# VIAVI Solutions

# QUICK CARD

# **Ethernet Packet Capture and Protocol Analysis**

This quick card describes how to set up the OneAdvisor 800 to capture and analyze live, in-service network traffic from a **TAP** (Test Access Point) or **SPAN** (Switch Port Analyzer) port on an Ethernet switch. A TAP is a passive optical splitter used to provide a monitor point for packet capture and protocol analysis. A SPAN port is a spare switch port configured to transmit a copy of the packets sent or received on another switch port. It allows the OneAdvisor to receive and analyze all network traffic, without being physically attached to that port. Bidirectional Traffic can be transmitted to the OneAdvisor on a single RJ-45, SFP, or QSFP port. The quick card documents a procedure to set up the OneAdvisor on a 1GigE Interface utilizing IPv4 address filters, but the same workflow may be applied to other data rates and filters.

### EQUIPMENT REQUIREMENTS

- OneAdvisor 800 equipped with the following:
  - RAxxMA-O Radio Analysis Module, SPA06MA-O Spectrum Analyzer Module, TM400GB-QQ 400G Module, or TM400GB-QO 400G Module.
  - Transport software release V5.1.0 or greater
  - CA10M1GE or ONA-SP-10M1GE
  - 1 Gigabit Ethernet option • CA10GCAPTURE or ONA-SP-1GECAP
  - 1 Gigabit Ethernet Capture option
- Optical Transceiver supporting the Ethernet Interface type to be tested (SFP, QSFP)
- SPAN port or Optical TAP (Observer nTAP)
- Cables to match the optical transceiver and the TAP or SPAN port
- Fiber optic inspection microscope (P5000i, FiberChek Probe, or INX-760)
- Fiber optic cleaning supplies

### LAUNCH TEST

- 1. Press the Power button on the ONA-800 base top panel to turn on the OneAdvisor.
- 2. Tap fr Home to display the Home Screen.
- 3. Tap 🛃 Tests to display the Tests menu.
- Tap Radio Analysis Transport > or
   400G Transport > to show the Transport test application.
- 5. Tap the Transport icon.









Figure 1: Equipment Requirements



### LAUNCH TEST (Continued)

- If the Select Test menu is not displayed, tap
   All Tests in the lower left screen corner.
- 7. Using the Select Test menu or favorite test list, launch the Ethernet Traffic test for the desired data rate. For example: Ethernet ▶1GigE Optical ▶ Layer 3 Traffic ▶IPv4 ▶P1 Terminate.
  - ► Note: Launch a Layer 3 Traffic ► IPv6 test if you wish to filter using IPv6 addresses. Launch a Layer 2 Traffic test if you do not require IP filters (TOS/DSCP, Protocol, or Source/Destination IP Address)

### CONFIGURE TEST

- 1. Insert desired transceiver into the Port 1 SFP or QSFP slot on the top of the ONA-800.
- 2. Tap the **Setup** soft key on the top right side of the screen.
- 3. Select the Interface/Connector folder.
- 4. Review SFP information:
  - Verify that the SFP operates on the correct wavelength (850nm, 1310nm, etc.).
  - Verify that the SFP supports the required data rate (1G, 10G, etc.)
- 5. Select the **Ethernet** folder.
  - If you are running a Layer 3 Traffic
     IPv4 tests, set ARP Mode to
     Disabled.
- 6. Select the **Capture** folder.
  - Set the desired Capture Buffer size (1 to 8MB)
  - Optionally set Capture frame slicing to 64 Bytes, 128Bytes, of 256 Bytes to conserve buffer space.



Figure 3: Select Test



Figure 4: Setup, Interface/Connector

🟫 Home 🛛 🔛 400G Tra	nsport 🗙				📃 🛃 📣 🦎	* 🛷 🚺	2 5:42 PN
Select ~ Port 1: 10/10	0/1000 Eth Layer 3 Traffic Te	rm × +			What's This?	1	
Interface Ethernet	Encapsulation	None	\$				Results
	ARP Mode	Disabled	\$				
Traffic	Frame Type	DIX	•				
Capture	Length Type	Packet Length	¢ Calc. F	acket Length (Bytes) 46			
Filters Timed Test	DA	SA	Туре	Data		FCS	

#### Figure 5: Setup, Ethernet

Test Port 1: 1G	ge Layer 2 traffic term 🗙 📕 🕂		what's This?	1 1 1
Interface	Capture buffer size (MB)		Results	
Ethernet Traffic	Capture frame slicing	None	•	
Capture	When capture buffer is filled	StoptCapture	•	
	Include frames from Traffic tab		\$	
Service Disruption	Use Filters as	Filter	\$	-
Timed Test	NOTE: Filter or Trigger settings can be configu NOTE: Changing buffer size or frame slicing w	red on the Filters tab. ill stop capture and delete capture data	3.	

#### Figure 6: Setup, Capture



### CONFIGURE TEST (Continued)

- 7. Select the **Filters** folder.
  - In Summary settings, set Filter Mode to Detailed.
  - > Ethernet settings:
    - For MAC Address Filters, tap DA or SA field and enter address type and MAC Address.
    - For VLAN filters, set Encapsulation to VLAN, tap the VLAN field and enter VLAN ID and Priority.
    - For Ethertype filters, tap the Type field and enter an Ethertype.
  - > In IP settings:
    - For IP Filter, set IP Filter to Enable and set Address Filter to Single Direction or Either Direction.
    - Tap TOS/DSCP, Protocol, Source IP Address, and Destination IP Address fields. Tap the check box to enable the filter and enter desired values.
  - In Payload settings, turn Payload Analysis off.
- 8. Tap the **Results** soft key.
- Set the right Results Window to display Ethernet/Capture results. Swipe up to view and select Capture.



#### Figure 7: Setup, Filters/Summary



#### Figure 8: Setup, Filters/Ethernet



#### Figure 9: Setup, Filters/IP



#### Figure 10: Setup, Payload Analysis

Running 5m:18s	Ethernet Payload			-	
i message	On + Traffic +	192.168.1.2	46 :		
Ethernet Chernet nc Acquired	Summary	Status	Packet Size	Ethernet	Capture + +
k-Actor k-Actor Packat Period ANF France Detect Cale of YL-W Detect Story	Sync Acquired Link Active Sync Loss Seconds Link Loss Seconds		0FF 0FF 318 318	Packets Processed Packets Captured Capture Progress %	L3 Link Stats L3 Link Counts L3 Filter Stats L3 Filter Stats L3 Config Status BERT Stats Error Stats Capture LLDP Stats AutoNeg Status
	Actions Peak IFG	Errors C	apture		

Figure 11: Results



### CAPTURE PACKETS

- 1. For Optical TAPs and Optical SPAN Ports:
  - Use the VIAVI P5000i, FiberChek Probe, or INX 760 microscope to inspect both sides of all connections (SFP, patch cables, and bulkheads)
    - Focus the fiber on the screen.
    - If it appears dirty, clean the fiber end-face and re-inspect.
    - If it appears clean, run the inspection test.
    - If it fails, clean the fiber and re-run the inspection test. Repeat until it passes.
  - > If you are using an optical SPAN port:
    - Connect the OneAdvisor SFP to the SPAN port using a duplex LC patch cable.
    - Select the Laser tab in the Actions panel.
       Press off
       The button will turn yellow and be relabeled
  - If you are using an optical TAP, connect the Rx side of the OneAdvisor SFP to the TAP using a simplex LC patch cable.
- 2. For Copper TAPs and Copper SPAN Ports:
  - Connect the OneAdvisor Copper SFP to the SPAN port using CAT5E or better cable for 1G, CAT6A or better cable for 10G.
- 3. Press the **Restart** soft key.
- 4. Verify the following:
  - **Summary** LED is green.
  - Sync Acquired LED is green.
  - Link Active LED is green.
  - Frame Detect is green.
- 5. Selection Start Capture tab in the Actions panel, and press Capture. The button will turn yellow and be relabeled Started.
- 6. When the desired capture per of packets have been processed, press to stop packet capture to stop packet capture.



Figure 12: Inspect Before You Connect

Running 2m:18s	Ethernet Bauland			
ending ARP request fo	On         Traffic         0         0 (lowest)         *           Auto Neg.         Test Mode         VLAN ID         Priority	192.168.1. Destination	11 Ping 46 + Packet Size	
red Dev (ppm) 23.1	Summary ‡ Status	•	Summary \$ SLA	/ KPI 🗢
A grant Answer A grant Answer I and Answer A start Answer I and Answ	Acterna lest raceet uenet	014	Infroughput, Current B RX Maps, L1 Tx Maps, L2 Tx Maps, L2 Tx Maps, L2 Rx Maps, L3 Trame Loss -RR B Lost Frame Loss Ratio Romal Trip Deby - FD (us) B Average Current Maximum	Unavailable Unavailable Unavailable Unavailable Unavailable Unavailable Unavailable Unavailable
			(@   @ )	
	Laser Actions Peak IFG Errors	Capture		
7 📺 🛄 ?	Laser Internal +1 +1 Clock Source Free Off	-10	+10	



Figure 14: Start Capture



## PROTOCOL ANALYSIS

 Press Save Capture Buffer
 Ensure "Launch Wireshark after saving" is checked and press Save to save the PCAP (Packet CAPture) file to the /user/bert/capture folder of the OneAdvisor hard drive.



Figure 15: Save Capture File

2. View and analyze the packet capture using WireShark.

Note: Go to <u>https://www.wireshark.org</u> for information and tutorials on WireShark.

3. Tap <u>File and Quit in the Wireshark menu bar to</u> return to the OneAdvisor test results.

📩 Home 🔛 400G Transport 📶	📑 📣 🦘 🚾 11:18 AM						
Elle <mark>1</mark> 5t <u>V</u> iew <u>Go</u> <u>Gapture</u> <u>Analyze</u> <u>Statistics</u> Telephony <u>Wireless</u> <u>Tools</u> <u>H</u> elp							
📶 ₫ ම 🚍 🗋 🕱 🗳 ۹. 🖛 🛸 🖀 7. 🖢 🛄 🔍 ۹. ۹. ۹. 11							
Apply a display filter «Ctrl-/>	💶 v +						
No. Time Source Destination Protocol Length Info							
□ 10.000000 192.168.1.135 20.127.250.238 TCP 64 61105 - 443	[ACK] Seq=1 Ack=1 Win=1028 Len=1 [TCP segme						
2 0.058347 20.127.250.238 192.168.1.135 TCP 70 443 → 61105	[ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2						
3 0.804028 192.168.1.135 208.67.222.222 UDP 242 49858 → 443	Len=196						
4 0.804308 192.168.1.135 208.67.222.222 UDP 242 49859 → 443	Len=196						
5 0.823083 192.168.1.135 52.87.138.107 TCP 70 61689 → 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256						
6 0.826638 208.67.222.222 192.168.1.135 UDP 350 443 → 49859	Len=304						
7 0.826666 208.67.222.222 192.168.1.135 UDP 414 443 → 49858	Len=368						
8 0.870354 52.87.138.107 192.108.1.135 TUP 70 443 → 01089	[STN, ACK] SEG=0 ACK=1 WIN=20003 LEN=0 MSS=						
9 0.0/103/ 192.100.1.135 52.0/.130.10/ TUP 04 01009 → 443	[ACK] SEQ-1 ACK-1 WIN-202050 LEN-0						
Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface rx, id 0							
Ethernet II. Src: Dell fd:1c:fe (38:14:28:fd:1c:fe), Dst: BelkinIn 76:44:ff (e8:9f:80:76:44:ff)							
- Internet Protocol Version 4, Src: 192.168.1.135, Dst: 20.127.250.238							
0100 = Version: 4							
0101 = Header Length: 20 bytes (5)							
<ul> <li>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)</li> </ul>							
Total Length: 41							
Identification: 0x90eb (37099)							
> Flags: 0x40, Don't fragment							
Fragment Offset: 0							
Time to Live: 128							
Protocol: TCP (6)							
Header Checksum: 0x9846 [validation disabled]							
[Header checksum status: Unverified]							
Source Address: 192.168.1.135							
Destination Address: 20.127.250.238	d table d table d						
, Transmission control Protocol, SFC Port: 61105, DSt Port: 443, Seq	* 1, ACK: 1, Len: 1						
0000 e8 9f 80 76 44 ff 38 14 28 fd 1c fe 08 00 45 00 ··· vD·8· (	••••E•						
dara da 5a aa 6D 4a da 8a ao 28 4o Ca 98 ar 8\ r4 \L \)							
Ø 2 VIAVI_2024_07_13_11_05_32_1000M.pcap	Packets: 937 · Displayed: 937 (100.0%) Profile: Default						

Figure 16: WireShark