SNMPv3 Configuration

- The SNMP Manager and Agent recognise each other through simple unencrypted community strings in SNMP version 1 and 2
- SNMPv3 supports authentication and encryption
- The SNMPv3 security model works with users and groups
- A matching user account is set up on the NMS server and network device
- Settings are derived from the group the user is a member of

SNMPv3 Security Levels

- 3 different security levels are available. They are configured at the group level:
  - noAuthnoPriv - no authentication password is exchanged and the communications between the agent and the server are not encrypted. The username serves as replacement for community string.
  - AuthNoPriv - Password authentication is used. No encryption is used for communications between the devices.
  - AuthPriv - Password authentication is used. Communications between the agent and the server are also encrypted.

SNMPv3 Configuration - Group

```
R1(config)#snmp-server group Flackbox-group v3 ?
  auth    group using the authNoPriv Security Level
  noauth  group using the noAuthNoPriv Security Level
  priv    group using SNMPv3 authPriv security level
```

SNMPv3 Configuration - Group

```
R1(config)#snmp-server group Flackbox-group v3 priv ?
  access   specify an access-list associated with this group
  context  specify a context to associate these views for the group
  match    context name match criteria
  notify   specify a notify view for the group
  read     specify a read view for the group
  write    specify a write view for the group
  <cr>
```

SNMPv3 Configuration - Group

- **Access** can be used to reference an access-list which limits the device to communicating with the IP address of the NMS server only
- **Contexts** are used on switches to specify which VLANs are accessible via SNMP

SNMPv3 Configuration - Views

- Views can be used to limit what information is accessible to the NMS server.
- If you don’t specify a read view then **all** MIB objects are accessible to read.
- If you don’t specify a write view then **no** MIB objects are accessible to write.
- The NMS server gets read only access to all MIBs by default.
- The notify view is used to send notifications to members of the group. If you don’t specify any then it will be disabled by default.

SNMPv3 Configuration - Group

```
R1(config)#snmp-server group Flackbox-group v3 priv
```

SNMPv3 Configuration - User

```
R1(config)#snmp-server user Flackbox-user Flackbox-group v3 auth ?
  md5  Use HMAC MD5 algorithm for authentication
  sha  Use HMAC SHA algorithm for authentication (most secure but slower)
```

SNMPv3 Configuration - User

```
R1(config)# snmp-server user Flackbox-user Flackbox-group v3 auth sha
AUTHPASSWORD priv ?
  3des  Use 168 bit 3DES algorithm for encryption
  aes   Use AES algorithm for encryption (most secure but slower)
  des   Use 56 bit DES algorithm for encryption
```

SNMPv3 Configuration - User

```
R1(config)# snmp-server user Flackbox-user Flackbox-group v3 auth sha
AUTHPASSWORD priv aes ?
  128  Use 128 bit AES algorithm for encryption
  192  Use 192 bit AES algorithm for encryption
  256  Use 256 bit AES algorithm for encryption
```

SNMPv3 Configuration - User

```
R1(config)# snmp-server user Flackbox-user Flackbox-group v3 auth sha
AUTHPASSWORD priv aes 128 PRIVPASSWORD
```

Lab