# Table of Contents

**Typical Enterprise Network Topology** ............................................................................................................ 4  
  For Small Sized Enterprise ............................................................................................................................... 4  
  For Medium and Large Sized Enterprise ........................................................................................................ 4  

**Typical Industrial Network Topology** ........................................................................................................ 6  

**Passive Sensor Deployment Scenarios and Port Mirroring** ......................................................................... 7  
  Local SPAN .................................................................................................................................................. 7  
  RSPAN ....................................................................................................................................................... 8  
  ERSPAN ................................................................................................................................................. 13  
  How to Extend Local Span Through Multiple Intermediate Switches to a Sniffer.............. 16  
  How to Sniff the Traffic of VM’s in the Standalone Esxi ................................................................. 17  
  Best Practices ........................................................................................................................................... 19
Typical Enterprise Network Topology

For Small Sized Enterprise

To ensure the best asset visibility, deploy Network Passive Sensor closer to the client access, at the distribution switch instead of deploying the passive sensor at the core. Deployments closer to access enable the Network Passive Sensor to see traffic within the client access networks, more specifically enable passive sensor to see MACs within the broadcast domain of a single distribution switch. Deployments of Network Passive Sensor at the core will only see router’s MAC and have limited visibility to the traffic within client access networks, resulting in less complete discovery.

Diagram 1 shows typical deployment of network passive sensors in a small sized enterprise. Network Passive Sensors are deployed at distribution layer in the same network.

Diagram 1: Small Enterprise Deployment

For Medium and Large Sized Enterprise

The recommended deployment is to have one Network Passive Sensor in each of the physical locations, closer to the access network with all Network Passive Sensors registered to a single Qualys account.

Alternatively, if deploying Network Passive Sensor in every physical location is not possible then a single Network Passive Sensor can be deployed at one location and traffic from each of the physical locations can be mirrored to the remote location where the sensor is deployed. Refer to Passive Sensor Deployment Scenarios and Port Mirroring for more information on remote mirroring. Depending upon the volume of the network traffic aggregated across sites, use a 1G, 4G or 10G appliance.

Diagram 2 shows typical topology of medium sized enterprise. It is a sample three-tier LAN network design for medium enterprises where the access, distribution, and core are all separate layers. Network Passive Sensors are deployed at distribution and core layer for different buildings at same premises.
Diagram 2: Medium Enterprise Deployment

Diagram 3: Large Enterprise Deployment

Diagram 3 shows typical topology for large size enterprises with multiple physical locations. Network Passive Sensors are deployed at distribution and core layer of different sites. There are different sites (Main Site, Remote Large Site and Remote Medium Site) connected using WAN.
**Typical Industrial Network Topology**

Many industrial protocols communicate over Layer 2 and vital information related to device identification is seen in the broadcast domain. Hence, it is recommended that get the stream of packet captures from access switches.

A lot of vital device identity information is seen during the communication between the engineering workstation and controller layer. Hence placing a sensor such that we can tap into this layer is critical. Network Passive Sensor should get a copy of traffic between the Scada servers / Operator stations / Engineering workstations to PLC / RTU / IEDs / RIOs etc. Discovery and configuration of the Controllers / Drivers / IOs etc. is most important and hence ensuring that copy of traffic between from EWS like Studio 5000 / TIA portal to controller layer is covered. Typically this is the switch between Purdue level 2 and level 1 devices.

To ensure complete visibility, it is recommended that you should forward mirrored traffic to the network passive sensors for the lowest Purdue level. The Network Passive Sensors also help with high-level detection of OT endpoints and other devices, such as the DMZ, Layer 3.5, Layer 3, and Layer 2 Perdue levels. Therefore, it is recommended to acquire a copy of the mirrored traffic from the high Purdue level of the OT environment to a passive sensor for comprehensive visibility. The Network Passive Sensor can check Windows / Linux / other OS-based assets at a high level. This helps to determine the Qualys Cloud Agent and Qualys Authenticated Scan strategies for these devices.
Passive Sensor Deployment Scenarios and Port Mirroring

Enterprises that use the Qualys Network Passive Sensors to monitor their networks have to feed a copy of their network traffic to the sensor. This can be accomplished by tapping into their network at an appropriate choke point using port mirroring.

There may be different types of network environments and topologies where it may or may not be possible to deploy the passive sensor at the same location as the tap point. Based on these choices different types of port mirroring options have to be exercised.

Note: In case multiple sniffing interfaces of the Network Passive Sensor are used (as available in 4G and 10G appliances) ensure that the mirrored traffic connected to the two interfaces is not coming from networks that have overlapping IP address space.

Local SPAN

Switch Port Analyzer (SPAN) is an efficient, high performance traffic monitoring system. It mirrors traffic from one or more interfaces or VLAN to one or more interfaces on the same switch. This method is also called as Local SPAN.

In this method appliance is connected to the switch at the same location as the switch and can be connected directly to one of the switch ports.

The switch has a spare port that can be dedicated for mirroring. The passive sensor is physically co-located with the switch and is directly connected to the mirror port. For this the SPAN method should be used.

The following image shows the connectivity for a physical appliance. You’ll see that the sniffing interface of the appliance is connected to the network switch and mirrored traffic is fed from the switch to the appliance. The management interface connects to the Qualys Cloud Platform.
The following picture shows connectivity for a virtual appliance. The virtual appliance is supported on the VMware ESXi Server virtualization platform and Microsoft Hyper-V. Again the sniffing interface is fed mirrored traffic from the network switch. The management interface is configured to connect to the Qualys Cloud Platform.

RSPAN

Remote Switch Port Analyzer (RSPAN) provides remote monitoring traffic from source ports distributed over multiple switches. It supports source ports, source VLANs, and destination ports on different switches.

In this method, appliance is in the same Layer 2 (L2) network but cannot be connected directly to the switch.

In all the situations mentioned below, RSPAN can be used. RSPAN method centralizes the mirror traffic from one/multiple Layer 2 switches by mirroring the traffic from the source ports of an RSPAN session to a VLAN that is dedicated for the RSPAN session. This VLAN is then trunked to the other switches allowing the RSPAN session traffic to be transported across multiple switches. On the switch that contains the destination port for the session, traffic from the RSPAN session VLAN is simply mirrored out to the destination port where Network Passive Sensor sniffing interface is connected.

a) Network Passive Sensor is in the same L2 network as the switch and appliance is not physically co-located with the switch OR
b) Network Passive Sensor is in the same L2 network as the switch and network has many Layer 2 switches. Then it may not be possible to do local mirroring on each Layer 2 switch and deploy multiple passive sensors connecting to SPAN port of each Layer 2 switch. OR
c) Network Passive Sensor is in the same L2 network as the switch and Local SPAN is not possible because all ports on a switch are occupied.
For RSPAN deployment the user must know the CPU utilization of the network switch beforehand. If the switches are already utilizing high CPU then enabling RSPAN may cause the switch to drop packets.

If your network has many Layer 2 switches then it may not be possible to do local mirroring on each Layer 2 switch and deploy multiple passive sensors connecting to SPAN port of each Layer 2 switch. To handle this situation, you need to use RSPAN method to centralize the mirror traffic from various Layer 2 switches. RSPAN works by mirroring the traffic from the source ports of an RSPAN session to a VLAN that is dedicated for the RSPAN session. This VLAN is then trunked to the other switches allowing the RSPAN session traffic to be transported across multiple switches. On the switch that contains the destination port for the session, traffic from the RSPAN session VLAN is simply mirrored out to the destination port where Network Passive Sensor sniffing interface is connected.

![Diagram showing RSPAN connectivity](image)

**Note**: The above diagram shows RSPAN connectivity for Physical Appliance, however the same connectivity works for Virtual Appliance.

**Sample RSPAN Configurations**

In this section, you’ll understand various configurations required on core, distribution, and access layer.

Following diagram illustrates how the mirrored traffic (red arrows) flows from Access layer to distribution layer and from distribution layer to core switch.
Sample Configuration on S31
This configuration helps to mirror the traffic on access layer (user connected) switches.
1. Create RSPAN VLAN

```bash
vlan 100
name rspan_vlan_100
remote-span
exit
```

2. Configure S31 uplink connected to S21 to allow RSPAN VLAN

```bash
interface GigabitEthernet1/0/15
switchport mode trunk
switchport trunk allowed vlan add 100
no shutdown
```

3. Mirror traffic of users vlan (for example - vlan 31) connected to configured RSPAN VLAN (vlan 100) on the switch

```bash
monitor session 1 source vlan 31 rx
monitor session 1 destination remote vlan 100
```

Sample Configuration on S21
This configuration helps to create RSPAN VLAN and allows RSPAN traffic to pass through trunk ports for distribution layer switches.

1. Create RSPAN VLAN

```bash
vlan 100
name rspan_vlan_100 remote-span
```
2. Configure S21 interface connected to S31 to allow RSPAN VLAN 100

```
interface GigabitEthernet1/0/19
switchport mode trunk
switchport trunk allowed vlan add 100
no shutdown
```

3. Configure S21 uplink connected to S11 to allow RSPAN VLAN

```
interface GigabitEthernet1/0/20
switchport mode trunk
switchport trunk allowed vlan add 100, 200
no shutdown
```

**Sample Configuration on S11**

This configuration helps to create RSPAN VLAN and allows RSPAN traffic to pass through trunk ports for core switches.

1. Create RSPAN VLAN

```
vlan 100
name rspan_vlan_100
remote-span
exit
vlan 200
name rspan_vlan_200
remote-span
exit
vlan 300
name rspan_vlan_300
remote-span
exit
vlan 400
name rspan_vlan_400
remote-span
exit
```

2. Configure S11 interface connected to S21 switch to allow RSPAN VLANs 100,200

```
interface GigabitEthernet1/0/24
switchport mode trunk
switchport trunk allowed vlan add 100, 200
no shutdown
```

3. Configure S11 interface connected to NPS sniffing port to allow all RSPAN VLANs traffic

```
interface GigabitEthernet1/0/25
switchport mode trunk
switchport trunk allowed vlan add 100, 200,300,400
no shutdown
```
VTP Configurations

VTP configuration can be used to centralize the RSPAN VLAN configurations on Cisco switches. For example, configure S11 as VTP server and remaining switches as VTP clients. Just adding RSPAN VLANs in S11 will advertise the new VLAN configuration to all other switches which are in VTP client mode and in the same VTP domain.

1. Sample VTP server configuration on S11

   ```
   (config)#vtp domain test
   (config)#vtp mode server
   (config)#vtp password mypassword
   (config)#exit
   ```

2. Sample VTP client configuration on other switches:

   ```
   (config)#vtp domain test
   (config)#vtp mode client
   (config)#vtp password mypassword
   (config)#exit
   ```

3. Sample config for creating RSPAN VLANs on S11

   ```
   vlan 100
   name rspan_vlan_100
   remote-span
   exit
   vlan 200
   name rspan_vlan_200
   remote-span
   exit
   vlan 300
   name rspan_vlan_300
   remote-span
   exit
   vlan 400
   name rspan_vlan_400
   remote-span
   exit
   ```

4. Now all other switches will receive RSPAN VLAN configurations from S11 (vtpserver). You can verify the configurations of VLANs using 'show vlan' command.
ERSPAN

In order to monitor traffic across a WAN or different networks, use Encapsulated Remote Switch Port Analyzer (ERSPAN). The ERSPAN feature supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network.

Some enterprises may have a requirement to passively monitor their networks, including those remotely located, and it may not be possible to install a sensor in each of the remote locations. To cater to such requirements, Encapsulated Remote Switch Port Analyzer (ERSPAN) should be used. ERSPAN allows mirrored traffic to be encapsulated and transported over the L3 network to a remote destination. This requires that each location have switches having ERSPAN capability and the switches be configured to tunnel mirror traffic to a destination L3 switch/router interface.

In this method, the appliance is deployed at a remote location that is reachable over the Layer 3 (L3) network.

Following diagram shows a sample topology that explains the above deployment scenario:
There are 3 networks seen in the diagram - Loc1, Loc2 and Loc3. The passive sensor appliance is deployed at location Loc3.

Switches S1 and S2 at Location Loc1 and Loc2 respectively, have to support ERSPAN source capability.

At location Loc3, on Router R1, reserve an interface and connect it to the sniffing interface of PS. Configure switch S1 with ERSPAN source and destination. Similarly configure S2. On Router R1, reserve an interface and configure it with an IP address that serves as the ERSPAN destination for S1 and S2. For details see sample configurations done for Cisco catalyst 9300 in the subsequent section.

**Sample ERSPAN Configurations for Physical Appliance**

**Sample Configurations for Cisco Catalyst 9300 Switch**

```
a) 9300 L3 Switch/Router 1 config
1. Assign an IP address to interface Gi1/0/26
   ```
   interface GigabitEthernet1/0/26
   no switchport
   ip address 10.10.10.10 255.255.255.0
   ```
2. Add routes to send ERSPAN traffic to PS sniffing interface
   ```
   ip route 10.10.20.0 255.255.255.0 10.10.10.20
   ip route 10.10.40.0 255.255.255.0 10.10.10.20
   ```
3. Add ERSPAN-source configuration and define source interface & src, dst IP address of GRE tunnel
   ```
   monitor session 1 type erspan-source
   source interface Gi1/0/25 rx
   destination
   erspan-id 2
   ip address 10.10.40.40
   origin ip address 10.10.30.30
   ```
   **Note**: Here, 10.10.40.40 is the IP address from unused subnet for ERSPAN GRE Tunnel.
```
b) 9300 L3 Switch/Router 2 config

1. Assign IP address to interface Gi1/0/26

```bash
interface GigabitEthernet1/0/26
no switchport
ip address 10.10.10.20 255.255.255.0
```

2. Assign IP address to interface Gi1/0/27

```bash
interface GigabitEthernet1/0/27
no switchport
ip address 10.10.20.1 255.255.255.252
no keepalive
no cdp enable
```

3. Add static ARP entry with any MAC address which is not in use, with any IP address belonging to same subnet of IP address assigned interface Gi1/0/27.

   **Note:** This step is required as there is no IP address assigned to PS sniffing interface.

   ```bash
   arp 10.10.20.2 02:00:00:xx:xx:xx ARPA
   ```

   **Note:** Replace xx:xx:xx with last three octets of the MAC address of the PS management interface

4. Add route to reach ERSPAN traffic to PS sniffing interface, use same IP address used in above command as gateway for this route

   ```bash
   ip route 10.10.40.0 255.255.255.0 10.10.20.2
   ```

**Sample ERSPAN Configurations for Virtual Appliance**

**With Extra VM Deployment with IP Address**
How to Extend Local Span Through Multiple Intermediate Switches to a Sniffer That is Multiple Switch Hops Away Without Using RSPAN.
1) Connect one additional switch in the network which supports the local span configuration.

2) Do a local span on the access layer switches.
   - **E.g.:** config on S31 Switch:
     - monitor session 1 source vlan 71 - 72 both
     - monitor session 1 destination interface Gi1/0/33

3) Connect span ports of access layer switches to the additional switch.

4) Choose vlan’s that are not used in the network & configure on the additional switch.
   - **E.g.:** config on the additional switch:
     - Interface Gi1/0/1
       - Switchport access vlan 81
       - Switchport mode access
       - Spanning-tree bpdufilter enable
     - Interface Gi1/0/2
       - Switchport access vlan 82
       - Switchport mode access
       - Spanning-tree bpdufilter enable

5) Do a local span on the additional switch.
   - **E.g.**:
     - monitor session 1 source interface Gi1/0/1 – 4 both
     - monitor session 1 destination interface Gi1/0/5
     
     Or
     - monitor session 1 source vlan 81-84 rx
     - monitor session 1 destination interface Gi1/0/5

6) Connect the span port of the additional switch to the NPS sniffing interface.

   **Note:** This technique can be used to pass through multiple intermediate switches with each switch configured similar to the extra switch introduced in this diagram.

   This mechanism of chaining multiple switches with local spans can terminate into a switch that supports RSPAN, and from there onwards, the RSPAN documentation can be used to bring the span traffic to PS.

**How to Sniff the Traffic of VM’s in the Standalone Esxi**

1) Create a new port-group (e.g. Mirror-traffic) and select vswitch for sniffing traffic of VM’s on standalone esxi. See the IMG 01.

2) Enable promiscuous mode, mac address changes & forged transmits on newly created port-group. See the IMG 01.

3) Allow all vlans (i.e. vlan id 4095) on the newly created port-group. See the IMG 01.

4) Connect PS sniffing interface to newly created port-group. See the IMG 03.
**IMG: 01**

Add port group - Mirror-traffic

- **Name**: Mirror-traffic
- **VLAN ID**: 4095
- **Virtual switch**: vSwitch0

**Security**

- **Promiscuous mode**: Accept
- **MAC address changes**: Accept
- **Forged transmits**: Accept

**IMG: 02**

vSwitch topology

- **Mirror-traffic**: VLAN ID: 4095, Virtual Machines (1): PS_Plate-P232, VM Address: 00:50:56:06:06:6a

- **Physical adapters**: vmnic29, 1000 Mbps, Full
Best Practices

The below best practices are followed specifically when spanning ICS traffic from switches,

- Source of span traffic should either select all access ports or all VLANs which have to be monitored.
- Selecting span source as uplink of the switch is not recommended for ICS device environments as the traffic between PLCs, HMIs, IO devices connected to the same switch may not reach the uplink of a switch.
- If engineering workstations are connected on a switch (S1) which is different from a switch (S2) on which PLCs and IO devices are connected, and both S1 & S2 connected to the aggregation switch, then uplink of S1 or S2 will see traffic between PLCs to engineering workstations. In this case, mirroring traffic from the uplink of S1 or S2 will be beneficial.