SYNESIS WHITEPAPER

Seven Reasons for Choosing SYNESIS

TOYO Corporation

SYNESIS Business Unit

2023-12-15 Rev1.0

Table of Contents

1. Introduction

SYNESIS is a packet capture product developed and marketed by Toyo Corporation.
This document outlines seven compelling reasons for selecting SYNESIS as the preferred choice in packet-capture applications.

1.1. What is SYNESIS?

SYNESIS is a high-capacity, high-performance, appliance-based packet capture and analysis device designed to monitor network traffic and analyze failures.

SYNESIS uses a technique that captures data flowing through a network at high speed and writes it in parallel to distributed storage. This technique ensures that all data can be stored at 100Gbps Ethernet, even when it flows over a large amount of data, without loss for a long period of time. This high-speed data writing technology is patented in Japan, the United States, and China.

1.2. Seven Reasons for Choosing a SYNESIS

Choosing SYNESIS over other packet-capture products allows you to overcome the following seven challenges commonly faced by users.

1. Loss of packets at high-capacity interfaces (i.e. 100G) during capture sessions causing incomplete data for analysis.
2. Unable to detect microburst traffic conditions and root cause due to the lack of granularity.
3. Deploying a temporary capture solution is costly and logistically challenging.
4. Current capture solution is limited in the number of line speed interfaces supported.
5. When packets are forwarded from a network packet broker to the capture device, the latency can occur and timestamps may be incorrect.
6. Repetitive manual tasks are time consuming.
7. Network failures in the field are hard to replicate in the lab.

2. Seven Issues and Solutions

2.1. Loss of packets at high-capacity interfaces (i.e. 100G) during capture sessions causing incomplete data for analysis

2.1.1. Background of the Task

100G Ethernet is now a popular line used in the backbone of datacenters. It is where user traffic and application protocols from various connected lines are aggregated. Troubleshooting communication failures on this high-speed backbone line requires reliable capture of the packets that caused the problem. Also, if a packet is identified as missing, it is crucial to ensure that it is not absent on the packet capture device itself, ensuring an accurate identification of the problem.

2.1.2. SYNESIS Solution

SYNESIS 200G offers high-performance NIC and patented disc-based distributed write capabilities to capture bi-directional traffic on 100G full-duplex lines without loss on two ports.

For capturing long packets, short packets, and random packet lengths, only models that successfully perform and pass a 48-hour continuous capture test are utilized.

2.1.3. User Benefit

When dealing with an unreliable packet capture device, determining whether a specific packet was present on the network or if it was dropped by the capture device can be challenging. To aid in troubleshooting, you can establish confidence in the initial packet data captured by eliminating the potential for packet loss originating from the capture device itself.

In addition, SYNESIS' specialized acquisition card is able to record VLAN headers, error frames, jumbo frames, etc. that cannot be acquired by off-the-shelf Network Interface Card (NIC).

2.2. Unable to detect microburst traffic conditions and root cause due to the lack of granularity

2.2.1. Background of the Task

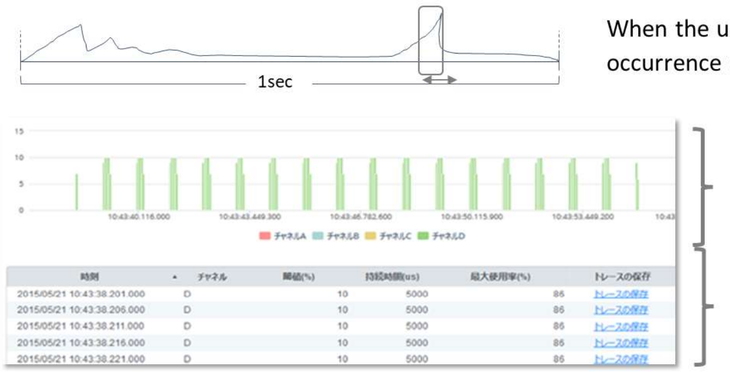
Microburst traffic causes congestion of routers/switches, which are network relay devices, due to a large amount of instantaneous traffic. Congestion causes packet loss, leading to retransmissions and response delays and ultimately negative user experiences. Because of instantaneous events that occur in a noticeably short period of time, it is difficult to detect and identify the cause of the occurrence when packets are collected without sufficient time granularity.

2.2.2. SYNESIS Solution

SYNESIS is capable of detecting microbursts on the network because of the high granularity of 100µsec used in calculations. By setting a threshold in advance, real-time detection can be performed during capture. SNMP Trap, Syslog, e-mail can notify you when a microburst occurs. SYNESIS can have further analysis by changing a threshold after capturing.
The line speed used for utilization may be set to a value that match the actual traffic rate in the feed. This is for cases when the physical capture interface line speed may be different from the source traffic rate.
You can also change the thresholds after discovery to ensure accurate detection. This prevents over-detection and detection leaks.

Microburst Detection feature of SYNESIS calculates usage rates at a specified time resolution

Resolution can be selectable, either 1000usec or 100usec



時刻	▲	チャネル	閾値(%)	持続時間(us)	最大使用率(%)	トレースの保存
2015/05/21 10:43:38.201.000		D	10	5000	86	トレースの保存
2015/05/21 10:43:38.206.000		D	10	5000	86	トレースの保存
2015/05/21 10:43:38.211.000		D	10	5000	86	トレースの保存
2015/05/21 10:43:38.216.000		D	10	5000	86	トレースの保存
2015/05/21 10:43:38.221.000		D	10	5000	86	トレースの保存

When the usage rate exceeds the specified consecutive occurrence count, it counts as one microburst

The number of occurrences of microburst

Detail information of each microburst

Microburst Function Specifications and Screens

2.2.3. User Benefit

Detecting bursts is a crucial element for enhancing network quality, and SYNESIS simplifies the process of identifying those events.
SYNESIS supports alerts in realtime or post-analysis of microburst occurrences allowing you to stay informed without the need to constantly monitor your network. Furthermore, identifying the source of the microburst is made simple by analyzing the packets at the time of its occurrence.

2.3. Deploying a temporary capture solution is costly and logistically challenging

2.3.1. Background of the Task

Troubleshooting a network requires packet capture at a different location to identify where the cause is from upstream to downstream in the network. Faults can occur in fields as well as in the data center, and large, heavy, and stationary packet capture devices cannot easily accommodate packet capture at different locations.

2.3.2. SYNESIS Solutions

SYNESIS offers a range of portable models. The line speed, capture performance, and storage size may be selected based on the application.
The device utilizes a durable SSD for storage. A dedicated convenient case equipped with casters makes it easy for transportation.

SYNESIS dedicated carry case in Paris

2.3.3. User Benefit

The SYNESIS portable model weighs less than 10 kilograms and is an all-in-one unit featuring a display and keyboard. It comes with a convenient case equipped with casters for easy transportation. This turnkey solution allows for immediate use upon power-up, enabling you to quickly set up and capture data in the field. Additionally, remote network control is supported, providing flexibility in operation.

2.4. Current capture solution is limited in the number of line speed interfaces supported

2.4.1. Background of the Task

There may be capture deployment situations where the line speeds and physical interfaces may differ between the upstream and downstream links. These variations may include 1G/10G/25G/40G/100G single/multimode fiber and RJ45copper physical interfaces. Purchasing a dedicated capture device for each specification is cost prohibitive.

2.4.2. SYNESIS Solutions

SYNESIS supports physical interfaces from 1G to 100G in a single NIC. Exchanging transceivers at SYNESIS along with a software configuration allows support for the various interfaces. It also supports branching with a breakout cable (*1) so that multiple lines can be captured efficiently.

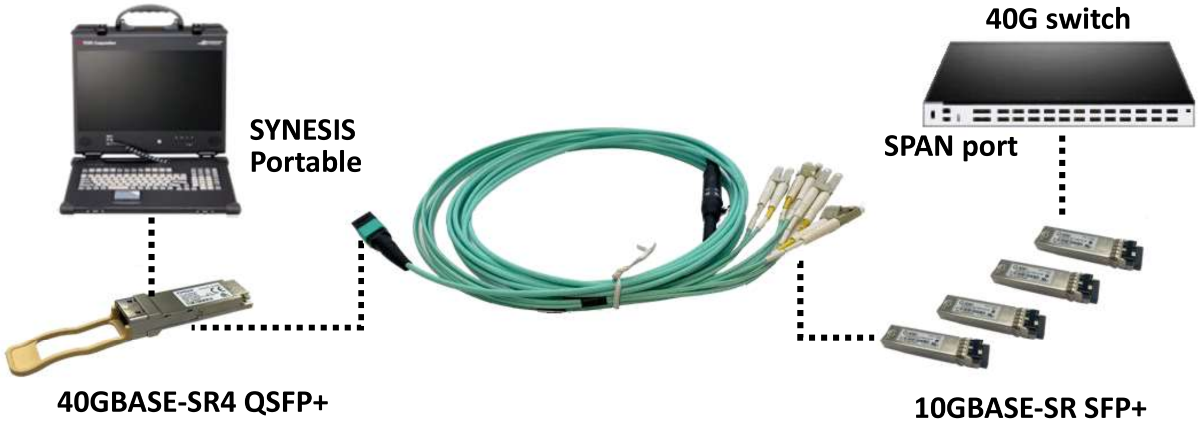
(*1) A breakout cable is a branch cable used to aggregate or distribute Ethernet bandwidth.

Link speeds supported by SYNESIS and corresponding accessories

Line Speed	Mode	Transceiver	Form Factor	Note
100G x2	Multi-Mode (SR4)	QSFP28	MPO12	
	Single Mode (LR4)	QSFP28	LC	
40G x2	Multi-Mode (SR4)	QSFP+	MPO12	
	Single Mode (LR4)	QSFP+	LC	
25G/10G x2	Multi-Mode (SR)	SFP28 / SFP+	LC	25G/10G dual, 25G only or 10G only
	Single Mode (LR)	SFP28 / SFP+	LC	
10G/1G x2	Multi-Mode (SR/SX)	SFP+ / SFP	LC	10G/1G dual, 10G only or 1G only
	Single Mode (LR/LX)	SFP+ / SFP	LC	
	Copper	SFP+ / SFP	RJ45	10G only or 1G only
25G x4	Multi-Mode (SR)	QSFP28	MPO12	with breakout cable
	Single Mode (PSM4)	QSFP28	MPO12	with breakout cable
10G x8	Multi-Mode (SR)	QSFP+	MPO12	with breakout cable
	Single Mode (PSM4)	QSFP+	MPO12	with breakout cable

2.4.3. User Benefit

You won't require multiple capture devices for your setup. Furthermore, selecting a model that supports high-speed interfaces from the start eliminates the need to invest in a new capture device to enhance network speed later on, offering a significant cost advantage.



SYNESIS Configuration Diagram Using Breakout

2.5. When packets are forwarded from a network packet broker to the capture device, the latency can occur and timestamps may be incorrect

2.5.1. Background of the Task

Network Packet Broker (NPB) efficiently receives and aggregates or duplicates packets from various sources. This eliminates the need for separate management of traditional SPAN or Network TAP, simplifies complex networks, and can lead to reduced operational costs.
NPB also has the capability to timestamp within the packet the time the packet was received. This allows network monitoring based on packet reception times.

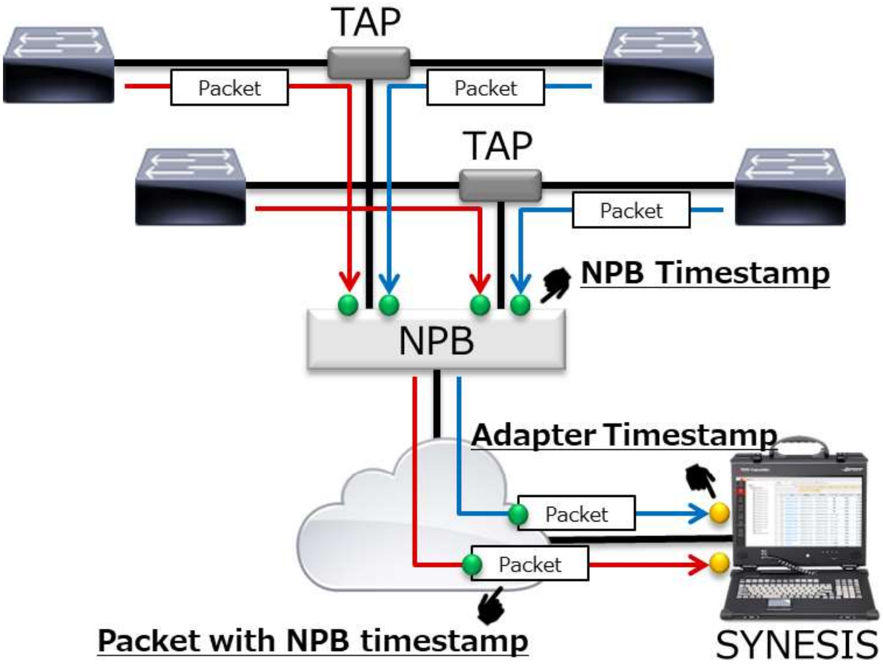
In captured data, the timestamp is added as the time of packet reception by the capture device. However, there may be discrepancies between the time the packet passes through various points in the network and the time it reaches the capture device. Therefore, analyzing based on the timestamp of the capture device may result in the inability to accurately analyze the performance of the network.

2.5.2. SYNESIS Solutions

SYNESIS supports the timestamp feature of the following network packet broker (NPB) vendors:

- CGS Tower
- VSS Monitoring compatible (for example, NetScout, CUBRO, ProfiTap)
- Gigamon

SYNESIS can use the timestamp provided by the NPB instead of the timestamp received from the internal acquisition adapter (NIC) of the main unit at the time of parsing. By analyzing packets captured and timestamped at the NPB installation points, you can more accurately measure network latency, quality of service (QoS), jitter, and end-to-end network performance.



Outline of NPB Timestamp Function

2.5.3. User Benefit

In today's networks, many companies deploy NPBs for network monitoring. By using the timestamps of NPBs located at every point on the network, you can accurately measure latency, jitter, and end-to-end network performance between local points, helping to identify bottlenecks in communication.

2.6. Repetitive manual tasks are time consuming

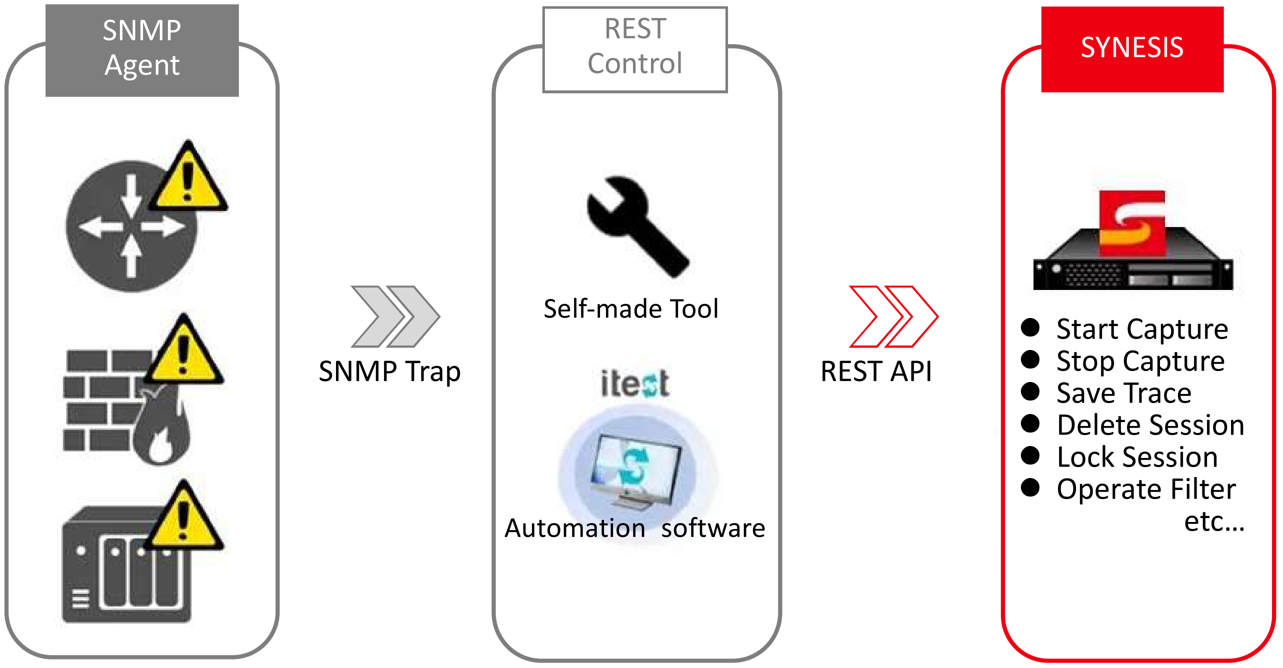
2.6.1. Background of the Task

Due to the increasing sophistication and complexity of networks and the shortage of engineers, automation of operation is becoming increasingly important in today's IT environment. Automating tasks for engineers leads to increased efficiency, reduced workloads, and a decrease in human errors.
When evaluating network systems and network devices, repeated testing is often performed while changing parameters on multiple devices.
If done manually, this process can be incredibly time-consuming and labor-intensive.

2.6.2. SYNESIS Solutions

SYNESIS provides a REST API which allows you to automate tasks and interact with other systems. All the major operations of SYNESIS are REST API and operational.

- Start/Stop capture
- Creating a trace file
- Deleting a capture session
- Locking capture Session
- Applying various filter, etc.



2.6.3. User Benefit

The following external devices may be linked by using REST API. This minimizes the potential for human error and simplifies network management tasks.

- Periodic operation (start/stop capture, status check)
- Creating and applying filters for IP addresses and communication sessions where event errors occur such as at routers and servers and for extracting data to trace files
- Transferring trace files locally, creating folders, renaming files, etc.
- Automatically changing capture points for SYNESIS through switches
- Various operations triggered by SNMP traps from SYNESIS or other devices (starting and stopping capture sessions, logging of traces and other devices, analysis, etc.)
- Automated Device Testing with Traffic Emulation Units in a Lab Environment

2.7. Network failures in the field are hard to replicate in the lab

2.7.1. Background of the Task

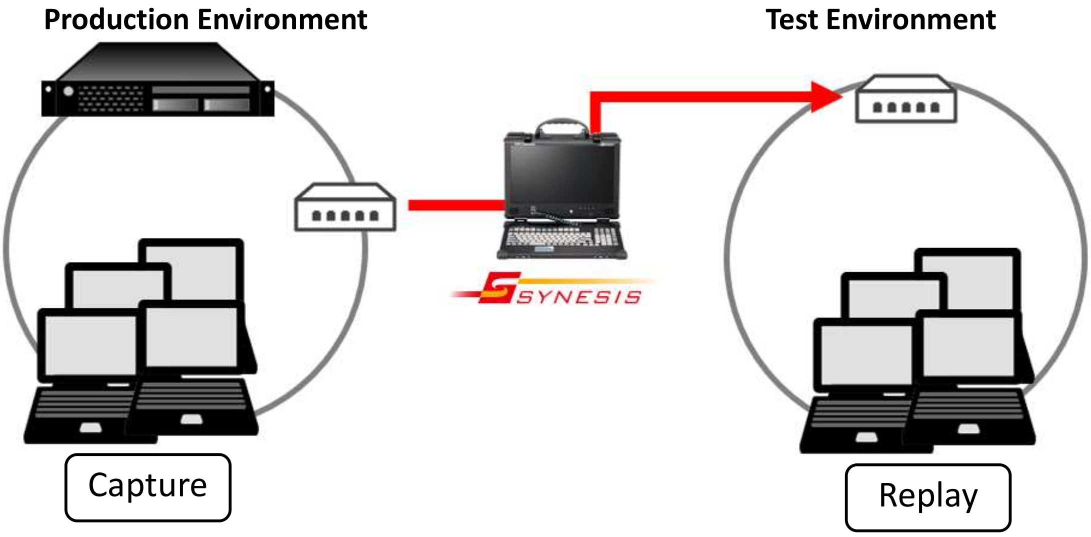
Capturing network traffic over extended periods is essential for investigating the root causes of intermittent network problems and security incidents. Furthermore, to identify problems that occur in a real network environment characterized by a mix of various network devices and fluctuating user data traffic, it may be necessary to perform a replication test using the actual data at the time of failure. This approach allows for a more comprehensive understanding of network dynamics and aids in the precise diagnosis and resolution of problems that may arise in complex and dynamic network scenarios.

2.7.2. SYNESIS Solutions

SYNESIS has a packet replay function. This function allows SYNESIS to send a large number of captured packets directly from SYNESIS. Packet transmission timing can be accurately replicated, including the faithful reproduction of burst traffic. Parameters such as MAC addresses, IP addresses, and port numbers can be adjusted to match the lab environment. Users can set the usage rate and the number of repetitions based on testing conditions. It also supports Rest API, which allows you to interact with other devices to automatically stream test traffic.

The data for transmission can be configured not only for information acquired by SYNESIS (capture session, pcap file) but also for data obtained by other devices (pcap file). When sending data as a capture session, it is possible to set up to 80% of the packet storage area, so terabyte sized data can also be replayed.

In addition, the performance mode replay allows accurate reproduction of even 100G full rate data.



Operational image of PacketReplayer

2.7.3. User Benefit

Replaying packets that were acquired at the time of failure in a more controlled lab environment enables a swift and dependable identification of the root cause of the failure. If repeated tests are required for evaluation of network devices, etc., automation can reduce test time and effort.

3. Contact Information

The contact information for this manual is as follows:

TOYO Corporation
SYNESIS business unit
Mail: synesis-marketing@toyo.co.jp