SwiftWing Sirius NDR

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

Rev.8 2022/12/20

SwiftWing Sirius NDR Overview

SwiftWing Sirius NDR Overview

MADE IN OTA, 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.

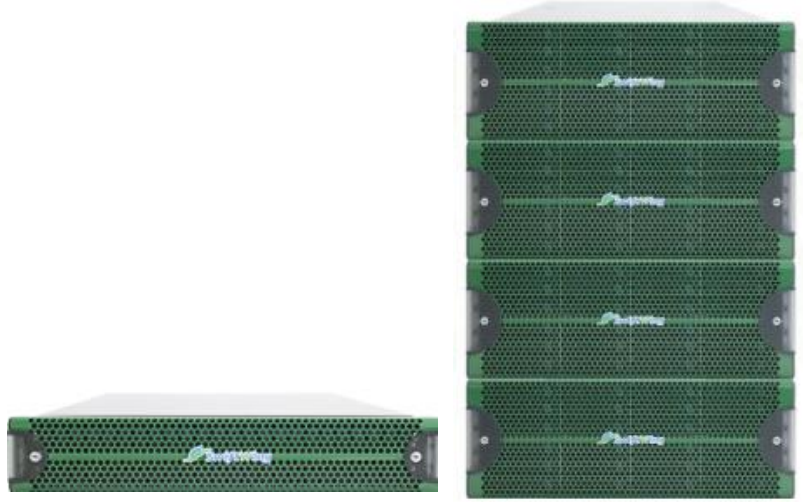
Storage Performance

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)	

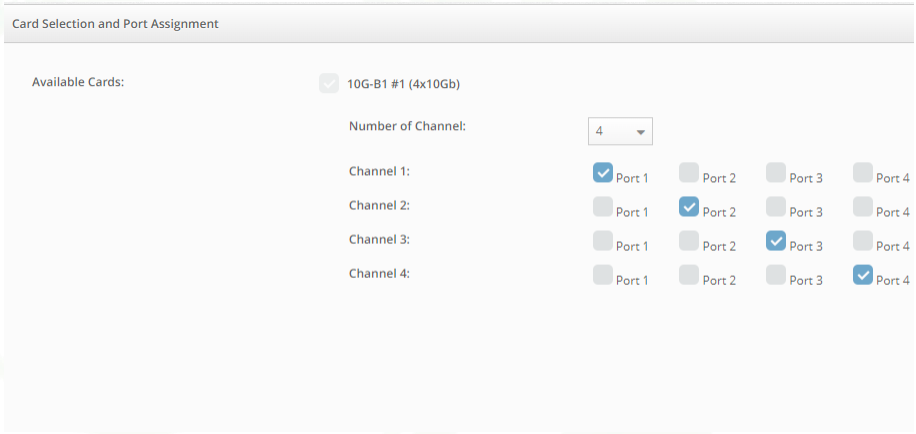
* 50G supports later

Multi Channel / Multi Port

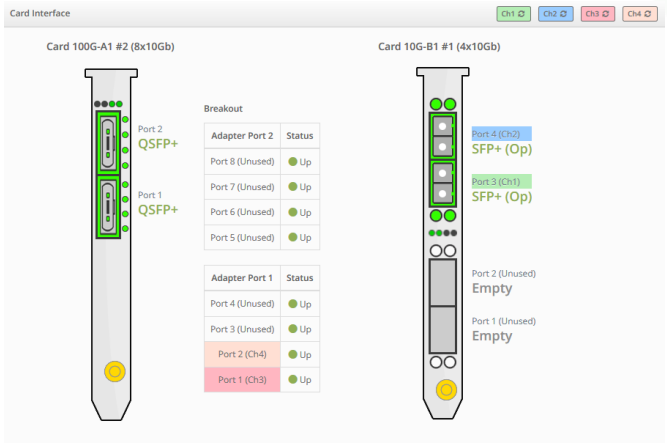
The Sirius NDR can be configured up to 4 channel according to the user settings and all 4 channels can capture simultaneously.
In each port configuration, up to 16 ports of media (100G-A2/A3 media interface card*2, 10G*8ports) can be assigned to each channel.

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

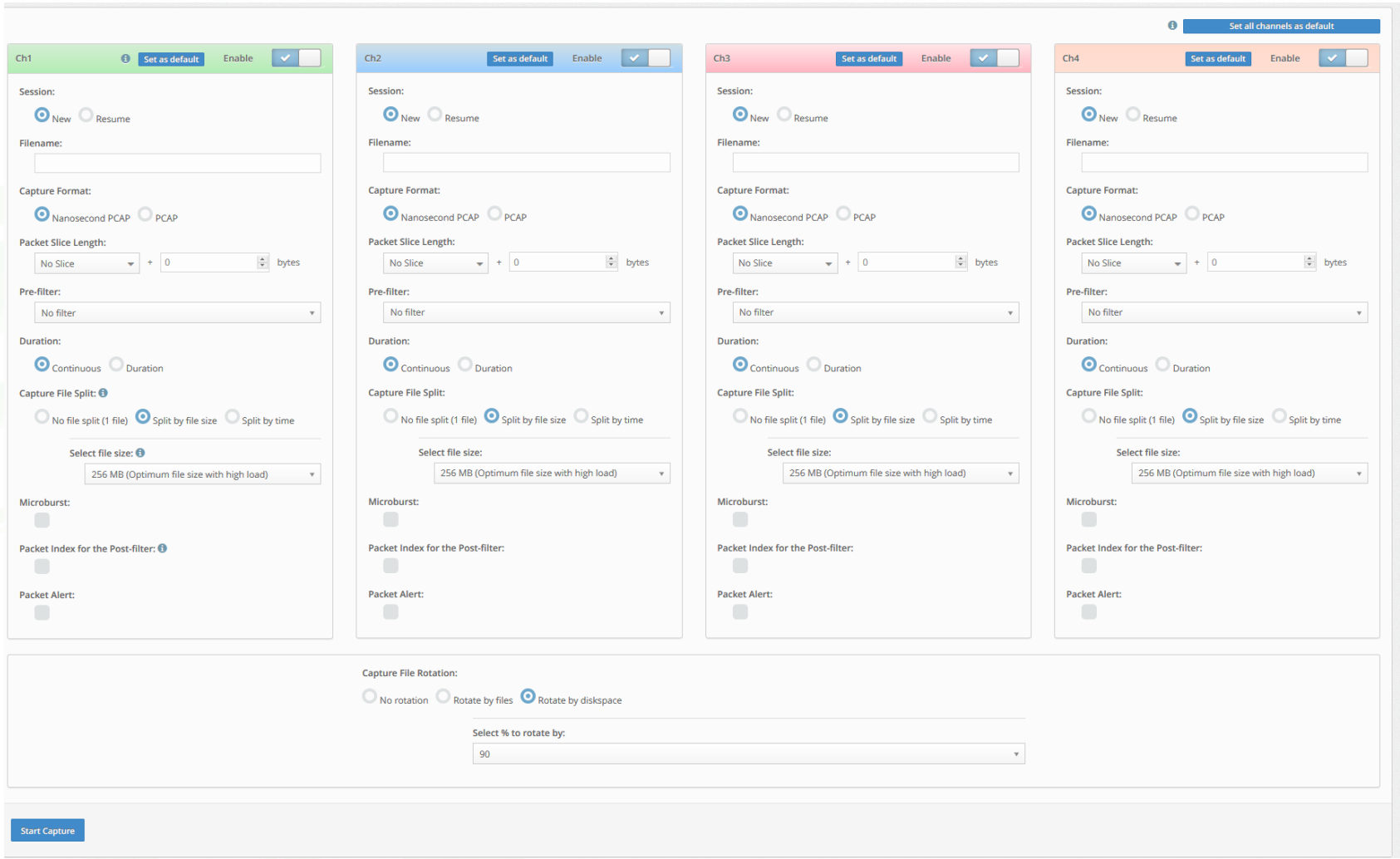


Channel configuration



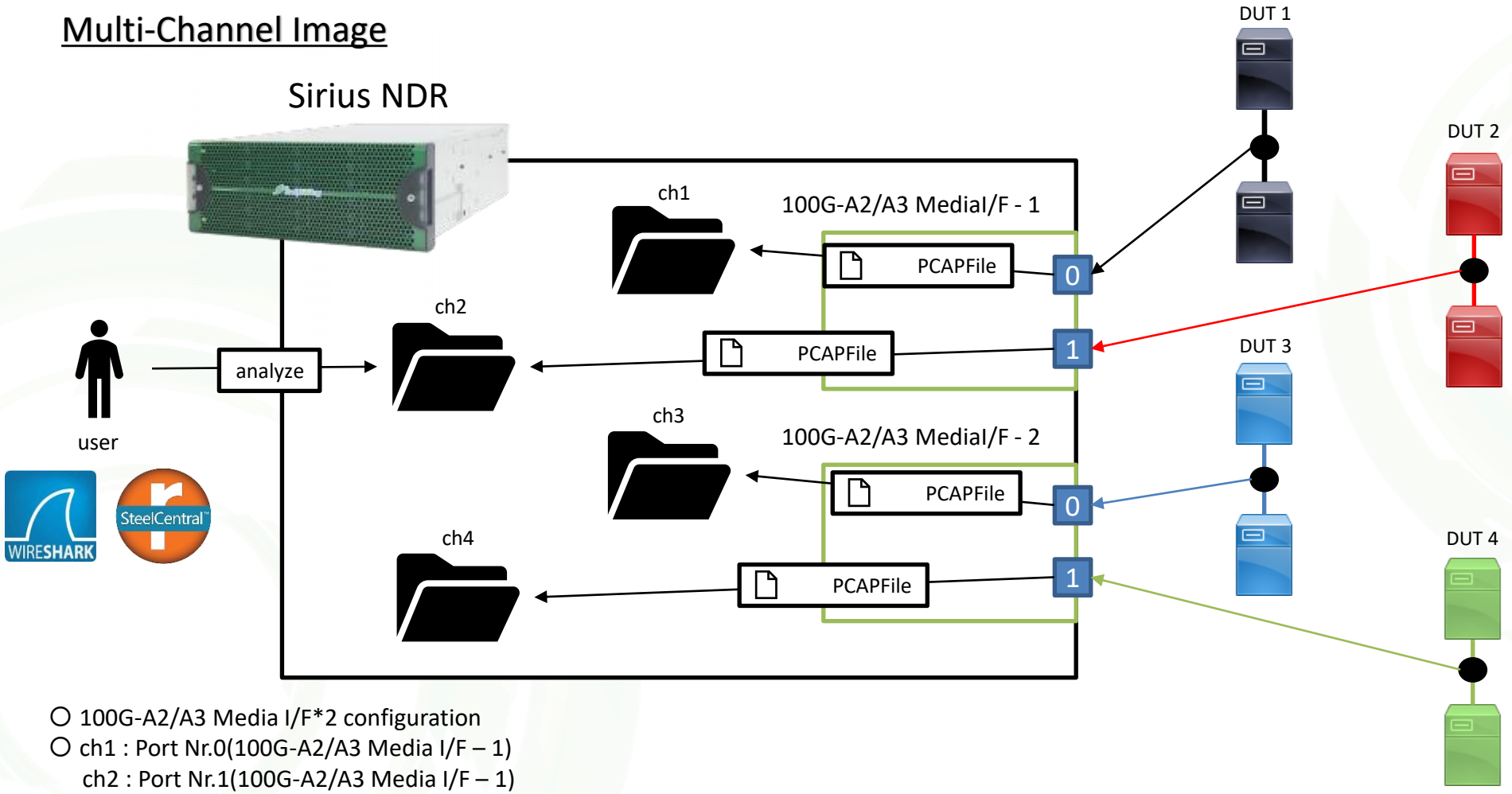
Dashboard

Multi Channel / Multi Port – 4-Channel configuration



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

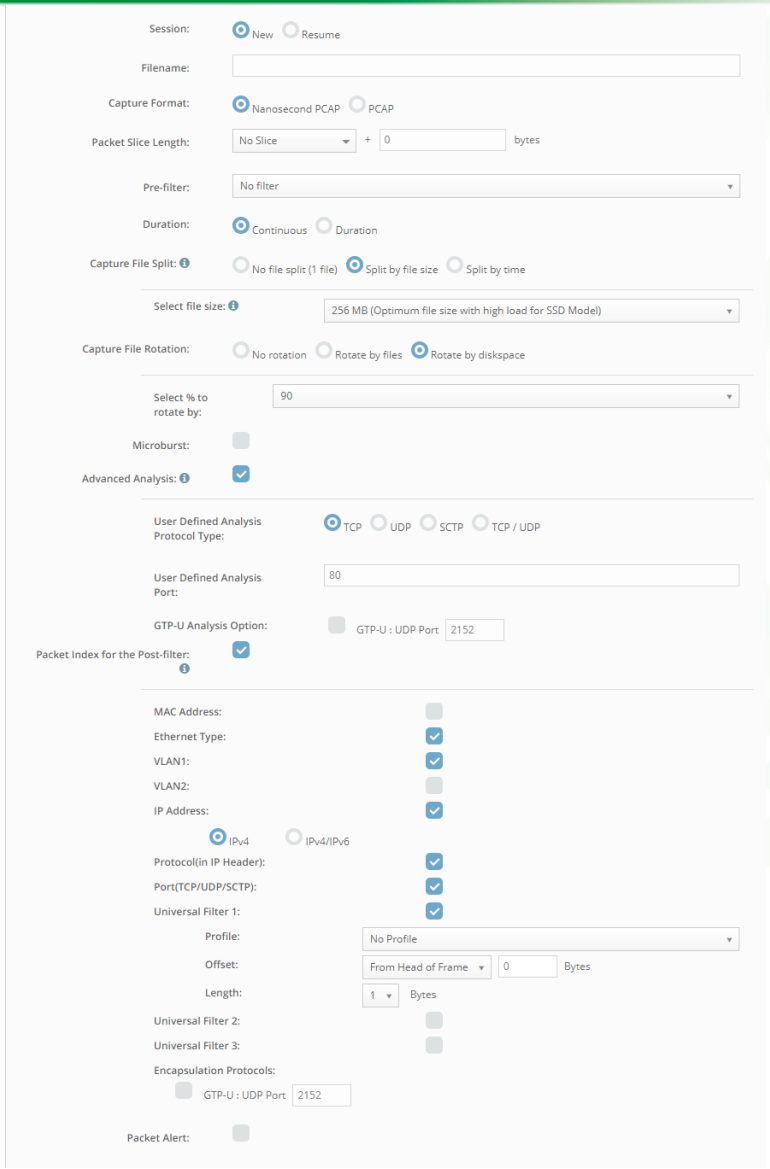
Capture-Function Overview

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

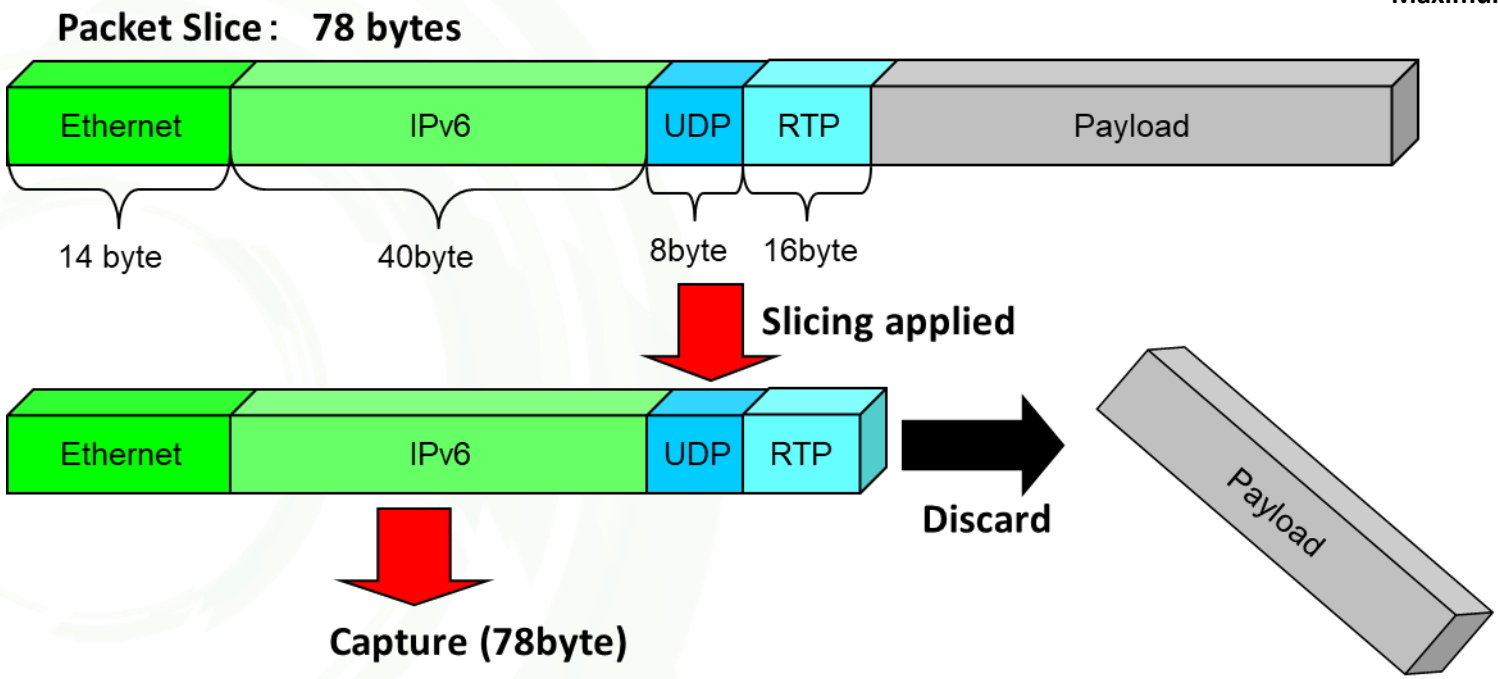


Capture Function – Packet Slice

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.

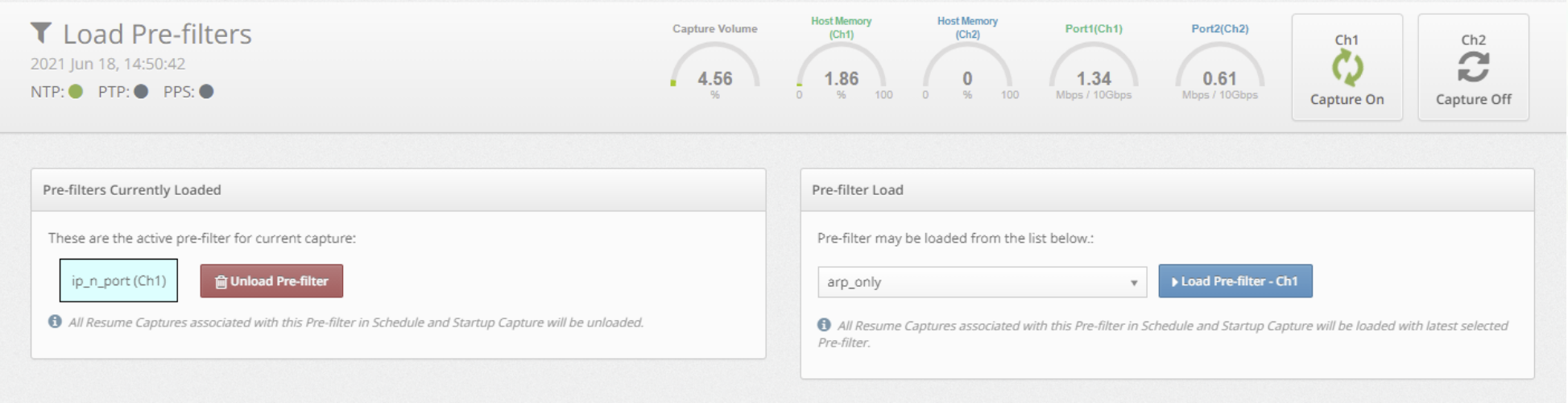
Minimum Packet-Slice size 64Byte
Maximum Packet-Slice size 10,000Byte



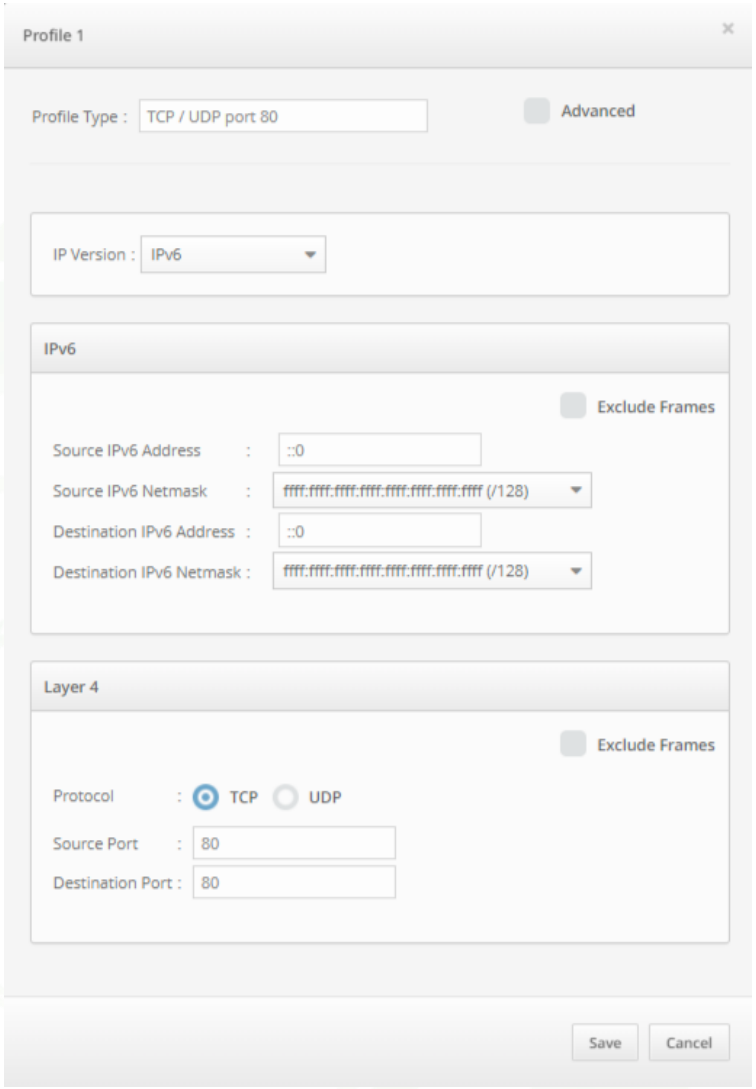
Capture Function – Pre-Filters

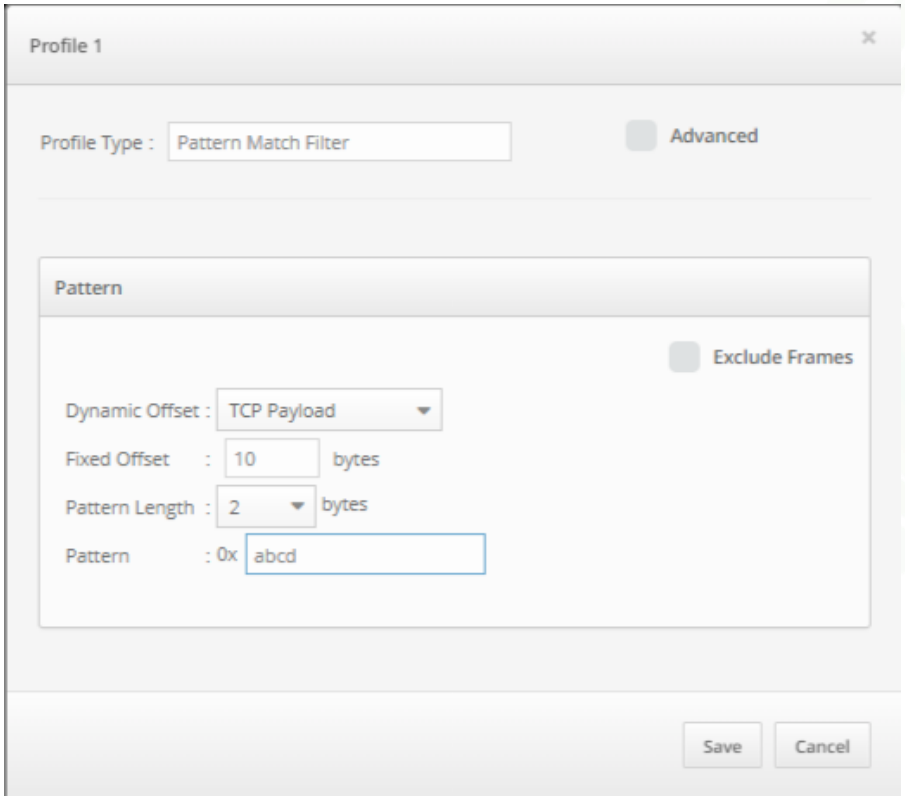
Pre-Filters can apply basic filters such as Mac address, IPv4 / IPv6 address, protocol type, TCP/UDP Port number and apply any value(Hex, Bit) to any offset of the packet.
Enabling this function will not affect capture performance.

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



Capture Function – Pre-Filters





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

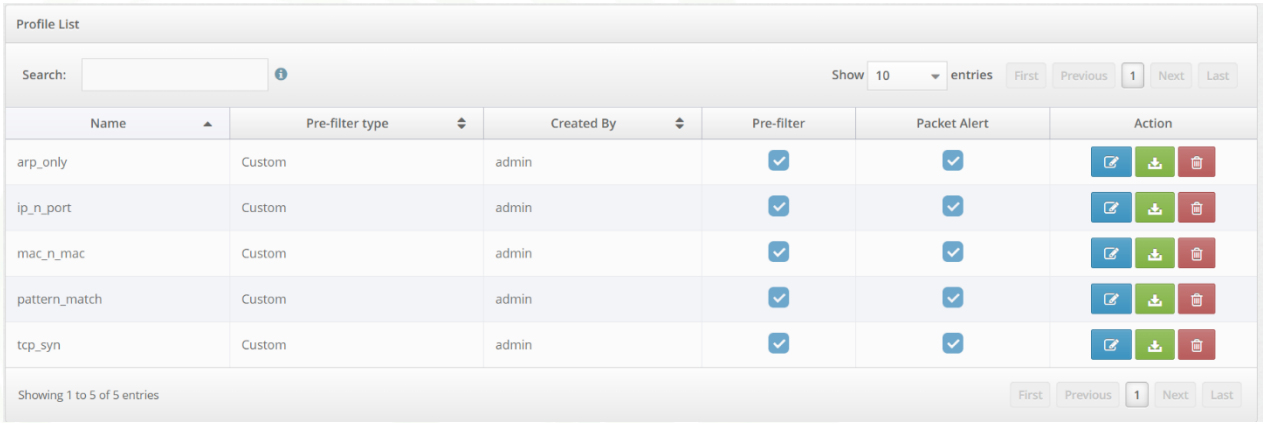
4. Error-type
   CRC、RUNT、Oversize、Fragment、Jabber、IP Checksum、TCP Checksum、UDP Checksum

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 .

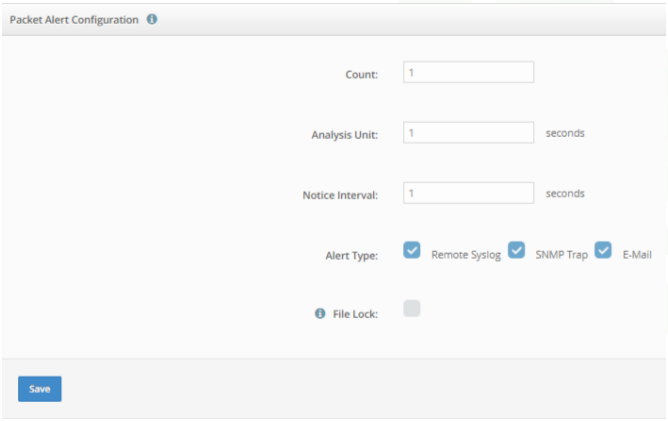
Capture Function – Packet-Alert Function

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.



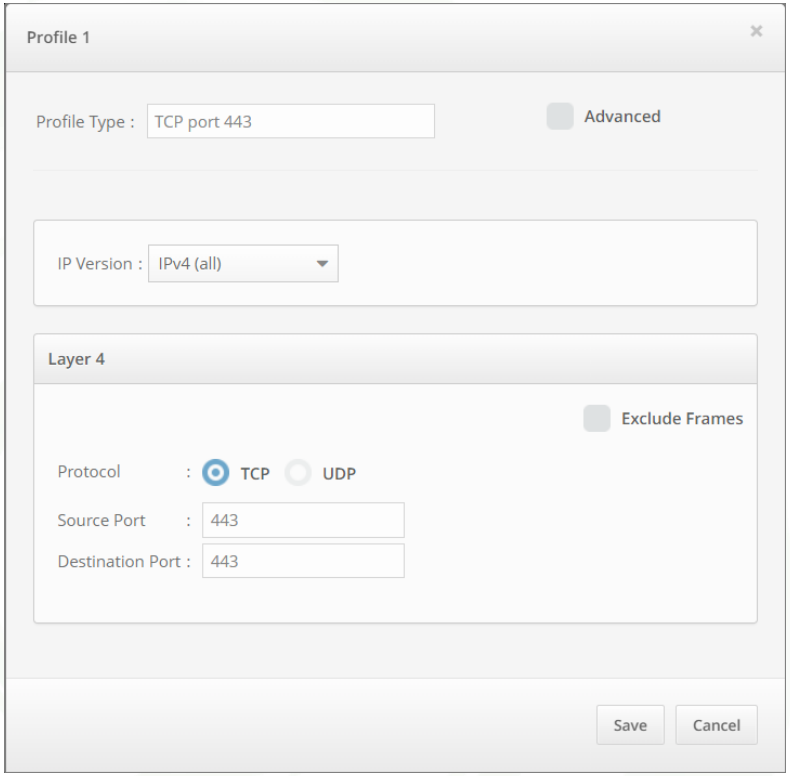
Packet-Alert definition control



Packet-Alert send Configuration

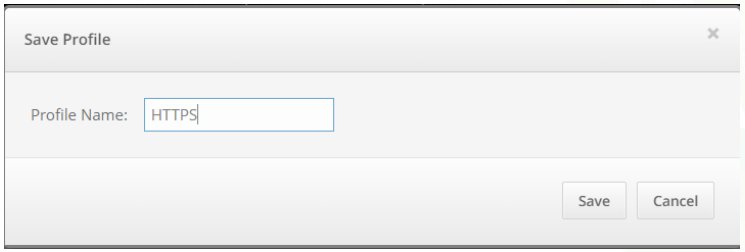
Example: Generate an alarm when detecting the following traffic

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



Packet-Alert definition configuration

Packet-Alert name configuration

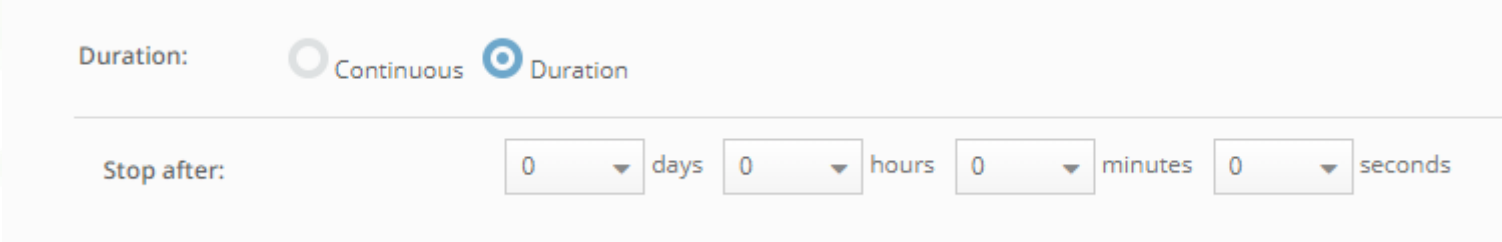


Capture configuration

Capture Function – Capture Period

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

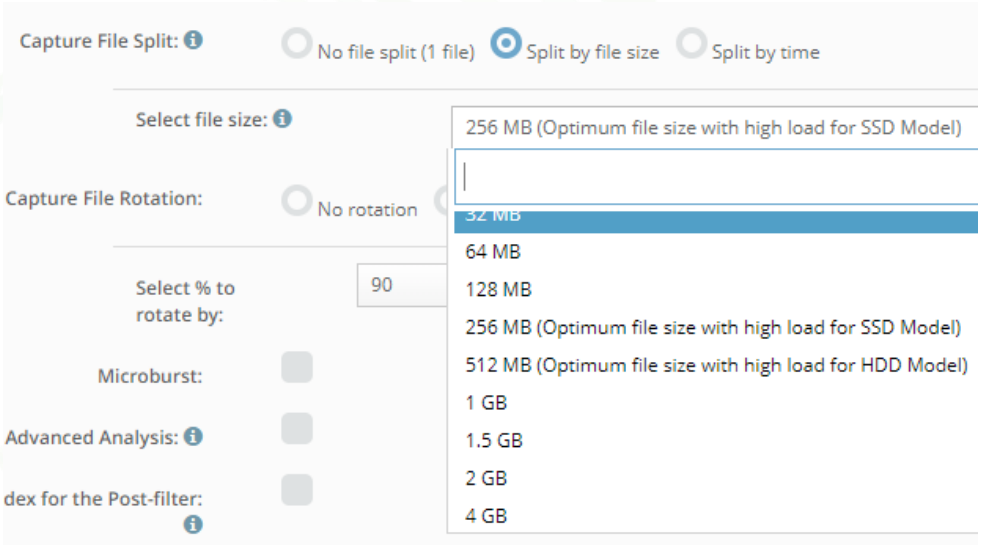


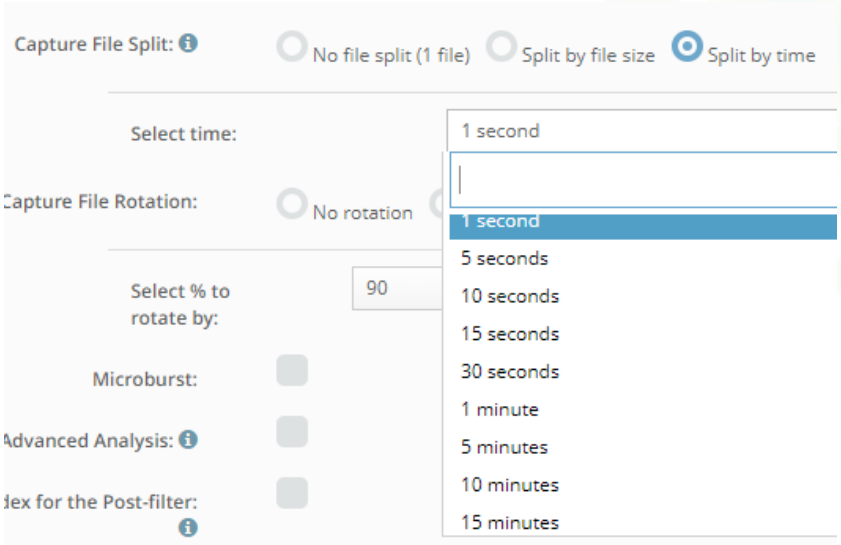
If the capture period is continuous, capture will continue until the stop button is pressed.

Capture Function – File Split

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

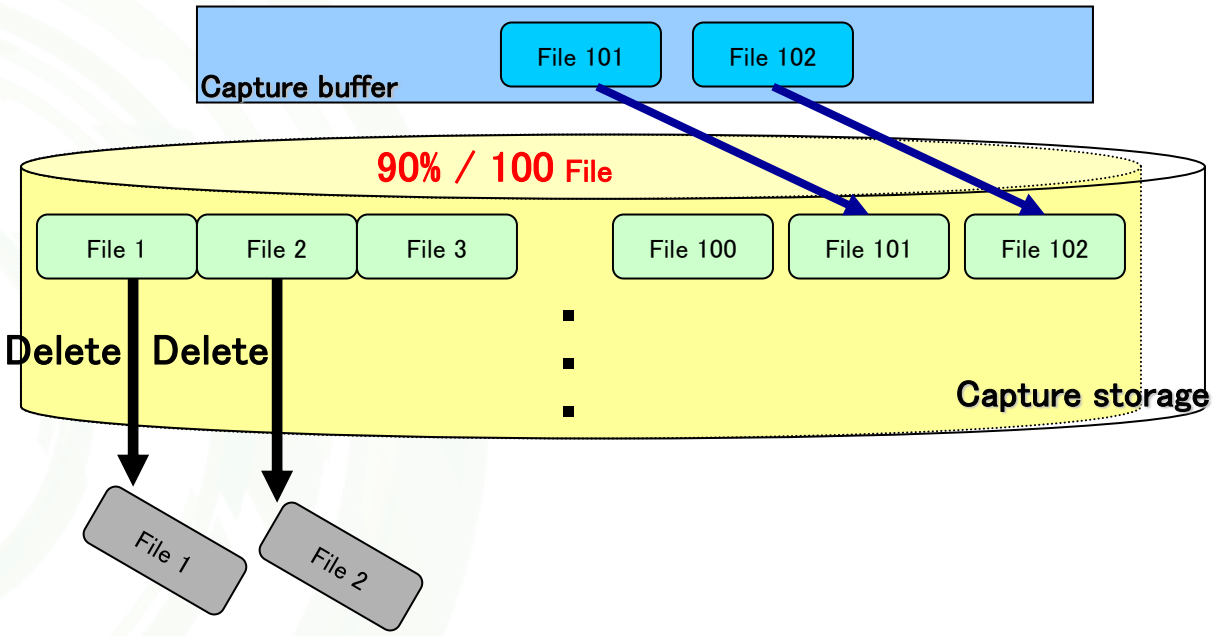




Capture Function – File Rotation

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.

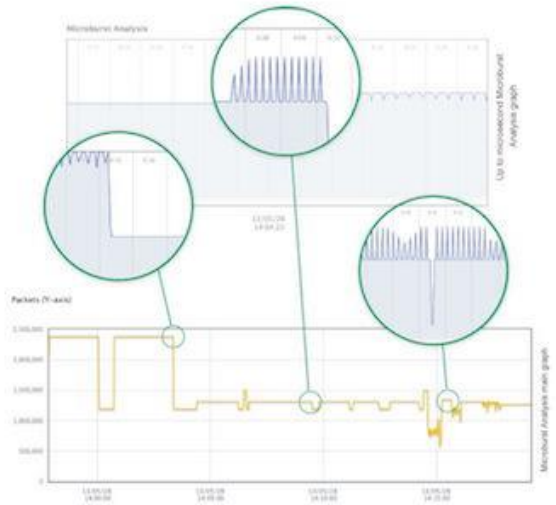
Using This function can realize continuous packet capture without interruption.

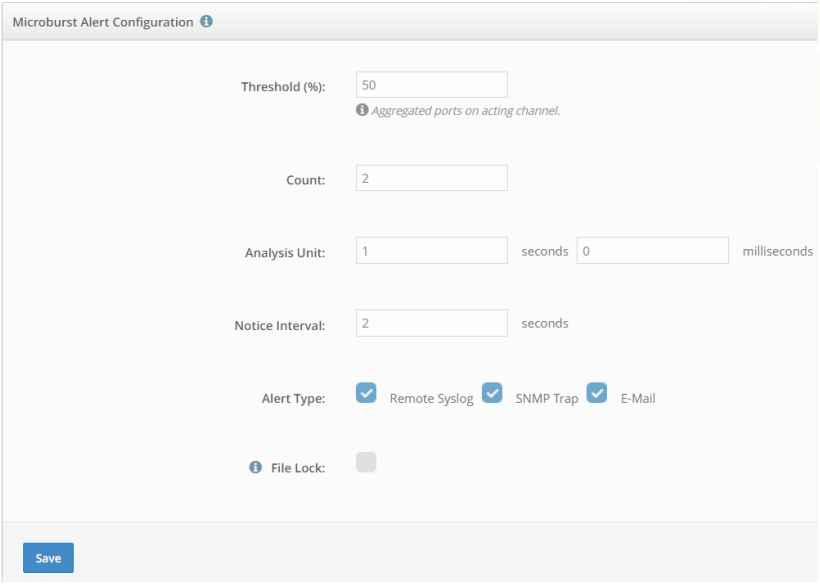


Capture Function – Microburst Analysis

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)





Capture Function – Traffic Analysis

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.

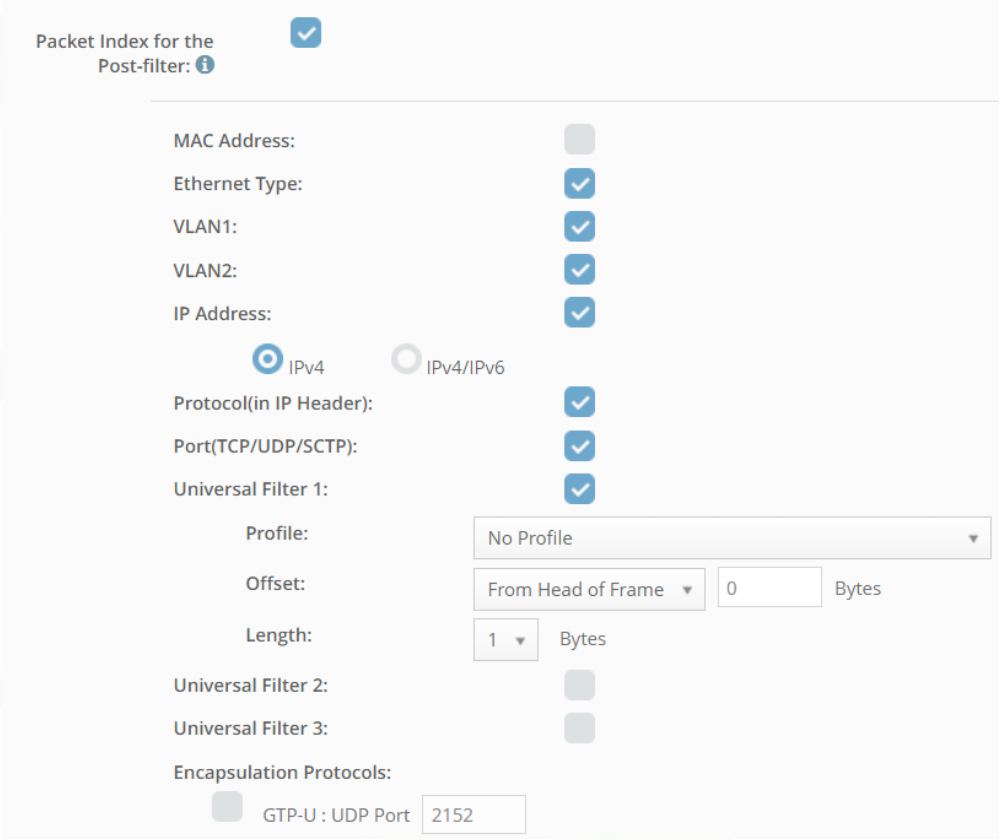
Traffic volume graph by application

Traffic volume graph by IPv4 address pair

Capture Function – Real-time Index File Creation

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

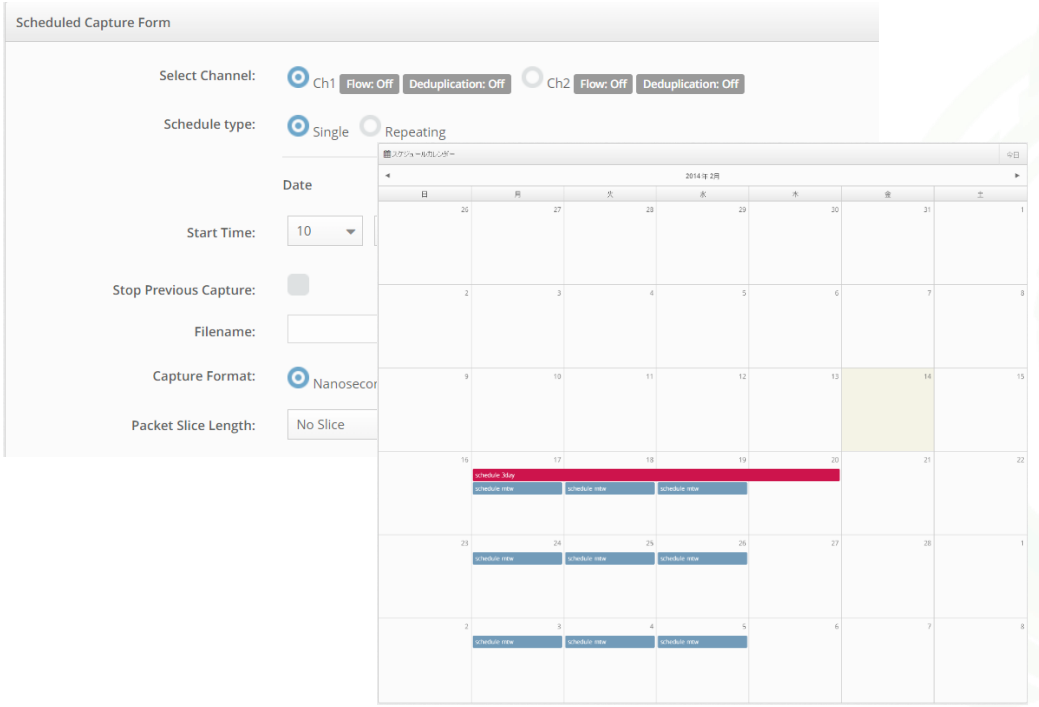
By using this function, it is possible to execute Post Filter immediately without waiting for index file creation time and extract desired packets.



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.

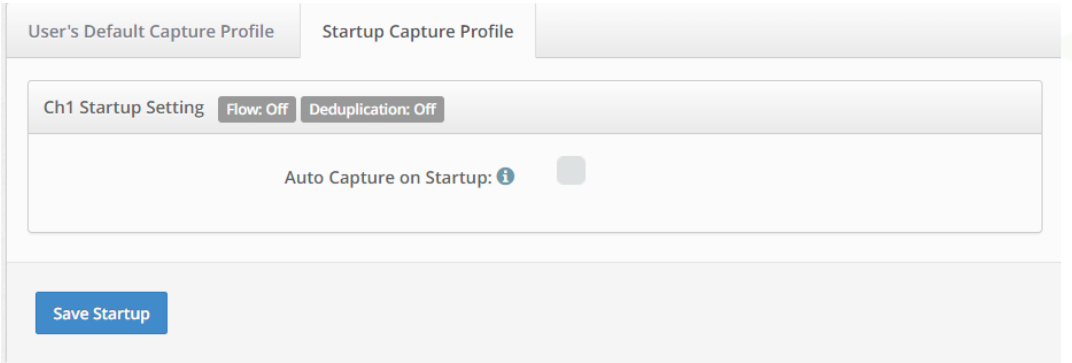
Schedule Capture

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.



Startup Capture

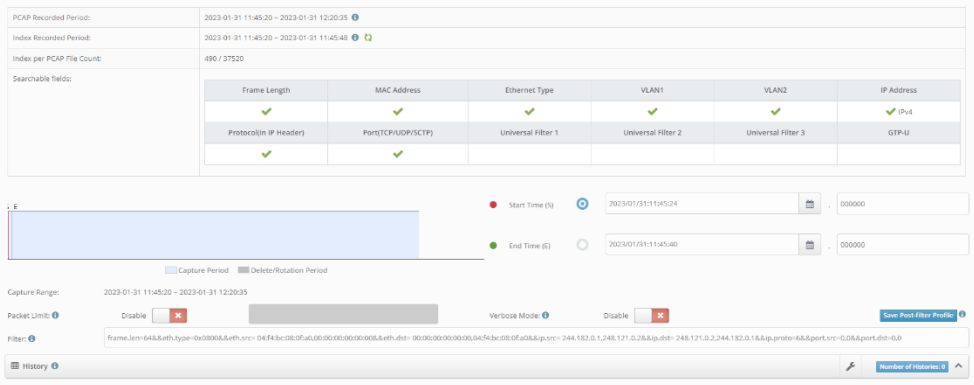
Startup capture is a function that starts capture automatically when Sirius starts.



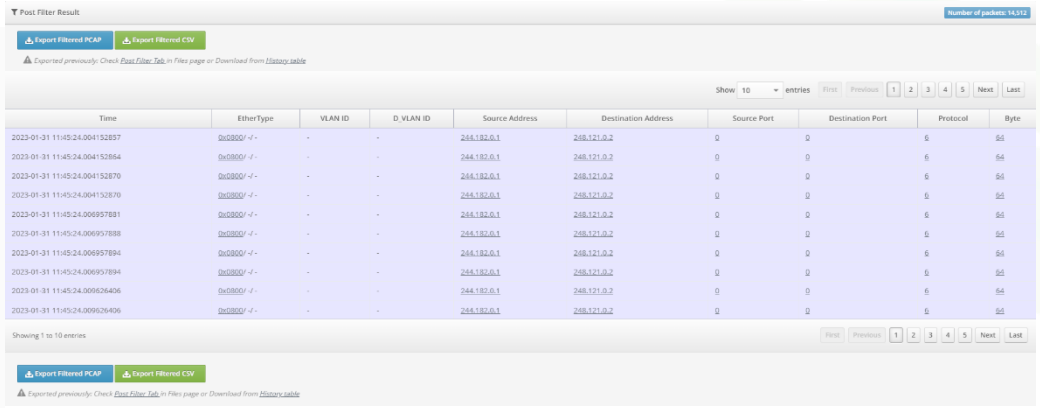
Post Filter Function

Post Filter is a function that enables fast search and extraction of stored packets using an index that created during or after packet capture.

New PCAP files can be created by extracting the desired packets using the fields specified at the time of index file creation as keys.
The files can be downloaded externally via Web GUI/FTP, etc.



Post Filter ①



Post Filter②

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 = ab:cd:ef:12:34:56 eth.addr != ab:cd:ef:12:34:56
Source MAC Address	eth.src	eth.src = ab:cd:ef:12:34:56 eth.src != ab:cd:ef:12:34:56
Destination MAC Address	eth.dst	eth.dst = ab:cd:ef:12:34:56 eth.dst != ab: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

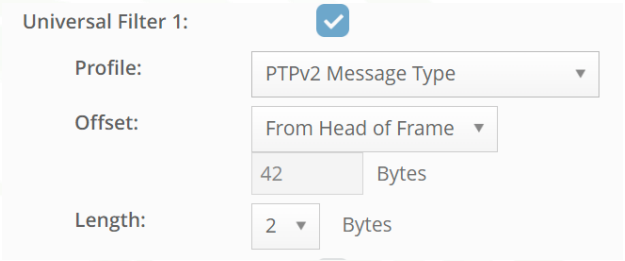
Filter Conditions ①

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.)



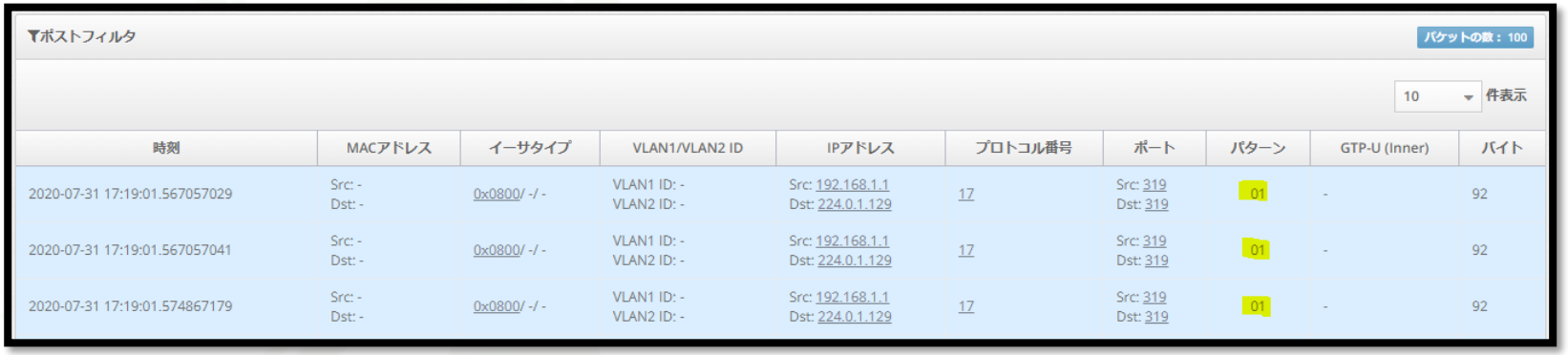
Post Filter Configuration

Specify filter conditions using ASCII codes (hexadecimal notation)

*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
v 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··· ··
```

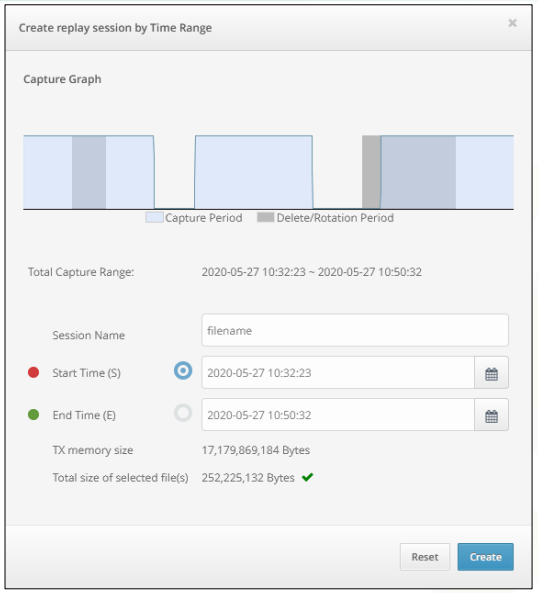
Overall of Packet Replay Function

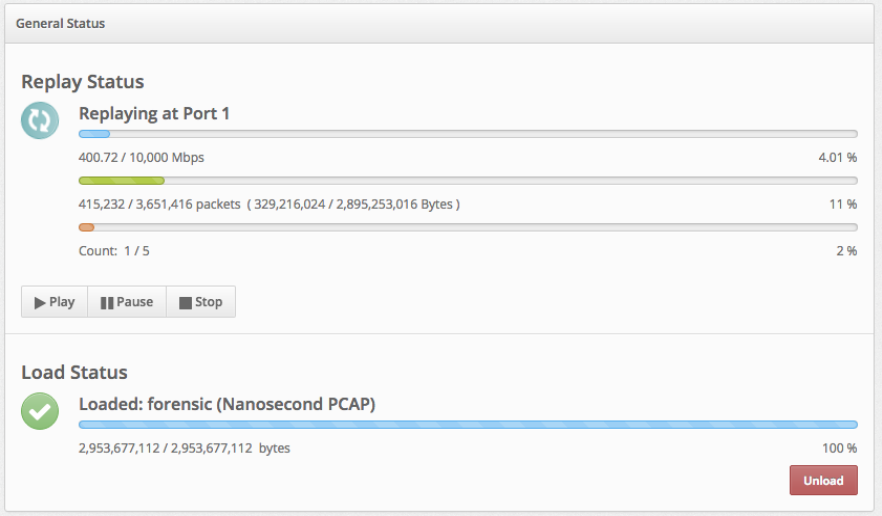
Packet Replay is a function to reproduce packets according to time stamp of the PCAP file; It sends packets to Sirius capture port. User can specify PCAP file from captured PCAP file by Sirius or user upload PCAP file.

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.

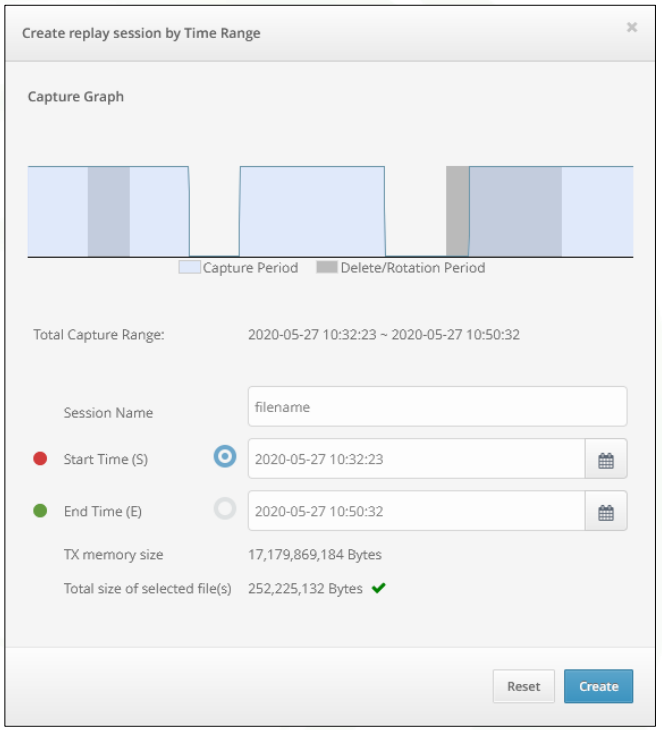


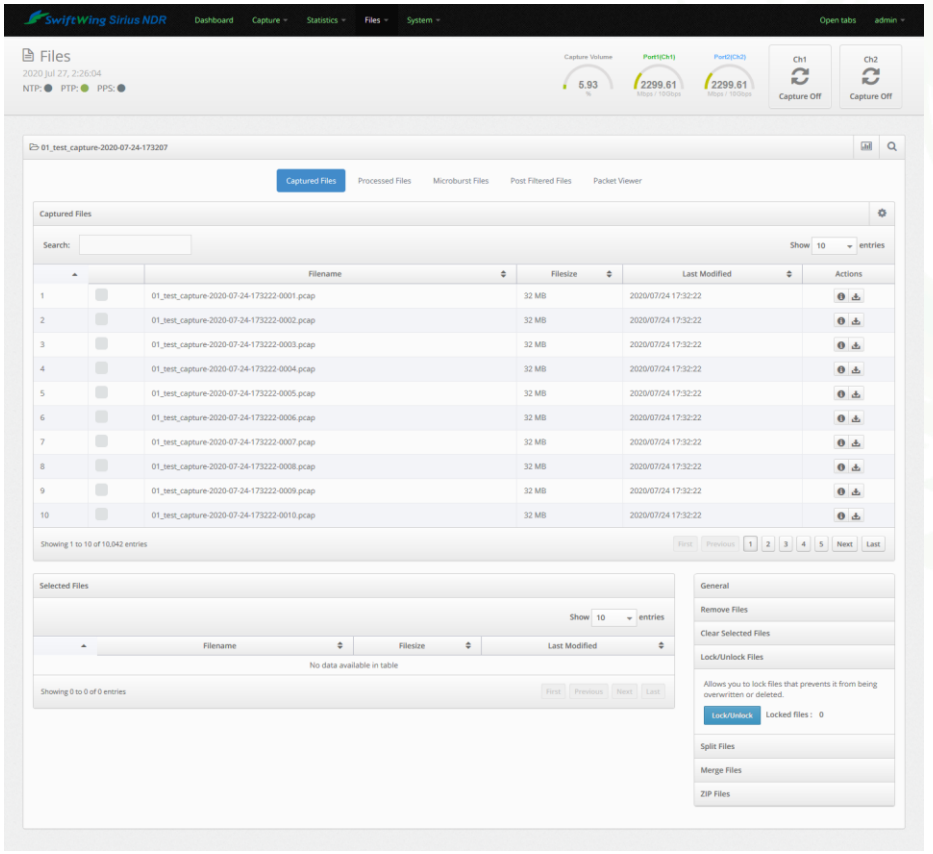


Configuration of Packet Replay Function

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





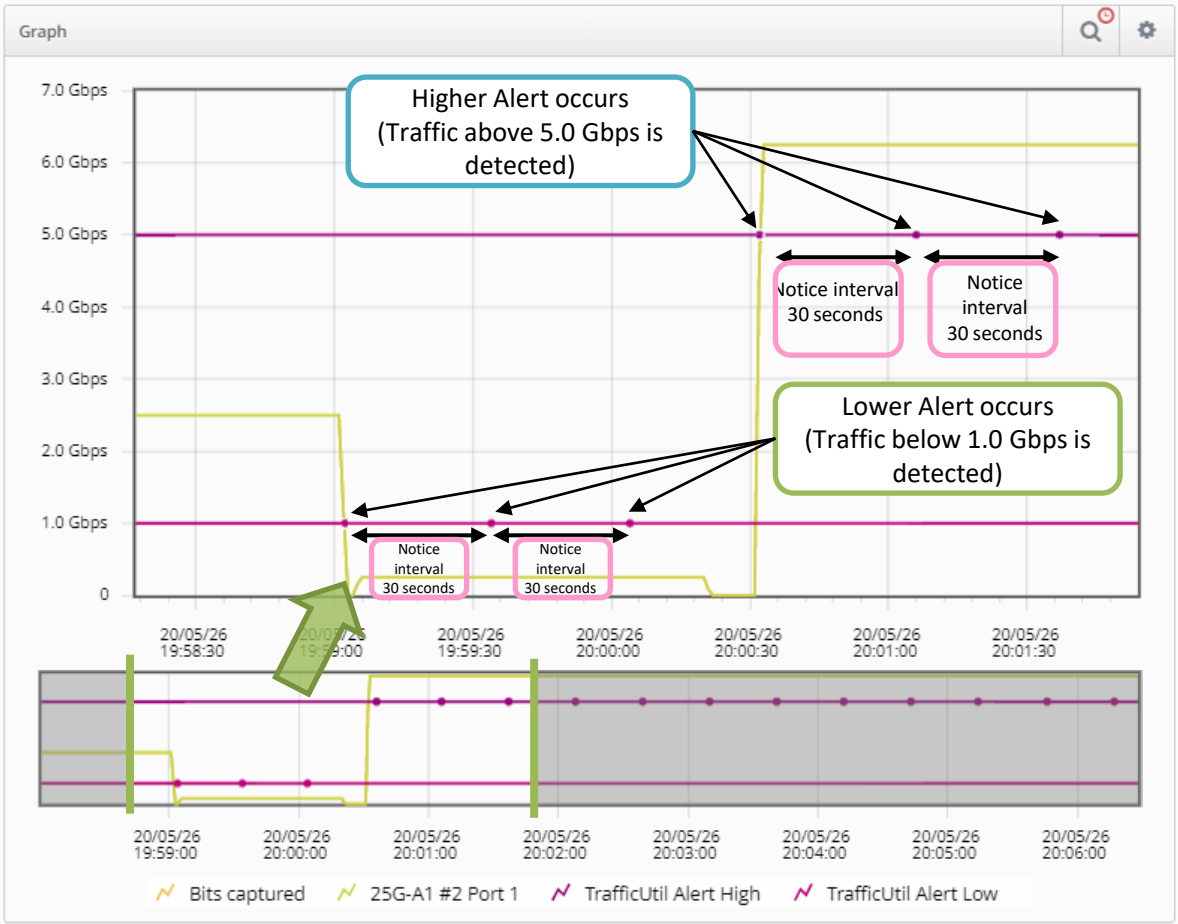
Realtime Monitor Function

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

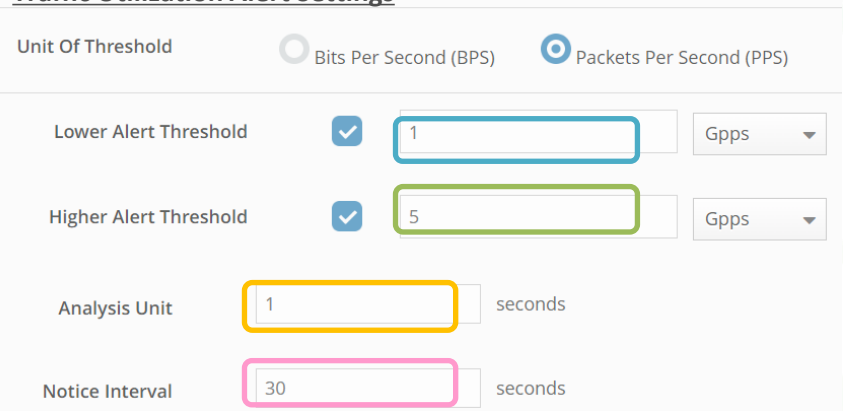
Realtime Monitor Function- Alert function linkage①

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



Lower Alert Threshold : Alerts when traffic volume is below 1.0 Gbps

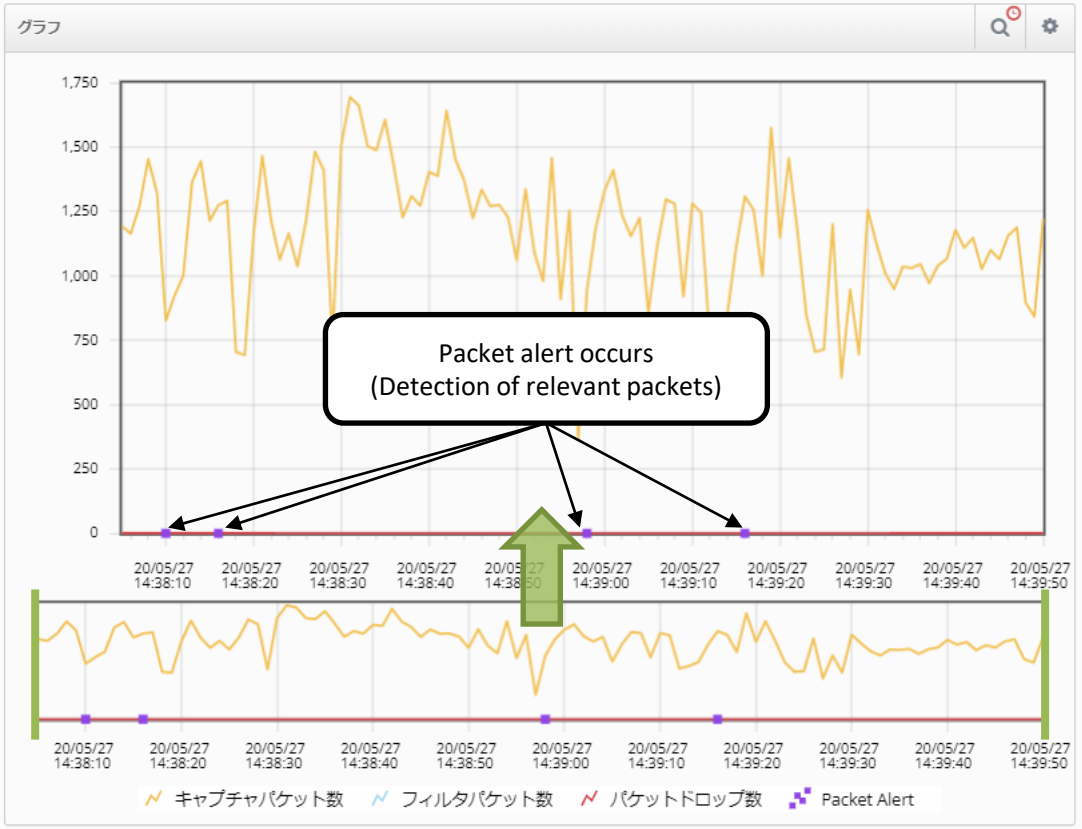
Higher Alert Threshold :Alerts when traffic volume exceeds 5.0 Gbps

Analysis Unit : 1 second. Alerts are generated if the threshold is exceeded or remains below during this time.

Notice Interval: 30 seconds. Interval between alerts.

Realtime Monitor Function- Alert function linkage②

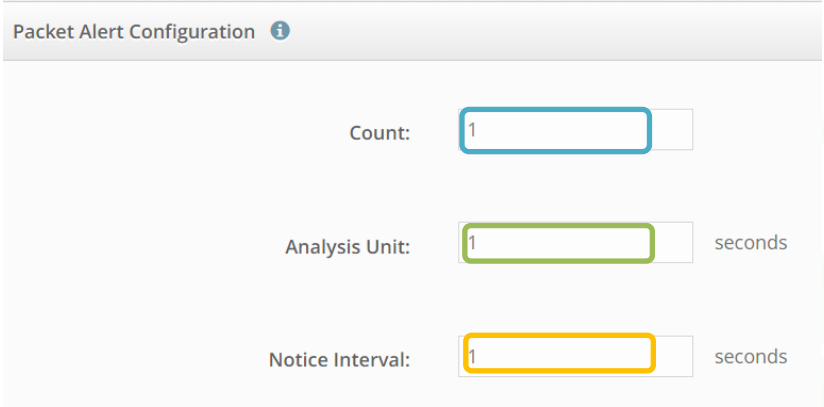
Linkage to Packet Alerts



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.)



Count : 1. Alerts are generated if more than this value of packets are detected during the analysis unit.

Analysis Unit : 1 second. Time to perform analysis.

Notice Interval 1 second. Interval between alerts.

Realtime Monitor Function- Packet View

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

Search: Show 10 entries

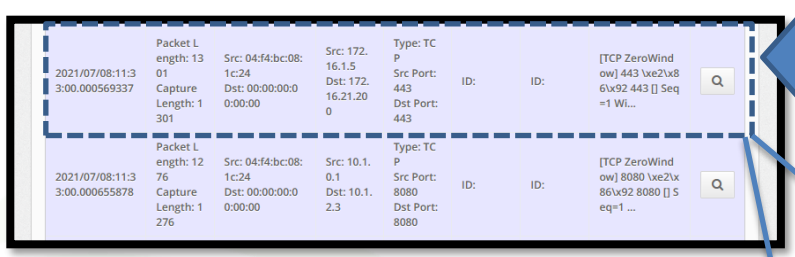
Time	Length	Mac Address	IP Address	Protocol/Port	VLAN 1	VLAN 2	Info	Action
2020/06/30:16:41:57.444346675	Packet Length: 64 Capture Length: 64	Src: 04:f4:bc:06:3a:50 Dst: 00:00:00:00:00:00	Src: 50.235.0.0 Dst: 0.0.0.0	Type: TCP Src Port: 22314 Dst Port: 0	ID:	ID:	22314 \xe2\x86\x92 0 [Reserved] Seq=5073 8 Win=822[Malfo...	
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

Realtime Monitor Function- Packet View



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.

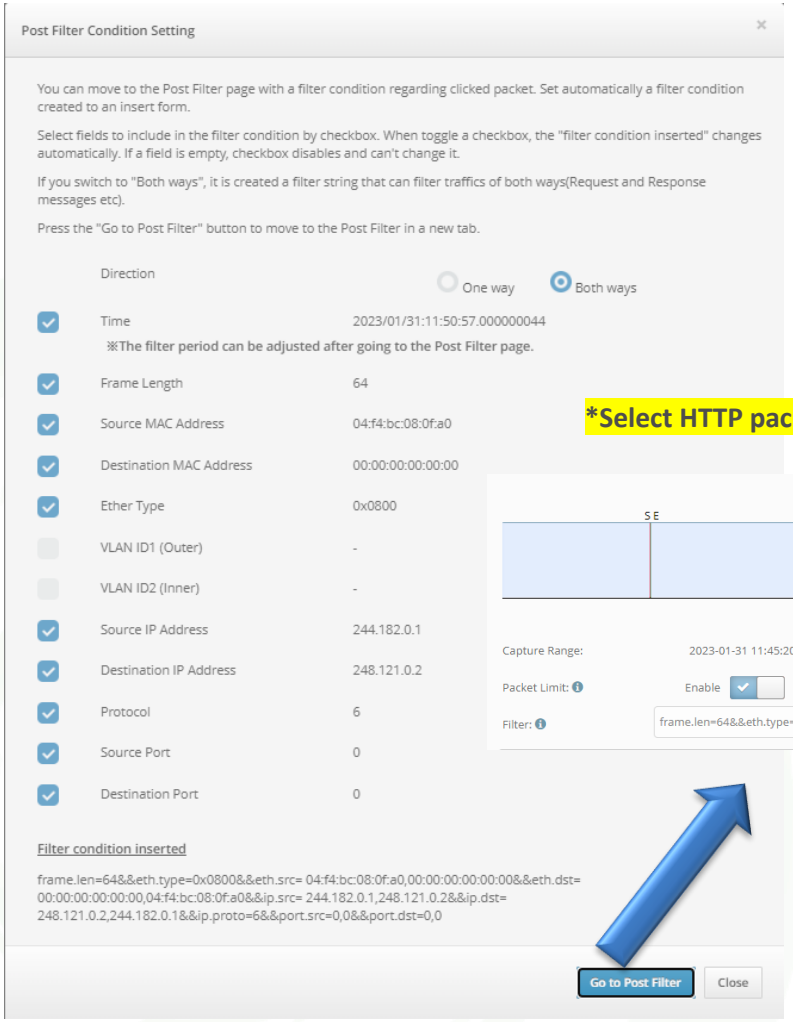
In addition, indentation of major items such as MAC address, IP address, and port number has improved visibility.

Realtime Monitor Function- One-touch packet extraction function

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.**



Post Filter Condition Setting

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.

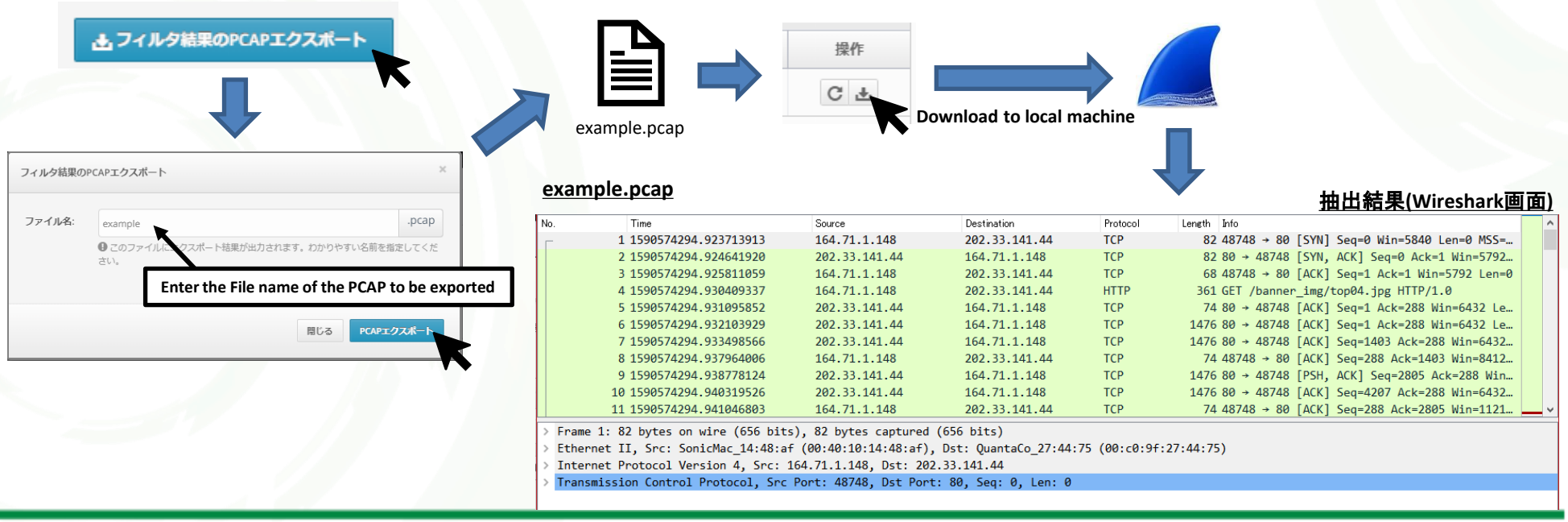
Realtime Monitor Function- One-touch packet extraction function

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



Statistics output function

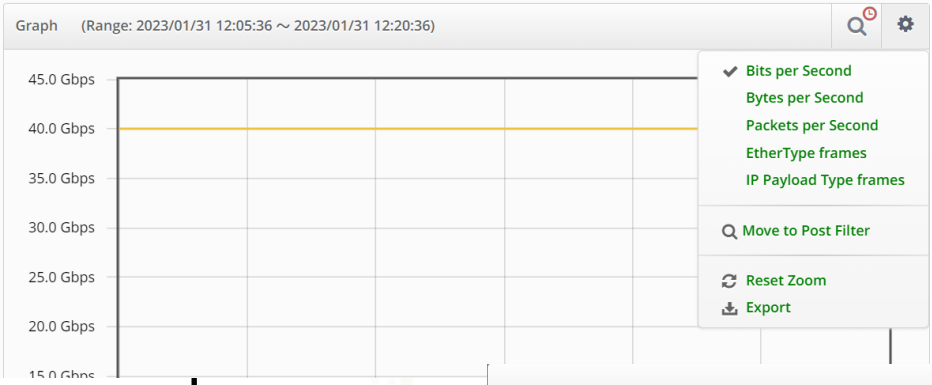
Various statistical information acquired by Sirius can be output in CSV format at the following intervals.

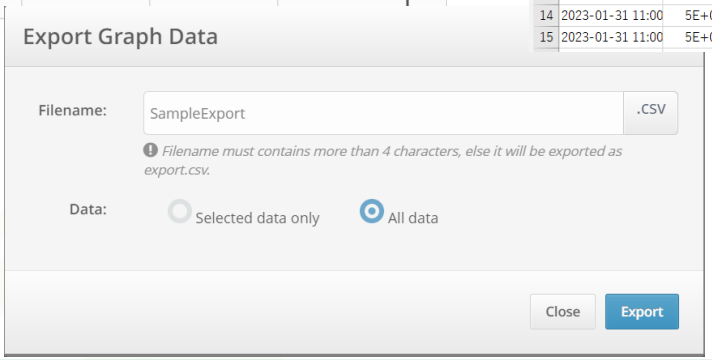
Acquisition Information

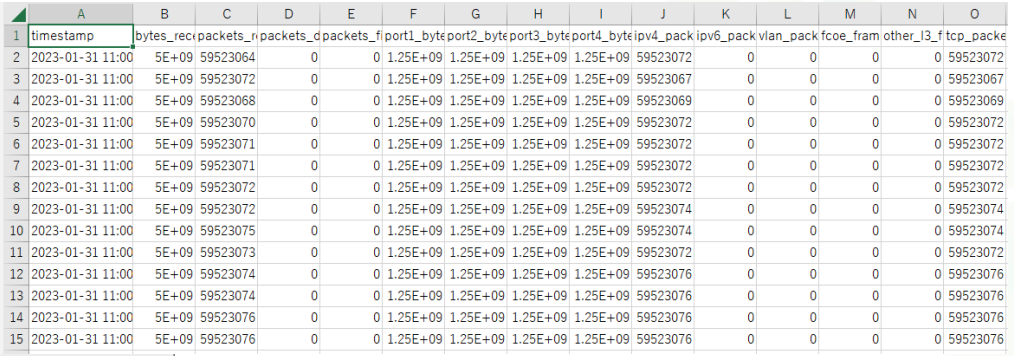
- Amount of data received (bytes)
- Number of packets received
- Number of filtered dropped frames
- Number of dropped frames
- Number of unicast frames
- Number of multicast frames
- Number of broadcast frames

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)





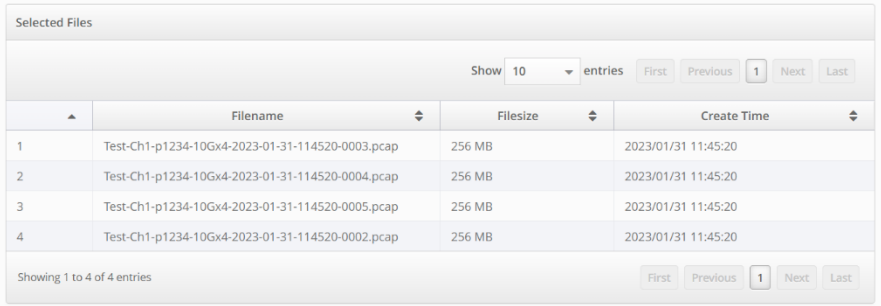


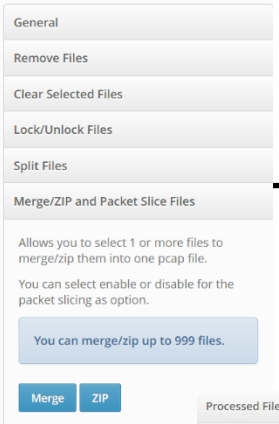
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	timestamp	bytes_rec	packets_r	packets_d	packets_fi	port1_byte	port2_byte	port3_byte	port4_byte	ipv4_pack	ipv6_pack	vlan_pack	fcoe_fram	other_l3_f	tcp_packe
2	2023-01-31 11:00	5E+09	59523064	0	0	1.25E+09	1.25E+09	1.25E+09	1.25E+09	59523072	0	0	0	0	59523072
3	2023-01-31 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

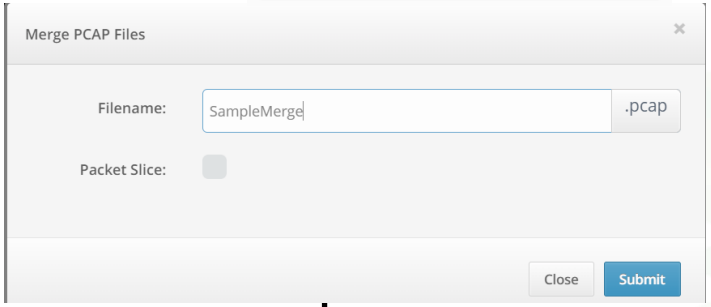
Management of Captured File Function

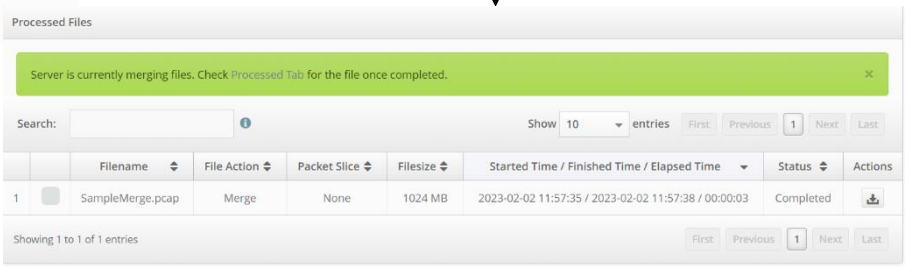
The Following management functions are available for captured files by Sirius.

- 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





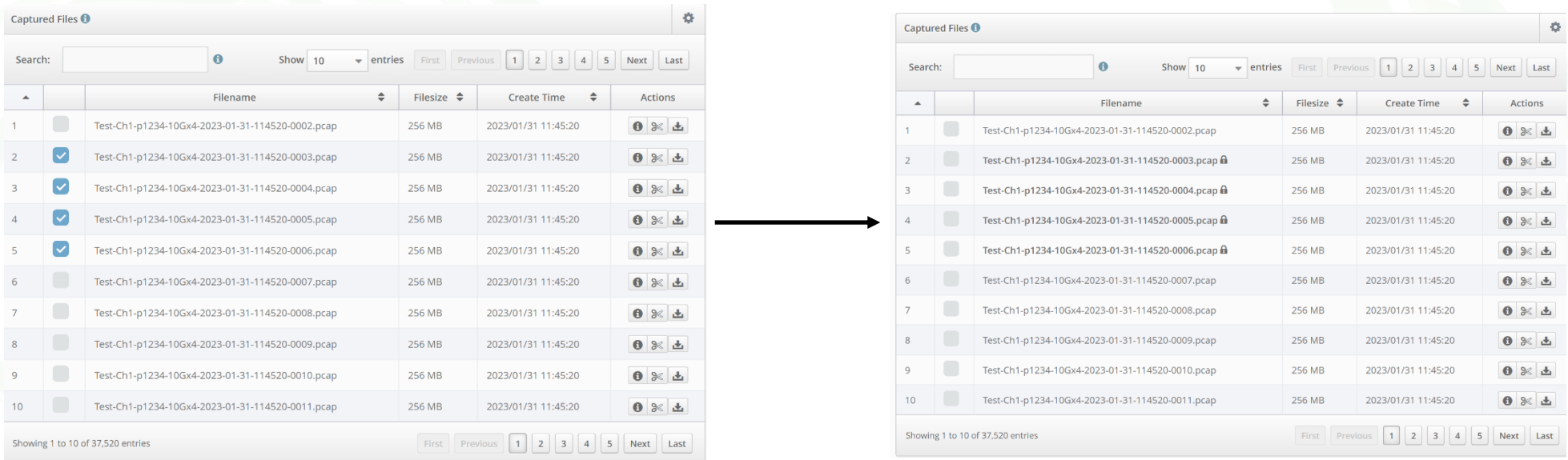




File Lock Function

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

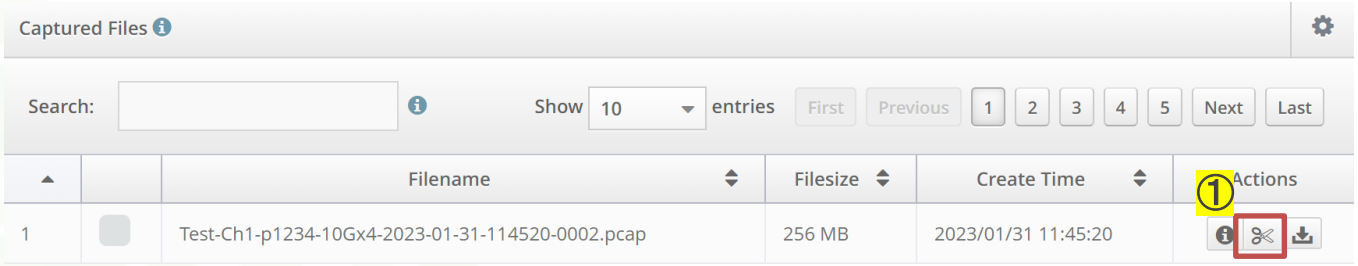
Locked capture files are not subjected to be deleted during rotation.
By linking with various alerts, it is possible to keep capture files and analyze abnormal packets.

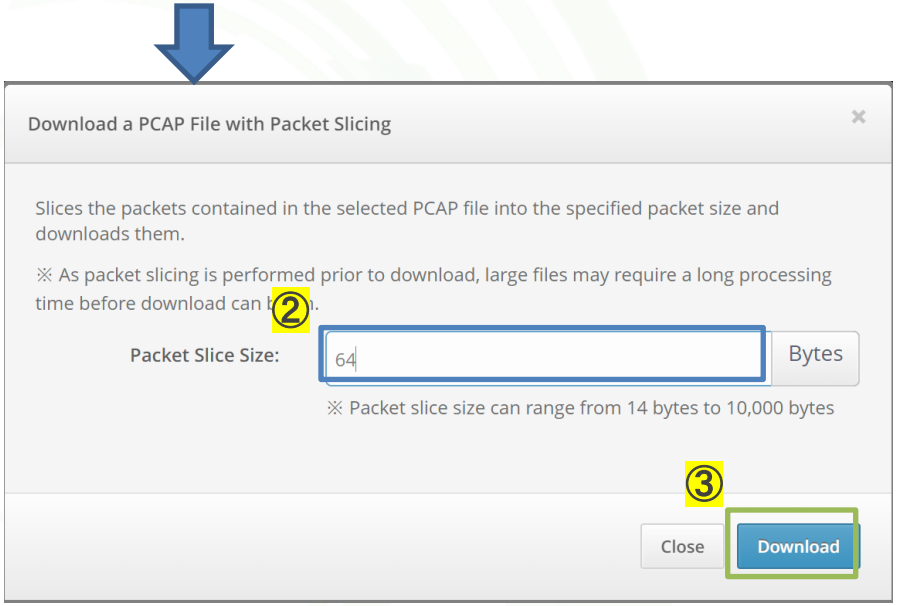


Management of Captured File Function- PCAP file packet slicing

Each saved PCAP files can be packet sliced.

Follow the steps below to perform packet slicing and downloading.





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.

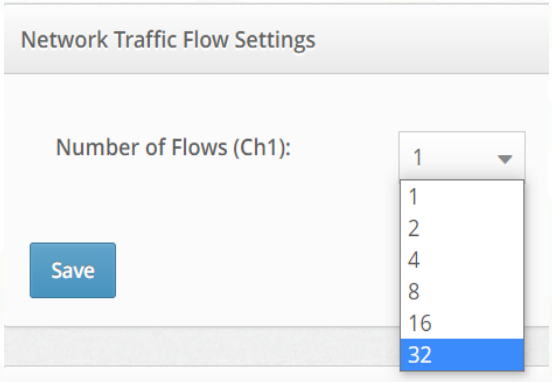
**If the size of the PCAP file is large, it may take time to download the file due to the time required to process the packet slices.*

Network Traffic Flow Settings -Packet Sampling by Flow

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.



Packet1 : Src=192.168.1.1 , Dst=192.168.2.100

Packet1 : Src=192.168.1.2 , Dst=192.168.2.100

Packet1 : Src=192.168.1.3 , Dst=192.168.2.100

⋮

Packet1 : Src=192.168.1.97 , Dst=192.168.2.100

Packet1 : Src=192.168.1.98 , Dst=192.168.2.100

Packet1 : Src=192.168.1.99 , Dst=192.168.2.100

Packet Sampling: 1 of 1

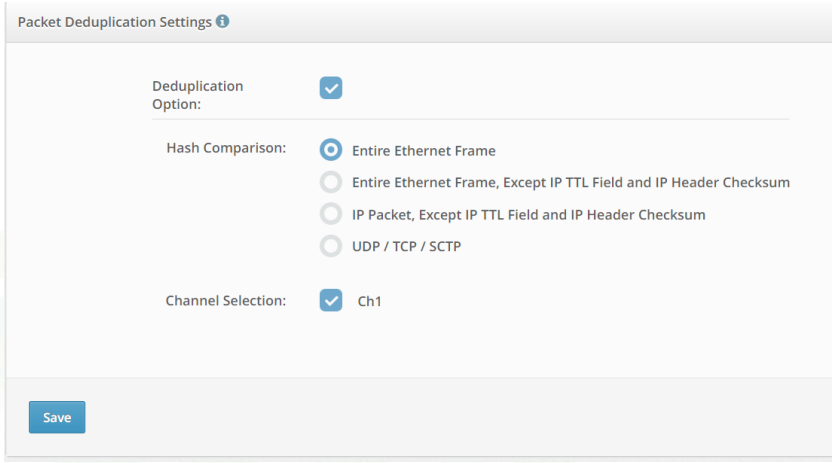
Capturing all packets.

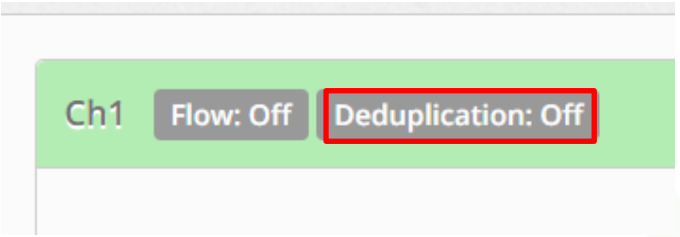
Packet Sampling: 1 of 2

PCAPFile

Number of packets for capture reducing half.

Duplicate Packet Elimination Function





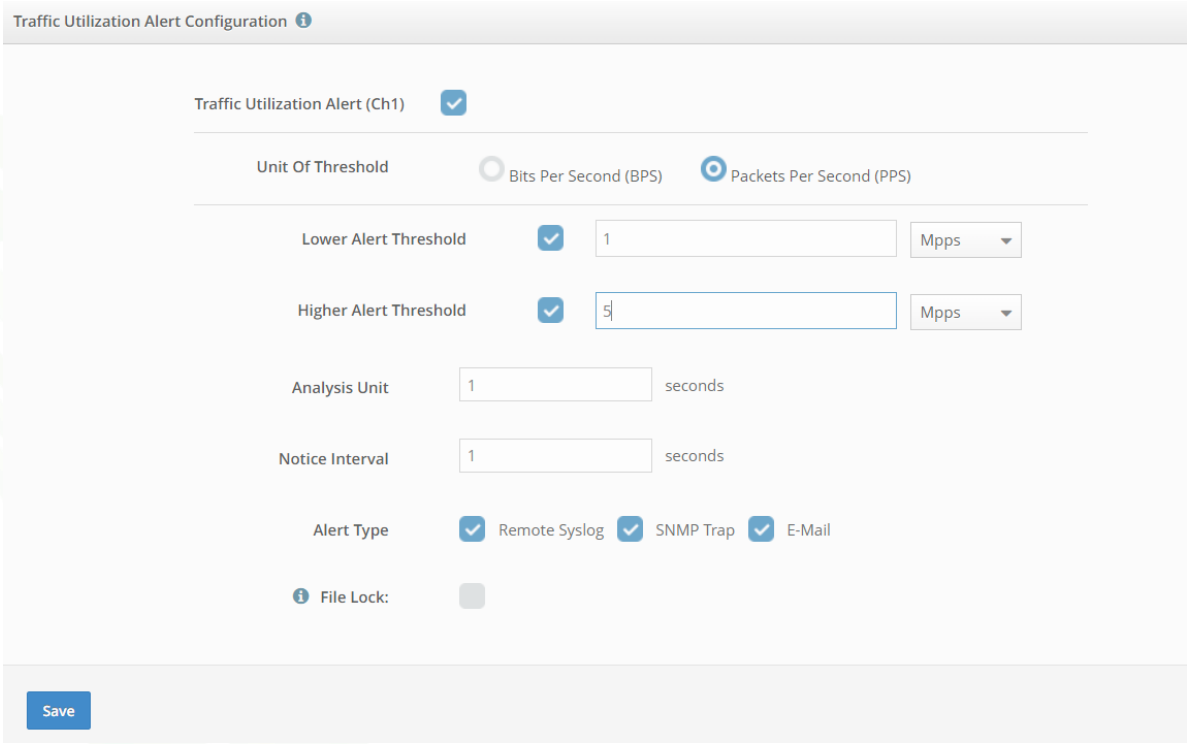
This function detects and eliminates duplicate packets from packets forwarded to each port on the same channel. It compares the hash values of packets received in a time frame of up to 100 ms and eliminates packets when the hash values are identical.
You can choose from the following four hash value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

Alert Function – Traffic Utilization Alert

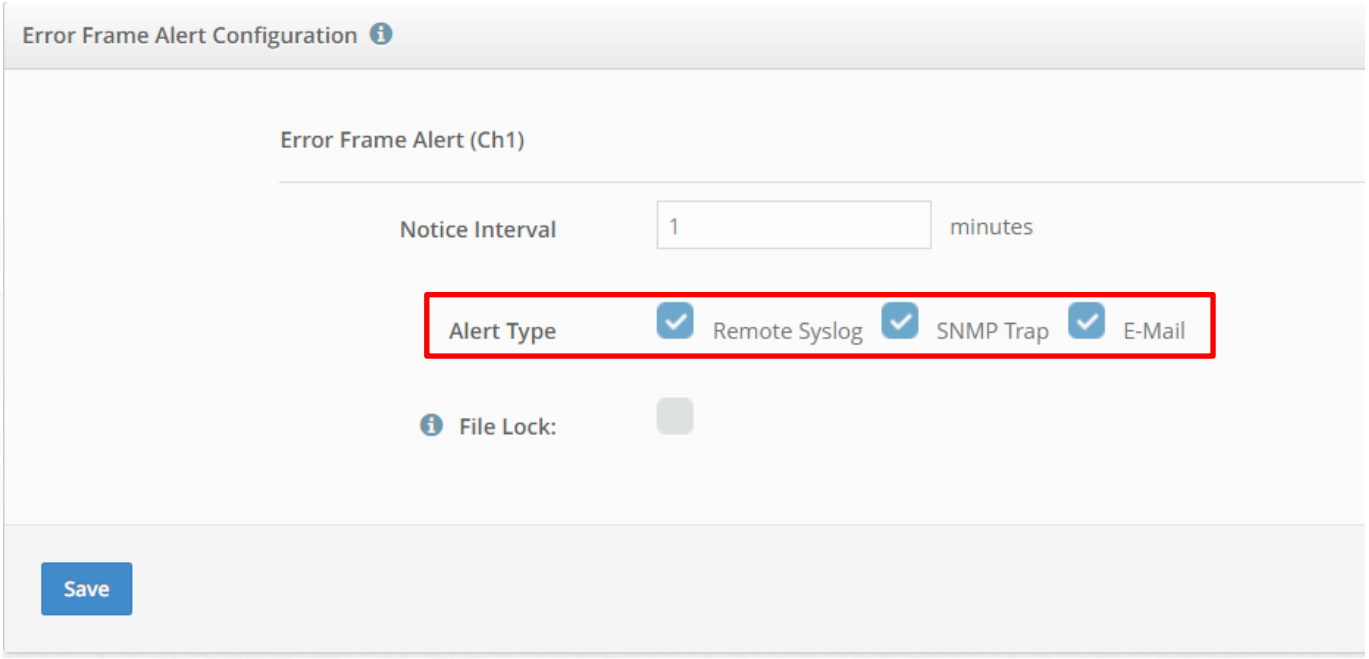
This function generates an alert when the amount of traffic exceeds or falls below a specified level. It can be configured for each channel.



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.**

Alert Function– Error Frame Alert



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

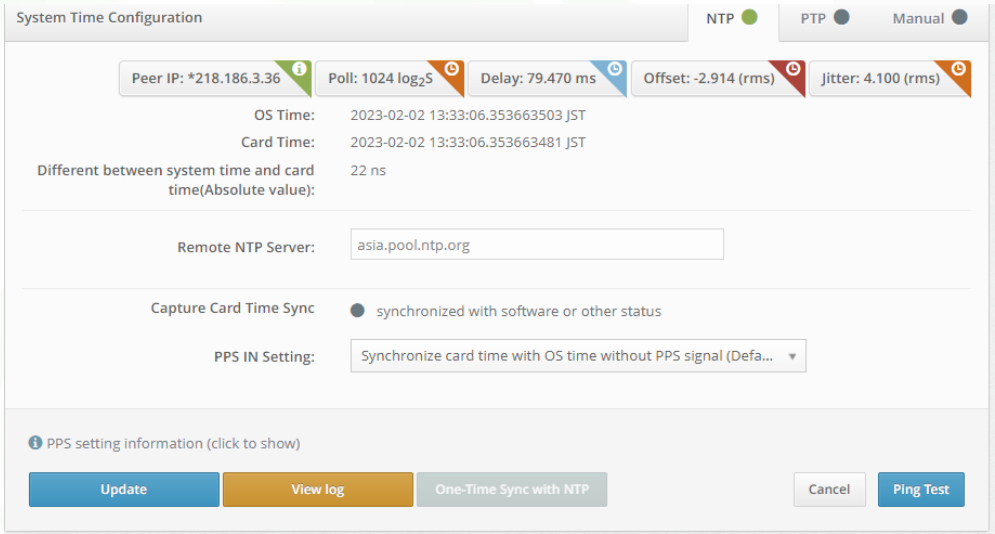
Alerts can be output to Remote Syslog, SNMP Trap, or E-mail.

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

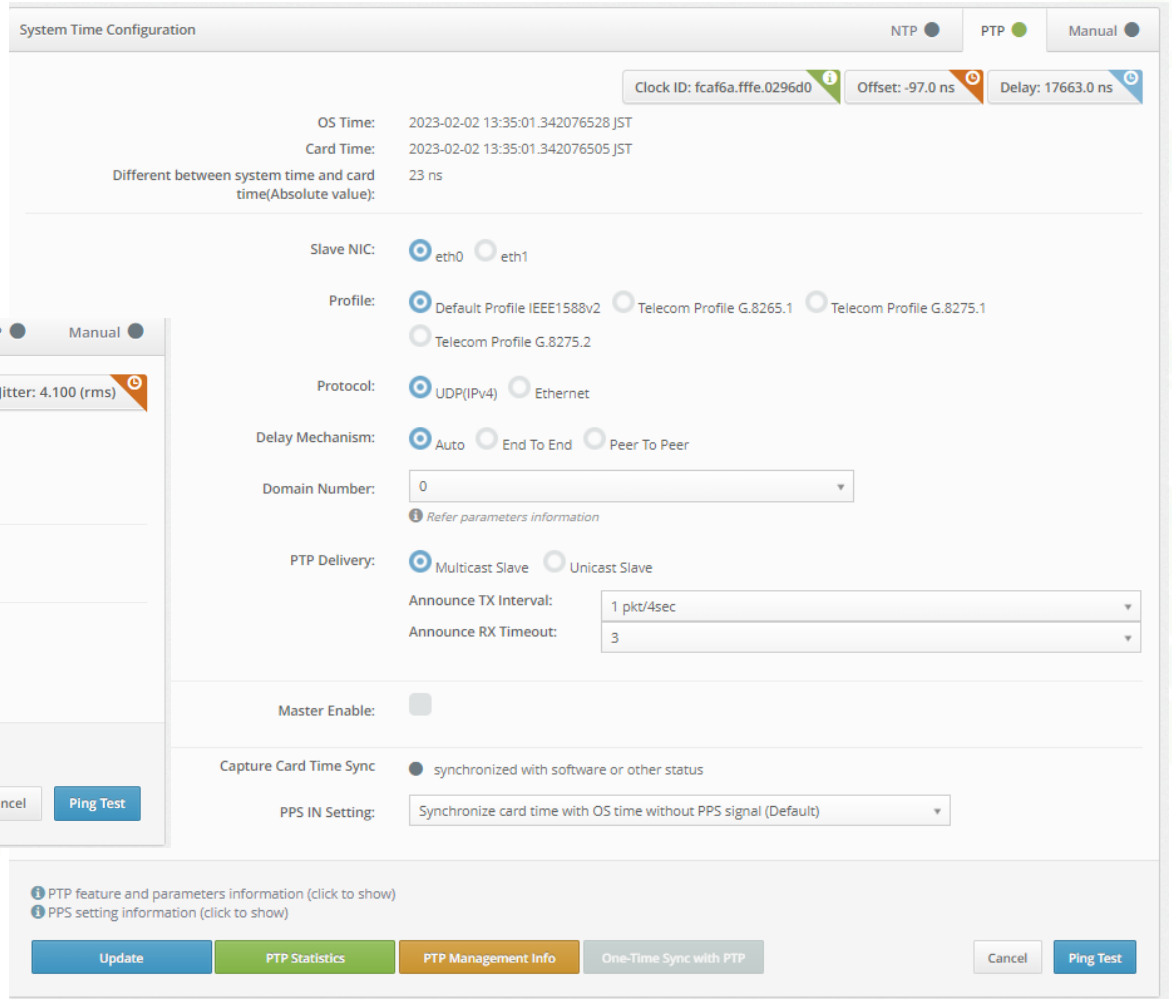
Time Synchronization Function

Sirius can synchronize the time in the following three ways

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



NTP Setting



PTP Setting

Monitoring Functions

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.