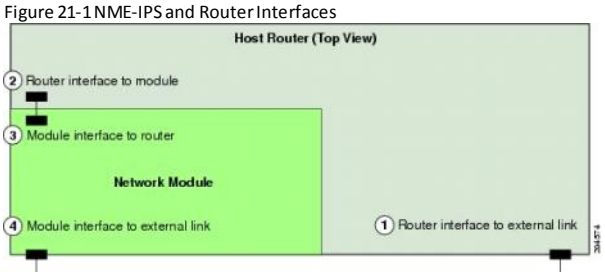
NME-IPS

The purpose of this document is explain how to configure a NME-IPS module.
The configuration guide can be a bit tricky to understand and this document tries a different approach to help understand the configuration required.

Figure 21-1 NME-IPS and Router Interfaces



1	Router interface to external link Configure the standard router settings using the Cisco IOS CLI.
2	Router interface to NME-IPS (ids-sensor x/0) Configure the IP address and default gateway router of NME-IPS using the Cisco IOS CLI.
3	NME-IPS interface to router (GigabitEthernet0/1) Configure the interface as inline or promiscuous using the Cisco IOS CLI.
4	NME-IPS interface to external link (Management0/1) Configure the command and control interface using the IPS CLI, IDM, IME, or CSM.

- **Step 4**
  Enable monitoring on the interface in either inline or promiscuous mode and associate the access list.
  router(config)# **interface** *monitored_interface*

  router(config-if)# ids-service-module monitoring [inline | promiscuous] [access-list]

- **Step 5**
  (For inline mode) Specify how the router handles traffic inspection during a module failure.
  router(config)# **interface ids-sensor 1/0**

  router(config-if)# service-module [fail-close | fail-open]

- **Used for:**
  Sending traffic that hits the external interface of router to the NME module .

  Check note *

- **Step 1**
  Assign an IP address and netmask to the loopback interface.

  router(config)# interface loopback 0
  router(config-if)# ip address 10.99.99.99 255.255.255.255

- **Step 2**
  Assign an unnumbered loopback interface to the IDS-Sensor interface. Use slot 1 for this example.

  router(config)# interface ids-sensor 1/0
  router(config-if)# ip unnumbered Loopback 0

- **Used for**:
  Reverse-telnet so that we can open a console session to nme module from router using:

  Router#service-module ids-sensor 1/0 status

- **Step 7**
  (Optional) Configure a monitoring access list on the router.
  router(config)# access-list 101 permit tcp any eq www any

  You can set up a standard access list and apply it to filter what type of traffic you want to inspect. A matched ACL causes traffic not to be inspected for that ACL. This example bypasses inspection of HTTP traffic only. Refer to your Cisco IOS Command Reference for more information on the options for the **access-list** command.