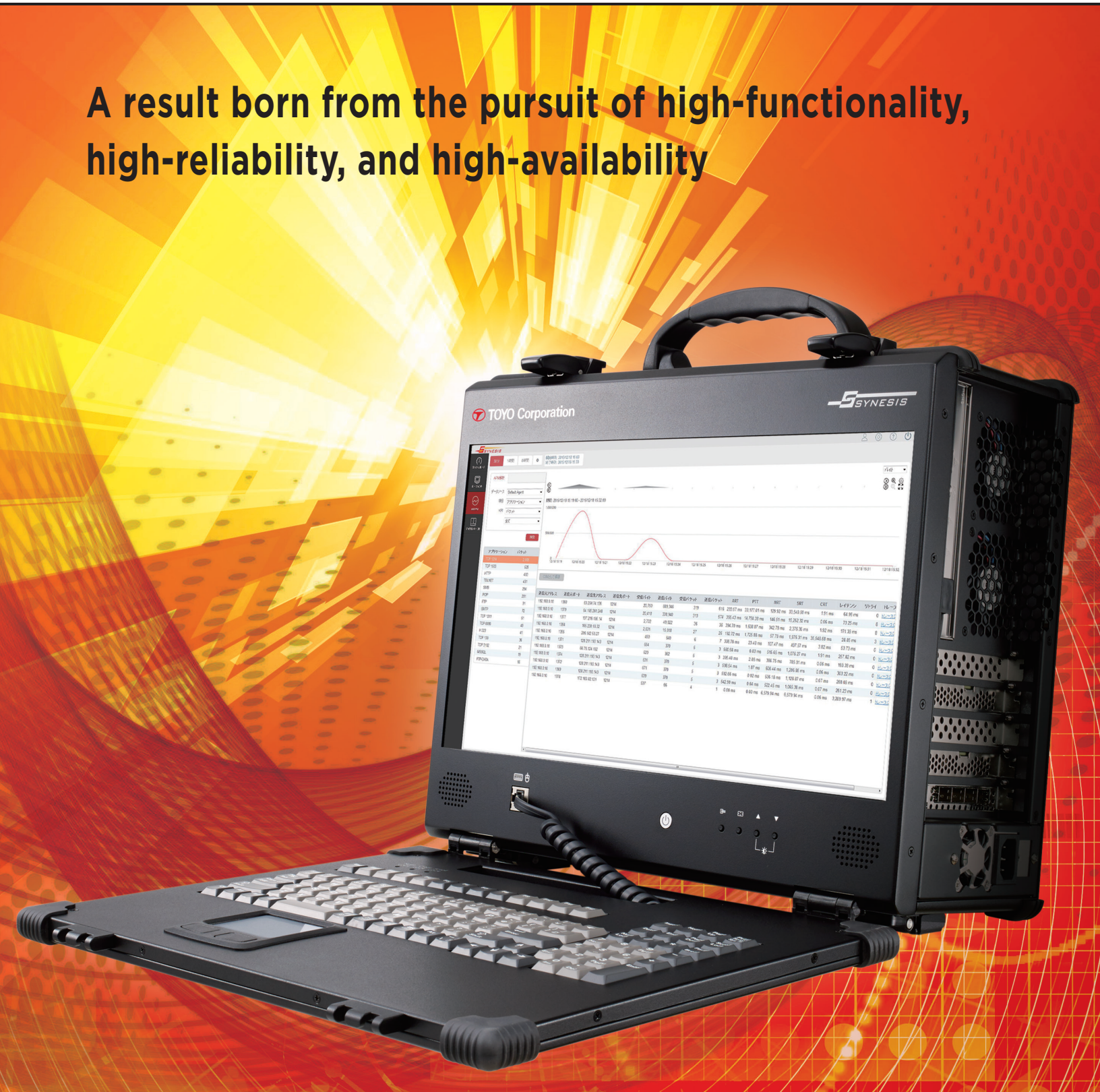
TOYO Corporation
Quest for Precision

TOYOTech LLC
A member of TOYO Corporation family

100GbE S2D Full-rate Packet Capture & Analyzer

SYNESIS

A result born from the pursuit of high-functionality, high-reliability, and high-availability



Overview

About 30 years ago, TOYO Corporation launched the sale of an analyzer capable of translating the seven layers of the TCP/IP protocol. Today, we continue in our tradition of providing industry renowned sales and maintenance of packet analyzers compatible with the latest communication standards.

With SYNESIS, we strive to address your demands and incorporate the cutting-edge technology, analysis, and measurement expertise, while aiming to create a product with excellent availability and cost-effectiveness that existing packet analyzers cannot match.

Features 1

High Performance and Quality

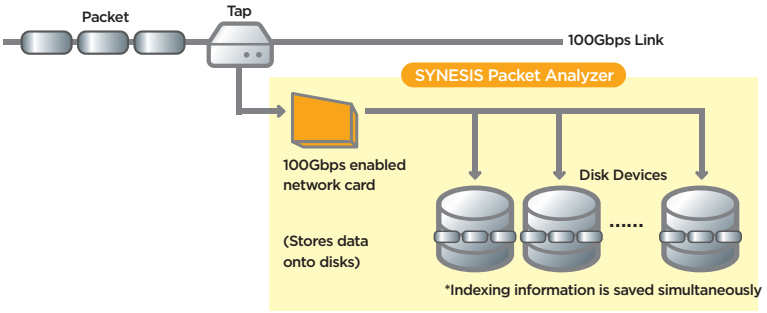
- The application developed by TOYO Corporation can capture and directly stream to storage high volume traffic -- even at a line rate 100Gbps -- without incurring any packet loss. This allows TOYO Corporation the ability to offer packet capture systems, a 100Gbps packet capture appliance and an innovative 40Gbps packet capture portable, that were not possible to implement until now.

- SYNESIS guarantees high performance capture regardless of packet size - whether short or long packets. Using disk optimization, SYNESIS captures at a higher capture speed than existing packet analyzers and in a more compact package. The result for our valued customers is a cost effective packet analyzer.

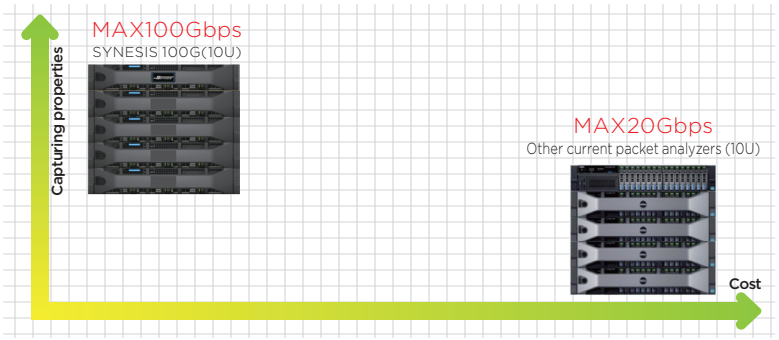
  ■ General packet analyzer
  - Capturing properties using 64-bytes (short packet)

  ■ SYNESIS Distributed / Portable
  - Capturing properties using 64-1518 bytes

■ HOW THE APPLICATION WORKS



■ Comparison with other packet analyzers

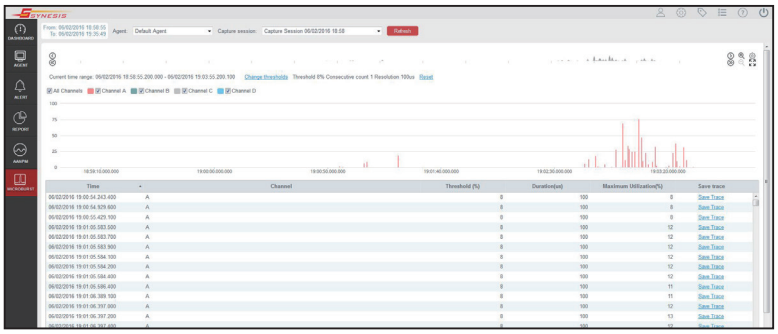


Features 2

Detection of microburst traffic

- SYNESIS will detect occurrences of microbursts against user defined threshold values during capture sessions. Related packets may be saved to trace files for more detailed analysis.

■ Detection of microburst traffic



Features 3

Greatly reduces the extraction time of trace files (AANPM analysis)

- SYNESIS incorporates the Application Aware Network Performance Method (AANPM) which can greatly reduce the time to detect and extract the target packet by saving a higher volume of information than current packet analyzers. This includes saving indexing information such as the IP address and ports concurrently during packet capture.

■ Packet Analysis and Performance Test Results

Creating trace files with AANPM	01:38.03(s)	· Search the periods during which the packet has been written. · Only download connections with a large connection volume as a trace file.
Creating trace files with a saved filter	3:47:01.89(s)	· Search the periods during which the packet has been written by applying the same condition as for APM to a saved filter. · The condition applied to the saved filter is an IP address.

* Verification conditions: Extracting the desired connection from 66TB of packet data (internal comparison)

■ Example of a comprehensive SYNESIS product lineup

Model	Portable 4G	Portable 40G	Portable 100G	Distributed 4G	Distributed 40G	Distributed 100G
Capture Port	4 x 1GbE	4 x 10GbE/1GbE	2 x 100GbE	4 x 1GbE	4 x 10GbE/1GbE	2 x 100GbE
Capture Performance	4Gbps	40Gbps	100Gbps	4Gbps	40Gbps	100Gbps

Use Case

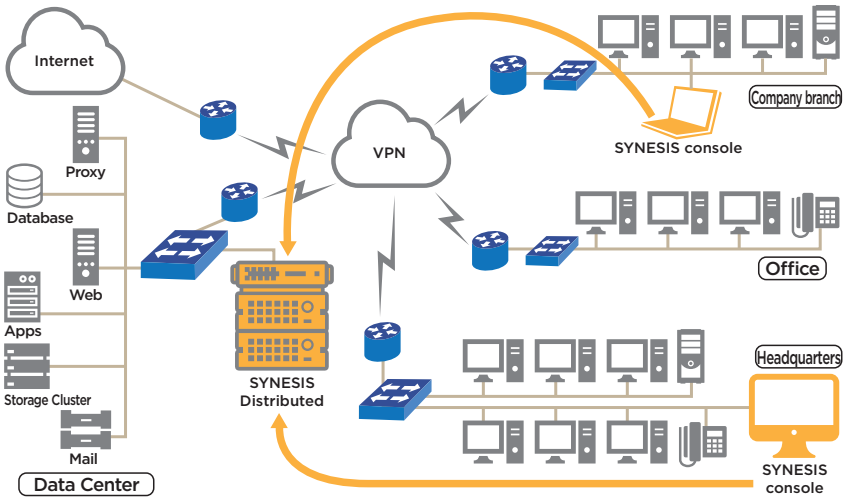
Use Case 1

▶ The implementation of “extended indexing” improves packet analysis and reduces overall analysis time.

Using extended indexing to significantly reduce the time required for extracting trace files

- Today’s corporate information systems utilize applications that connect numerous business offices. When communication quality deteriorates or a security issue arises, a system administrators troubleshooting workflow includes going through massive volumes of timestamped packets, typical of conventional packet analyzers. This task can easily take tens of hours per issue.
- With a SYNESIS deployment, system administrators will be able to easily find and extract the corresponding packet data for network issues by using connection flows, including timestamp information, alerts based on thresholds, as well as site addresses, applications, and selected server information.

■SYNESIS Distributed Installation Example 1



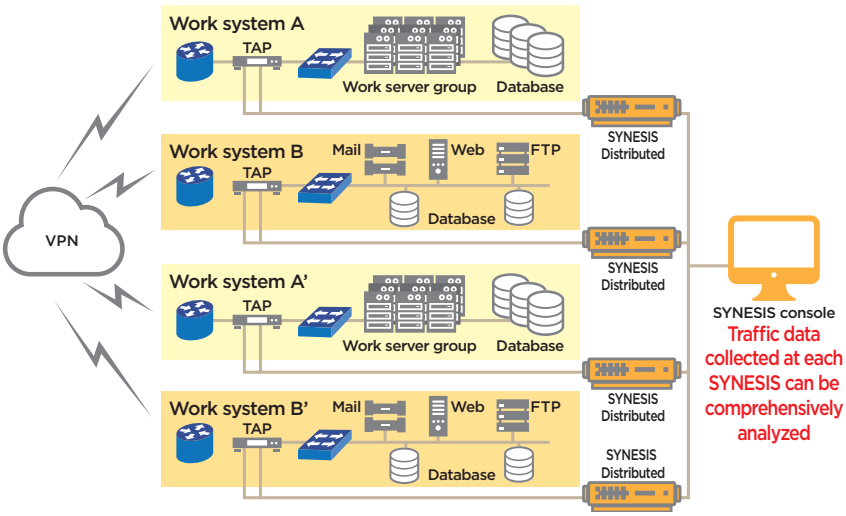
Use Case 2

▶ **Integrated network monitoring tool: Comprehensive communication content analysis of multiple agents and network lines.**

Comprehensive Analysis of Data from Multiple SYNESIS Distributed Components

- The system administrator is able to comprehensively analyze traffic collected by the various SYNESIS Distributed consoles. By creating a list of the most used applications ordered by site during a designated period, the system administrator can perform detailed analysis of a selected connection at the packet-level.
- With SYNESIS, it is possible to set a three-level threshold volume in order to supervise frequent data re-transmission and low-response occurring with a certain site or server. The system administrator can ascertain disruptions even before receiving complaints from users via the alerts sent by SYNESIS. This allows system administrators to start troubleshooting straight from the packet data related to the alerts.

■SYNESIS Distributed Installation Example 2



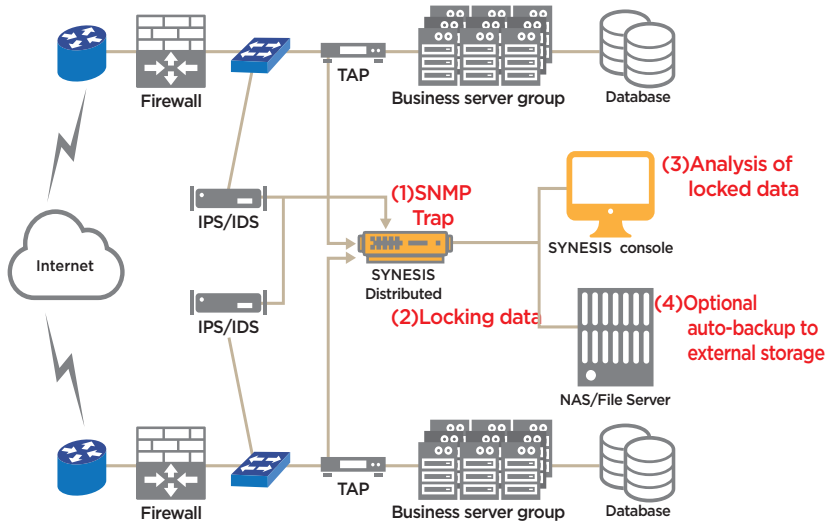
Use Case 3

▶ **Working with external security devices: Protection of captured data**

Packet data lock function using SNMP trap as a trigger

- This enables packet data from a few minutes before and after an incident to be locked, preventing it from being overwritten. This in turns allows system managers to obtain the actual attacking packets and leaked data, in order to analyze the risks that have actually occurred.
- The system administrator can schedule automatic backups of SYNESIS data to external storage devices (i.e. NAS).

■SYNESIS Distributed Installation Example 3

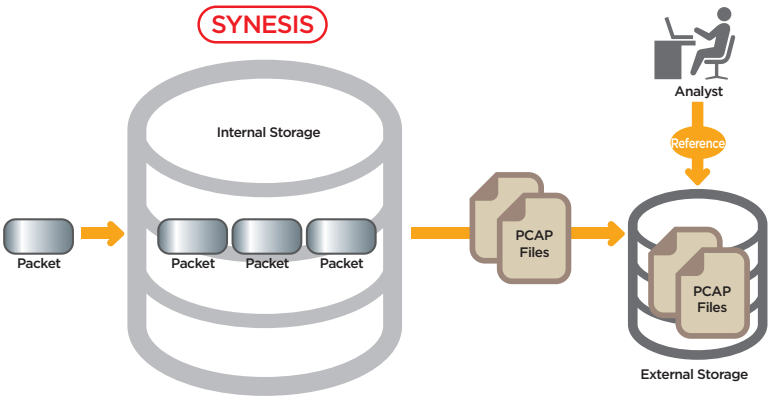


Capture Functions

The packets will be continuously captured and accumulated without omissions.
Not missing any packet in a device is the most crucial aspect in troubleshooting.

Packet Capture

SYNESIS is a capture appliance compatible with 10M/100M/1G/10G/100G networks that can capture traffic at wire speed without data loss. SYNESIS users can perform packet analysis without having to stop capture.
A backup function allows saving to PCAP files automatically while capturing. The storage destination can either be a local or remote file system.

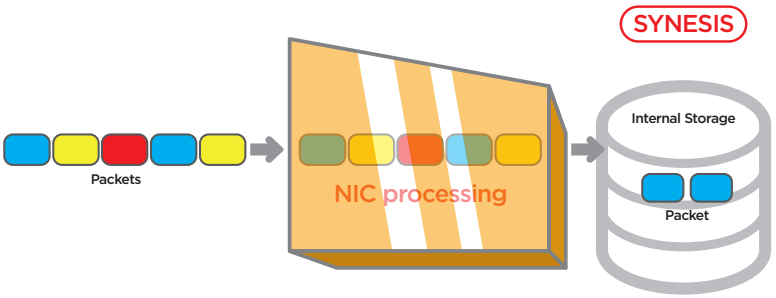


After creating PCAP files from capture data, the data is continuously and automatically saved to the specified location

Filter/Slice

The filter slicing function of SYNESIS can limit capture to only store required data or layers (model dependent) insuring sensitive information is never compromised. Since the slicing process is conducted on a specialized capture card, critical data is never lost regardless of the traffic load.

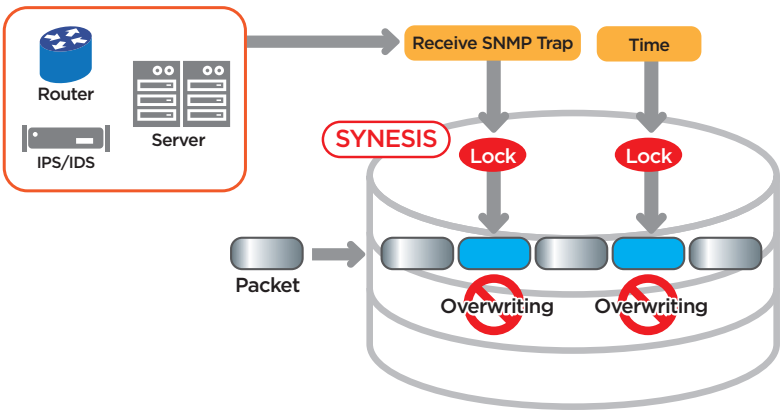
- Capture Filter: Captures only the data that meet a user defined criteria (IP Address, TCP/UDP Port#, MAC, VLAN ID)
- Slice: Captures only the data after a specified number of bytes relative to the start of the frame header



Locking

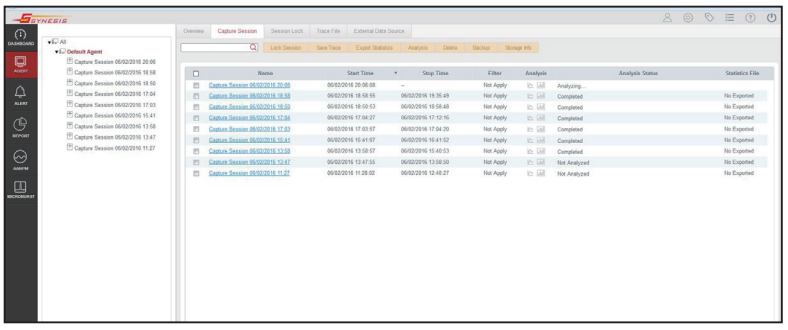
When storage is full, the oldest data will be overwritten by newer data. Critical data may be protected from being overwritten by the "lock" function.

- Before Capture: Lock specified by time and SNMP trap
- After Capture: Lock specified by time



Record Management

SYNESIS manages the capture as a single record from the start to the termination of capture. Users can perform management operations such as locking important records while deleting those that have already been analyzed. Operations such as locking, deleting, saving trace files, and exporting statistics, can be performed rapidly via the record list.



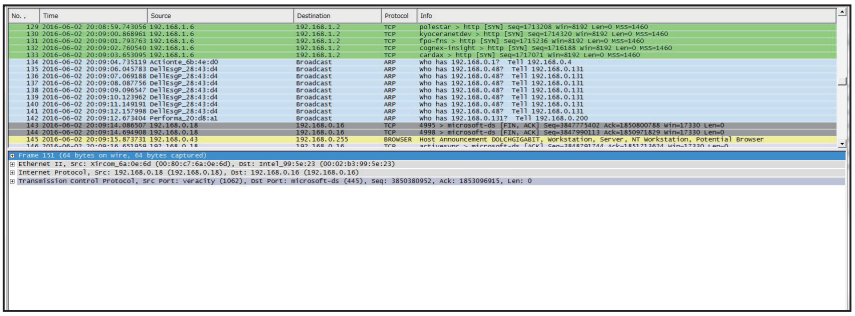
Record management screen

Analysis Functions

Being able to swiftly retrieve the target packet or communications from a large volume of accumulated data is a crucial matter. With SYNESIS, packets are visualized from various angles, allowing the users to perform analysis with different approaches to suit their objectives.

Real-time decoding

Packets can be decoded in real-time during capture. Since this function allows you to get an overview of the network status while capturing, it is a function that will prove indispensable, whether on the field or in a lab.

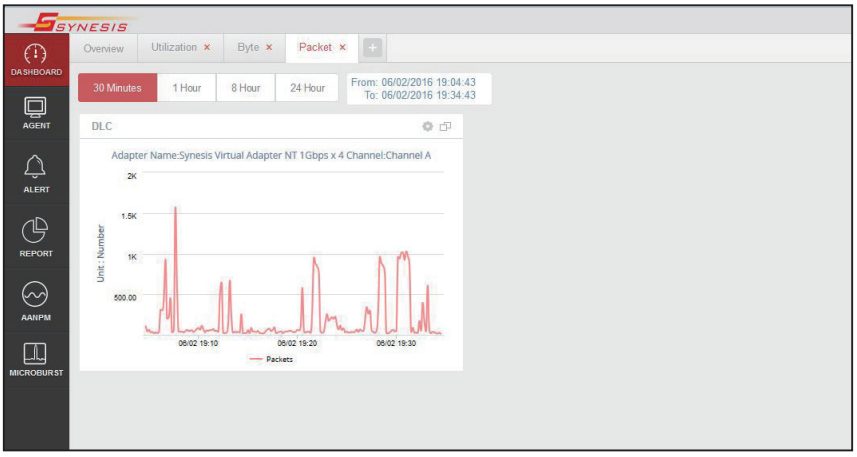


Real-time decoding screen

Real-time statistics

Corresponding traffic statistics are created and saved in one-second granularity while data is captured. With a single glance, users can determine usage differences by time and port source. Furthermore, users can create customizable dashboards that display Layer 2 and Top N statistics.

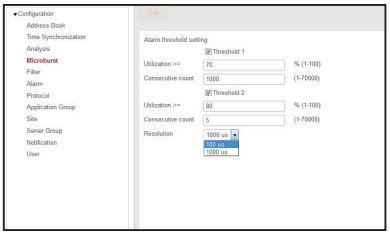
- Trend item
  - L2 Traffic
    -Usage rate, bytes/sec, packets/sec, throughput
  - TOP N application and application group
    -in/out traffic, throughput
  - TOP N host
    -in/out traffic, throughput

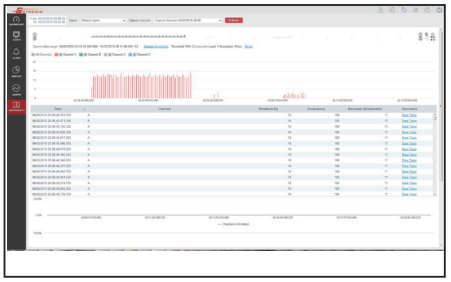


Real-time statistic screen

Detection of microbursts

SYNESIS detects microbursts that cannot be detected with conventional network supervisors and packet analyzers. Microbursts refer to a phenomenon that that triggers the convergence of network devices and can be a significant cause of packet loss. With SYNESIS, users can set the threshold value at an interval of a minimum of 100µsec, making it easy to identify and analyze packets and to see when and where microbursts occurred.





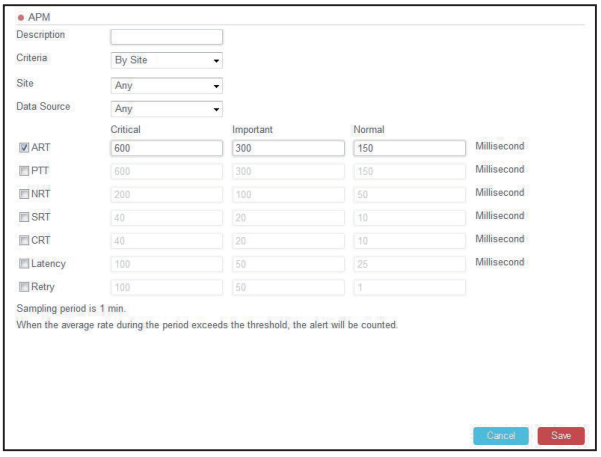
(Right) Microburst detection screen
(Left) Microburst detection screen

Alert items

SYNESIS can issue alerts by detecting any abnormalities in traffic. In order to display the alerts, users must set corresponding threshold values for each item.
The AANPM alert can have its threshold values set to three different levels (Critical/Important/Normal). Furthermore, only sessions that become an issue can be saved as a trace file.

- Alert items
  -DLC
  -NPM
  -APM

- Alert actions
  -E-mail
  -Syslog
  -SNMP Trap



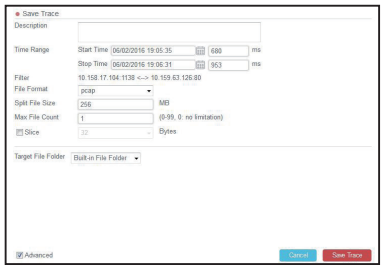
APM alert setting screen

Index Function

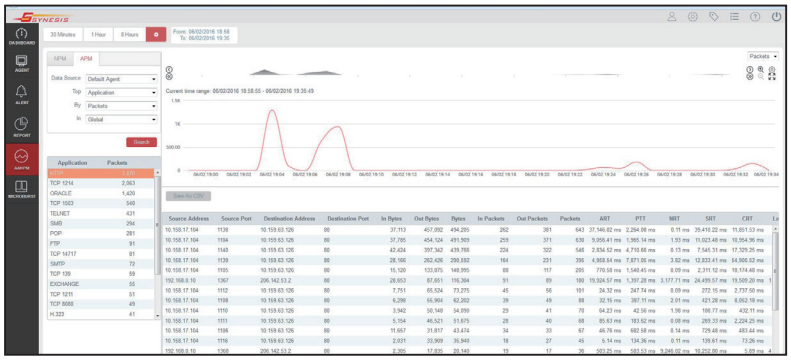
Finding communication issues by investigating each individual packet from a large volume of data is a time-consuming, laborious task. With SYNESIS, users can visualize network trends over a large volume of data and, furthermore, identify problematic connections by indexing captured data.

APM/NPM analysis

By using the capture indexing function, the KPI (Key Performance Indicator) network status can be ascertained at a trend level basis.



Context filter from the APM function



APM function

Displays KPI (Key Performance Indicator) per item ▶ Extracts only the specific connections based on the network status

■ **Items to be analyzed**

- Site: Displays for each site (subnet)
- Application: Displays for each application
- Server group: Displays for each server group (IP combinations)
- Server: Displays for each server

■ **KPI**

- Packet: ..... Number of communication packets
- Byte: ..... Number of bytes communicated
- ART (Application Response Time) ..... The time it takes for the server application to respond to a client request
- CRT (Client Response Time): ..... The time it takes for the client to initiate a request
- NRT (Network Round-trip Time): ..... The average time it takes for the packet to make a round trip across the network
- PTT (Payload Transfer Time): ..... The time it took for the server to send a response to the client request
- SRT (Server Response Time): ..... The time it took for the server to respond to the client request and complete responding.
- Latency: ..... The average time it takes for a packet to pass through a one-way network
- Retries: ..... The number of TCP packet sequences that has been retransmitted
- Throughput: ..... Values calculated by [Received bytes + sent bytes]/sample time [Kbit/sec]
- Burst throughput: ..... The maximum throughput during a certain time period. If the period is 10 minutes, then 10 throughput values would exist. The highest value among those is the burst throughput.

Optional

Packet re-player

Packets can be sent at the same link speed during the capturing of the pcap file (1GbE supported). Users can set the number of replays using the options.
Furthermore, the following items can be replaced from the packet header within the PCAP file.

-MAC address
-VLAN ID
-IP address (v4/v6)

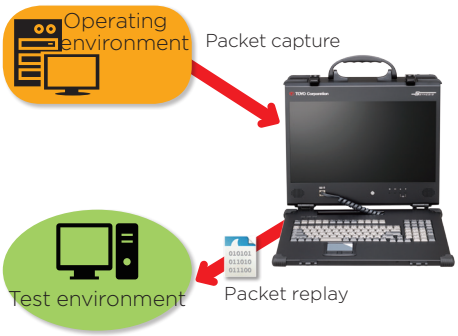
■ Usage example

Support teams may use SYNESIS to capture intermittent issues found at customer sites and recreate them in a more controlled lab environment.

1. Deploy SYNESIS in an Operating environment and set to capture continuously.
2. When the failure occurs save the corresponding packets to a trace file.
3. Redeploy SYNESIS in a Test environment that duplicates the Operating environment. Replay the saved trace file to recreate the fault.

The support team may also test engineering fixes before applying them in the Operating environment.

■ **Packet re-player image**



Usability

SYNESIS is a product designed so that the users can use it immediately after taking it out of the box. Even the smallest aspects have been designed intricately to provide an intuitive interface and enable working with other systems.

■ **Easy to understand user interface:**
SYNESIS is easily deployed. It's intuitive interface may be accessed locally or remotely via most common browsers.

■ **Open API-support:**
SYNESIS data may be accessed from external tools through its open API. This enhances automation of common network engineering operations. For example, when an incident reporting tool alerts on a network issue, corresponding packet data stored in SYNESIS may be saved automatically using scripts written in common programming languages.

■ **Time synchronization:**
Identifying the cause of communication failures may still be difficult if the related packet data isn't properly synchronized to a common time source. SYNESIS may be synchronized using GPS (Global Positioning System) or NTP (Network Time Protocol).

■ **Privilege per user:**
Users can be created by setting different privilege levels between operating users and viewing users. This will enable the prevention of operational human errors in advance.

■ **Trace storage execution management:**
Trace files saved with filters will be listed with those conditions displayed.

■ **Linux-based system:**
SYNESIS is a Linux-based application. It is designed to emphasize reliability, availability, and maintainability.

Capturing method

SYNESIS may be deployed to capture and store packet data in either of the following methods:
1. Connect using a network TAP
2. Connect using a SPAN (mirror) port on a switch

■ **TAP connection**
TAP is inserted into the network in order to extract the packet.

Advantages
・ Packets can be extracted by separating full-duplex line traffic into incoming and outgoing.

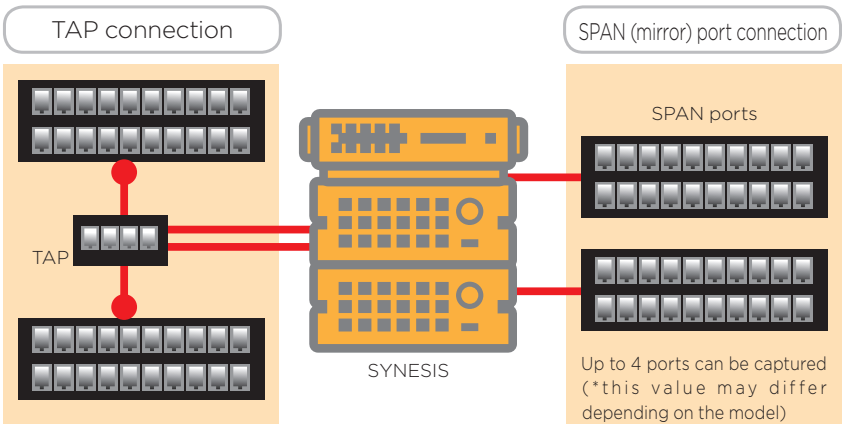
Disadvantages
・ When inserting a TAP, the network needs to be disconnected first.

■ **SPAN (mirror) port connections**
The packet is extracted by setting the appropriate SPAN (mirror) port on the switch

Advantages
・ It has no impact on the communication network performance.

Disadvantages
・ Since networks communicating using full-duplex line traffic are extracted in a semi-duplex packet, packet loss may occur as a result.

■**Connection Diagram**



Packet Analyzer Sales History

1986
Network General (US) releases Sniffer.

1987
TOYO Corporation obtains the agency right from Network General (US), and launches the sale of Sniffer in Japan.

1989
TOYO Corporation launches the sale of the Sniffer laptop model with its own Japanese localization.

1996
Sniffer University, a paid training program developed by Network General (US), starts in Japan.

1997
McAfee (US) acquires Network General (US).

2003
TOYO Corporation purchases an American venture company and establishes a wholly-owned subsidiary, ClearSight Networks (US). In October of the same year, the sale of the ClearSight Analyzer starts.

2006
The sale of the ClearSight Network Time Machine, a stream-to-disk capture appliance that would go on to become the global standard, is launched ahead of its competitors.

2007
The sale of the 10GbE-enabled ClearSight Analyzer is launched ahead of its competitors. The sale of ClearSight Network Time Machine Portable is also started.

2009
Fluke Networks (US) acquires ClearSight Networks.
TOYO Corporation continues to provide sales and development support as the sole agency in Japan for Fluke Networks.

2012
Network Time Machine Portable wins the Best of the Show Award at Interop Tokyo.

2014
Japanese sales of the Network Time Machine surpasses 700 units.

2014
NetScout (US) acquires FlukeNetworks. TOYO Corporation continues to carry out sales in Japan as its sole agency.

The SYNESIS 100G packet analyzer developed by TOYO Corporation is launched!

TOYOTech LLC

Fremont Business Park

42840 Christy St., Ste. 209
Fremont, CA 94538, USA
Phone : 1.510.438.9548
FAX : 1.510.438.9653
Email : info@toyotechus.com

www.toyotechus.com