Packet Capture with HUB/Switch

While troubleshooting we required packet capture to analyze, some time we need hub to capture full packet.

Now a days HUB is difficult to get in market, so we have to find other option.

There are difference in HUB and a normal network switch. We cannot use a normal switch to do this function unless do some other setting.

1, In a Cisco switch, we can use command to change the Switch to HUB using "No mac learning "command

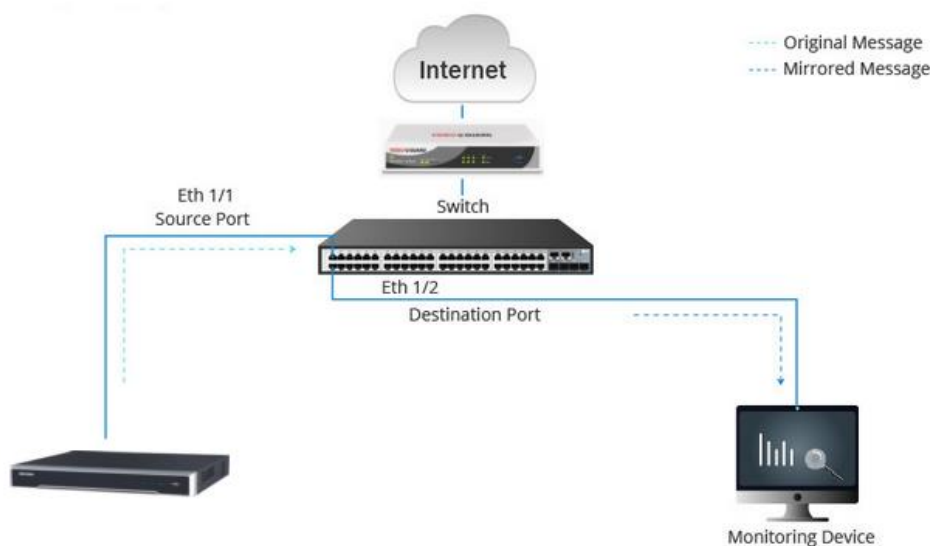2, Make a normal switch with port mirror and capture.

A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it.

A switch is an intelligent device, transmitting to specific MAC addresses within the LAN

Follow below topology, Connect the Switch and laptop and capture packet.

Source port should be the LAN connect to NVR/DVR or the cable connect to main Source (e.g. Video guard)

Monitor Port, which connect to Laptop or PC, which run Wireshark or other capture tool .

How to Enable Port Mirror

Local port mirroring is the most basic form of mirroring. All source ports are located on the same network device as the destination ports. As figure 1 shows, local port mirroring enables the network switch to forward the copy of the packet on the source port (Eth 1/1) to the destination port (Eth 1/2). Then the monitoring device connected with the destination port can monitor and analyze the packet.

Make sure the Switch is Managed and able to do port Mirror

How to Configure Port Mirroring?

The prerequisite of configuring port mirroring is ensuring the network device (no matter a switch or router) supports port mirroring. And then select one mode, local port mirroring or remote port mirroring configuration.

Local port mirroring configuration roadmap:

1. Create a VLAN.

2. Add the source port and destination port to VLAN.

3. Configure IP address.

4. Configure port mirroring on the destination port, and copy the packet from the source port to the destination port.

On the setup page, click **Maintenance** > **Diagnostics** > **Port Mirroring**.

NOTE: Some of the subtabs may vary slightly depending on the exact model number of your device.
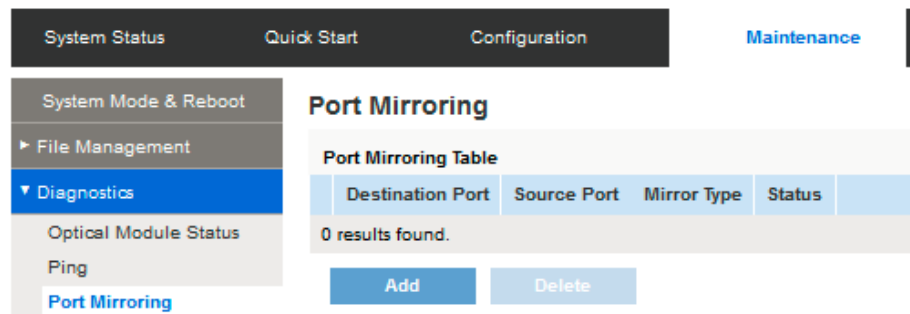
The Port Mirroring Table will display the following information:
- **Destination Port** – The analyzer port to which traffic is to be copied.
- **Source Port** – The interface port where the traffic to be sent to the analyzer port is from.
- **Mirror Type** – Type of monitoring: incoming to the port (Rx), outgoing from the port (Tx) or both.
- **Status** – Displays one of the following values:
  - Active – Both source and destination interfaces are up and forwarding traffic.
  - Not Ready – Either the source or destination port (or both) are down or not forwarding traffic for some reason.