



**Hewlett Packard**  
Enterprise

# **HPE Synergy Port Monitoring Configuration Guide**

Version 1.1, October. 2023

Executive Summary .....	3
Target Audience.....	3
Equipment .....	3
HPE Synergy Port Monitoring Overview .....	3
Local Port Monitoring .....	5
Remote Port Monitoring .....	5
Synergy Port Monitoring Configuration .....	6
Configuring Synergy Local Port Monitoring.....	7
Local Port Monitoring Using Internal Server .....	7
Local Port Monitoring Using External Server .....	11
Configuring Synergy Remote Port Monitoring.....	12
Resources and additional links.....	18

## Executive Summary

This white paper aims to help customers to understand the concept and the configuration of HPE Synergy Virtual Connect Port Monitoring.

## Target Audience

This guide is intended for network and server architects, administrators and engineers who manage and operate the HPE Synergy platform.

## Equipment

DEVICE	VERSION	QTY
HPE Synergy managed by OneView	8.50 and HPE Synergy SSP 2023.05.01	1
HPE Virtual Connect SE 100Gb F32 Module for Synergy	2.6.0.1001	2
Cisco ACI APIC	6.0(2h)	1
Cisco Nexus 93180YC-EX	16.2(2h)	2

**Note:** All discussions within this white paper are applicable to the HPE Synergy Virtual Connect SE 40Gb F8 module as well. Additionally, it includes an example using Cisco ACI fabric for upstream data center switches. It is important to note that the concept and configuration of HPE Synergy Port Monitoring can also be applied to other switch vendors and models.

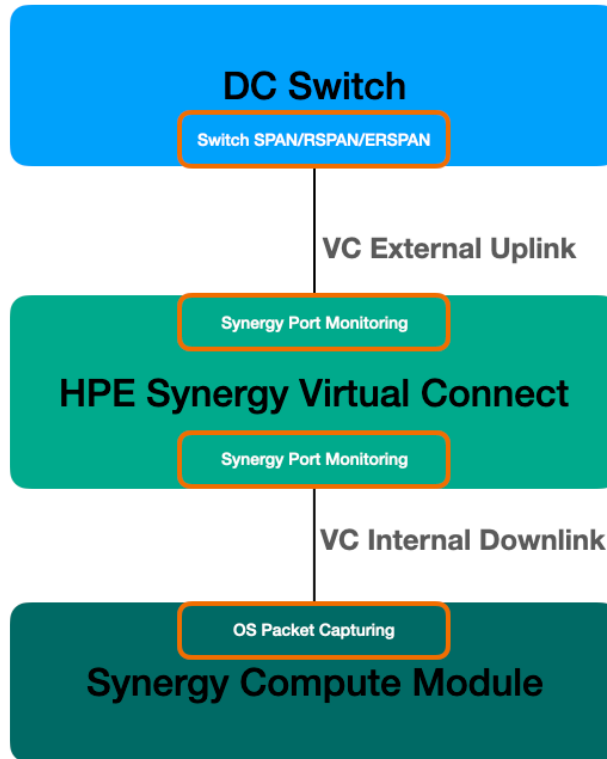
## HPE Synergy Port Monitoring Overview

HPE Synergy port monitoring provides the ability to analyze network traffic passing through specific ports by mirroring the traffic from source ports to a designated destination port connected to a network analyzer. Port monitoring is one of the features provided by HPE Synergy Virtual Connect modules, which are responsible for serving customer traffic within the HPE Synergy platform.

The port monitoring feature in HPE Synergy serves a similar troubleshooting purpose as Cisco switches' SPAN and VMware's DVS Port Mirroring. The table below summarizes the comparison of terms used by HPE, Cisco, and VMware:

SYNERGY	CISCO	VMWARE
Port Monitoring	SPAN	Port Mirroring

The diagram below shows the capture points along the server’s traffic flow:



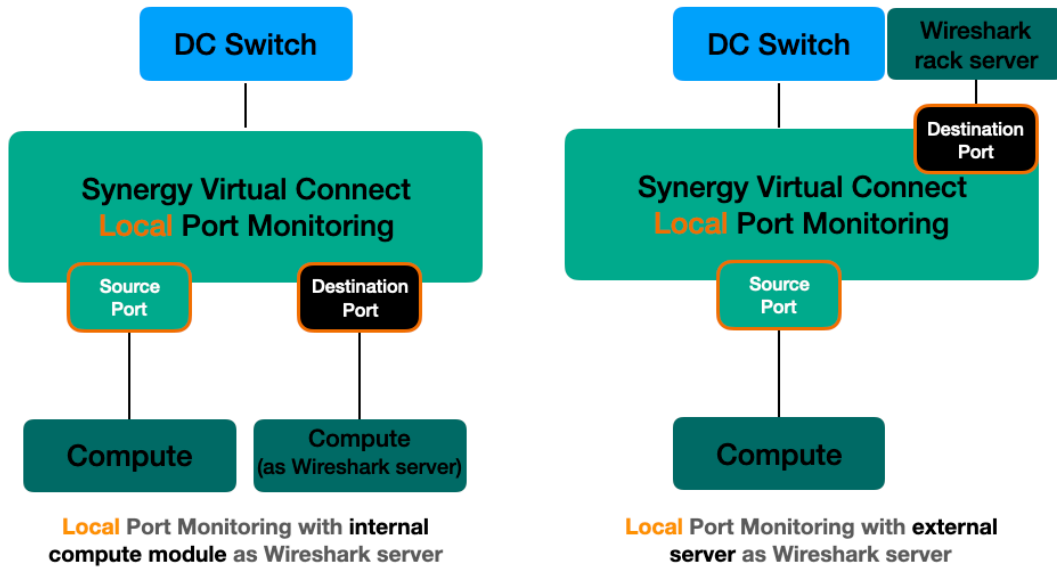
HPE Synergy Virtual Connect supports traffic monitoring for both its uplinks connected with upstream switches and its downlinks connected with HPE Synergy compute modules. Most networking admins use switch side traffic monitoring tools like Cisco SPAN to monitor in/out switch traffic so this white paper will focus on how to monitor the in/out HPE Synergy compute module traffic.

HPE Synergy Virtual Connect has two types of port monitoring shown in the table below:

VIRTUAL CONNECT PORT MONITORING TYPE	DEFINITION
Local Port Monitoring	The monitored server traffic will be sent to a downlink port of HPE Synergy Virtual Connect module acting as Wireshark server or an uplink port connected directly to a rack Wireshark server.
Remote Port Monitoring	The monitored server traffic will be sent to an uplink port of HPE Synergy Virtual Connect module. The uplink port is connected to a data center switch. The traffic will be encapsulated in an 802.1Q VLAN header when leaving HPE Synergy. This specific VLAN is configured in HPE OneView and dedicated for this remote port monitoring purpose.

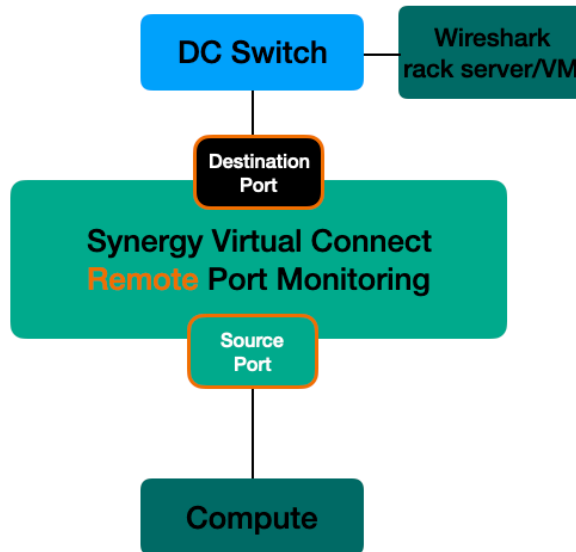
### Local Port Monitoring

In local port monitoring, the traffic from the server being monitored (i.e. the network analyzer port) can be directed to either a downlink port on the HPE Synergy Virtual Connect module that is connected to a compute module serving as the Wireshark server, or it can be sent directly to an uplink port that is connected to a separate rack-mounted Wireshark server. The following diagram illustrates these two use cases:



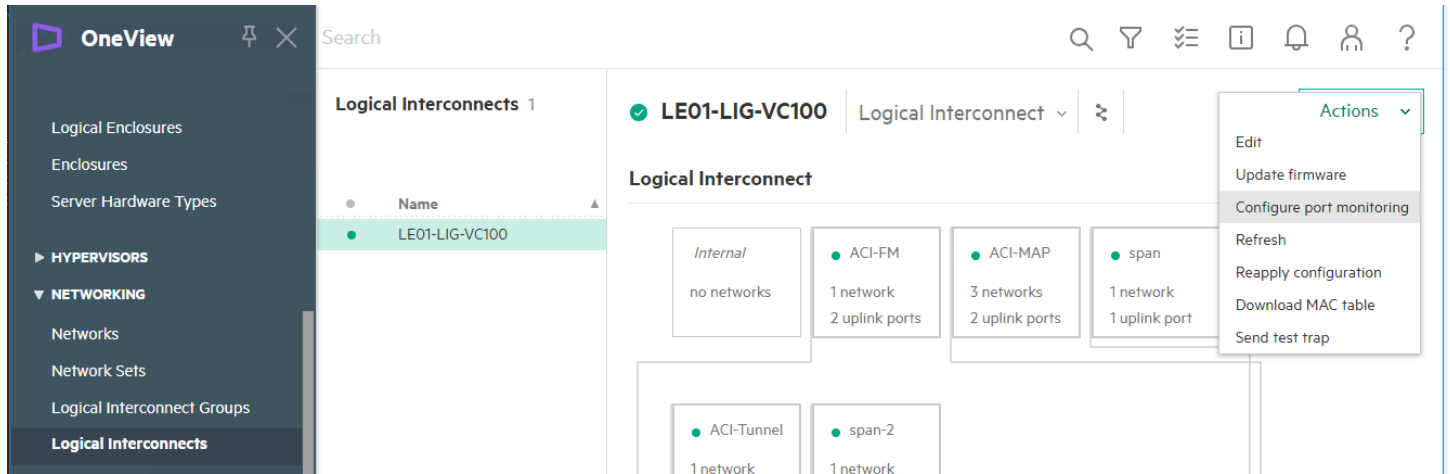
### Remote Port Monitoring

In remote port monitoring, the traffic from the monitored server is directed to an uplink port on the HPE Synergy Virtual Connect module. This uplink port is connected to a data center switch. Before leaving the HPE Synergy frame, the traffic is encapsulated in an 802.1Q VLAN header. This VLAN is specifically configured in HPE OneView and is dedicated for the purpose of remote port monitoring. The Wireshark server, which captures and analyzes network traffic, is connected to the data center switch network. It's important to note that a separate uplink port must be assigned exclusively for this purpose and cannot be used for regular user traffic:

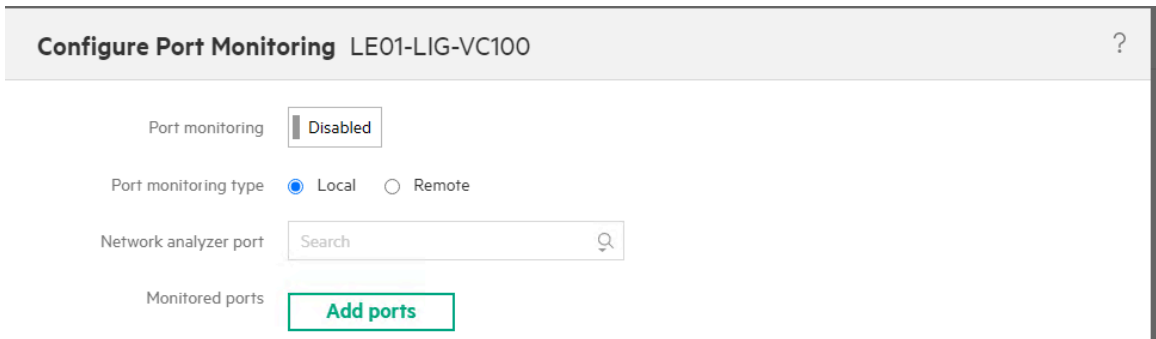


## Synergy Port Monitoring Configuration

Synergy port monitoring configuration is under **Networking / Logical Interconnects**. Users can select **Actions** from the top right corner and then select **Configure port monitoring**:



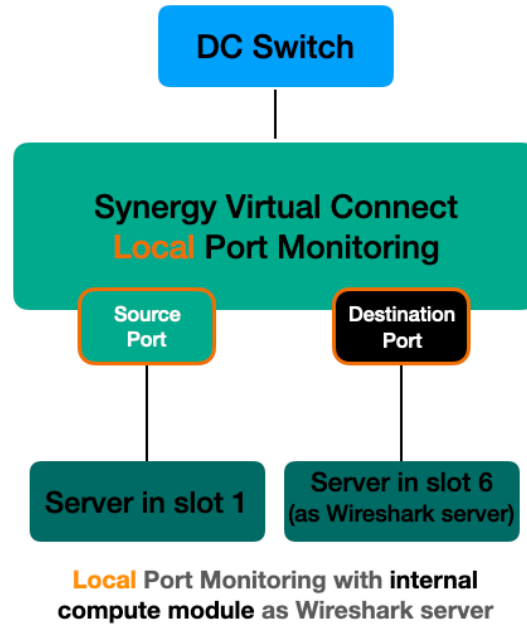
The following is the starting screen for port monitoring configuration:



## Configuring Synergy Local Port Monitoring

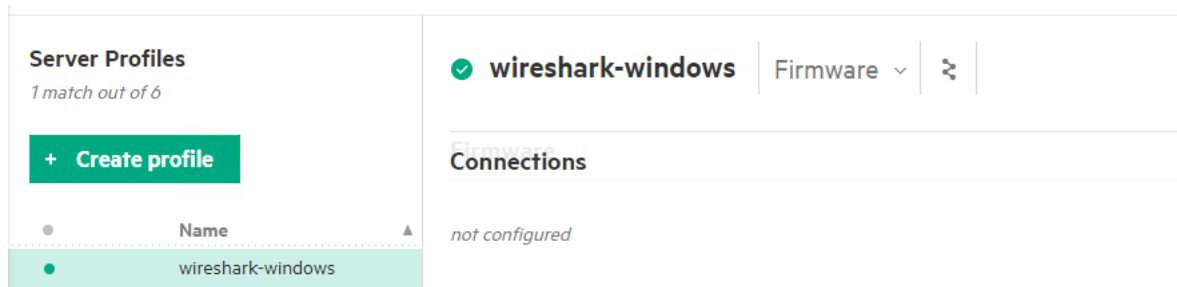
### Local Port Monitoring Using Internal Server

In this section, we configure a local port monitoring session to monitor the traffic from or to the compute module located in bay 1. The captured traffic is then sent to the Wireshark server located in bay 6:



In this use case, it's important to note that the server in slot 6, which is the Wireshark server, cannot have any server profile connections assigned to it. You have two options:

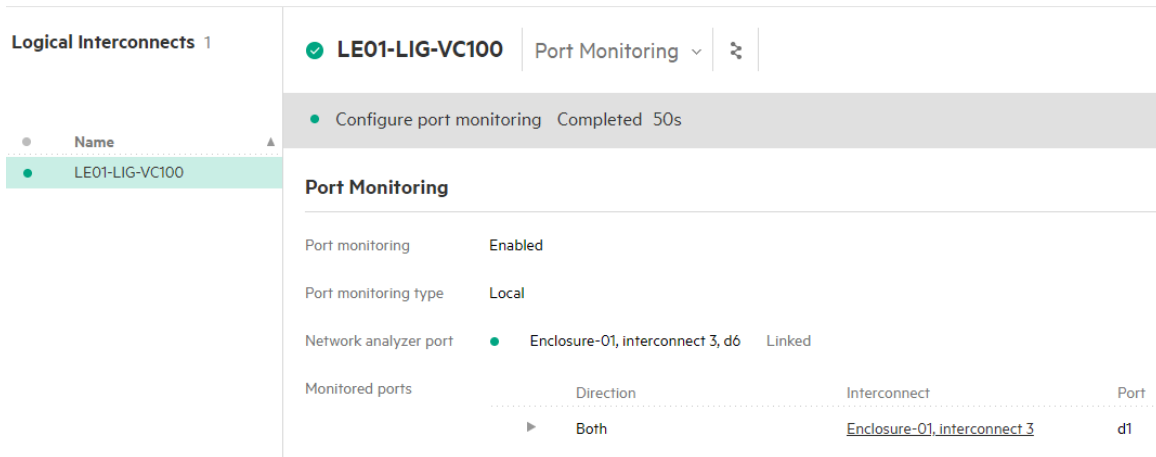
- You can choose not to assign any server profile to this server.
- Alternatively, you can assign a server profile to the Wireshark server, but make sure that the server profile does not have any "connections" configured like the screen capture below:



A typical server CNA adapter nowadays has two 10/20/25/50Gb physical ports. It's commonly referred as side A and side B for server network redundancy. HPE Synergy uses server profile "connections" to configure the network ports. Anytime a server profile connection is established to one of the physical ports on the adapter, all ports on that CNA adapter will change to "Flex Mode". The "Flex Mode" is the right configuration mode when the server is passing user data traffic.

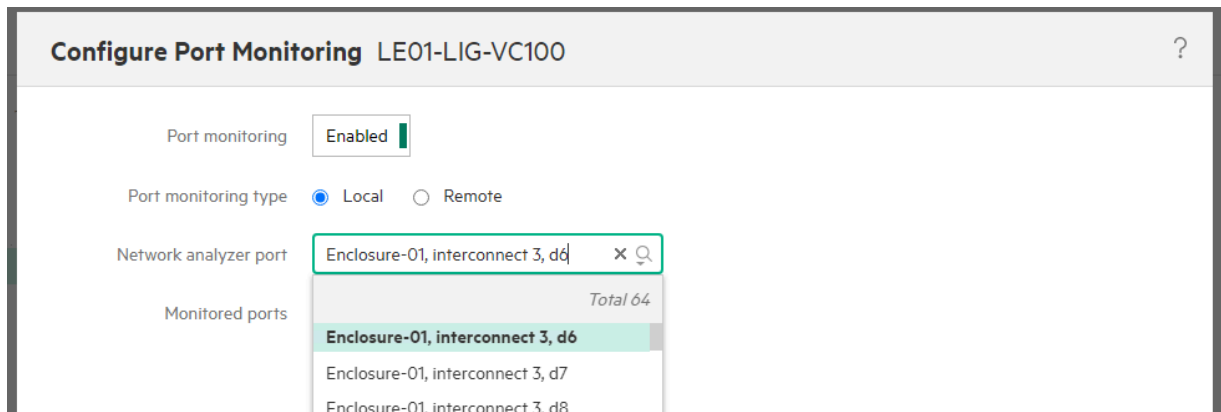
To leverage a server NIC for receiving captured traffic, the CNA adapter of the server must be in its original physical port format and not in "Flex mode". This requires ensuring that no server profile "connections" are assigned to the server's CNA adapter. In other words, either no server profile should be assigned to this server at all, or if a server profile is assigned, it should not have any connections configured for the server CNA adapter.

The completed local port monitoring configuration is as below:



The first step in the configuration is to select a network analyzer port, which is equivalent to a “SPAN destination port”.

Users will notice that the first available port displayed in the network analyzer's port drop-down list is labeled "d6". This port corresponds to the first physical port of the server located in bay 6. The reason why no ports from servers in bays 1 to 5 are listed as eligible network analyzer ports is because those servers are being utilized as regular compute nodes and have server profile connections assigned to them. These server ports are set to "Flex mode" and, as a result, cannot be used as network analyzer ports.



The next step is to select the specific server port that you want to monitor. In this scenario, both ports of the CNA for server 1 are chosen. These ports are identified as "d1" on Virtual Connect module 3 and module 6 respectively. By selecting these ports, you ensure that all traffic from this server is being monitored:

### Add Ports

1 selected

Interconnect	Port	Adapter Port	Server Hardware	Server Profile	Connection ID, Network/Network Set
Enclosure-01, interconnect 3	d1	Mezzanine 3, port 1	Enclosure-01, bay 1	aci-vc-tunnel-host1	1 ACI-Tunnel-Net 2 ACI-Tunnel-Net
Enclosure-01, interconnect 3	d2	Mezzanine 3, port 1	Enclosure-01, bay 2	aci-vc-tunnel-host2	1 ACI-Tunnel-Net 2 ACI-Tunnel-Net
Enclosure-01, interconnect 3	d3	Mezzanine 3, port 1	Enclosure-01, bay 3	aci-FM-host1	1 VLAN-160 2 VLAN-160 3 network-set-for-FM 4 network-set-for-FM

#### Configure Port Monitoring LE01-LIG-VC100

Port monitoring:  Enabled

Port monitoring type:  Local  Remote

Network analyzer port: Enclosure-01, interconnect 3, d6

Direction	Interconnect	Port
Both	Enclosure-01, interconnect 3	d1
Both	Enclosure-01, interconnect 6	d1

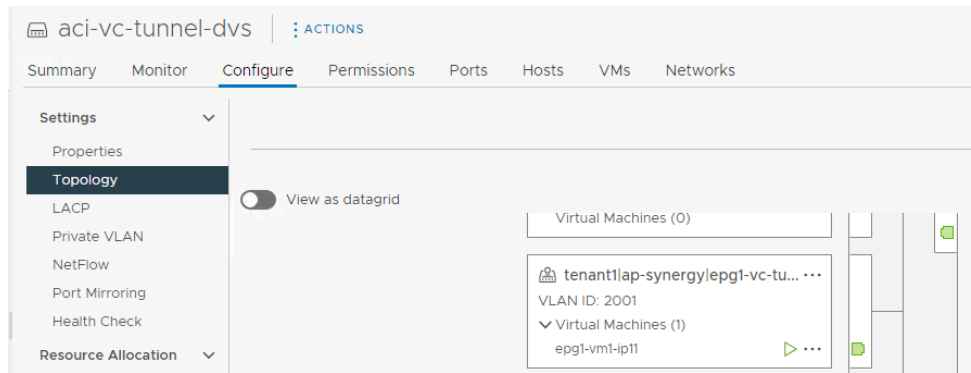
With the completed configuration shown above, here is the Wireshark screen capture for the server in bay 6 when an ESXi VM on the compute module in bay 1 sends ping requests to the internet:

\*PCIe Slot 3 Port 1

icmp and ip.addr==8.8.8.8

No.	Time	Source	Destination	Protocol	Length	Info
53	2.868644	192.168.13.11	8.8.8.8	ICMP	102	Echo (ping)
56	2.873928	8.8.8.8	192.168.13.11	ICMP	106	Echo (ping)
63	3.870487	192.168.13.11	8.8.8.8	ICMP	102	Echo (ping)
64	3.875838	8.8.8.8	192.168.13.11	ICMP	106	Echo (ping)

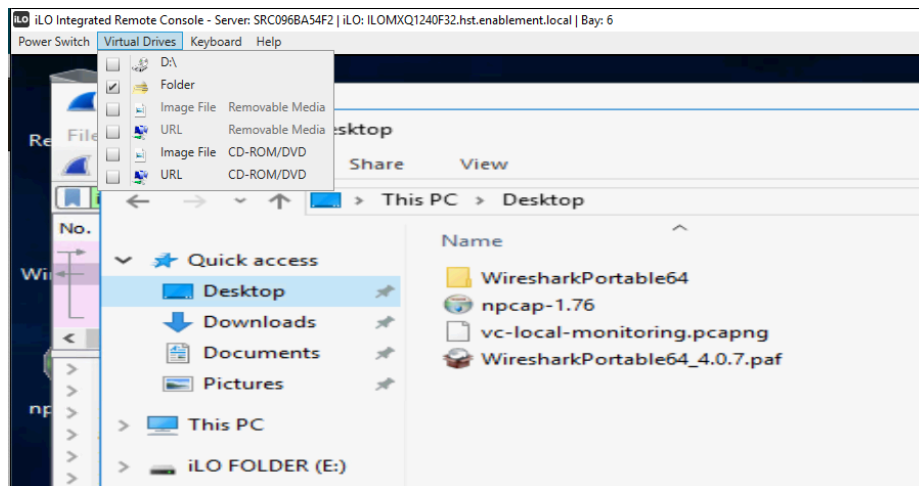
> Frame 53: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface  
 > Ethernet II, Src: VMware\_82:97:fd (00:50:56:82:97:fd), Dst: Cisco\_f8:19:ff (08:00:0c:27:f8:19)  
 > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2001  
 > Internet Protocol Version 4, Src: 192.168.13.11, Dst: 8.8.8.8  
 > Internet Control Message Protocol



The captured traffic from the monitored server using Synergy port monitoring shows that ICMP traffic is successfully captured, and the correct DVS port-group VLAN is verified in the captured traffic.

To transfer the capture files from the Wireshark server, users have two options. They can either use the iLO virtual folder or apply a standard server profile to the server. By applying a normal server profile, the NIC port on the server will be assigned a valid management IP address for file transfer. (Note that applying a profile does require the server to be powered down).

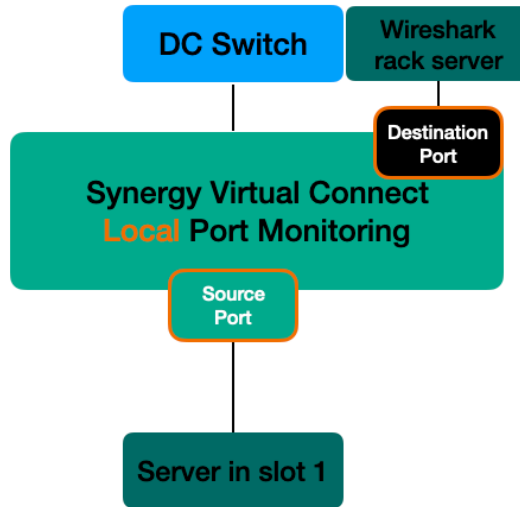
The following capture shows the utilization of the iLO virtual folder to transfer the captured file from the Wireshark server to a local destination:



**Note:** During this specific test, both the Wireshark Portable executable file and npcap-1.76 are used. It has been reported that npcap-1.70 may not function correctly when capturing traffic, whereas npcap-1.60 does not encounter this issue. The configuration details of Wireshark and npcap extend beyond the scope of this white paper, so users are advised to take note of this or consider alternative tools such as Linux TCPDUMP for capturing traffic.

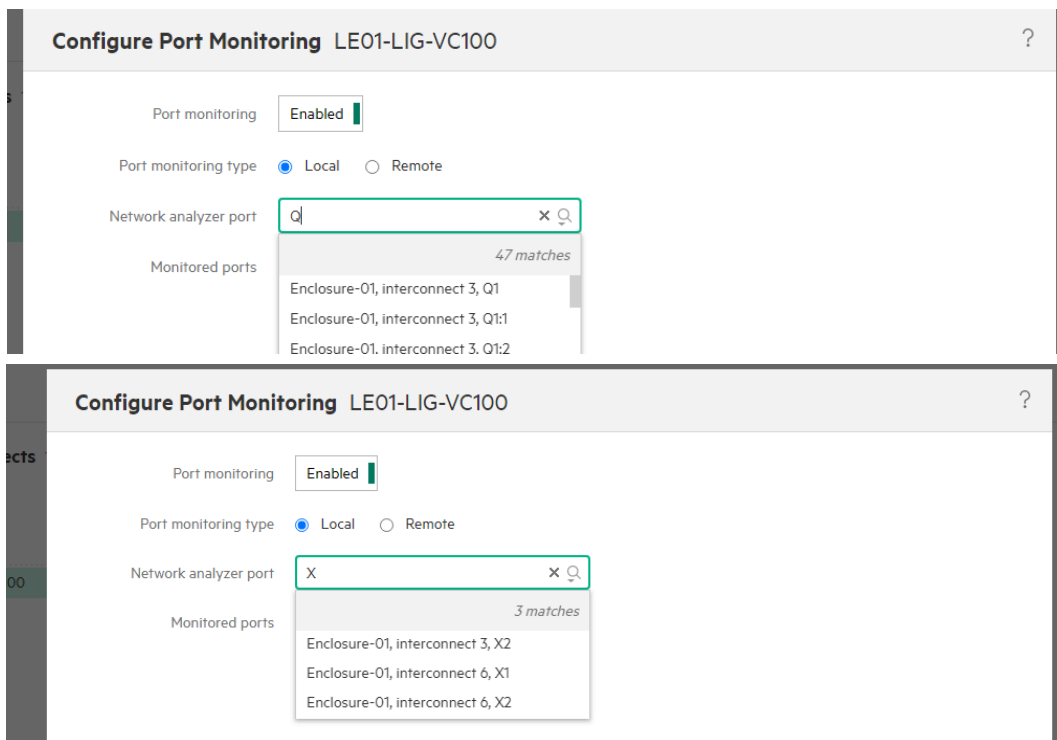
### Local Port Monitoring Using External Server

If users want to configure a local port monitoring session using an external server directly connected to Synergy Virtual Connect uplink as Wireshark server, the configuration flow remains the same as the use case above:



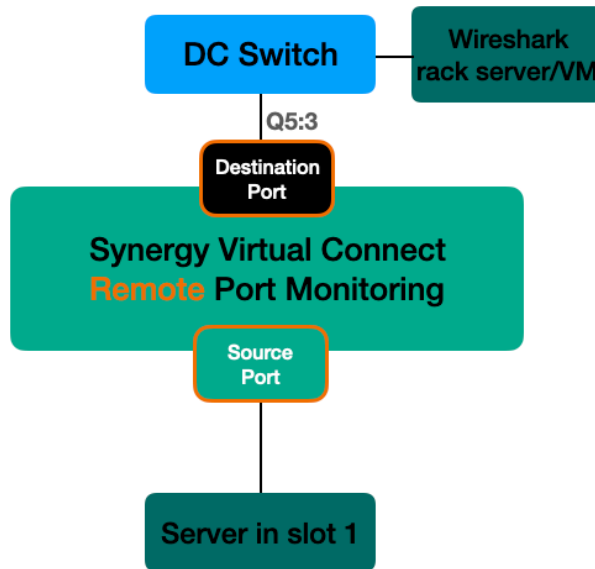
**Local Port Monitoring with external server as Wireshark server**

The only difference in the configuration is that users will now choose any available QSFP uplink ports or the newly supported X1/X2 ports (since HPE OneView 8.10) for the Network analyzer port:



### Configuring Synergy Remote Port Monitoring

In this section, we will set up a remote port monitoring session to monitor the traffic from/to the server in bay 1. The captured traffic will be sent to a Wireshark server that is connected to the Cisco ACI fabric:




---

**Note:** The uplink port used by Synergy remote port monitoring must be assigned to a dedicated ethernet shared uplink set. It is also important to note that this port cannot carry any regular user data traffic.

---

A complete Synergy remote port monitoring configuration is illustrated below:

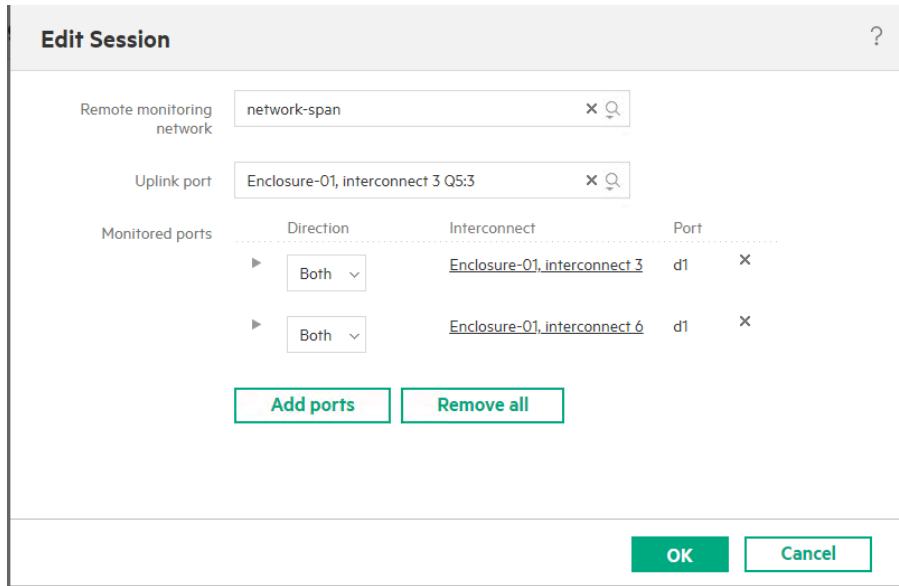
**Configure Port Monitoring** LE01-LIG-VC100 ?

Port monitoring  Enabled

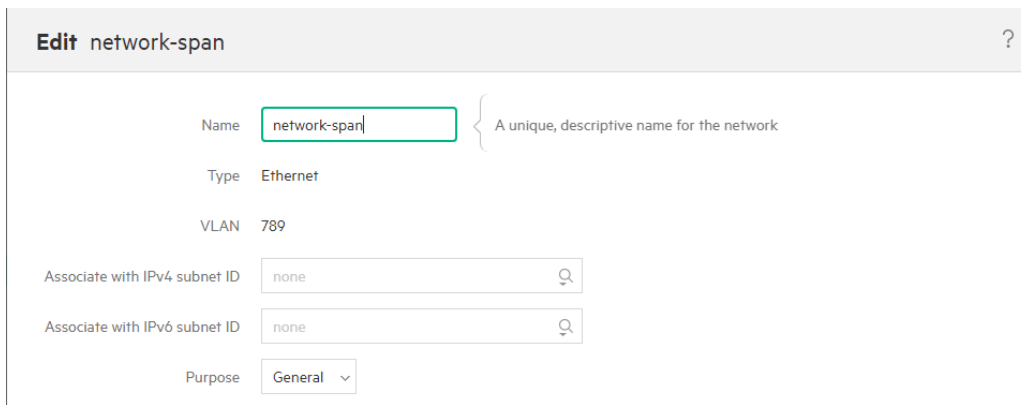
Port monitoring type Remote

Sessions	Remote Monitoring Network	Uplink Port
▶ network-span 789	● Enclosure-01, interconnect 3, Q5:3	Linked <span style="color: green;">✎</span> <span style="color: red;">✕</span>

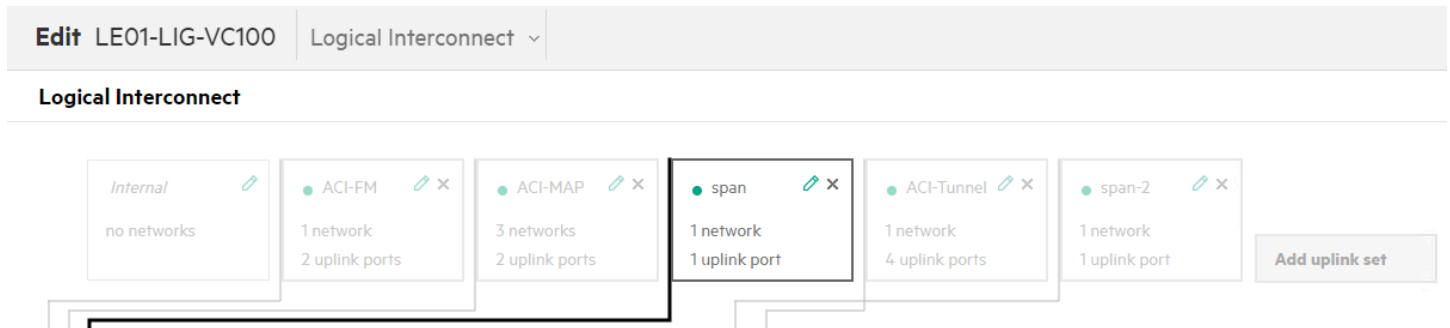
Add sessions
Remove all



First, users need to create a dedicated network for this remote port monitoring session. In this test, VLAN 789 is used:



Then users need to create an ethernet uplink set in the HPE Synergy Logical Interconnect. The uplink set will include the previous network defined and attach to the physical uplink to the upstream switch. In the screen capture below, the 10Gb uplink port Q5:3 on the HPE Virtual Connect module in slot 3 is selected:



**Edit span** General ?

ACP distribute uplink ports

### General

#### Networks

Name	Type	VLAN ID	Network Sets	Native
network-span	Ethernet	789		<input type="checkbox"/> x

*There are no available Ethernet networks to add.*

[Remove networks](#)

#### Network Sets

*There are no network sets available to add.*

#### Uplink Ports

Interconnect Module	Port	Capability	Speed	FEC Mode
Enclosure-01, interconnect 3	Q5:3	Ethernet + FCoE	Auto	Auto x

[Add uplink ports](#) [Remove uplink ports](#) [Remove all](#)

Users have the option to confirm the status of the uplink connectivity by accessing the HPE Synergy Interconnect section and also checking the upstream switch side. In this particular scenario, the HPE Synergy uplink is connected to a Cisco ACI fabric. The following captures show that the link is operational and actively exchanging LLDP (Link Layer Discovery Protocol) information:

**Interconnects** 2

- Enclosure-01, interconnect 3
- Enclosure-01, interconnect 6

**Enclosure-01, interconnect 3** Uplink Ports ?

#### Uplink Ports

Q5:2	Ethernet	Linked active	10	ACI-MAP
Q5:3	Network analyzer	Linked active	10	span

▶ Connector  
▶ Digital diagnostics  
▼ Remote connection

Type	Port ID type	Port ID	Port description
External	Local	Eth1/8	topology/pod-1/paths-101/patchep-[eth1/8]

System name: hst-acleaf-01  
System description: topology/pod-1/node-101  
System capabilities: Bridge, Router  
Chassis ID: 78:0c:f0:7d:8a:c6  
Chassis ID type: macAddress

```

hst-aciapic-01# fabric 101 show lldp neigh int eth1/8 det
-----
Node 101 (hst-acileaf-01)
-----
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf      Hold-time  Capability  Port ID
-----
Chassis id: 2200.a3e0.0003
Port id: ethernet0/0/5:3
Local Port id: Eth1/8
Port Description: Ethernet Interface Port 120
System Name: LE01-LIG-VC100
System Description: VC SE 100Gb F32 Module, Software Version 2.6.0-1001
Time remaining: 54 seconds
System Capabilities: not advertised
Enabled Capabilities: not advertised
Management Address: 10.16.41.25
Vlan ID: not advertised

Total entries displayed: 1

```

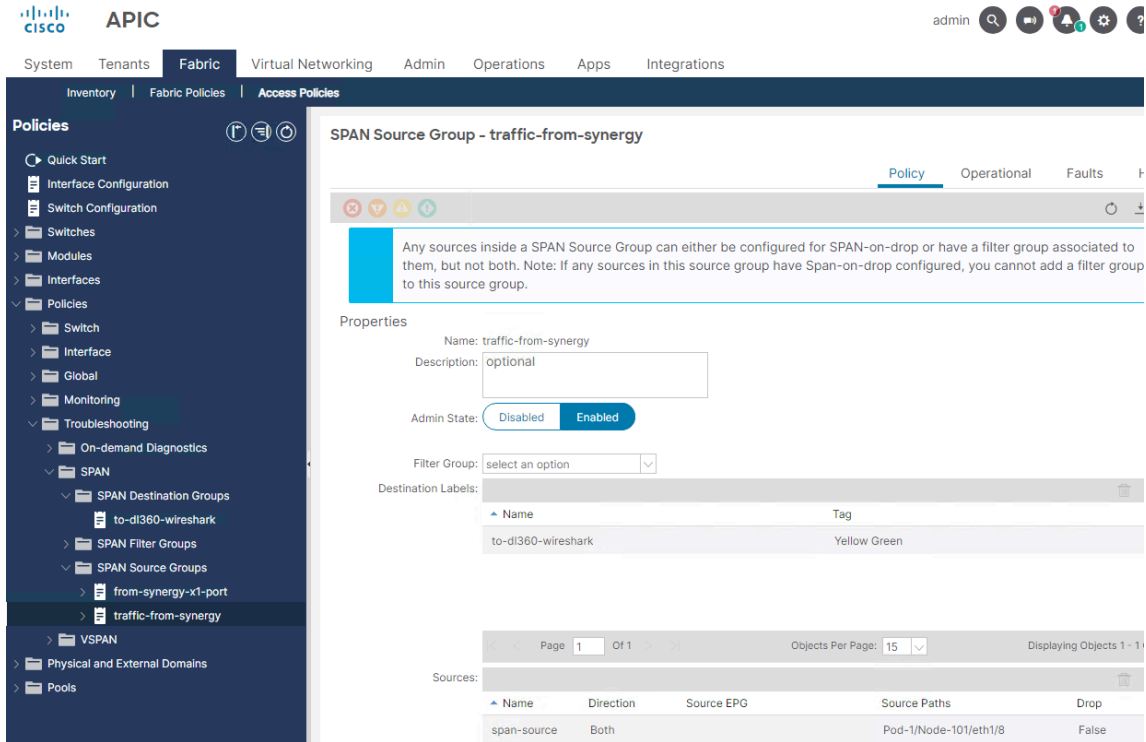
Once the captured packets reach the switch port, network administrators have the ability to set up a SPAN (Switch Port Analyzer) session on the switch side. This allows them to direct the traffic towards the designated Wireshark VM/server for further analysis. In this particular setup, ACI Access ERSPAN is configured to forward the traffic to the IP address of the Wireshark server.

In the captures below, ACI access policies for source and destination groups are shown. The traffic was captured from leaf switch 101 eth1/8 (connected to HPE Virtual Connect uplink port Q5:3) and then forwarded to the Wireshark server 10.16.160.15.

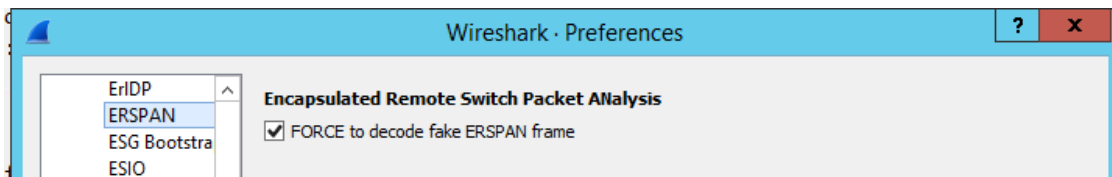
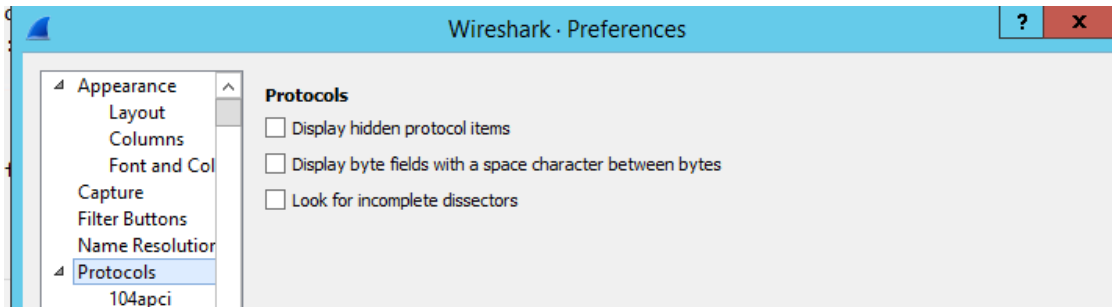
The screenshot displays the Cisco APIC (Application Policy Infrastructure Controller) web interface. The navigation menu on the left shows the path: Policies > Troubleshooting > SPAN > SPAN Destination Groups > to-dl360-wireshark. The main content area shows the configuration for the 'SPAN Destination Group - to-dl360-wireshark'.

**Properties:**

- Name: to-dl360-wireshark
- Description: optional
- Destination EPG: uni/tn-tenant1/ap-ap-mgmt/epg-mgmt-epg
- SPAN Version: Version 1 (selected), Version 2
- Enforce SPAN Version:
- Destination IP: 10.16.160.15
- Source IP/Prefix: 10.16.160.100
- Flow ID: 1
- TTL: 64
- MTU: 1518
- DSCP: Unspecified



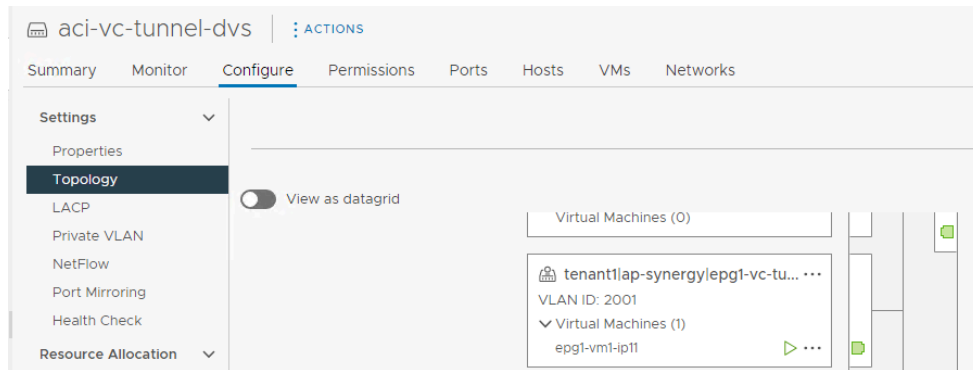
In Wireshark server, the Wireshark preference for ERSPAN protocol may need to be set as below to view the decoded packets:



The screenshot displayed on the Wireshark server shows the packet capture when an ESXi virtual machine on the Synergy compute module sends ping requests to the internet. By examining the captured packets, users can observe that the original ICMP packets are encapsulated within Cisco ACI Access ERSpan GRE and Synergy remote port monitoring headers. Additionally, the capture also confirms the presence of the original DVS (Distributed Virtual Switch) port-group user VLAN 2001.

No.	Time	Source	Destination	ERSpan.vlan	VLAN ID	Protocol	Length	Info
→ 183	19:01:46.198960	192.168.13.11	8.8.8.8		2001	ICMP	152	Echo (ping) request
← 189	19:01:46.204478	8.8.8.8	192.168.13.11		2001	ICMP	152	Echo (ping) reply
270	19:01:47.200135	192.168.13.11	8.8.8.8		2001	ICMP	152	Echo (ping) request
272	19:01:47.205502	8.8.8.8	192.168.13.11		2001	ICMP	152	Echo (ping) reply
305	19:01:48.202114	192.168.13.11	8.8.8.8		2001	ICMP	152	Echo (ping) request
307	19:01:48.207473	8.8.8.8	192.168.13.11		2001	ICMP	152	Echo (ping) reply

Frame 183: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0  
 Ethernet II, Src: Cisco\_f8:19:ff (00:22:bd:f8:19:ff), Dst: HewlettP\_10:d9:e0 (38:ea:a7:10:d9:e0)  
 Internet Protocol Version 4, Src: 10.16.160.100, Dst: 10.16.160.15  
 Generic Routing Encapsulation (ERSpan) ← Cisco ACI GRE/ERSpan header  
 Encapsulated Remote Switch Packet Analysis  
 Ethernet II, Src: Vmware\_82:97:fd (00:50:56:82:97:fd), Dst: Cisco\_f8:19:ff (00:22:bd:f8:19:ff)  
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 789 ← Synergy Remote Port Monitoring encapsulation VLAN  
 IEEE 802.1ad, ID: 2  
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2001 ← User host ESXi DVS port-group VLAN  
 Internet Protocol Version 4, Src: 192.168.13.11, Dst: 8.8.8.8  
 Internet Control Message Protocol



**Note:** HPE OneView for Synergy supports maximum 60 mirrored downlink ports per Logical Interconnect since [release 5.20](#). This is applicable to both local port mirroring and remote port mirroring. In addition, a maximum 4 remote port monitoring sessions per Logical Interconnect is supported. Users can refer to the HPE OneView user guide at the end of this white paper for more details.

## Resources and additional links

For additional descriptions of HPE Synergy port monitoring, see:

[HPE OneView 8.5 User Guide for HPE Synergy](#)

To help us improve our documents, please provide feedback at [hpe.com/contact/feedback](https://hpe.com/contact/feedback).

## Learn more at

[hpe.com](https://hpe.com)

---

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Trademark acknowledgments, if needed. All third-party marks are property of their respective owners.



a00140906ENW