Monitor Capture Overview

Monitor Capture is a tool that can assist with verifying new traffic configurations or assist in trouble shooting.

The Monitor Capture tool supports the following capabilities:

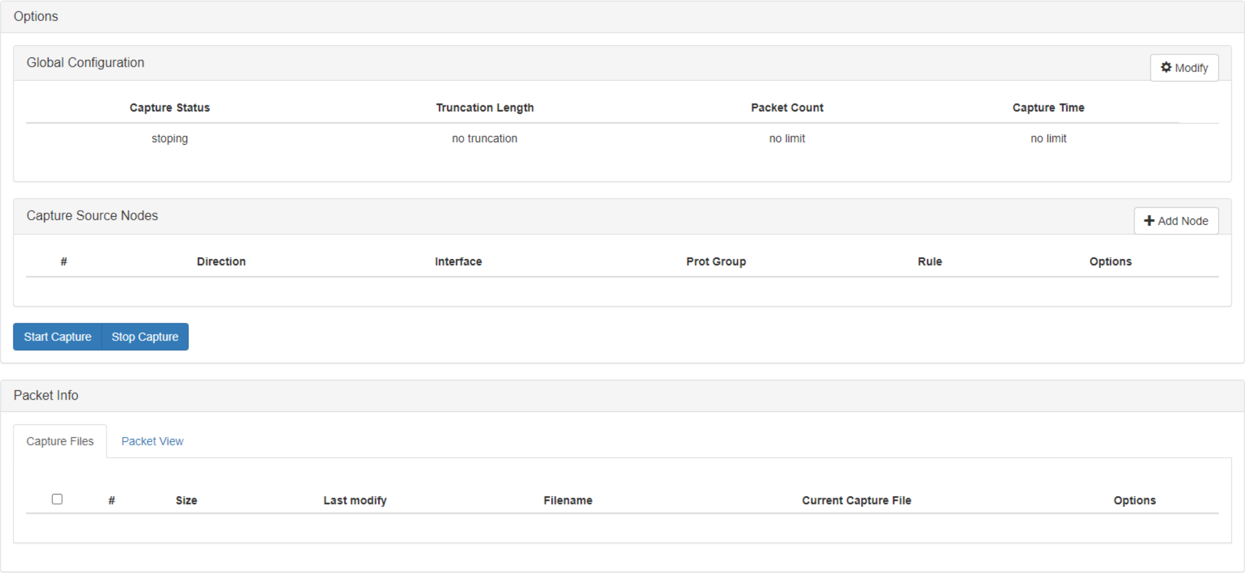
- The monitor capture tool requires a TAP Group to be created
- Supports truncation, 64 to 144 bytes
- Supports packet count
- Support capture time
- Ingress packet capture options
    - A flow may be applied to filter the captured packets
    - A single port or group of ports may be selected
    - A link aggregation group may be selected
    - A port group may be selected.
- Egress packet capture options
    - An ACL may be applied to filter the captured packets
    - A single port or group of ports may be selected
    - A link aggregation group may be selected
- The monitor capture tool must be manually started
- The monitor capture tool must be manually stopped
- A txt file is created to view the last 1000 captured packets
- A pcap file may be created from the txt file

Monitor Capture Setup

1. Select tools.

2. Select Monitor Capture.

The Options panel will be displayed.



Options

Global Configuration

Capture Status	Truncation Length	Packet Count	Capture Time
stoping	no truncation	no limit	no limit

Capture Source Nodes

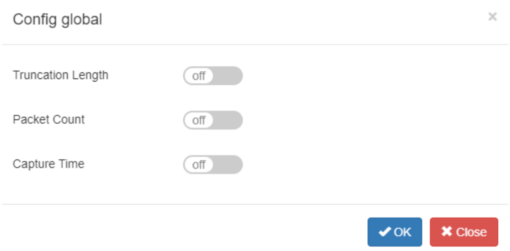
#	Direction	Interface	Prot Group	Rule	Options

Packet Info

☐	#	Size	Last modify	Filename	Current Capture File	Options

3. Select the Global Configuration Modify.

The Config global panel will be displayed. The defaults may be used if desired.



Config global

Truncation Length off

Packet Count off

Capture Time off

4. Truncation Length enable

5. If enabled, enter the truncation length, 64 to 144 bytes.

6. Packet Count enable

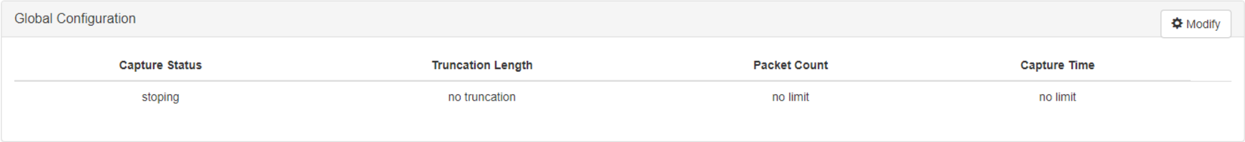
7. If enabled, enter the number, 1 to 1000 packets.

8. Capture Time enable

9. If enabled, enter the number, 1 to 120 seconds.

10. Select OK.

The Global Configuration options will be displayed

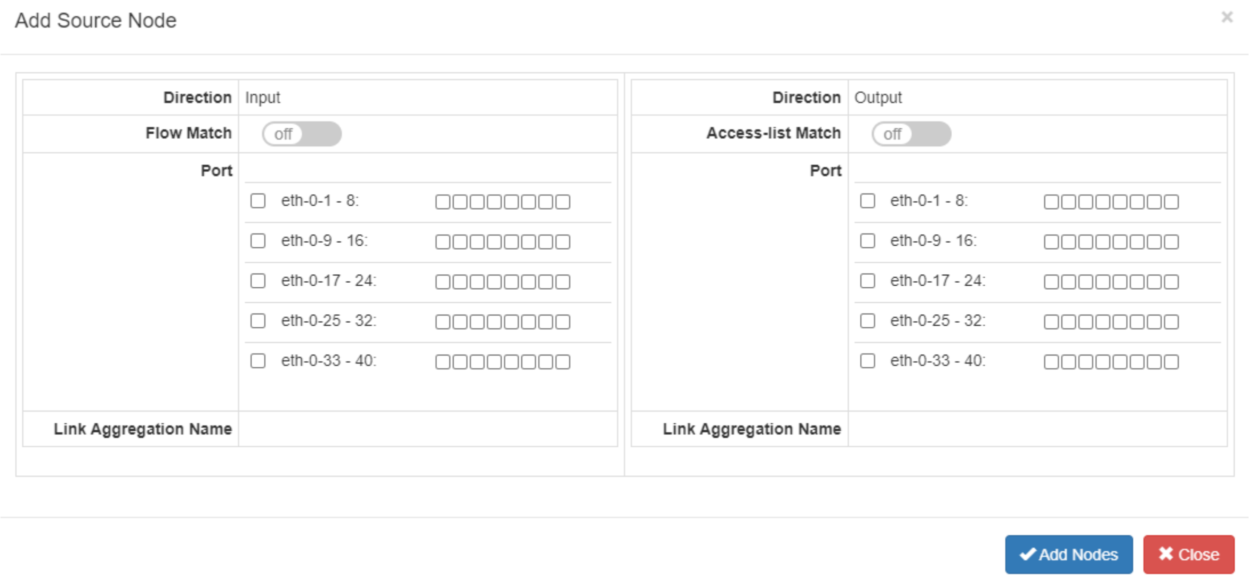


Global Configuration

Capture Status	Truncation Length	Packet Count	Capture Time
stoping	no truncation	no limit	no limit

11. Select the Capture Source Nodes + Add Node.

The Add Source Node panel will be displayed



Add Source Node

Direction	Input	**Direction**	Output
Flow Match	off	**Access-list Match**	off
Port	☐ eth-0-1 - 8: □□□□□□□□ ☐ eth-0-9 - 16: □□□□□□□□ ☐ eth-0-17 - 24: □□□□□□□□ ☐ eth-0-25 - 32: □□□□□□□□ ☐ eth-0-33 - 40: □□□□□□□□	**Port**	☐ eth-0-1 - 8: □□□□□□□□ ☐ eth-0-9 - 16: □□□□□□□□ ☐ eth-0-17 - 24: □□□□□□□□ ☐ eth-0-25 - 32: □□□□□□□□ ☐ eth-0-33 - 40: □□□□□□□□
Link Aggregation Name		**Link Aggregation Name**	

Ingress Entities

12. Flow Match — enable, optional

13. Flow — Select the desired flow
 Must be previously created

14. Port — Select the desired port(s)
 A TAP group must be previously created

15. Link Aggregation Name — Select the desired link aggregation group
 Must be previously created

16. Port Group — Select the desired port group
 Must be previously created.

Egress Entities

17. Access-list Match — enable, optional

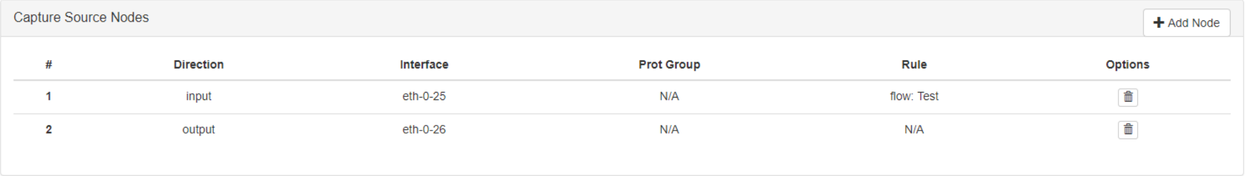
18. Access-list — Select the desired access list
 Must be previously created

19. Port — Select the desired port(s)
A TAP group must be previously created

20. Link Aggregation Name — Select the desired link aggregation group
Must be previously created

21. Select Add Nodes.

The Capture Source Nodes will be displayed



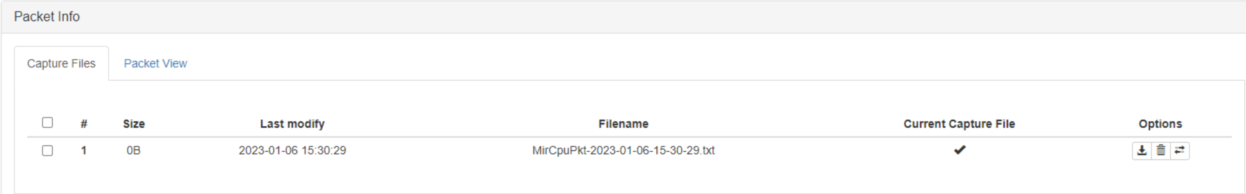
Capture Source Nodes

#	Direction	Interface	Prot Group	Rule	Options
1	input	eth-0-25	N/A	flow: Test	🗑
2	output	eth-0-26	N/A	N/A	🗑

22. Select the Trash Can in the Options column to delete a node.

23. Select Start Capture.

The Packet Info panel will display the txt file. A (check) will be displayed indicating the Current Capture File

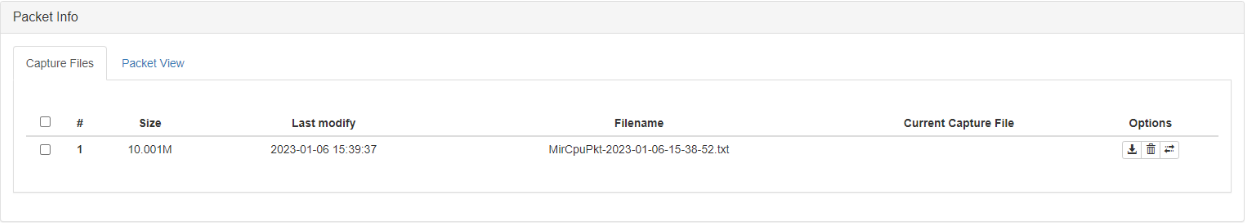


Packet Info

□	#	Size	Last modify	Filename	Current Capture File	Options
□	1	0B	2023-01-06 15:30:29	MirCpuPkt-2023-01-06-15-30-29.txt	✔	⬇ 🗑 ⇄

24. Select Stop Capture.

The Packet Info panel will display the txt file. A (check) will not be displayed indicating the Current Capture File



Packet Info

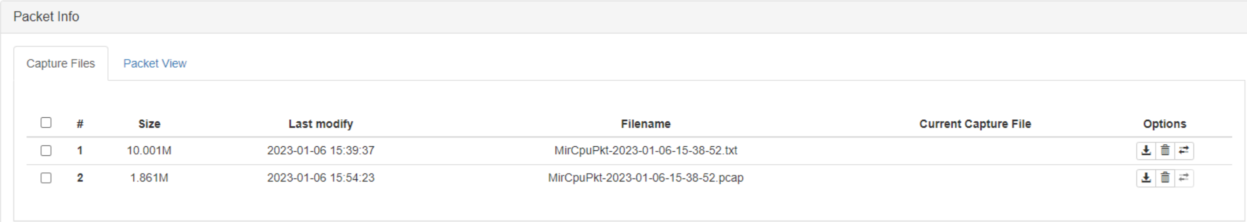
□	#	Size	Last modify	Filename	Current Capture File	Options
□	1	10.001M	2023-01-06 15:39:37	MirCpuPkt-2023-01-06-15-38-52.txt		⬇ 🗑 ⇄

25. Select Download in the Options column to download the txt file.

26. Select Trash Can in the Options column to delete the txt file.

27. Select Convert to pcap in the Options column to create a pcap file.

The Packet Info panel will display the pcap file



Packet Info

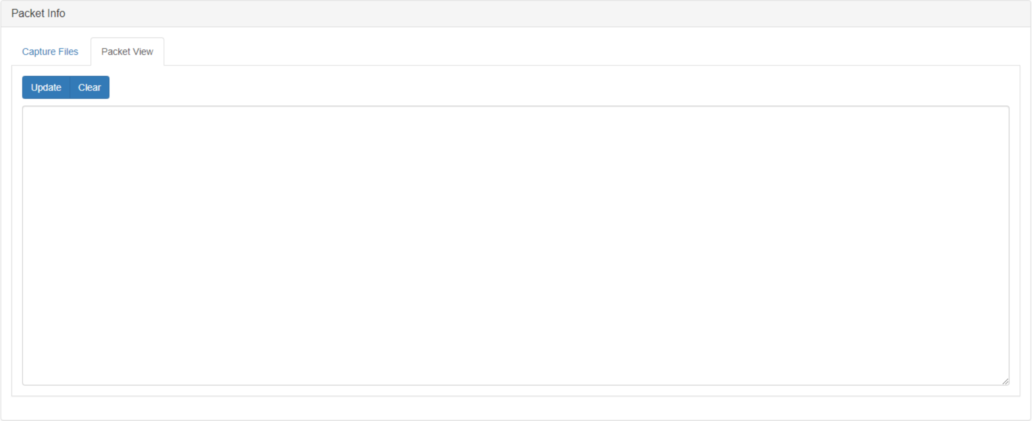
□	#	Size	Last modify	Filename	Current Capture File	Options
□	1	10.001M	2023-01-06 15:39:37	MirCpuPkt-2023-01-06-15-38-52.txt		
□	2	1.861M	2023-01-06 15:54:23	MirCpuPkt-2023-01-06-15-38-52.pcap		

28. Select Download in the Options column to download the pcap file.

29. Select Trash Can in the Options column to delete the pcap file.

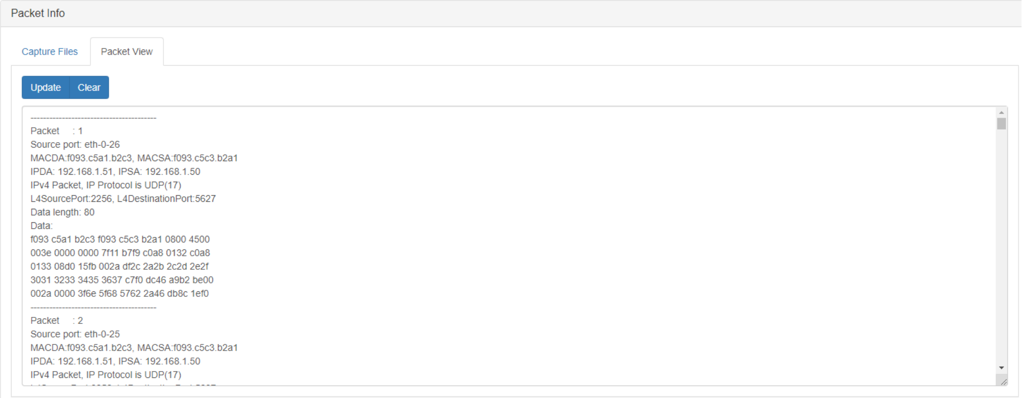
30. Select Packet View Tab.

The Packet View panel will be displayed



31. Update.

The Packet View panel will display the latest packets.



```
----------------------------------------
Packet     : 1
Source port: eth-0-26
MACDA:f093.c5a1.b2c3, MACSA:f093.c5c3.b2a1
IPDA: 192.168.1.51, IPSA: 192.168.1.50
IPv4 Packet, IP Protocol is UDP(17)
L4SourcePort:2256, L4DestinationPort:5627
Data length: 80
Data:
f093 c5a1 b2c3 f093 c5c3 b2a1 0800 4500
003e 0000 0000 7f11 b7f9 c0a8 0132 c0a8
0133 08d0 15fb 002a df2c 2a2b 2c2d 2e2f
3031 3233 3435 3637 c7f0 dc46 a9b2 be00
002a 0000 3f6e 5f68 5762 2a46 db8c 1ef0
----------------------------------------
Packet     : 2
Source port: eth-0-25
MACDA:f093.c5a1.b2c3, MACSA:f093.c5c3.b2a1
IPDA: 192.168.1.51, IPSA: 192.168.1.50
IPv4 Packet, IP Protocol is UDP(17)
```

32. Select Clear to clear the packet information.