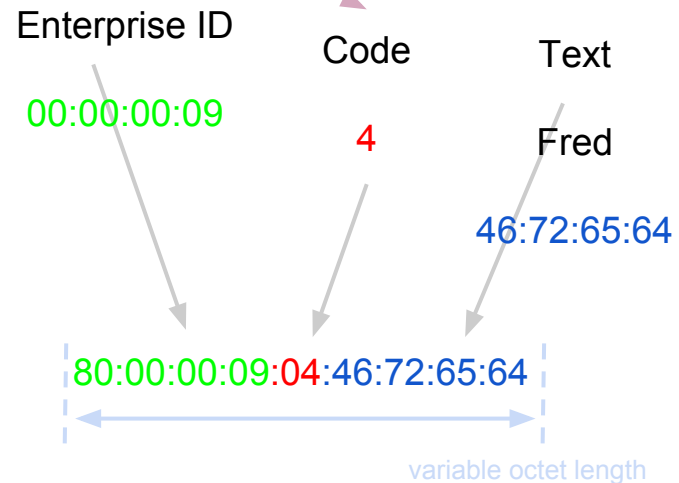
The fifth octet specifies the Text format scheme ('4').

The sixth thru final octets specify user-supplied text.



<> Example:

The administrator chooses the word "Fred".



The format of SNMP Engine IDs

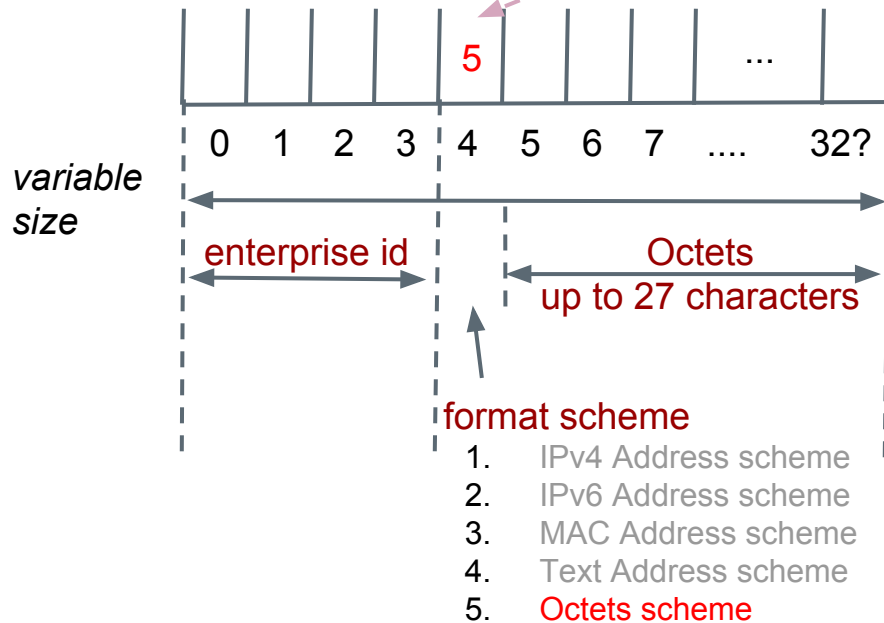
<> Method #2.5: Octets String format scheme. (RFC 3411)

The SNMP Engine ID can be from 5 up to 32 octets in length. The first bit must be '1'.

The first four octets identify an enterprise. Ex: Cisco is '9', Sprint is '1421', IBM is '2'.

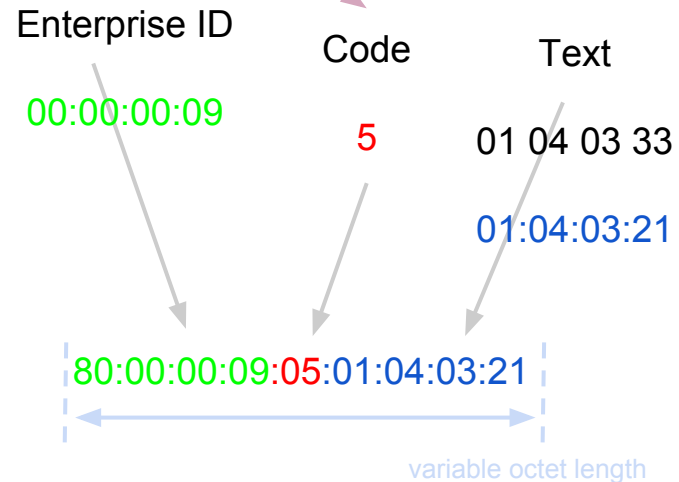
The fifth octet specifies the Octet String format scheme ('5').

The sixth thru final octets specify user-supplied values.



<> Example:

The administrator chooses the values "01 04 03 33".



The format of SNMP Engine IDs

<> Method for creating default NerveCenter SNMP Engine ID

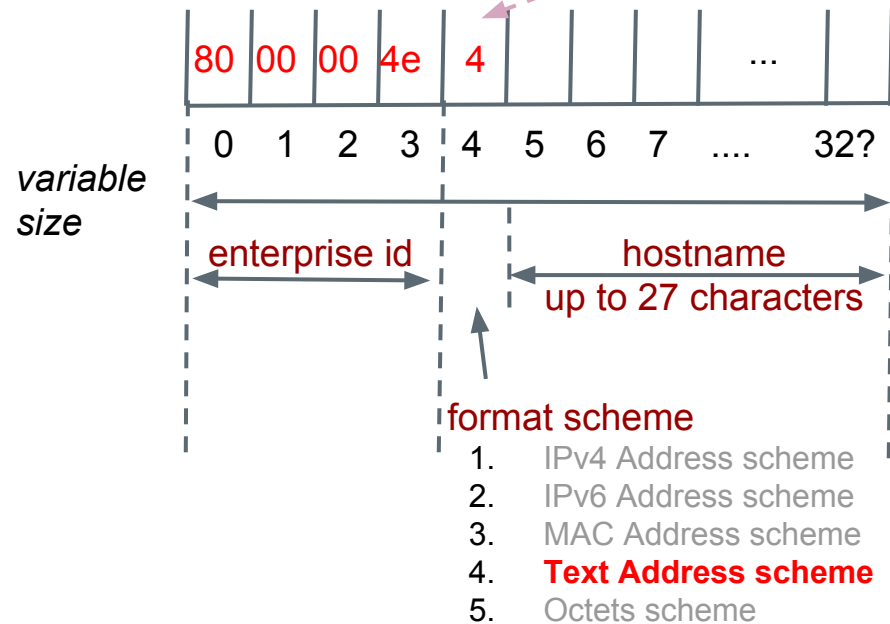
Based on Method #2.4: Text format scheme. (RFC3411)

LogMatrix' enterprise id is "78", as assigned by IANA. "78" is "4e" hex.

The first four octets hold this enterprise id, plus the required high bit turned on: 80 00 00 4e.

The fifth octet specifies the Text format scheme ('4').

The sixth thru final octets specify the first 27 characters of the hostname.



<> Example:

The NCServer host is "nms01".

