

SwiftWing Sirius NDR

ComWorth Co., Ltd.
Communication Equipment Div.
Sirius Ver5.8

SwiftWing Sirius NDR Overview

MADE IN TA, TOKYO



Since 2003, The SwiftWing Sirius series is developed, designed and built in Japan.

For more than 15years, we develop and sell SwiftWing Sirius to customers around the world.

The SwiftWing Sirius NDR(Network Drive Recorder) is the only device that supports 10MbE to 100GbE (10M/100M/1G/10G/25G/40G/50G*/100G).



* 50G coming soon

SwiftWing Sirius NDR Performance

We have full-choice-system due to offer the best system that fits customer's environment.

We can provide various combination such as media-interface, storage performance, capacity, operating environment, and required functions.

Currently we have 3 media-interface types and each interface can built with all storage-unit.
(Rack Mount , Portable, Portable L, Portable Compact, Portable Super Light)

Since version 5.2, Sirius supported multi-card which can carry up to 2 media- interface in one chassis.



Rack Mount



Portable M



Portable L



Portable Compact



Portable Super Light

High-capacity storage

The Sirius NDR supports high-capacity storage up to 20.0PB(Type11LX).

Because of high-capacity storage, it can capture traffic over time.

The Sirius NDR supports RAID50/60, even HDD has problem, SIRIUS can be recovered.

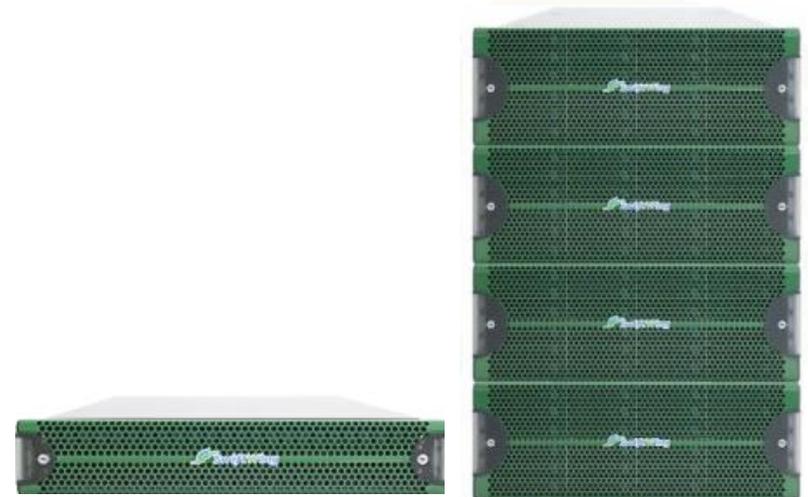
Storage Performance

Storage performance can achieve up to 200Gbps in writing performance.

Sample model	Storage Performance
Sirius NDR 1U Model	25Gbps **
Sirius NDR 2U Model	80Gbps **
Sirius NDR SSD 4U Model	110Gbps
Sirius NDR Multibox Type 2LH	25Gbps
Sirius NDR Multibox Type 2L	50Gbps
Sirius NDR Multibox Type 3L	100Gbps
Sirius NDR Multibox Type 11LX	Over 200Gbps
Sirius NDR Portable M	55Gbps **
Sirius NDR Portable L	110Gbps **
Sirius NDR Portable Compact	50Gbps

*Varies depending on the model (all values are in RAID 5/ 50)

** Varies depending on the type of SSD installed



4 types of multi-rate media interface

We offer 4 types of multi-rate media interface that is compatible with multiple media with one capture card.

Sirius can carry up to 2 multi-rate media interface in one unit.

10G-A2 Multi-rate media interface		
Supported media module	SFP/SFP+	
Total Port	2	
Supported media-rate	10Mbps : 10Base-T 100Mbps : 100Base-TX 1Gbps : 1000BASE-SX/-LX/-T 10Gbps : 10Gbase-SR/-LR/-T	
10G-B1 Multi-rate media interface		
Supported media module	SFP/SFP+	
Total Port	4	
Supported media-rate	10Mbps : 10Base-T 100Mbps : 100Base-TX 1Gbps : 1000BASE-SX/-LX/-T 10Gbps : 10Gbase-SR/-LR/-T	

100G-A2/100G-A3 Multi-rate media interface		
Supported media module	QSFP+/QSFP28	
Total Port	2	
Supported media-rate	10Gbps : 10Gbase-SR/-LR/-T 25Gbps : 25Gbase-SR/-LR/-CR (RS-FEC supported) 40Gbps : 40Gbase-SR4/-LR4/-CR4 50Gbps : 50Gbase-SR2/-LR2/-CR2 * 100Gbps : 100Gbase-SR4/-LR4/-PSM4/-CLR4/ -CR4/-ER4 (RS-FEC supported)	

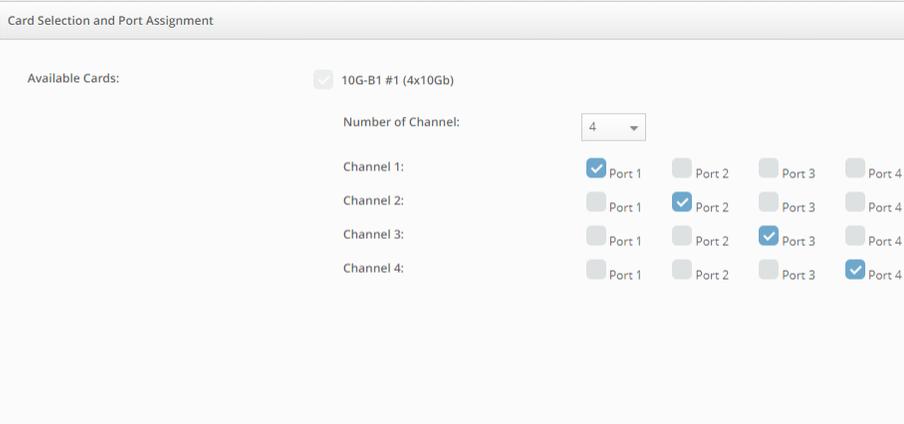
* 50G supports later

The Sirius NDR can be configured up to 4 channel according to the user settings and all 4 channels can capture simultaneously.

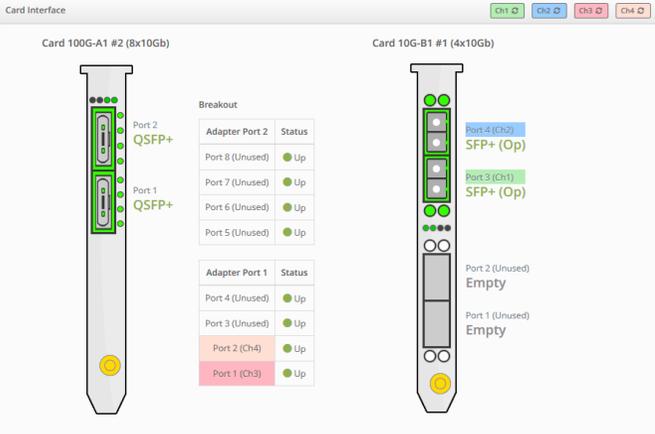
In each port configuration, up to 16 ports of media (100G-A2/A3 media interface card*2, 10G*8ports) can be assigned to each channel.

Channels generate streams for each capture in separate PCAP files. Therefore, it can be analyzed immediately from application *1 on built-in Wireshark and hypervisor. It can also be downloaded to the user terminal by using FTP/SFTP.

(*1) option



Channel configuration



Dashboard

Multi Channel / Multi Port – 4-Channel configuration

Ch1 Set as default Enable

Session: New Resume

Filename:

Capture Format: Nanosecond PCAP PCAP

Packet Slice Length: + bytes

Pre-filter:

Duration: Continuous Duration

Capture File Split: No file split (1 file) Split by file size Split by time

Select file size:

Microburst:

Packet Index for the Post-filter:

Packet Alert:

Ch2 Set as default Enable

Session: New Resume

Filename:

Capture Format: Nanosecond PCAP PCAP

Packet Slice Length: + bytes

Pre-filter:

Duration: Continuous Duration

Capture File Split: No file split (1 file) Split by file size Split by time

Select file size:

Microburst:

Packet Index for the Post-filter:

Packet Alert:

Ch3 Set as default Enable

Session: New Resume

Filename:

Capture Format: Nanosecond PCAP PCAP

Packet Slice Length: + bytes

Pre-filter:

Duration: Continuous Duration

Capture File Split: No file split (1 file) Split by file size Split by time

Select file size:

Microburst:

Packet Index for the Post-filter:

Packet Alert:

Ch4 Set all channels as default Set as default Enable

Session: New Resume

Filename:

Capture Format: Nanosecond PCAP PCAP

Packet Slice Length: + bytes

Pre-filter:

Duration: Continuous Duration

Capture File Split: No file split (1 file) Split by file size Split by time

Select file size:

Microburst:

Packet Index for the Post-filter:

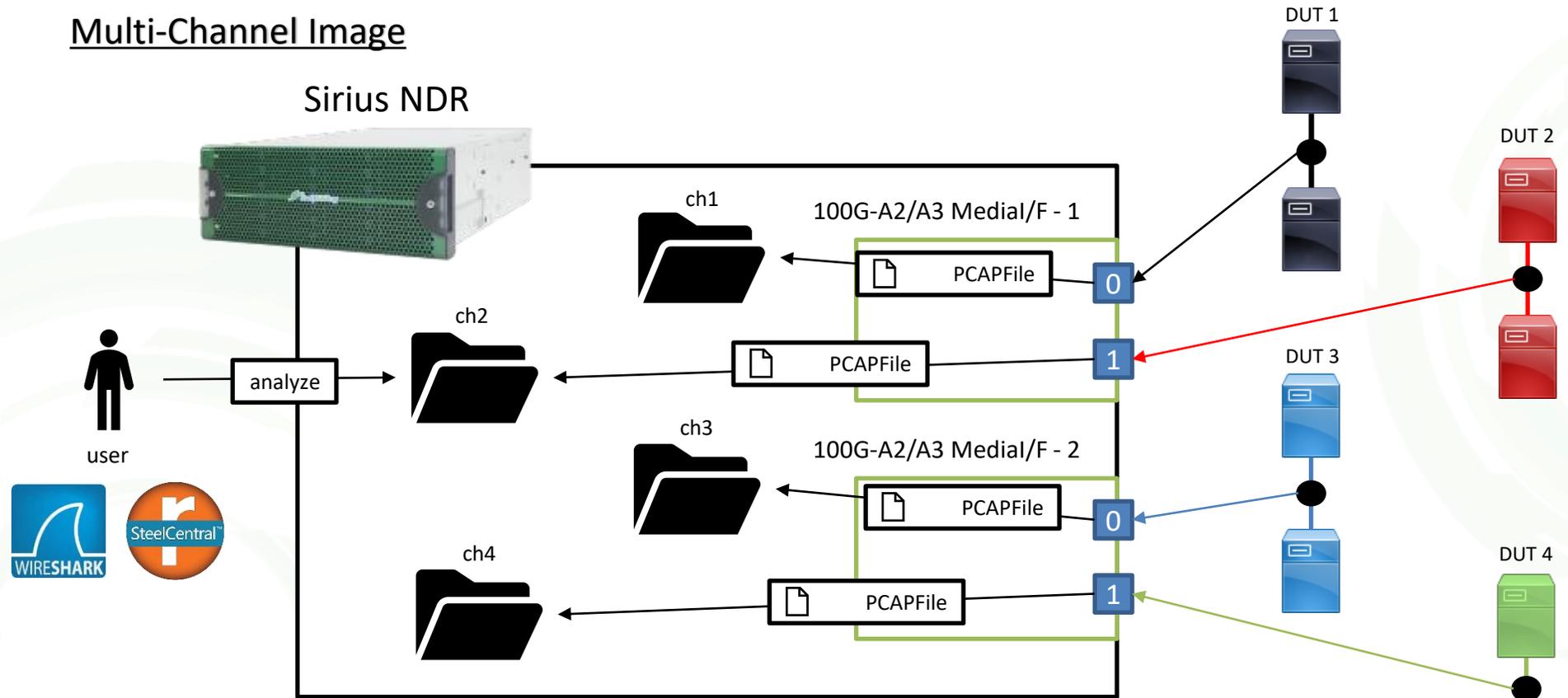
Packet Alert:

Capture File Rotation: No rotation Rotate by files Rotate by diskpace

Select % to rotate by:

4-Channel configuration

Multi-Channel Image



- 100G-A2/A3 Media I/F*2 configuration
- ch1 : Port Nr.0(100G-A2/A3 Media I/F - 1)
- ch2 : Port Nr.1(100G-A2/A3 Media I/F - 1)
- ch3 : Port Nr.0(100G-A2/A3 Media I/F - 2)
- ch4 : Port Nr.1(100G-A2/A3 Media I/F - 2)

Capture-Function Overview

Sirius NDR can set and capture the configuration for each channel that being set by the user.

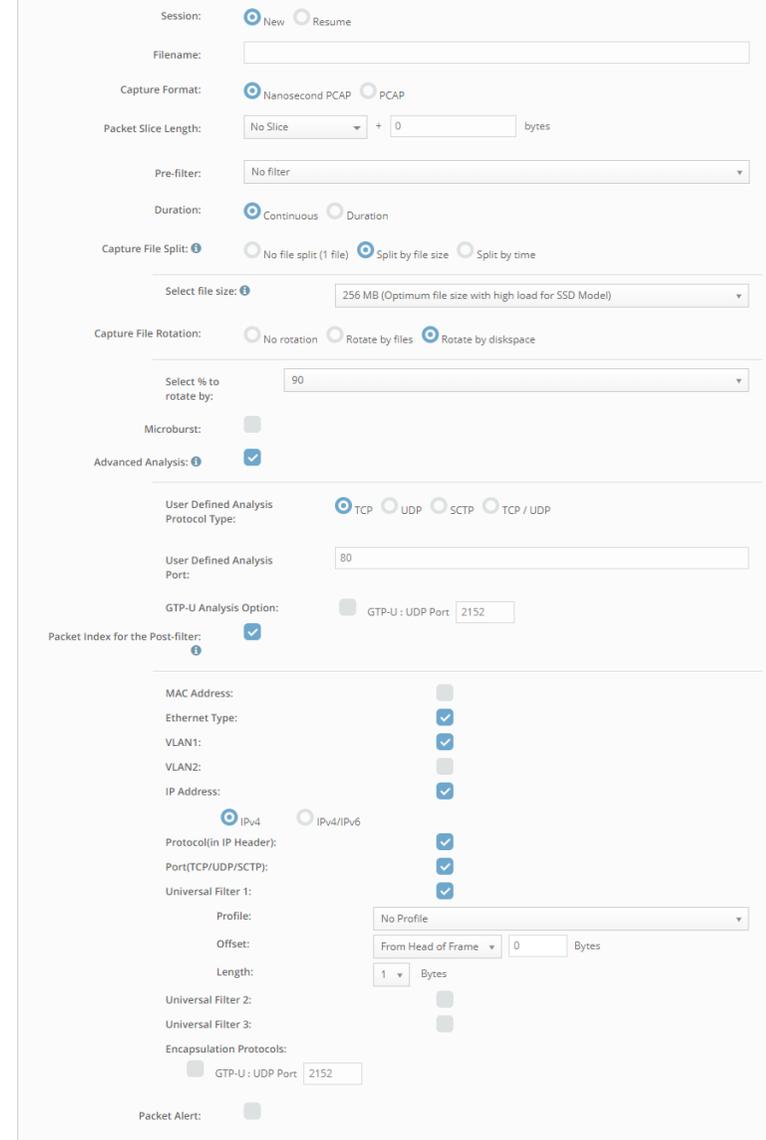
It is possible to capture without falling down to the rate below the storage performance of each model* (see page 6) .

Capture files (in PCAP format) are generated in different directories for each channel.

- Performance may drop if other functions are used simultaneously with capture.

The following items can be set when starting the capture

- PCAP File Format
- Packet-Slice
- Pre-Filter
- Capture Period
- File-Split Method & Conditions
- Rotation Method & Conditions
- Micro-Burst Analysis Enable/ Disable
- Traffic Analysis Enable/ Disable
- Indexing Enable/ Disable
- Packet-Alert Enable/ Disable



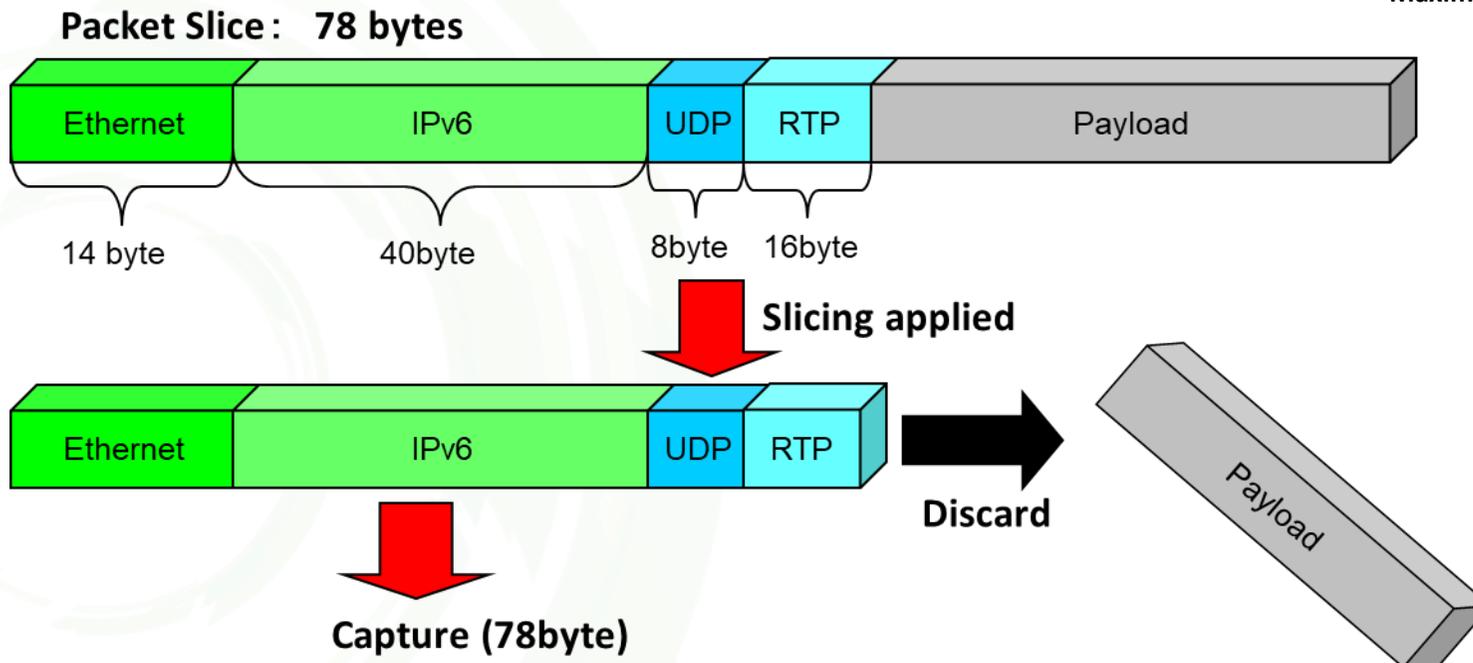
The screenshot displays the configuration interface for the Capture Function. The settings are as follows:

- Session:** New Resume
- Filename:** [Empty text field]
- Capture Format:** Nanosecond PCAP PCAP
- Packet Slice Length:** No Slice + 0 bytes
- Pre-filter:** No filter
- Duration:** Continuous Duration
- Capture File Split:** No file split (1 file) Split by file size Split by time
- Select file size:** 256 MB (Optimum file size with high load for SSD Model)
- Capture File Rotation:** No rotation Rotate by files Rotate by disk space
- Select % to rotate by:** 90
- Microburst:**
- Advanced Analysis:**
- User Defined Analysis Protocol Type:** TCP UDP SCTP TCP / UDP
- User Defined Analysis Port:** 80
- GTP-U Analysis Option:** GTP-U : UDP Port: 2152
- Packet Index for the Post-filter:**
- MAC Address:**
- Ethernet Type:**
- VLAN1:**
- VLAN2:**
- IP Address:**
- Protocol(in IP Header):**
- Port(TCP/UDP/SCTP):**
- Universal Filter 1:**
- Profile:** No Profile
- Offset:** From Head of Frame 0 Bytes
- Length:** 1 Bytes
- Universal Filter 2:**
- Universal Filter 3:**
- Encapsulation Protocols:** GTP-U : UDP Port: 2152
- Packet Alert:**

Sirius NDR can slice captured packet to any size and save it in PCAP File. The packet sliced size specifies the length in bytes from the beginning of the Ethernet frame header to the portion to be acquired. Data after the Packet-Slice setting size will be discarded.

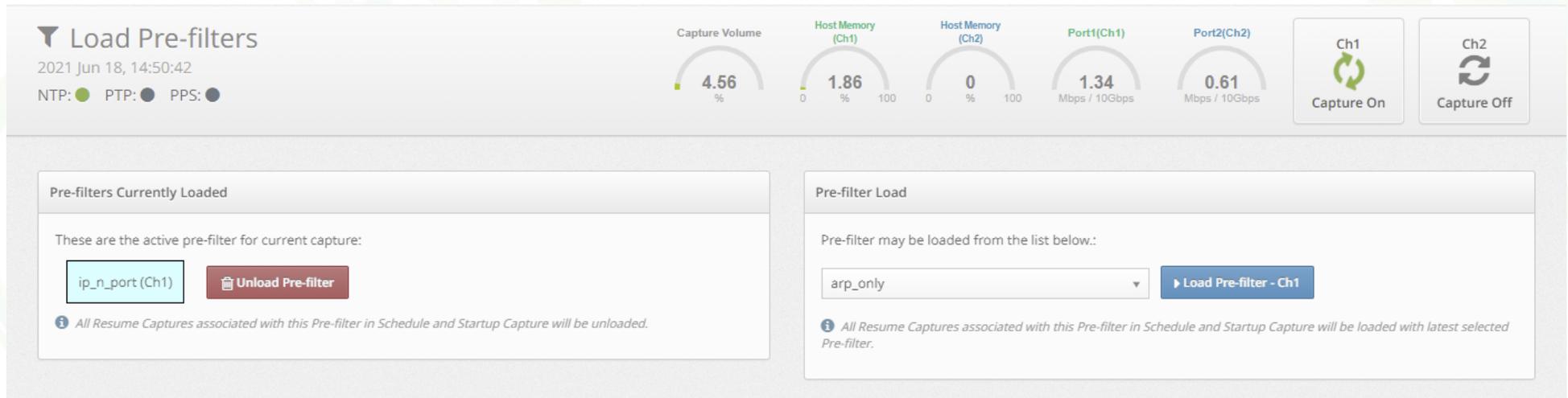
Packet-Slice saves space of capture storage by removing payload portions that are not needed for analysis.

Minimum Packet-Slice size 64Byte
Maximum Packet-Slice size 10,000Byte



Pre-Filters can apply basic filters such as Mac address, IPv4 / IPv6 address, protocol type, TCP/UDP Port number and apply any value(Hex, Bit) to any offset of the packet. Enabling this function will not affect capture performance.

Pre-Filters can easily change the filter or cancel the filter setting as well as during capture.



The screenshot displays the 'Load Pre-filters' section of the ComWorth interface. At the top, it shows the current time as 2021 Jun 18, 14:50:42 and filter status for NTP (green), PTP (black), and PPS (black). A row of five gauges provides real-time metrics: Capture Volume at 4.56%, Host Memory (Ch1) at 1.86%, Host Memory (Ch2) at 0%, Port1(Ch1) at 1.34 Mbps / 10Gbps, and Port2(Ch2) at 0.61 Mbps / 10Gbps. To the right are 'Capture On' and 'Capture Off' buttons for Ch1 and Ch2. Below these are two panels: 'Pre-filters Currently Loaded' and 'Pre-filter Load'. The 'Pre-filters Currently Loaded' panel shows an active filter 'ip_n_port (Ch1)' with an 'Unload Pre-filter' button. The 'Pre-filter Load' panel features a dropdown menu with 'arp_only' selected and a 'Load Pre-filter - Ch1' button. Both panels include a note: 'All Resume Captures associated with this Pre-filter in Schedule and Startup Capture will be unloaded.' (or 'loaded with latest selected Pre-filter.' for the load panel).

Profile 1

Profile Type : Advanced

IP Version :

IPv6

Exclude Frames

Source IPv6 Address :

Source IPv6 Netmask : ▼

Destination IPv6 Address :

Destination IPv6 Netmask : ▼

Layer 4

Exclude Frames

Protocol : TCP UDP

Source Port :

Destination Port :

Profile 1

Profile Type : Advanced

Pattern

Exclude Frames

Dynamic Offset : ▼

Fixed Offset : bytes

Pattern Length : ▼ bytes

Pattern : 0x

Filter Conditions that can be set by Pre-Filters

1. Mac address, Ethernet type, VLAN, IPv4/IPv6 address (incl. net mask)、TCP/UDP Port number
2. Frame length –Selectable from 64 to 10,000 Bytes
3. Protocol
 - Layer2 : ETHERNET II 、 LLC、 SNAP、 RAW
 - Layer3 : IPv4、 IPv6、 IPX、 IPv4 IPPROTO、 IPv6 NEXT HEADER
 - Layer4 : IPv4 ICMP、 IPv6 ICMP
 - Other : JUMBO、 BROADCAST、 MULTICAST、 MPLS、
L3 NOT RECOGNISED、 L4 NOT RECOGNISED、 ISL、 VLAN
4. Error-type
 - CRC、 RUNT、 Oversize、 Fragment、 Jabber、 IP Checksum、 TCP Checksum、 UDP Checksum
5. Dynamic offset
 - Any offset value can be specified in the Packet and a range of up to 64 bytes can be specified as a filter condition from the offset .

Packet-Alert function is a function to send an alert to SNMP Trap / Syslog / Email when a specific packet is detected. If an abnormal packet is detected, the administrator will be notified immediately with SNMP Trap or Email to take action.

For packet detection can used the same filter definition as the Pre-Filter. This can detect not only the usual IP/TCP protocol headers, but also the payload, so alerts can be applied to application methods and responses to them.

Profile List

Search: ⓘ

Show 10 entries First Previous 1 Next Last

Name	Pre-filter type	Created By	Pre-filter	Packet Alert	Action
arp_only	Custom	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	  
ip_n_port	Custom	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	  
mac_n_mac	Custom	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	  
pattern_match	Custom	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	  
tcp_syn	Custom	admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	  

Showing 1 to 5 of 5 entries

First Previous 1 Next Last

Packet-Alert definition control

Packet Alert Configuration ⓘ

Count:

Analysis Unit: seconds

Notice Interval: seconds

Alert Type: Remote Syslog SNMP Trap E-Mail

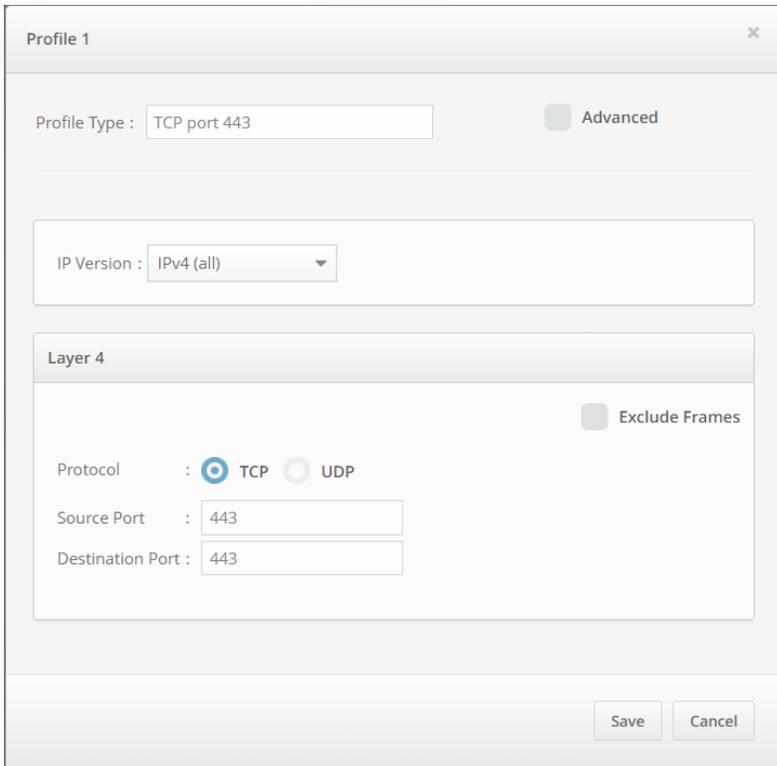
File Lock

Save

Packet-Alert send Configuration

Example: Generate an alarm when detecting the following traffic

- The source TCP port number is 443 and the destination port is 36578



Profile 1

Profile Type : TCP port 443 Advanced

IP Version : IPv4 (all)

Layer 4 Exclude Frames

Protocol : TCP UDP

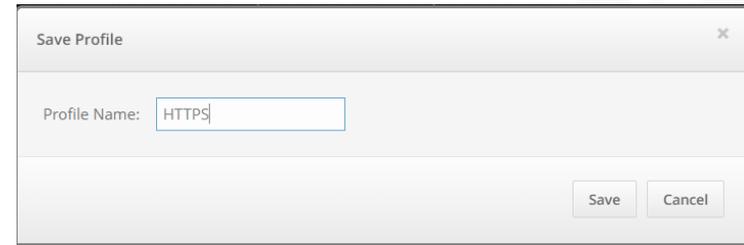
Source Port : 443

Destination Port : 443

Save Cancel

Packet-Alert definition configuration

Packet-Alert name configuration



Save Profile

Profile Name: HTTPS

Save Cancel



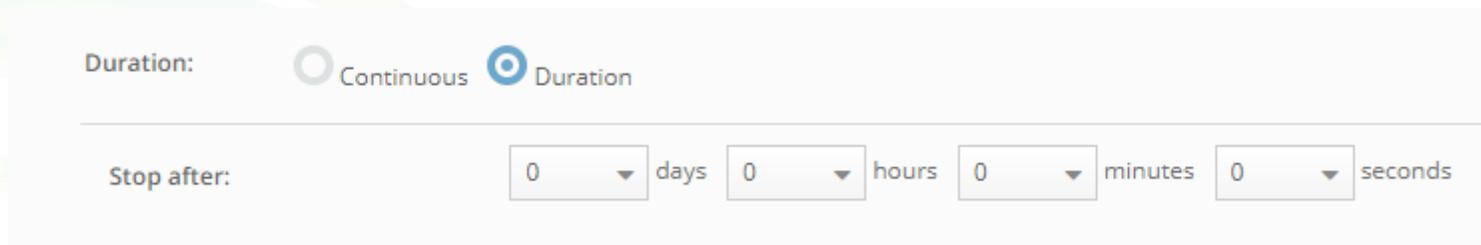
Packet Alert:

Profile: HTTPS

Capture configuration

It is a function that can automatically stop capture after a certain period of time from the start of Capture. It is useful when you want to capture to run a test for a fixed amount of time.

Specifiable period : 1 second to 99 days 23 hours 59 minutes 59 seconds

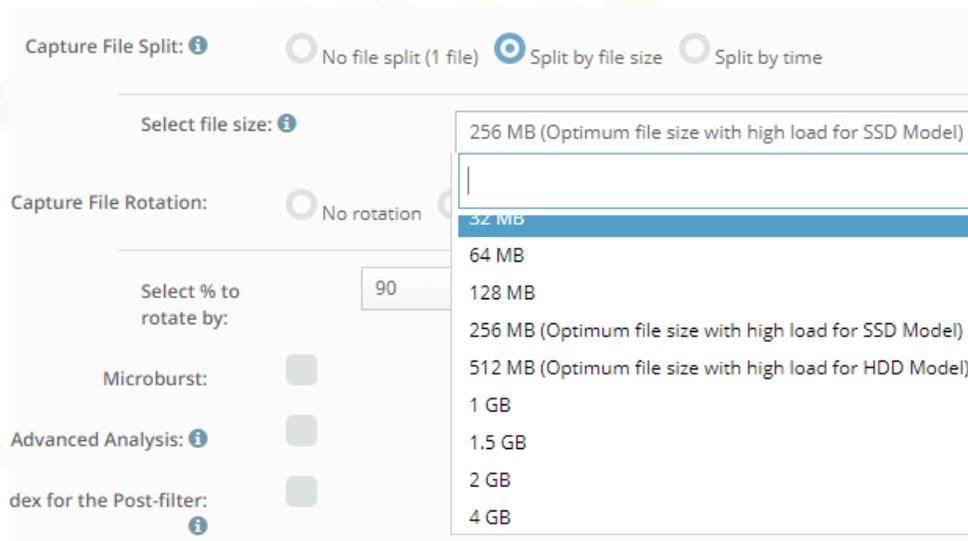


The screenshot shows a user interface for configuring the capture duration. It features two radio buttons: 'Continuous' (unselected) and 'Duration' (selected). Below the radio buttons, there is a 'Stop after:' label followed by four dropdown menus for 'days', 'hours', 'minutes', and 'seconds', each currently set to '0'.

If the capture period is continuous, capture will continue until the stop button is pressed.

The division method and conditions of captured PCAP file can be specified. The division method corresponds to the following 3 types and conditions.

- Invalid(only 1 file)
- Split by file size
 - 32MB / 64MB / 128MB / 256MB / 512MB / 1GB / 1.5GB / 2GB / 4GB
- Split by time
 - 1sec / 5sec / 10sec / 15sec/ 30sec / 1min / 5min / 10min / 15min / 30min / 1hour



Capture File Split: No file split (1 file) Split by file size Split by time

Select file size:

Capture File Rotation: No rotation

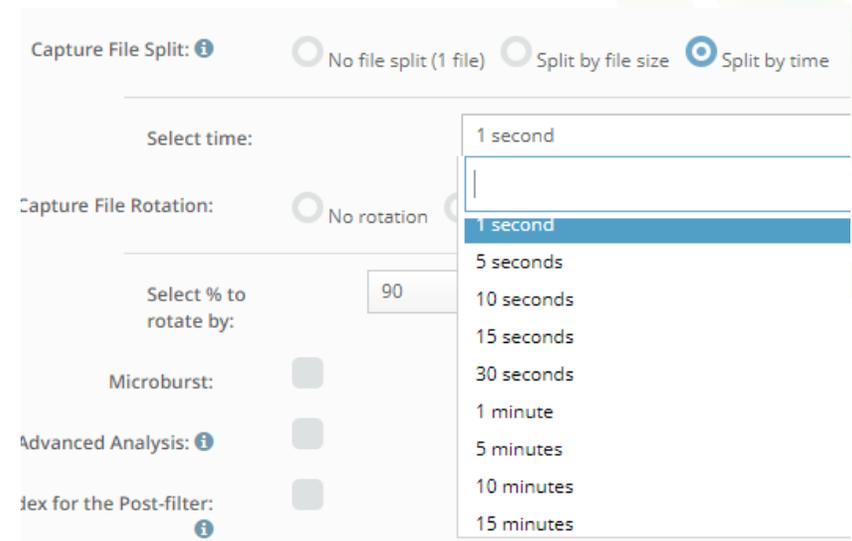
Select % to rotate by:

Microburst:

Advanced Analysis:

Index for the Post-filter:

- 256 MB (Optimum file size with high load for SSD Model)
- 32 MB
- 64 MB
- 128 MB
- 256 MB (Optimum file size with high load for SSD Model)
- 512 MB (Optimum file size with high load for HDD Model)
- 1 GB
- 1.5 GB
- 2 GB
- 4 GB



Capture File Split: No file split (1 file) Split by file size Split by time

Select time:

Capture File Rotation: No rotation

Select % to rotate by:

Microburst:

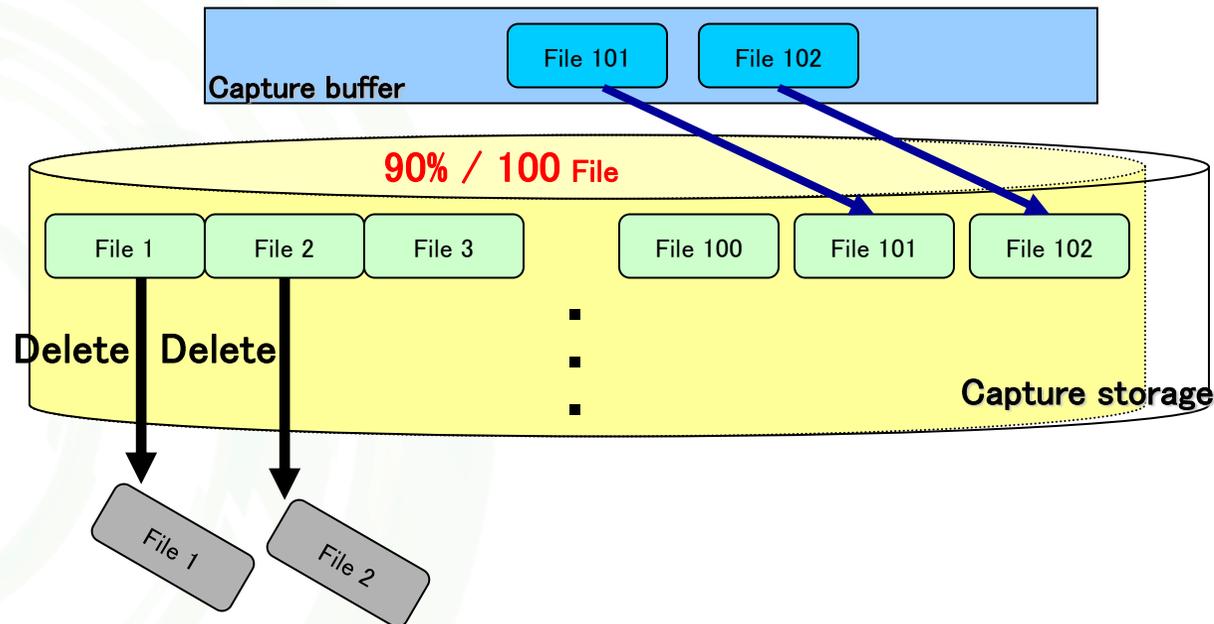
Advanced Analysis:

Index for the Post-filter:

- 1 second
- 5 seconds
- 10 seconds
- 15 seconds
- 30 seconds
- 1 minute
- 5 minutes
- 10 minutes
- 15 minutes

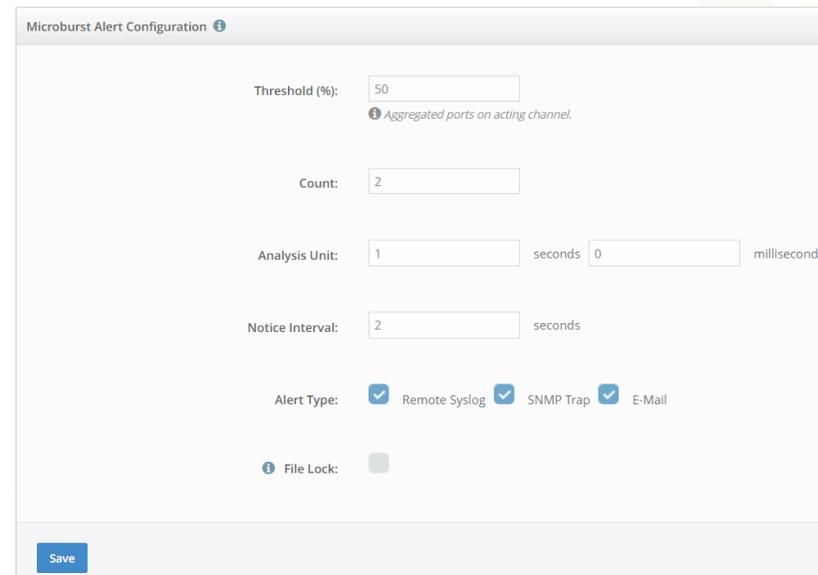
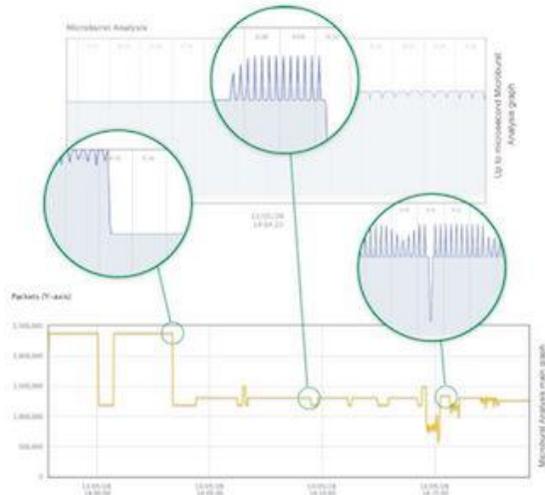
Sirius NDR supports file rotation function that automatically deletes the oldest file when the saved capture file reaches a specified storage capacity. The function can be specified by the capture storage volume usage or the number of files.

Using This function can realize continuous packet capture without interruption.



Microburst analysis aggregates and records throughput information every 500 microseconds. You can set a threshold for throughput, the function generates an alert (SNMP Trap / Syslog / Event log) when throughput is exceeded. Also, the function is possible to automatically Lock the PCAP files of containing the packets for not overwrite.

- Record at the same time as capture (only 1ch)
- Record throughput statistics every 500 microseconds (2000 records per second)
- Store last 7 days of statistics data
- Support for statistics data export in CSV format
- Alert Notification (Event log / SNMP trap) and PCAP file overwrite prohibition by threshold setting (Traffic rate, Number of counts vs Detection time)



The image shows the 'Microburst Alert Configuration' interface. The configuration includes the following settings:

- Threshold (%): 50 (with a note: Aggregated ports on acting channel)
- Count: 2
- Analysis Unit: 1 seconds 0 milliseconds
- Notice Interval: 2 seconds
- Alert Type: Remote Syslog SNMP Trap E-Mail
- File Lock:

A 'Save' button is located at the bottom of the configuration panel.

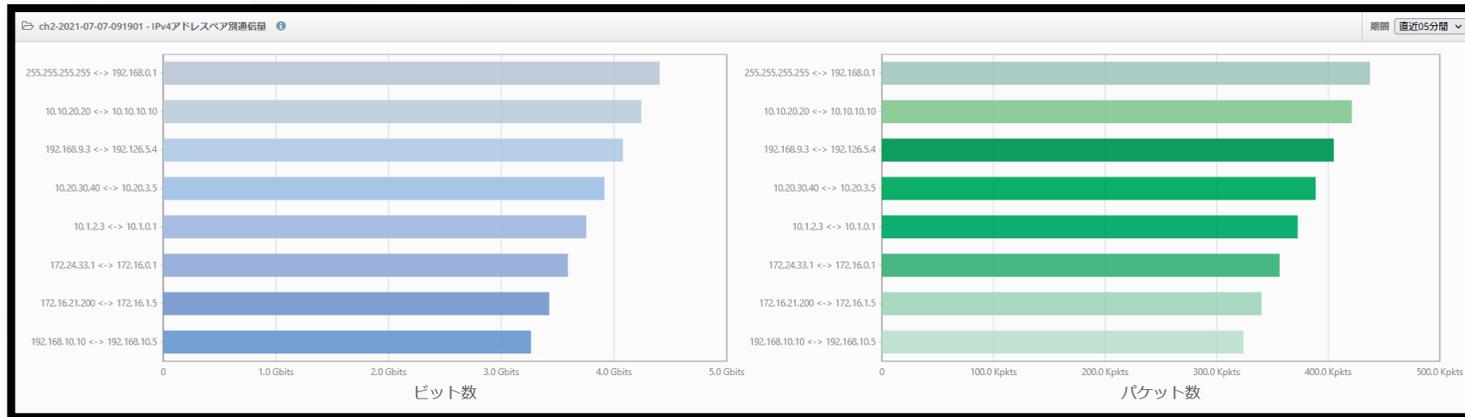
This function analyzes and graphically displays the amount of captured traffic by application and IPv4 address pair.

By using this function, the status of captured traffic can be analyzed by application and IPv4 address pair. This function is useful for getting an overview of the traffic and investigating the cause of bursts.

Traffic volume graph by application

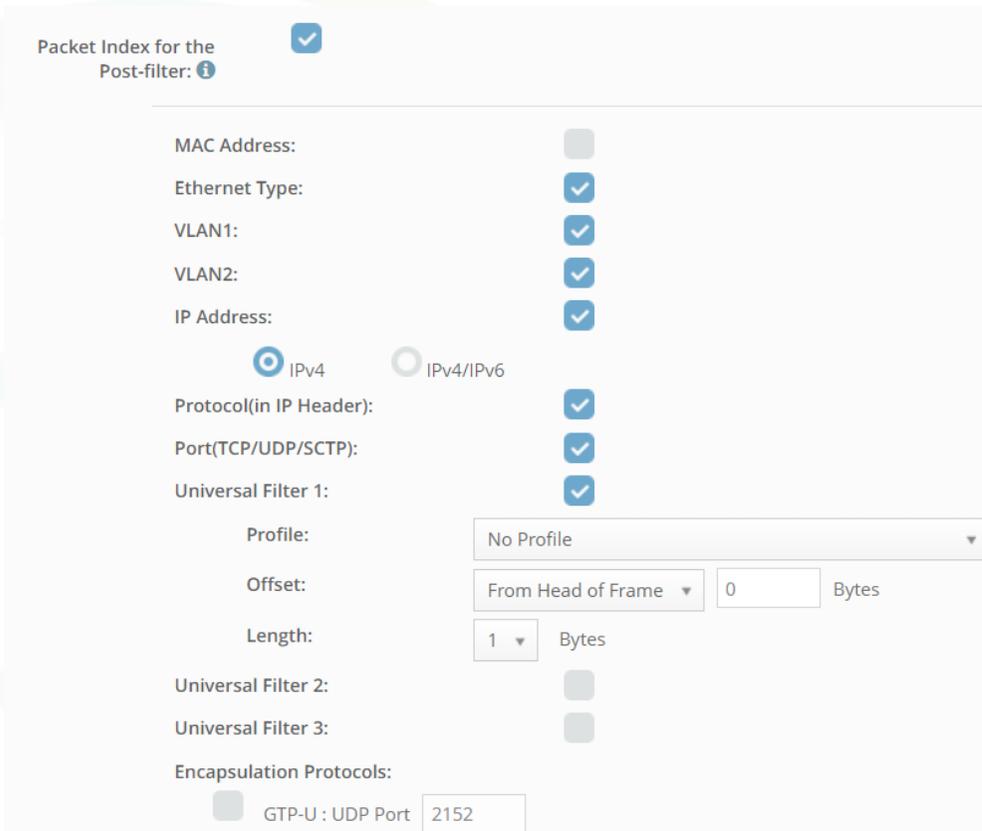


Traffic volume graph by IPv4 address pair



The function is to create an index file for Post Filter at the same time as capture.

By using this function, it is possible to execute Post Filter immediately without waiting for index file creation time and extract desired packets.



The screenshot shows the 'Packet Index for the Post-filter' configuration window. It includes a checked checkbox at the top left. The configuration options are as follows:

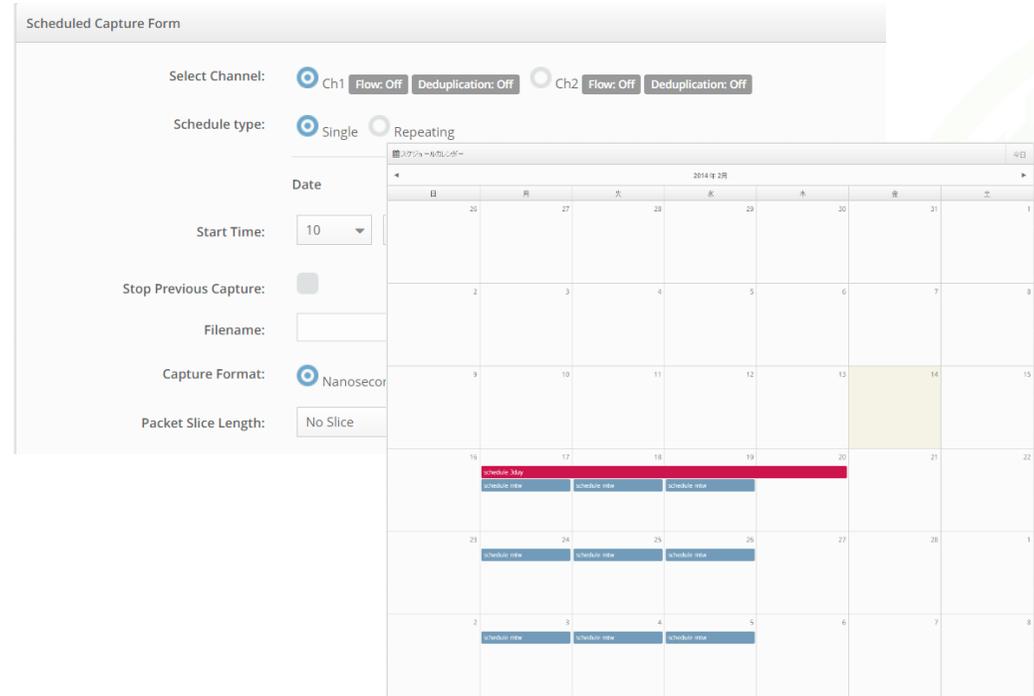
- MAC Address:
- Ethernet Type:
- VLAN1:
- VLAN2:
- IP Address:
Radio buttons: IPv4, IPv4/IPv6
- Protocol(in IP Header):
- Port(TCP/UDP/SCTP):
- Universal Filter 1:
Profile: No Profile (dropdown)
- Offset: From Head of Frame (dropdown), 0 (text input), Bytes
- Length: 1 (dropdown), Bytes
- Universal Filter 2:
- Universal Filter 3:
- Encapsulation Protocols: GTP-U : UDP Port 2152 (text input)

Any field can be selected for the index, as shown in the left figure. By selecting only the fields that are scheduled to be extracted in the post-filter, the speed of index file generation can be improved and storage capacity can be used more efficiently.

Schedule Capture

Schedule capture is the function to start capture on a set date, time or day of the week.

Capture settings can be set for each task. It is used when you want to start capture at a fixed time.



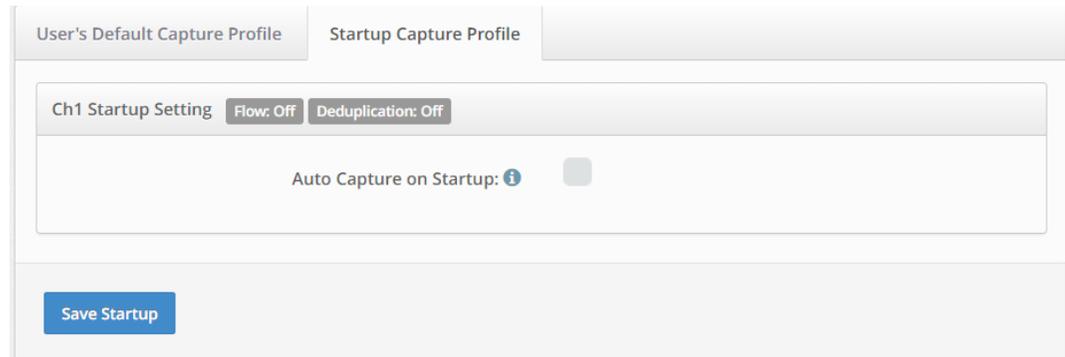
The screenshot shows the 'Scheduled Capture Form' interface. It includes the following settings:

- Select Channel:** Ch1 (selected) with 'Flow: Off' and 'Deduplication: Off' buttons. Ch2 is also available with 'Flow: Off' and 'Deduplication: Off' buttons.
- Schedule type:** Single (selected) and Repeating.
- Date:** A calendar view for 2014年2月 (February 2014) with a date picker set to 10.
- Start Time:** 10 (dropdown menu).
- Stop Previous Capture:** Unchecked checkbox.
- Filename:** Empty text field.
- Capture Format:** Nanosecond (selected).
- Packet Slice Length:** No Slice.

The calendar shows a red bar for 'Schedule Start' on Feb 10 and blue bars for 'Schedule Stop' on Feb 10, 11, and 12.

Startup Capture

Startup capture is a function that starts capture automatically when Sirius starts.



The screenshot shows the 'Startup Capture Profile' configuration window. It includes the following settings:

- User's Default Capture Profile:** Selected tab.
- Startup Capture Profile:** Selected tab.
- Ch1 Startup Setting:** Flow: Off, Deduplication: Off.
- Auto Capture on Startup:** Unchecked checkbox with an information icon (i).
- Save Startup:** Blue button.

Filter Condition

- MAC Address
- Ether Type
- First VLAN ID
- Second VLAN ID
- Source / Destination IP Address (Accept Range)
- Protocol Number
- Source / destination Port Number (Accept Range)
- Universal Filter (Up to 3)
- GTP-U inner packet(IP Address, Protocol, Port Number)

Filter conditions can combine multiple conditions with “and”. It also supports complex syntax conditions, such as comma separators and range specifications.

Current Filter:
(Empty)

General	Aggregation	List	Range	Combination	Not Operator	Universal Filter	Packet Limit
Frame							
Filter fields		Filter syntax			Example		
Frame Length (Decimal)		frame.len			frame.len = 100 frame.len != 100		
Layer 2							
Filter fields		Filter syntax			Example		
Any MAC Address		eth.addr			eth.addr = abc:cd:ef:12:34:56 eth.addr != abc:cd:ef:12:34:56		
Source MAC Address		eth.src			eth.src = abc:cd:ef:12:34:56 eth.src != abc:cd:ef:12:34:56		
Destination MAC Address		eth.dst			eth.dst = abc:cd:ef:12:34:56 eth.dst != abc:cd:ef:12:34:56		
Ethernet Type (Decimal,Hexadecimal)		eth.type			eth.type = 0x0800 eth.type != 0x86dd		
VLAN1 ID (Decimal)		vlan.id vlan1.id			vlan1.id = 32 vlan1.id != 32		
VLAN2 ID (Decimal)		vlan2.id			vlan2.id = 64 vlan2.id != 64		
Layer 3							
Filter fields		Filter syntax			Example		
Any IP Address		ip			ip = 168.64.0.0 ip != 192.168.1.1		
Source IP Address		ip.src			ip.src = 168.64.0.0 ip.src != 192.168.1.1		
Destination IP Address		ip.dst			ip.dst = 168.64.0.0 ip.dst != 192.168.1.1		
Protocol (Decimal)		ip.proto			ip.proto = 17 ip.proto != 17		

Filter Conditions ①

Extraction by PTPv2 Message Type

Many message types exist in PTPv2, including Sync/Follow Up/Delay Request/Delay Response.

In this example, only Delay Request messages are extracted from PTPv2 communications using post-filter pattern matching (universal filter).

Capture Configuration

Suppose PTPv2 exists on top of Ethernet (14 bytes)/IP (20 bytes)/UDP (8 bytes).
 (*If the packet size changes depending on the VLAN, it is necessary to adjust Offset and Length, or select "from the end of the frame" to set the packet size.)

Universal Filter 1:

Profile: PTPv2 Message Type

Offset: From Head of Frame

42 Bytes

Length: 2 Bytes



Post Filter Configuration

Specify filter conditions using ASCII codes (hexadecimal notation)

Filter: i

*The message type is indicated by the value of the last 4 bits

Sync Message : 0x00

Delay Request Message : 0x01 (This time, this message is extracted.)

Follow Up Message : 0x08

Delay Response Message: 0x09

*The upper 4 bits are the transportSpecific field and their values change depending on the hardware. In this example, it is assumed that 0x0 is always specified.



Filter result

時刻	MACアドレス	イーサタイプ	VLAN1/VLAN2 ID	IPアドレス	プロトコル番号	ポート	パターン	GTP-U (Inner)	バイト
2020-07-31 17:19:01.567057029	Src: - Dst: -	0x0800/ -/-	VLAN1 ID: - VLAN2 ID: -	Src: 192.168.1.1 Dst: 224.0.1.129	17	Src: 319 Dst: 319	01	-	92
2020-07-31 17:19:01.567057041	Src: - Dst: -	0x0800/ -/-	VLAN1 ID: - VLAN2 ID: -	Src: 192.168.1.1 Dst: 224.0.1.129	17	Src: 319 Dst: 319	01	-	92
2020-07-31 17:19:01.574867179	Src: - Dst: -	0x0800/ -/-	VLAN1 ID: - VLAN2 ID: -	Src: 192.168.1.1 Dst: 224.0.1.129	17	Src: 319 Dst: 319	01	-	92

Analysis screen in wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	1590486676.282045664	172.24.166.22	224.0.1.129	PTPv2	90	Delay_Req Message
2	1590486676.285317235	172.24.166.22	224.0.1.129	PTPv2	90	Delay_Req Message
3	1590486676.286381548	172.24.118.190	224.0.1.129	PTPv2	90	Delay_Req Message
4	1590486676.287299078	172.24.166.22	224.0.1.129	PTPv2	90	Delay_Req Message
5	1590486676.289128838	172.24.118.190	224.0.1.129	PTPv2	90	Delay_Req Message

> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)

> Ethernet II, Src: AlbedoTe_00:15:66 (00:db:1e:00:15:66), Dst: IPv4mcast_01:81 (01:00:5e:00:01:81)

> Internet Protocol Version 4, Src: 172.24.166.22, Dst: 224.0.1.129

> User Datagram Protocol, Src Port: 319, Dst Port: 319

▼ Precision Time Protocol (IEEE1588)

- > 0000 = transportSpecific: 0x0
- ... 0001 = messageId: Delay_Req Message (0x1)
- 0010 = versionPTP: 2
- messageLength: 44
- subdomainNumber: 0
- > flags: 0x0000
- > correction: 0.000000 nanoseconds
- ClockIdentity: 0x00db1efffe001566
- SourcePortID: 1
- sequenceId: 1068
- control: Delay_Req Message (1)
- logMessagePeriod: 127
- originTimestamp (seconds): 1588044691
- originTimestamp (nanoseconds): 243955650

```

0000 01 00 5e 00 01 81 00 db 1e 00 15 66 08 00 45 00  ..^.....-f..E.
0010 00 48 00 00 40 00 40 11 06 f5 ac 18 a6 16 e0 00  .H..@. @.....
0020 01 81 01 3f 01 3f 00 34 00 00 01 02 00 2c 00 00  ...??.4.....,
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 db  ....
0040 1e ff fe 00 15 66 00 01 04 2c 01 7f 00 00 5e a7  ...f...^
0050 a3 93 0e 8a 77 c2 81 e8 01 15  ....w...
    
```

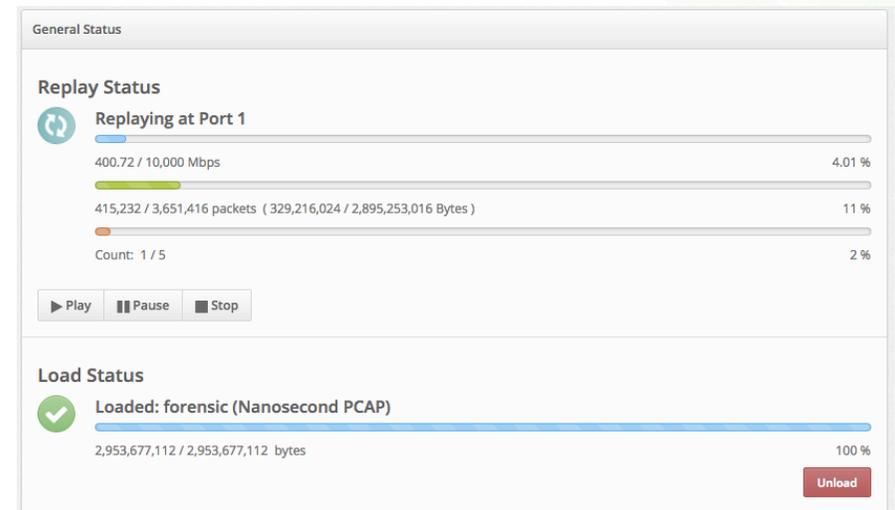
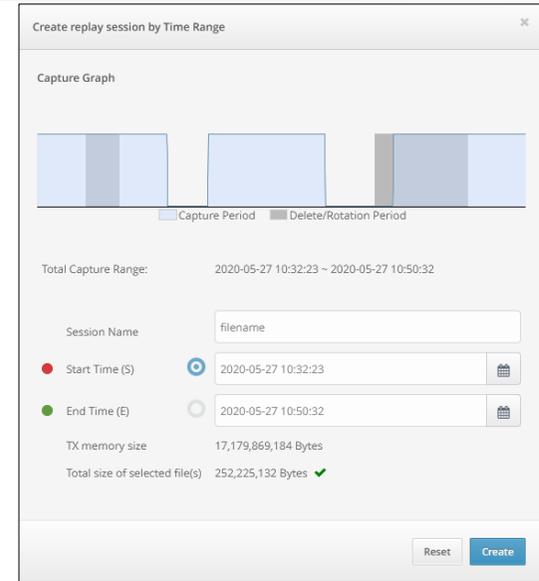
Overall of Packet Replay Function

Packet Replay is a function to reproduce packets according to time stamp of the PCAP file; It sends packets to Sirius capture port. User can specify PCAP file from captured PCAP file by Sirius or user upload PCAP file.

It is possible to reproduce and verify problems on the reproduced packets according to the time stamp.

Replayable PCAP file size supports up to 500GB * and can perform long-term packet replay.

* Require extra memory option.



Configuration of Packet Replay Function

There are 3 ways to specify a PCAP file for packet replay:

- Specify a time range within a capture session
- Specify multiple files in a capture session
- Upload PCAP file by user

Create replay session by Time Range

Capture Graph

Total Capture Range: 2020-05-27 10:32:23 ~ 2020-05-27 10:50:32

Session Name:

Start Time (S):

End Time (E):

TX memory size: 17,179,869,184 Bytes

Total size of selected file(s): 252,225,132 Bytes ✓

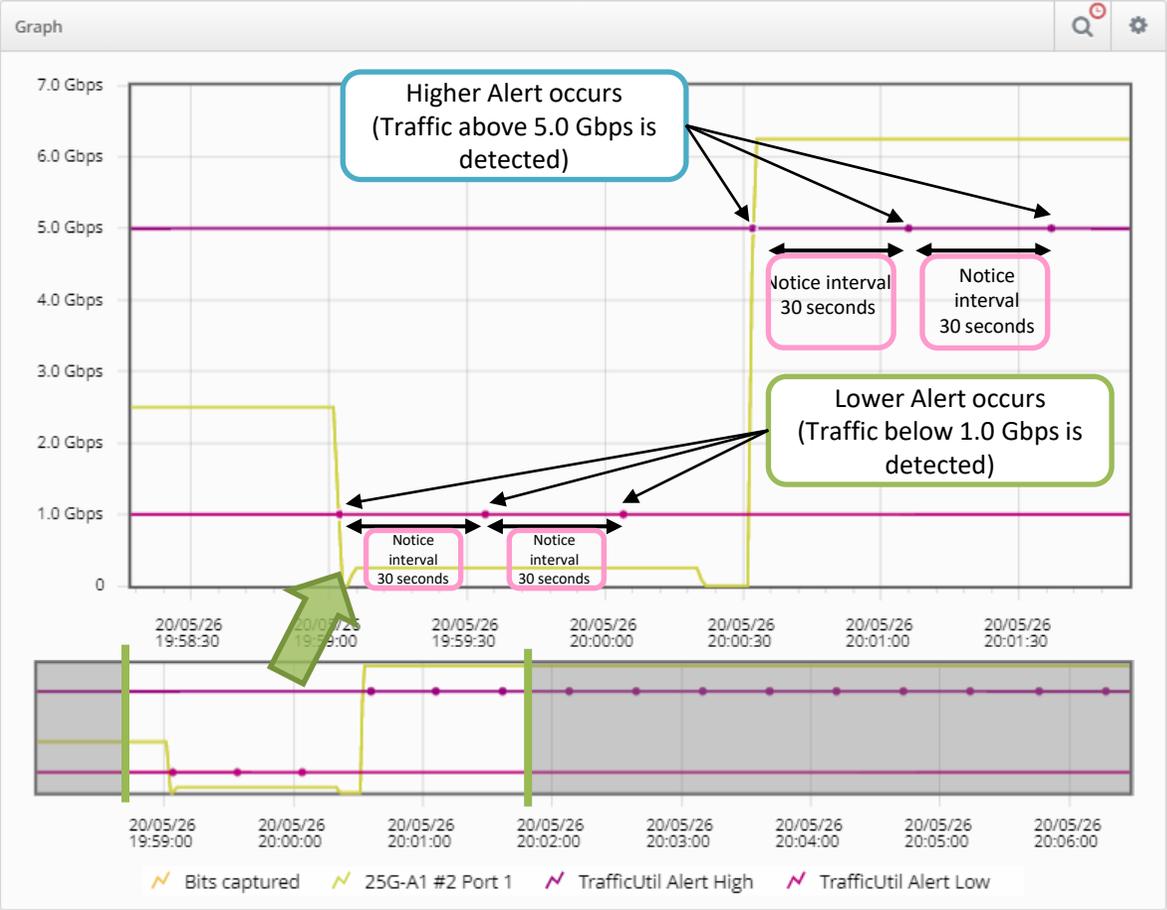
	Filename	Filesize	Last Modified	Actions
1	01_test_capture-2020-07-24-173222-0001.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
2	01_test_capture-2020-07-24-173222-0002.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
3	01_test_capture-2020-07-24-173222-0003.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
4	01_test_capture-2020-07-24-173222-0004.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
5	01_test_capture-2020-07-24-173222-0005.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
6	01_test_capture-2020-07-24-173222-0006.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
7	01_test_capture-2020-07-24-173222-0007.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
8	01_test_capture-2020-07-24-173222-0008.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
9	01_test_capture-2020-07-24-173222-0009.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>
10	01_test_capture-2020-07-24-173222-0010.pcap	32 MB	2020/07/24 17:32:22	<input type="button" value="Download"/> <input type="button" value="Delete"/>

At a glance, you can see the long-term traffic fluctuations. Displaying traffic statistics in real-time graph which the statistics data can be exported in CSV format.



Linkage with various alerts, such as traffic utilization alerts, to display the location of alerts in the graph when they occur.

Linkage with Traffic Utilization Alerts



Traffic Utilization Alert Settings

Unit Of Threshold Bits Per Second (BPS) Packets Per Second (PPS)

Lower Alert Threshold Gpps

Higher Alert Threshold Gpps

Analysis Unit seconds

Notice Interval seconds

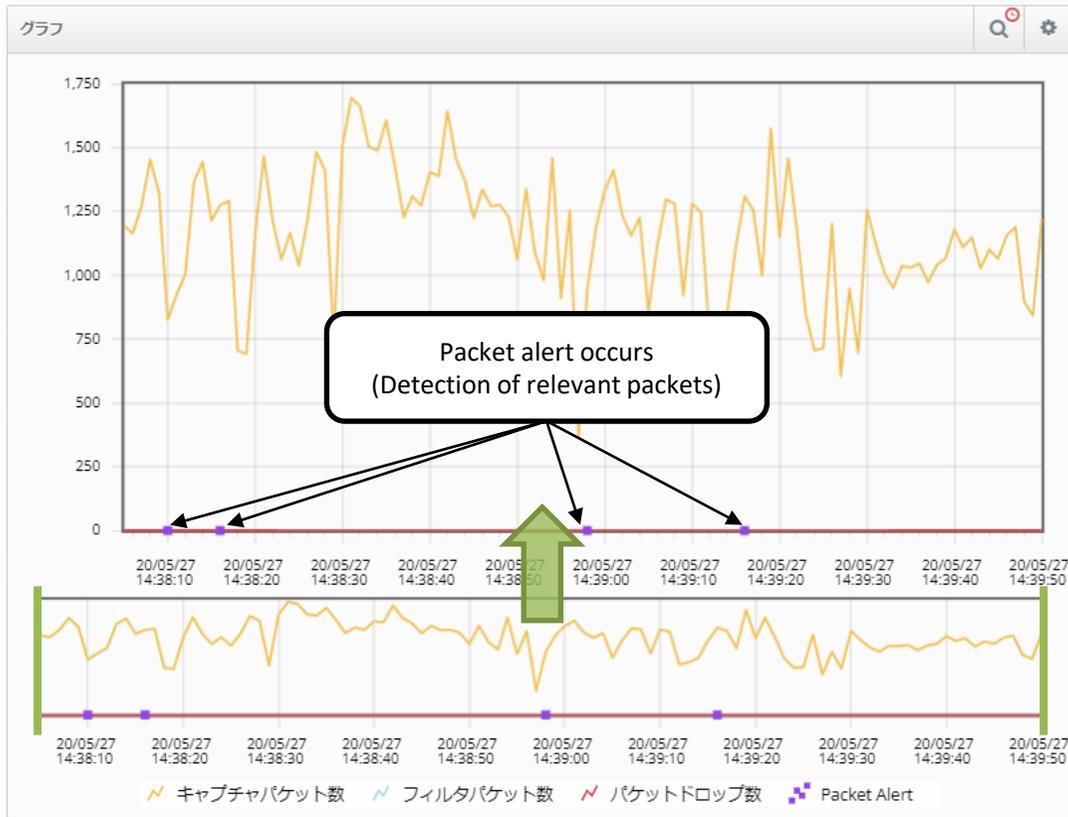
Lower Alert Threshold : Alerts when traffic volume is below

Higher Alert Threshold :Alerts when traffic volume exceeds

Analysis Unit : Alerts are generated if the threshold is exceeded or remains below during this time.

Notice Interval: interval between alerts.

Linkage to Packet Alerts



Packet Alert Settings

Alerts when a specific source IP address (64.215.171.61) is detected during capture.

(*Alert conditions can be set using Ethertype, protocol number, port number, pattern match, etc. in addition to IP address.)

Packet Alert Configuration

Count:

Analysis Unit: seconds

Notice Interval: seconds

Count : Alerts are generated if more than this value of packets are detected during the analysis unit.

Analysis Unit : Time to perform analysis.

Notice Interval Interval between alerts.

Packet View displays the last 100 packets information. It is possible to display a decoding summary (for 100 packets) of the previous packets by sliding the slide bar (red line at the right end) of the graph in the upper right corner with the mouse. It is also possible to display their detailed decodes by clicking on each packet summary line.

Packet Viewer | Capture Period: 2020-06-30 16:40:19 ~ 2020-06-30 16:45:33

Total Files 5205	Total Size 162.65 GB	Aquisition Period 5 minutes 14 seconds	Total Packets 2,217,518,764 (approx)	Timeline 2020-06-30 16:41:57	
---------------------	-------------------------	---	---	---------------------------------	--

Search: Show 10 entries

Time	Length	Mac Address	IP Address	Protocol/Port	VLAN 1	VLAN 2	Info	Action
2020/06/30:16:41:57.444346675	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 50.235.0.0 Dst: 0.0.0.0	Type: TCP Src Port: 22314 Dst Port: 0	ID:	ID:	22314 \xe2\x86\x92 0 [Reserved] Seq=5073 8 Win=822[Malf...	
2020/06/30:16:41:57.444346745	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 248.188.0.0 Dst: 0.0.0.0	Type: UDP Src Port: 63676 Dst Port: 45597	ID:	ID:	63676 \xe2\x86\x92 45597 Len=18	
2020/06/30:16:41:57.444346809	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 50.236.0.0 Dst: 0.0.0.0	Type: TCP Src Port: 61479 Dst Port: 0	ID:	ID:	61479 \xe2\x86\x92 0 [NS, Reserved] Seq=1 Win=822, bogu...	
2020/06/30:16:41:57.444346873	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 248.189.0.0 Dst: 0.0.0.0	Type: UDP Src Port: 63677 Dst Port: 29067	ID:	ID:	63677 \xe2\x86\x92 29067 Len=18	
2020/06/30:16:41:57.444346944	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 50.237.0.0 Dst: 0.0.0.0	Type: TCP Src Port: 43606 Dst Port: 0	ID:	ID:	43606 \xe2\x86\x92 0 [Reserved] Seq=1 Wi n=822, bogus TC...	
2020/06/30:16:41:57.444347014	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 248.190.0.0 Dst: 0.0.0.0	Type: UDP Src Port: 63678 Dst Port: 23992	ID:	ID:	63678 \xe2\x86\x92 23992 Len=18	
2020/06/30:16:41:57.444347078	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 50.238.0.0 Dst: 0.0.0.0	Type: TCP Src Port: 12260 Dst Port: 0	ID:	ID:	12260 \xe2\x86\x92 0 [NS, Reserved] Seq=1 Win=822, bogu...	
2020/06/30:16:41:57.444347142	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 248.191.0.0 Dst: 0.0.0.0	Type: UDP Src Port: 63679 Dst Port: 40913	ID:	ID:	63679 \xe2\x86\x92 40913 Len=18	
2020/06/30:16:41:57.444347212	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 50.239.0.0 Dst: 0.0.0.0	Type: TCP Src Port: 30442 Dst Port: 0	ID:	ID:	30442 \xe2\x86\x92 0 [] Seq=1 Win=822, bo gus TCP ...	
2020/06/30:16:41:57.444347283	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 50.240.0.0 Dst: 0.0.0.0	Type: TCP Src Port: 26159 Dst Port: 0	ID:	ID:	26159 \xe2\x86\x92 0 [Reserved] Seq=1 Wi n=822, bogus TC...	

Showing 1 to 10 of 100 entries

[Go to Post Filter](#)
[More Packets](#)
[First](#)
[Previous](#)
[1](#)
[2](#)
[3](#)
[4](#)
[5](#)
[Next](#)
[Last](#)

Packet View Summary Table

Time	Packet Length	Source	Destination	Type	Details
2021/07/08:11:33:00.000569337	1301	04:f4:bc:08:1c:24	172.16.1.5	TCP	[TCP ZeroWindow] 443 x8 6x92 443 [Seq =1 Wi...
2021/07/08:11:33:00.00055878	276	04:f4:bc:08:1c:24	10.1.0.1	TCP	[TCP ZeroWindow] 8080 x8 86x92 8080 [Seq eq+1 ...

Select

Displayed below the packet record

Packet details in the Packet Viewer are displayed directly below the packet summary. Moving up and down the page is no longer necessary, making it easier to check detailed information on the selected packet.

Frame 6: 1301 bytes on wire (10408 bits), 1301 bytes captured (10408 bits)

Ethernet II, Src: XenaNetw_08:1c:24 (04:f4:bc:08:1c:24), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)

Destination : 00:00:00_00:00:00 (00:00:00:00:00:00)
Address : 00:00:00_00:00:00 (00:00:00:00:00:00)
... 0. = **LG bit** : Globally unique address (factory default)
... 0. = **IG bit** : Individual address (unicast)

Source : XenaNetw_08:1c:24 (04:f4:bc:08:1c:24)
Address : XenaNetw_08:1c:24 (04:f4:bc:08:1c:24)
... 0. = **LG bit** : Globally unique address (factory default)
... 0. = **IG bit** : Individual address (unicast)

Type : IPv4 (0x0800)
Frame check sequence : 0xdb4058ba [unverified]
FCS Status : Unverified

Internet Protocol Version 4, Src: 172.16.1.5, Dst: 172.16.21.200

0100 = Version : 4
... **0101 = Header Length :** 20 bytes (5)
Differentiated Services Field : 0x00 (DSCP: CS0, ECN: Not-ECT)

In addition, indentation of major items such as MAC address, IP address, and port number has improved visibility.

Post Filter Condition Setting

You can move to the Post Filter page with a filter condition regarding clicked packet. Set automatically a filter condition created to an insert form.

Select fields to include in the filter condition by checkbox. When toggle a checkbox, the "filter condition inserted" changes automatically. If a field is empty, checkbox disables and can't change it.

If you switch to "Both ways", it is created a filter string that can filter traffics of both ways(Request and Response messages etc).

Press the "Go to Post Filter" button to move to the Post Filter in a new tab.

Direction: One way Both ways

- Time: 2023/01/31:11:50:57.000000044
※The filter period can be adjusted after going to the Post Filter page.
- Frame Length: 64
- Source MAC Address: 04:f4:bc:08:0f:a0
- Destination MAC Address: 00:00:00:00:00:00
- Ether Type: 0x0800
- VLAN ID1 (Outer): -
- VLAN ID2 (Inner): -
- Source IP Address: 244.182.0.1
- Destination IP Address: 248.121.0.2
- Protocol: 6
- Source Port: 0
- Destination Port: 0

Filter condition inserted

```
frame.len=64&&eth.type=0x0800&&eth.src= 04:f4:bc:08:0f:a0,00:00:00:00:00:00&&eth.dst= 00:00:00:00:00:00,04:f4:bc:08:0f:a0&&ip.src= 244.182.0.1,248.121.0.2&&ip.dst= 248.121.0.2,244.182.0.1&&ip.proto=6&&port.src=0,0&&port.dst=0,0
```

By clicking on the "magnifying glass icon" of a packet displayed in the Packet Viewer, you can create a post-filter to extract that packet with a single touch.

In addition, by selecting the "Both ways" option and choosing a time period from the slide bar in the post-filter window, you can immediately extract packets from a series of socket communications.

***Select HTTP packets from the packet viewer in the figure on the left.**

Start Time (S) 2023/01/31:11:50:57 000000

End Time (E) 2023/01/31:11:50:57 000001

Capture Range: 2023-01-31 11:45:20 - 2023-01-31 12:20:35

Packet Limit: Enable 1

Verbose Mode: Enable

Filter: `frame.len=64&ð.type=0x0800&ð.src= 04:f4:bc:08:0f:a0,00:00:00:00:00:00&ð.dst= 00:00:00:00:00:00,04:f4:bc:08:0f:a0&&ip.src= 244.182.0.1,248.121.0.2&&ip.dst= 248.121.0.2,244.182.0.1&&ip.proto=6&&port.src=0,0&&port.dst=0,0`

Post Filter

※The page opens with a filter set to allow extraction of the target packets.

Click the "Go to Post Filter" button to go immediately to the post filter page.

Post Filter Result Table

時刻	MACアドレス	イーサタイプ	VLAN1/VLAN2 ID	IPアドレス	プロトコル番号	ポート	パターン	GTP-U (Inner)	バイト
2020-05-27 19:11:34.923713913	Src: 00:40:10:14:48:AF Dst: 00:C0:9F:27:44:75	0x0800/ - / -	VLAN1 ID: - VLAN2 ID: -	Src: 164.71.1.148 Dst: 202.33.141.44	6	Src: 48748 Dst: 80	-	-	82
2020-05-27 19:11:34.924641920	Src: 00:C0:9F:27:44:75 Dst: 00:40:10:14:48:AF	0x0800/ - / -	VLAN1 ID: - VLAN2 ID: -	Src: 202.33.141.44 Dst: 164.71.1.148	6	Src: 80 Dst: 48748	-	-	82
2020-05-27 19:11:34.925811059	Src: 00:40:10:14:48:AF Dst: 00:C0:9F:27:44:75	0x0800/ - / -	VLAN1 ID: - VLAN2 ID: -	Src: 164.71.1.148 Dst: 202.33.141.44	6	Src: 48748 Dst: 80	-	-	68
2020-05-27 19:11:34.930409337	Src: 00:40:10:14:48:AF Dst: 00:C0:9F:27:44:75	0x0800/ - / -	VLAN1 ID: - VLAN2 ID: -	Src: 164.71.1.148 Dst: 202.33.141.44	6	Src: 48748 Dst: 80	-	-	361

*Since "bidirectional" is selected in the settings window on the previous page, the response message to the specified packet can also be extracted together.

The following button under the post-filter result table can be pressed to output the extraction results to a PCAP file

フィルタ結果のPCAPエクスポート

example.pcap

Download to local machine

抽出結果(Wireshark画面)

Enter the File name of the PCAP to be exported

No.	Time	Source	Destination	Protocol	Length	Info
1	1590574294.923713913	164.71.1.148	202.33.141.44	TCP	82	48748 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=...
2	1590574294.924641920	202.33.141.44	164.71.1.148	TCP	82	80 → 48748 [SYN, ACK] Seq=0 Ack=1 Win=5792...
3	1590574294.925811059	164.71.1.148	202.33.141.44	TCP	68	48748 → 80 [ACK] Seq=1 Ack=1 Win=5792 Len=0
4	1590574294.930409337	164.71.1.148	202.33.141.44	HTTP	361	GET /banner_img/top04.jpg HTTP/1.0
5	1590574294.931095852	202.33.141.44	164.71.1.148	TCP	74	80 → 48748 [ACK] Seq=1 Ack=288 Win=6432 Le...
6	1590574294.932103929	202.33.141.44	164.71.1.148	TCP	1476	80 → 48748 [ACK] Seq=1 Ack=288 Win=6432 Le...
7	1590574294.933498566	202.33.141.44	164.71.1.148	TCP	1476	80 → 48748 [ACK] Seq=1403 Ack=288 Win=6432...
8	1590574294.937964006	164.71.1.148	202.33.141.44	TCP	74	48748 → 80 [ACK] Seq=288 Ack=1403 Win=8412...
9	1590574294.938778124	202.33.141.44	164.71.1.148	TCP	1476	80 → 48748 [PSH, ACK] Seq=2805 Ack=288 Win...
10	1590574294.940319526	202.33.141.44	164.71.1.148	TCP	1476	80 → 48748 [ACK] Seq=4207 Ack=288 Win=6432...
11	1590574294.941046803	164.71.1.148	202.33.141.44	TCP	74	48748 → 80 [ACK] Seq=288 Ack=2805 Win=1121...

> Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
 > Ethernet II, Src: SonicMac_14:48:af (00:40:10:14:48:af), Dst: QuantaCo_27:44:75 (00:c0:9f:27:44:75)
 > Internet Protocol Version 4, Src: 164.71.1.148, Dst: 202.33.141.44
 > Transmission Control Protocol, Src Port: 48748, Dst Port: 80, Seq: 0, Len: 0

Statistics output function

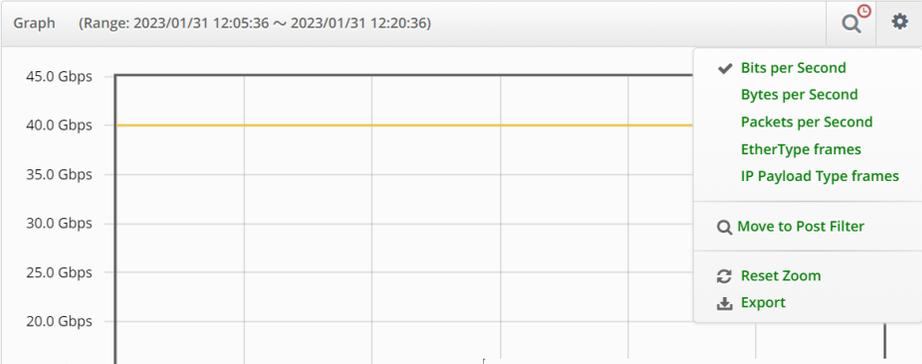
Various statistical information acquired by Sirius can be output in CSV format at the following intervals.

Acquisition Information

- Amount of data received (bytes)
- Number of packets received
- Number of filtered dropped frames
- Number of dropped frames
- Number of unicast frames
- Number of multicast frames
- Number of broadcast frames

Output Interval

- 1 second (data within the past 1 day)
- 15 seconds (data within the past 1 to 7 days)
- 1 minute (Data within the past 7 days but less than 1 month)
- 5 minutes (data within the past 30 days but less than 4 months)
- 15 minutes (data for the past 4 months or more but less than 1 year)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	timestamp	bytes_rec	packets_n	packets_d	packets_f	port1_byte	port2_byte	port3_byte	port4_byte	ipv4_pack	ipv6_pack	vlan_pack	fcsoe_fram	other_13_f	tcp_packe
2	2023-01-31 11:00	5E+09	59523064	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523072	0	0	0	0	59523072
3	2023-01-31 11:00	5E+09	59523072	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523067	0	0	0	0	59523067
4	2023-01-31 11:00	5E+09	59523068	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523069	0	0	0	0	59523069
5	2023-01-31 11:00	5E+09	59523070	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523072	0	0	0	0	59523072
6	2023-01-31 11:00	5E+09	59523071	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523072	0	0	0	0	59523072
7	2023-01-31 11:00	5E+09	59523071	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523072	0	0	0	0	59523072
8	2023-01-31 11:00	5E+09	59523072	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523072	0	0	0	0	59523072
9	2023-01-31 11:00	5E+09	59523072	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523074	0	0	0	0	59523074
10	2023-01-31 11:00	5E+09	59523075	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523074	0	0	0	0	59523074
11	2023-01-31 11:00	5E+09	59523073	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523072	0	0	0	0	59523072
12	2023-01-31 11:00	5E+09	59523074	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523076	0	0	0	0	59523076
13	2023-01-31 11:00	5E+09	59523074	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523076	0	0	0	0	59523076
14	2023-01-31 11:00	5E+09	59523076	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523076	0	0	0	0	59523076
15	2023-01-31 11:00	5E+09	59523076	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523076	0	0	0	0	59523076

Export Graph Data

Filename: .CSV

Filename must contains more than 4 characters, else it will be exported as export.csv.

Data: Selected data only All data

Buttons: Close, Export

The Following management functions are available for captured files by Sirius.

- Information view of capture files
- Delete capture files one by one
- Capture file lock
- Split capture file
- Merge multiple capture files
- Zip compression of multiple capture files

Selected Files

Show 10 entries First Previous 1 Next Last

	Filename	Filesize	Create Time
1	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0003.pcap	256 MB	2023/01/31 11:45:20
2	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0004.pcap	256 MB	2023/01/31 11:45:20
3	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0005.pcap	256 MB	2023/01/31 11:45:20
4	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0002.pcap	256 MB	2023/01/31 11:45:20

Showing 1 to 4 of 4 entries First Previous 1 Next Last

General

Remove Files

Clear Selected Files

Lock/Unlock Files

Split Files

Merge/ZIP and Packet Slice Files

Allows you to select 1 or more files to merge/zip them into one pcap file. You can select enable or disable for the packet slicing as option.

You can merge/zip up to 999 files.

Merge ZIP

General

Remove Files

Clear Selected Files

Lock/Unlock Files

Split Files

Merge/ZIP and Packet Slice Files

Merge PCAP Files

Filename: SampleMerge.pcap

Packet Slice:

Close Submit

Processed Files

Server is currently merging files. Check Processed Tab for the file once completed.

Search: Show 10 entries First Previous 1 Next Last

	Filename	File Action	Packet Slice	Filesize	Started Time / Finished Time / Elapsed Time	Status	Actions
1	SampleMerge.pcap	Merge	None	1024 MB	2023-02-02 11:57:35 / 2023-02-02 11:57:38 / 00:00:03	Completed	

Showing 1 to 1 of 1 entries First Previous 1 Next Last

File Lock Function

This function is to disable deletion for individual capture files in Sirius.

Locked capture files are not subjected to be deleted during rotation.
By linking with various alerts, it is possible to keep capture files and analyze abnormal packets.

Captured Files ⓘ

Search: ⓘ Show 10 entries First Previous 1 2 3 4 5 Next Last

▲		Filename	Filesize	Create Time	Actions
1	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0002.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
2	<input checked="" type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0003.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
3	<input checked="" type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0004.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
4	<input checked="" type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0005.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
5	<input checked="" type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0006.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
6	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0007.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
7	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0008.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
8	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0009.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
9	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0010.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
10	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0011.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇

Showing 1 to 10 of 37,520 entries First Previous 1 2 3 4 5 Next Last



Captured Files ⓘ

Search: ⓘ Show 10 entries First Previous 1 2 3 4 5 Next Last

▲		Filename	Filesize	Create Time	Actions
1	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0002.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
2	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0003.pcap 🔒	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
3	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0004.pcap 🔒	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
4	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0005.pcap 🔒	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
5	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0006.pcap 🔒	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
6	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0007.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
7	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0008.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
8	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0009.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
9	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0010.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇
10	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0011.pcap	256 MB	2023/01/31 11:45:20	ⓘ Ⓞ ⬇

Showing 1 to 10 of 37,520 entries First Previous 1 2 3 4 5 Next Last

Each saved PCAP files can be packet sliced.

Follow the steps below to perform packet slicing and downloading.

Captured Files ⓘ ⚙️

Search: ⓘ Show entries First Previous 1 2 3 4 5 Next Last

▲		Filename	Filesize	Create Time	① Actions
1	<input type="checkbox"/>	Test-Ch1-p1234-10Gx4-2023-01-31-114520-0002.pcap	256 MB	2023/01/31 11:45:20	ⓘ ✂️ ⬇️



Download a PCAP File with Packet Slicing ✕

Slices the packets contained in the selected PCAP file into the specified packet size and downloads them.

※ As packet slicing is performed prior to download, large files may require a long processing time before download can be completed. ②

Packet Slice Size: Bytes

※ Packet slice size can range from 14 bytes to 10,000 bytes

③ Close Download

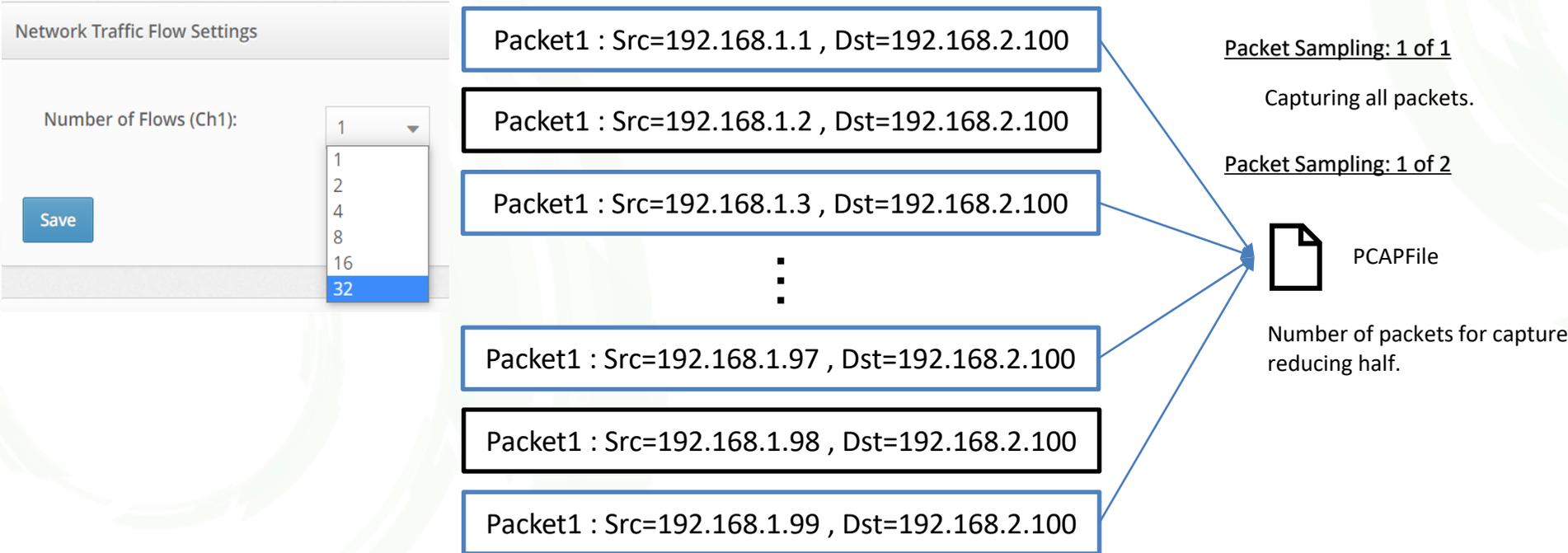
- ① Click on the ✂️ button in the Operation column of the target File.
- ② A popup will appear. Enter the slice size in bytes in the "Packet Slice Size" field in the popup.
- ③ Click the "Download" button.

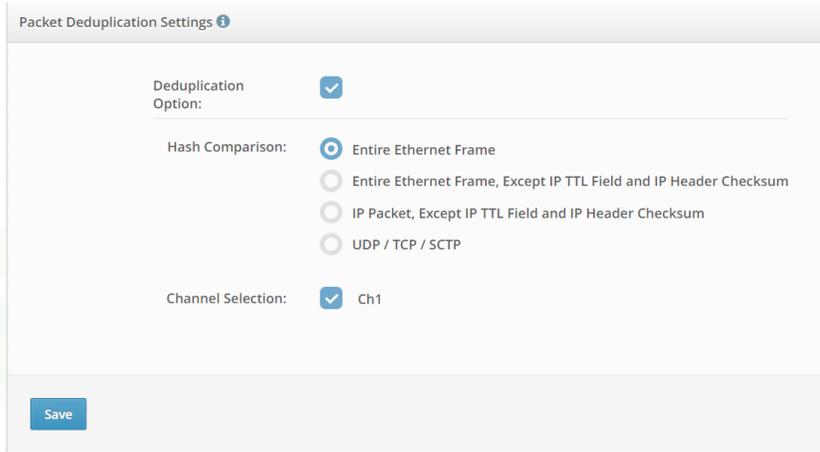
**If the size of the PCAP file is large, it may take time to download the file due to the time required to process the packet slices.*

This function randomly reduces the number of Sirius capture packets based on IP pairs

You can reduce the number of captured packets to 1/32 IP pair by setting the flow packet rate to “32”.

Calculating statistics more accurately by randomly reducing data based on IP pairs from large number of packets.





Packet Deduplication Settings ⓘ

Deduplication Option:

Hash Comparison:

- Entire Ethernet Frame
- Entire Ethernet Frame, Except IP TTL Field and IP Header Checksum
- IP Packet, Except IP TTL Field and IP Header Checksum
- UDP / TCP / SCTP

Channel Selection: Ch1

Save



Ch1 Flow: Off Deduplication: Off

This function detects and eliminates duplicate packets from packets forwarded to each port on the same channel. It compares the hash values of packets received in a time frame of up to 100 ms and eliminates packets when the hash values are identical.

You can choose from the following four hash value generation methods.

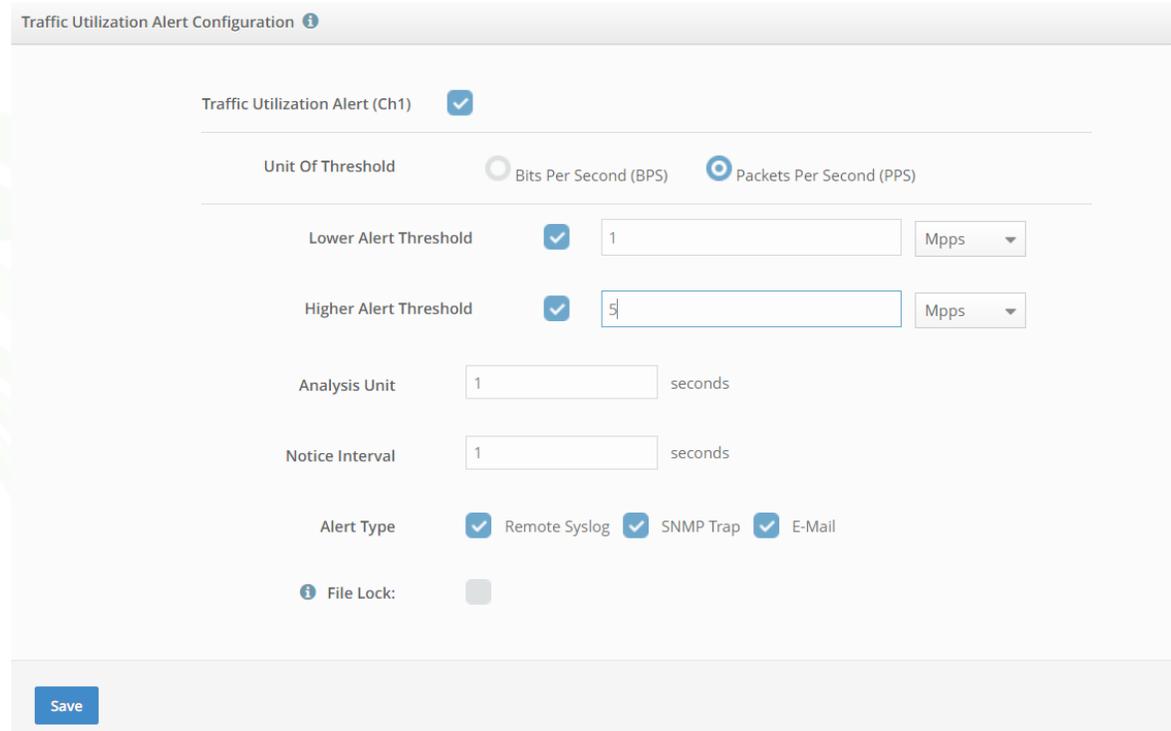
- Entire Ethernet frame
- Use byte sequence
- Use the byte sequence of the entire Ethernet frame (excluding the TTL field of the IP header and the checksum)
- Use the byte sequence of the entire IP packet (excluding the TTL field of the IP header and the checksum)
- Uses the entire UDP / TCP / SCTP header and payload byte sequence

Duplicate packet elimination can be applied to each channel.

The **setting status** is displayed on the Capture Settings screen and Capture Session page.

The number of packets eliminated is counted in the "Number of filtered packets" in the statistics page.

This function generates an alert when the amount of traffic exceeds or falls below a specified level. It can be configured for each channel.



The screenshot shows the 'Traffic Utilization Alert Configuration' window. At the top, there is a title bar with the text 'Traffic Utilization Alert Configuration' and an information icon. Below the title bar, the main configuration area is divided into several sections. The first section is 'Traffic Utilization Alert (Ch1)' with a checked checkbox. The second section is 'Unit Of Threshold' with two radio buttons: 'Bits Per Second (BPS)' (unselected) and 'Packets Per Second (PPS)' (selected). The third section contains two rows for thresholds: 'Lower Alert Threshold' with a checked checkbox, a text input field containing '1', and a dropdown menu set to 'Mpps'; 'Higher Alert Threshold' with a checked checkbox, a text input field containing '5', and a dropdown menu set to 'Mpps'. The fourth section is 'Analysis Unit' with a text input field containing '1' and the text 'seconds'. The fifth section is 'Notice Interval' with a text input field containing '1' and the text 'seconds'. The sixth section is 'Alert Type' with three checked checkboxes: 'Remote Syslog', 'SNMP Trap', and 'E-Mail'. The seventh section is 'File Lock:' with an unchecked checkbox. At the bottom left of the configuration area, there is a blue 'Save' button.

Traffic Utilization Alert Setting

***The above image is an example of a setting that generates an alert when the rate falls below 1 Gbps or exceeds 5 Gbps.**

Error Frame Alert Configuration ⓘ

Error Frame Alert (Ch1)

Notice Interval minutes

Alert Type Remote Syslog SNMP Trap E-Mail

File Lock:

Save

Alerts can be output and File locks and SNMP traps can be sent when error frames are received.

Alerts can be output to Remote Syslog, SNMP Trap, or E-mail.

Alerts are sent to the administrator upon receipt of an error frame, allowing immediate detection of network anomalies.

Sirius can synchronize the time in the following three ways

- NTP(Network Time Protocol)
- PTP(Precision Time Protocol)
- Manual setting

The screenshot shows the 'System Time Configuration' window for NTP. At the top, 'NTP' is selected with a green dot, while 'PTP' and 'Manual' are unselected. The configuration includes: Peer IP: *218.186.3.36; Poll: 1024 log₂5; Delay: 79.470 ms; Offset: -2.914 (rms); Jitter: 4.100 (rms). It displays OS Time and Card Time as 2023-02-02 13:33:06.353663503 JST and 2023-02-02 13:33:06.353663481 JST, with a 22 ns difference. The Remote NTP Server is set to 'asia.pool.ntp.org'. The 'Capture Card Time Sync' is 'synchronized with software or other status' and the 'PPS IN Setting' is 'Synchronize card time with OS time without PPS signal (Default)'. At the bottom, there are buttons for 'Update', 'View log', 'One-Time Sync with NTP', 'Cancel', and 'Ping Test'.

NTP Setting

The screenshot shows the 'System Time Configuration' window for PTP. At the top, 'PTP' is selected with a green dot, while 'NTP' and 'Manual' are unselected. The configuration includes: Clock ID: fcaf6a.ffe.0296d0; Offset: -97.0 ns; Delay: 17663.0 ns. It displays OS Time and Card Time as 2023-02-02 13:35:01.342076528 JST and 2023-02-02 13:35:01.342076505 JST, with a 23 ns difference. The Slave NIC is 'eth0', Profile is 'Default Profile IEEE1588v2', Protocol is 'UDP(IPv4)', Delay Mechanism is 'Auto', Domain Number is '0', and PTP Delivery is 'Multicast Slave'. The 'Announce TX Interval' is '1 pkt/4sec' and 'Announce RX Timeout' is '3'. The 'Master Enable' checkbox is unchecked. The 'Capture Card Time Sync' is 'synchronized with software or other status' and the 'PPS IN Setting' is 'Synchronize card time with OS time without PPS signal (Default)'. At the bottom, there are buttons for 'Update', 'PTP Statistics', 'PTP Management Info', 'One-Time Sync with PTP', 'Cancel', and 'Ping Test'.

PTP Setting

SNMP Agent Function

A external SNMP manager can monitor Sirius status with SNMP MIB information.

SNMP Receive Trap Function

Sirius can lock capture files when receiving SNMP Trap from other devices.

SNMP Send Trap Function

Sirius can send an SNMP Trap if getting any status error.

File Lock Event Function

Sirius can lock capture files when sending SNMP Trap from Sirius.

Remote Syslog Function

Sirius can transfer own syslog to external device.

Packet Alert Mail Function

Sirius can send notification by e-mail if Packet Alert function detects matching packet as configured in advance.

Channel-to-channel exclusive control function

This is an extended group authorization method that allows assignment of authorization to perform key functions such as capture, capture file download, post filter, etc., on a per-channel basis.

Permissions to perform key functions such as capture, capture file download, and post-filter can be assigned on a per-channel basis. Each group can manage the resources of the same chassis by physical port, allowing multiple users to use a single chassis as multiple independent capture systems. As shown in the figure on the under, users belonging to Group A is only allowed to access physical ports 1 and 2 (channel 1), users belonging to Group B is only allowed to access physical ports 3 and 4 (channel 2). At the same time, users belonging to Group C can be configured to allow access to both Channel 1 and Channel 2. It is also possible to flexibly assign various privileges to each group.

