



White Paper

Unispeed Netlogger™ FT 3.2 Data Retention and Analysis Probe White Paper

Version 3.6, 5. July 2011

©2011 Unispeed A/S. All rights reserved

Unispeed A/S
Engvej 139
DK-2300 Copenhagen S
Denmark, Europe
Tel: (+45) 33 44 55 00
www.unispeed.com

Unispeed®

Table of Contents

1 Introduction.....	2
2 Architecture.....	3
2.1 Netlogger™ hardware architecture.....	3
2.2 Connectivity.....	3
2.3 Capture devices.....	4
2.4 Light and Gateway versions.....	4
2.5 Layout regulatory compliance.....	5
2.6 Layout "Mass surveillance".....	6
3 Probe design.....	7
3.1 Interceptor design.....	7
3.2 Netlogger FT™ design (Post-processing module).....	8
4 Netlogger FT GUI.....	8
5 Uniqueness.....	10
5.1 Product comparison.....	10
5.2 Flexibility = Productivity.....	11
5.1 Performance	12
5.1 Scalability.....	12
5.2 Other technical differentiators.....	13
6 Netlogger Commercial and Security Application Areas	14
6.1 Web Analysis and business intelligence.....	14
6.2 Traffic and Content Billing.....	16
6.3 Network Performance and optimisation.....	17
6.4 Network Security.....	18
6.5 Business critical data protection.....	19
6.6 Cyber defense.....	20

1 Introduction

During the last decade requirements for network traffic analyses has been constantly growing. Most countries and organisations have realized the importance of knowing the activities on their networks, and have thus dedicated considerable resources to decipher network trends and communication.

The classic approach to log, analyse and decipher network traffic has lead to the installation of multiple load balancers, monitoring devises, mediation platforms and ad-ons to network routers and switches, often producing large amounts of net-flows and increased load on the production network.

Lawful interception is traditionally handled by writing massive amount of Ethernet traffic (PCAP) to storage, and forwarding unfiltered data to external protocol sequencing and reassembly systems before writing the extracted data to database. This method is reasonable with a limited number of intercepted targets but it fails grossly when the purpose is a broad spectre monitoring solution. Solutions are often rigid, complicated to configure and maintain and bottlenecks are introduced when data flows through several components.

Unispeed Netlogger and derived products ^{a)} are designed to counter this adverse effect, by introducing a device that handles all such processes real-time in a zero-copy environment. Whether the primary task is Regulatory data interception, mass surveillance, network security or commercial traffic analysis, this method greatly improves performance and reduces the complexity. The full Netlogger tool set is available to the customer through an intuitive interface to reconfigure and exploit the vast amount of functionalities and benefits that a Netlogger can offer it's users.

Basically, with Unispeed Netlogger you have access to the hole story in real-time, allowing customers to deep packet inspect fully loaded network links with zero packet loss, aggregate data, determine traffic amounts and composition and store data in one central place, or hand on relevant data sets directly to business intelligence and lawful reporting suites such as the Unispeed Blue Shield system. The Netlogger provides loss-less capture on fully loaded Ethernet links and delivers extracted output to any database with just one GUI to configure.

This white paper will give you a brief introduction to the Unispeed Netlogger and how to benefit from the wealth of information it provides. As you will learn, it is not difficult at all! And when you have finished, you will have a whole new knowledge of the traffic on your network.

*a) The Unispeed **Netlogger TM** is a high capacity and fully configurable packet intercept and analysis device. **Unispeed LI probes**, the **Unispeed Interceptor** and **Unispeed Bluegate** devices are basically Netloggers optimized for specific purposes.*

*The Unispeed **FT framework** is the highly flexible Linux based SW package installed on all Unispeed probes and devices.*

*The Unispeed **Blue Shield system** is a control, monitoring and data mining system which supervises a random number of Unispeed probes and devices.*

*The Blue Shield system consists of the **Blue Shield GUI** and data presentation component, the **Blueserver** probe monitoring and control server system, the **BS probe** SW package installed on Unispeed probes and devises which are controlled by the Blueserver.*

*The **Bluegate** system is a compilations of SW components which transforms Unispeed probes into advanced **Gateway units**. It configures and controls the gateway functionalities (firewall, authentication, routing , policy enforcement, shaping etc.) either via the Bluegate configuration interface or via the Blue Shield GUI*

2 Architecture

2.1 Netlogger™ hardware architecture

Before going into details about the Netlogger™ device, we will present you with a quick overview. This will help you to realize the many great features, which are directly usable in your day-to-day routines.

Basically, Unispeed Netlogger is a passive Data retention sniffer, traffic analyser and data center.

The system can be installed on literally any hardware platform supporting Linux OS.

Extensive use of commodity servers helps Unispeed keeping up with the highest requirements when performance, security and durability is considered. The server versions are designed for mounting in a standard 19" rack.

All connectivity to the Netlogger is handled over secure tunnels and hardware protection and rugged designs for field use are available.



Illustration 1: Unispeed Netlogger, Interceptor and CDR/LI probes

2.2 Connectivity

The Netlogger receives data from a span/mirrored ports on routers or switches, or network traffic is copied by installing copper or optical taps at relevant traffic junctions. Up to 16 x 1 GB ports, 2 x Duplex 10GB (32 million pps each) or one Duplex 40GB port capture interfaces are supported, and line speed capability is achieved on a single "off the shell server". Clustered installations will easily scale to Duplex 80 Gbit/s and beyond.



Illustration 2: Netoptics 10Gbit Fiber Regeneration tap

2.3 Capture devices

All standard Network adapters are supported including Intel, Broadcom and Chelsio. For ultimate performance the hardware accelerated Napatech NT capture or in-line adapters are the preferred choice, offering both channel-merging and load sharing for parallel processing of Internet frames on up to 32 CPU cores using a single multi core server or a cluster of servers. Offload and pre filtering on port, IP ranges, etc is available on the adapter itself.

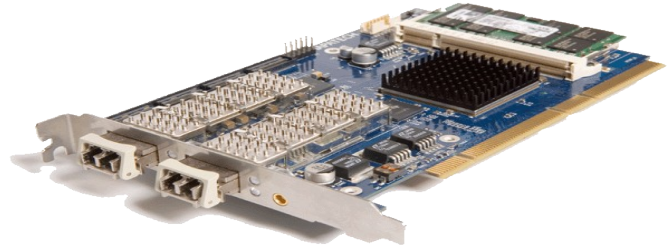


Illustration 3: Napatech NT20E - Duplex 10GBASE Capture/In line adapter

2.4 Light and Gateway versions

Netlogger light versions are designed for mobile or corporate needs. The fan-less device is completely silent and can be supplied from battery power. Light versions are available with wireless network cards and are typically capable of processing 200Mbit/s to 500 Mbit/s.

The Blue Shield Gateway (Bluegate) unit is a by-pass unit offering both data retention capability and a complete packet of network services and monitoring, including customer landing page configuration, routing, dhcp server, firewall, packet and content filtering and traffic shaping.

The Bluegate is designed for the hospitality sector where Network address translation requires the unit to correlate assigned local IP with the public IP's and to track unique user identity.

For more information about the Bluegate, please refer to the Unispeed Blue Shield documentation



Illustration 4: Light versions and Gateways

The exact hardware configuration of the Netlogger™ device is adjusted to the traffic load on the network it captures from and the data processing demands. Before setting up the Netlogger™ device or a cluster of Netloggers you will receive expert advise from the unispeed team.

2.5 Layout regulatory compliance

Illustration 3 demonstrates a sample set-up of the Netlogger configured for Regulatory data retention (Unispeed Blue Shield LI / CDR probe). Here, the Netlogger probe is logging network traffic to a network attached storage through the Blueserver, but this could also be done exclusively on the Netlogger device, depending on customer requirements and the amount of data to be retained.

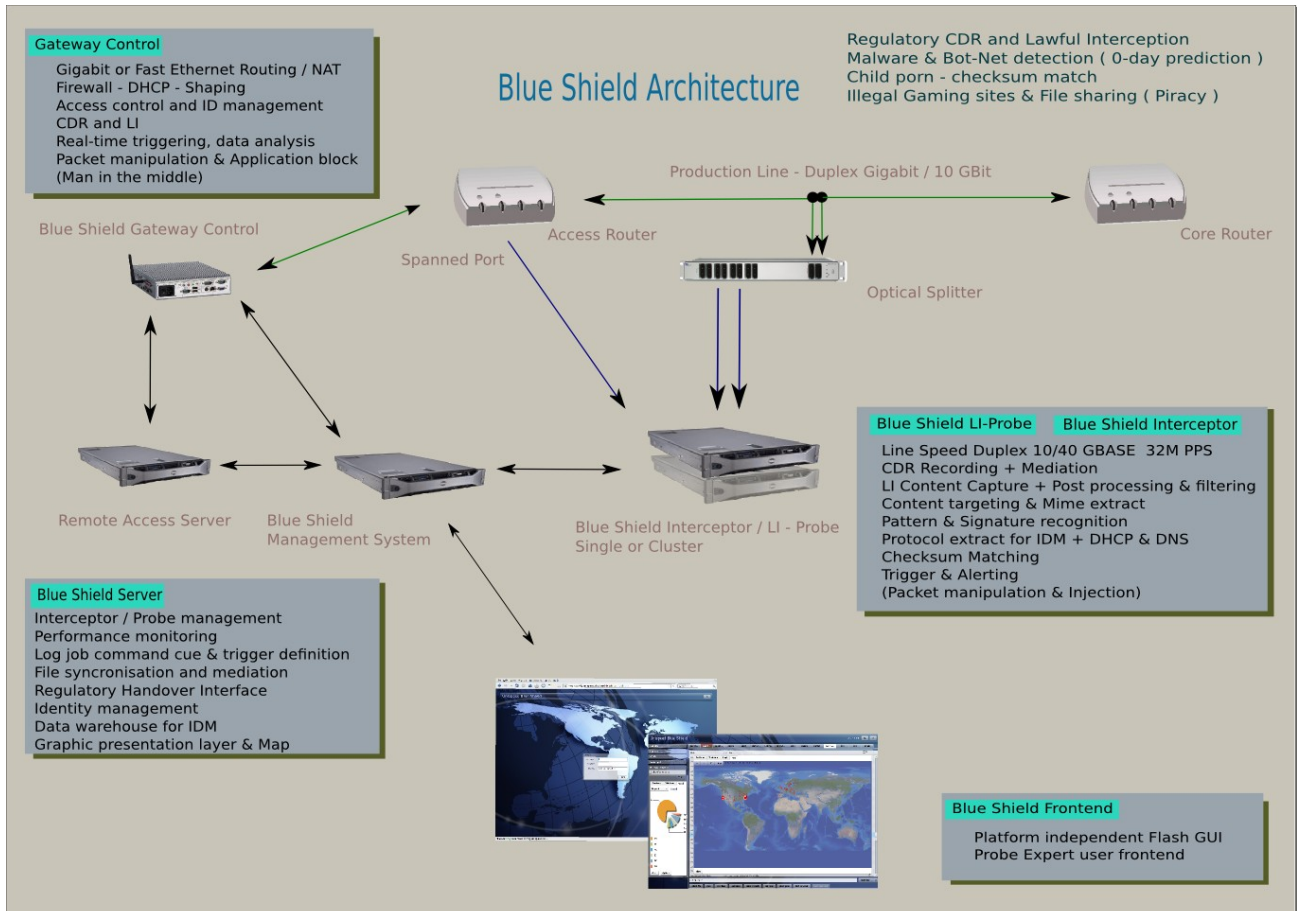


Illustration 5: Sample set-up data retention system

When configured for regulatory Call data retention, the Unispeed LI / CDR probe has the ability to store CDR data sets remotely in a highly compressed binary log format. Whilst the device is installed with a extreme high performance data extract system, the probe completely relieves the need for a massive central data storage system. When a query is provisioned from the Blueserver (central management function) the workload is distributed to all the controlled units. This means that when the monitored network grows, the mediation function automatically grows with it.

Customers and organisations installing Unispeed probes for regulatory data retention can further draw on the benefits of the fully embedded tool set for various tasks associated with Cyber criminal activity and QoS tasks.

2.6 Layout "Mass surveillance"

Illustration 4 demonstrates a sample set-up of the Netlogger configured for Mass surveillance (Unispeed Blue Shield Interceptor / LI-probe). Here, the Netlogger's primary function is to extract and reassemble communication and voice protocols in real-time and forward the data sets to a high performance storage and mining system.

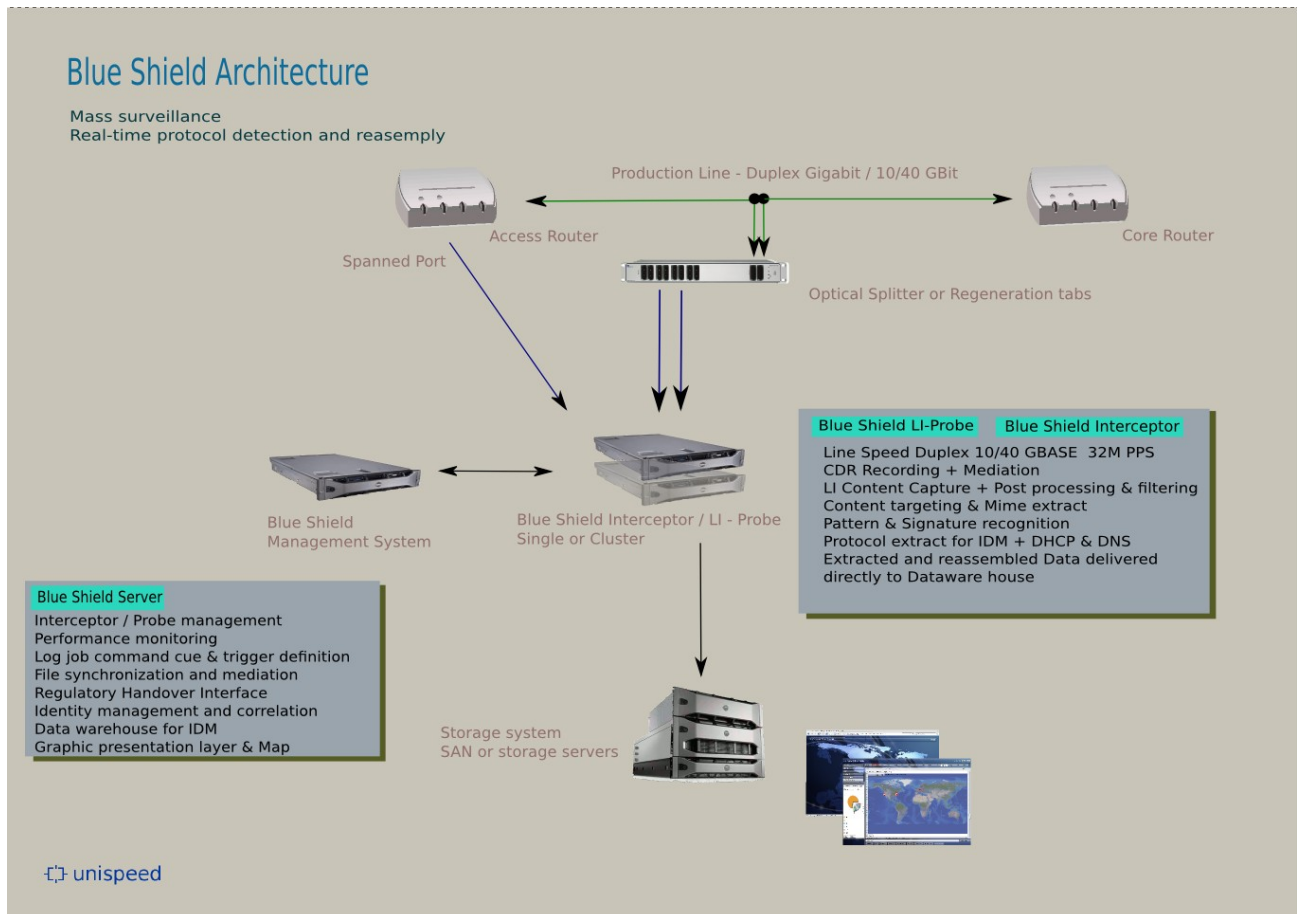


Illustration 6: Sample set-up mass surveillance system

The Unispeed "Mass surveillance" solutions consistently breaks with the traditional approach to lawful interception.

The system allows organisations to identify and target criminal activity by content or application layer protocol headers.

Traditional lawful interception is designed to target a single or more individuals by their assigned IP address. Lawful interception assumes that a given IP address can be mapped to a unique user. With today's nomadic nature of Internet users this can be an almost impossible task.

The Unispeed "Mass surveillance" solution allows for targeting correspondence between mail servers (mail interchange) where the traffic is less likely to be encrypted, and other types of traffic to / from anonymous clients based on their mail addresses, user names, session cookies or by keywords or patterns in the content identifying traffic of interest.

The system allows for monitoring of chat forums and social networks like Facebook or twitter and can prove a valuable tool to provide the intelligence required to act proactively.

3 Probe design

3.1 Interceptor design

The Unispeed Interceptor is designed to add string/pattern matching capability to the Duplex 10/40 GB blue Shield data retention and analysis device.

With the interceptor module installed on a standard Unispeed Blue Shield probe (Netlogger FT) the operator is allowed to target strings and patterns in the full packet content and forward/stream the intercepted sessions as original Ethernet traffic or UDP/RTP encapsulated packet stream (CALEA specification)

All intercepted traffic, both matched and unmatched packets / sessions are in turn made available for the Post processing module (Netlogger FT) analytic tool-set to allow for regulatory data retention and lawful inspection or other traffic analysis needs. The functionality also caters for creation of index files of matched traffic, to speed up the data mining process.

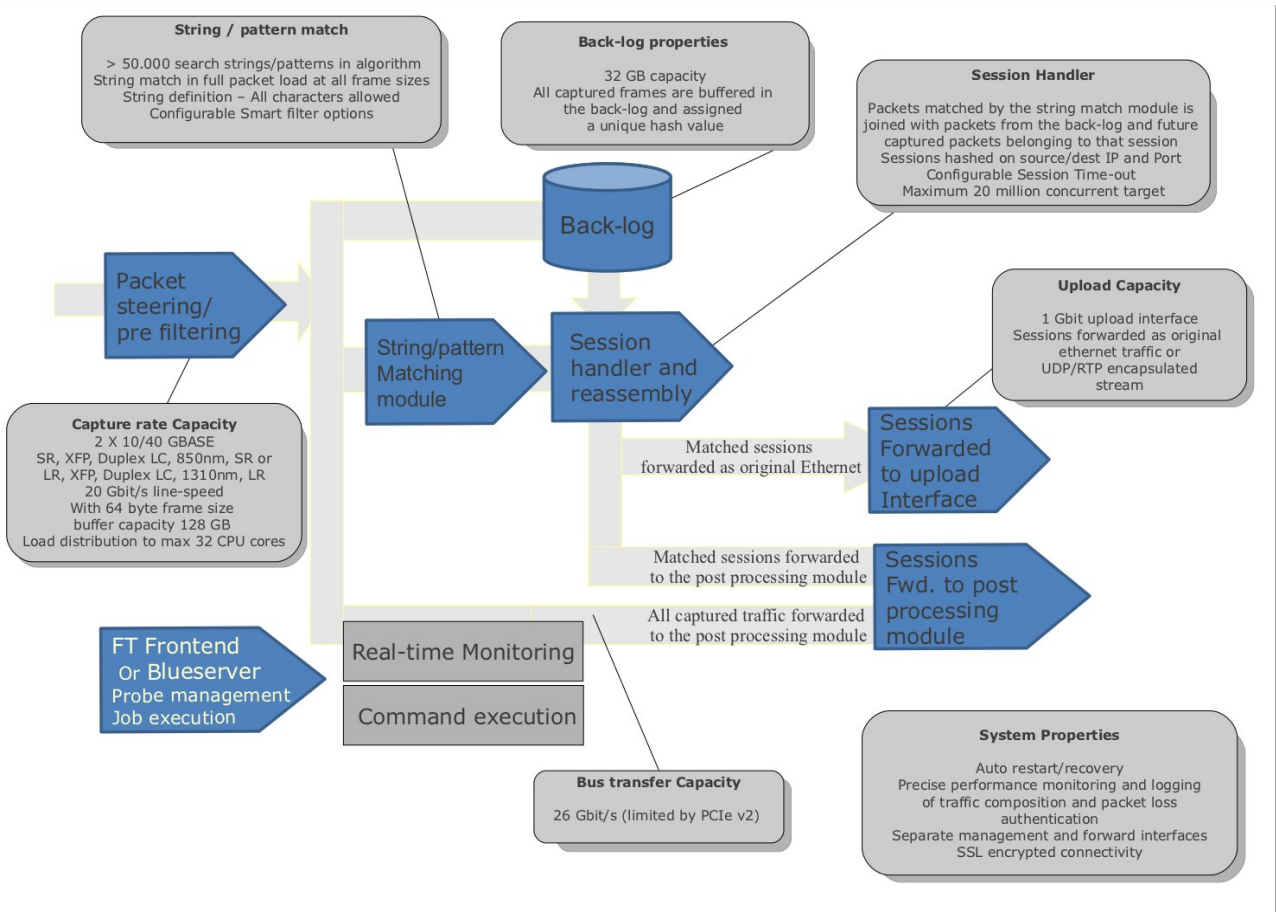


Illustration 7: Unispeed Interceptor module

The Interceptor system is a highly scalable system which is equally suitable for detection of criminal activity, cyber crime, malicious traffic like virus, trojan's and bot-nets.

3.2 Netlogger FT™ design (Post-processing module)

The Netlogger FT post processing module (Illustration 8) is with its 60 configurable tool probably the most versatile network processing engine on the market.

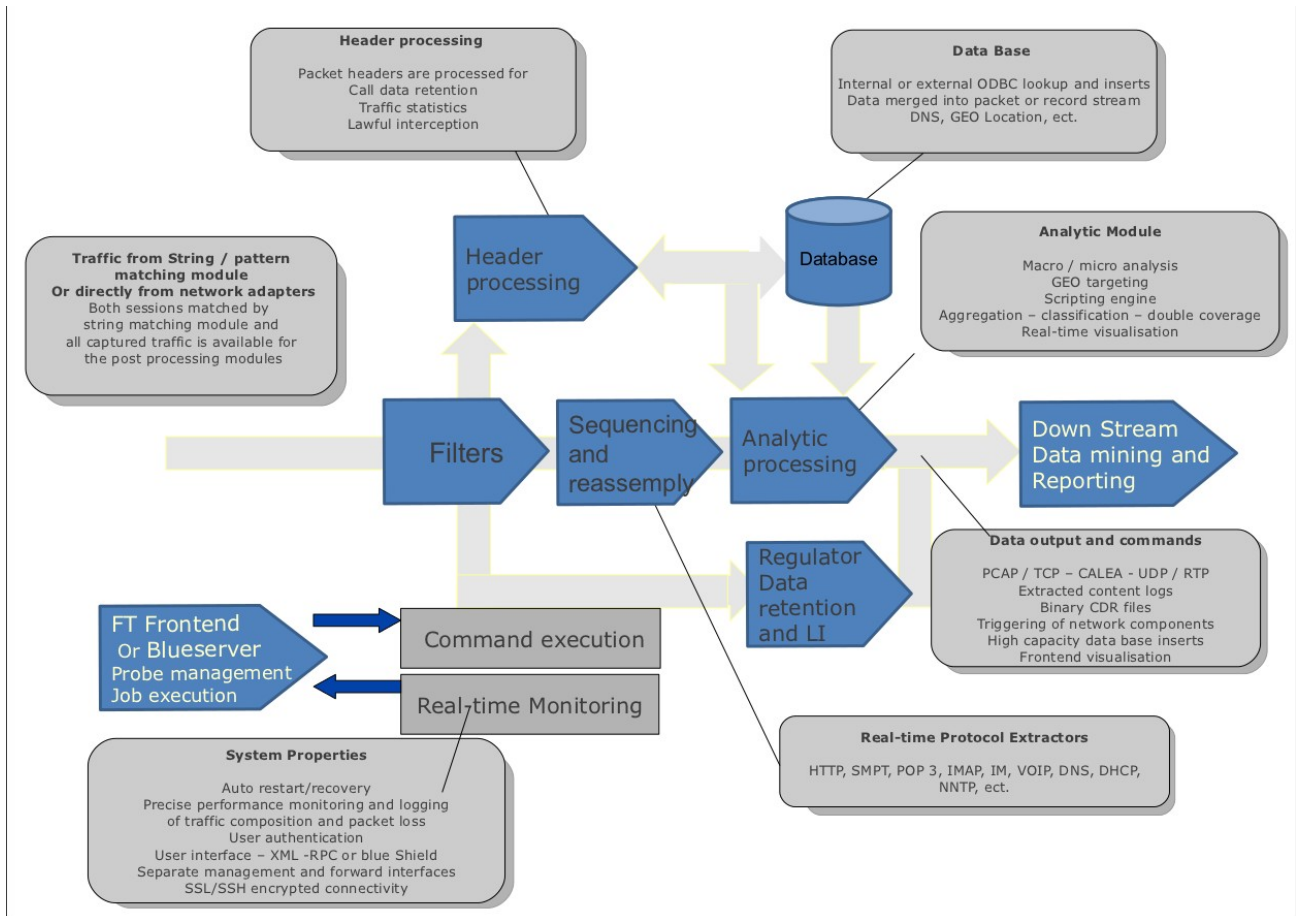


Illustration 8: Netlogger processing schematic

4 Netlogger FT GUI

The Netlogger FT post processing module (Illustration 8) is with its 60 configurable tool probably the most versatile network processing engine on the market

Illustration 9 shows the unique configuration interface for the Netlogger and its derivatives. Every configuration change can be performed by simply dropping a new tool from the left menu onto the canvas, connect it to stream and configure it. When it is turned on it starts doing it's duty without interruption to the working processes and without packet loss.

In the depicted example approximately 7 Gbit/s (4.6M pps average 196 byte each) is distributed across 8 CPU cores, producing less than 50% load on each CPU core

Each core processing about 580.000 pps - as the frames are matched against a target filter containing 20.000 target strings.

The packets matched by the pattern match module (about 10%) are forwarded to the forwarding interface.

One of the treads is further channelled through the extract packet header tool both concerning the dark blue tread total captured stream and the light blue tread matched frames stream.

The duty of the extract packet header tool is to read the header from each and every packet passing through the tread.

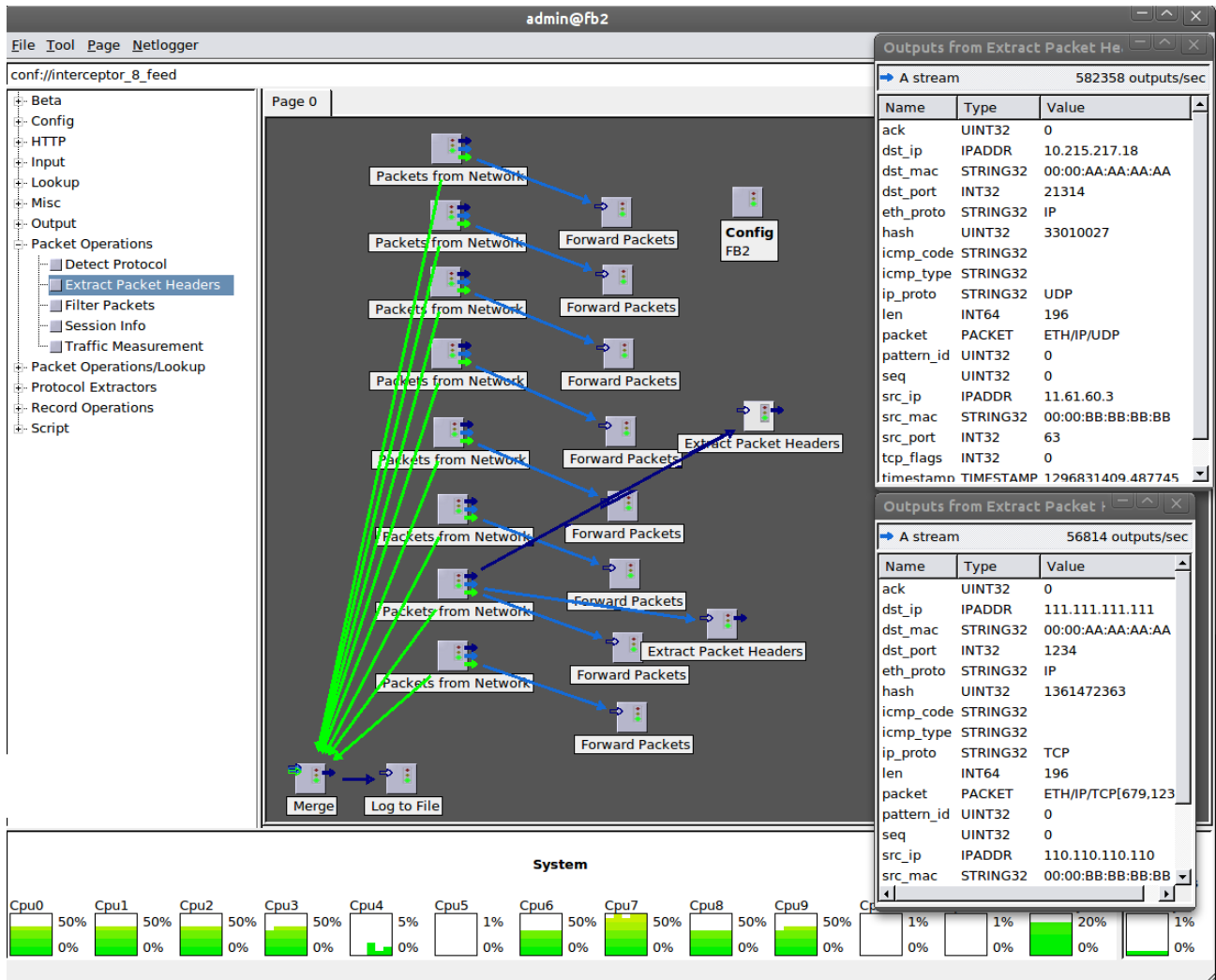


Illustration 9: The Netlogger FT canvas

5 Uniqueness

5.1 Product comparison

The Technology developed by Unispeed over the last decade is the result of an intensive focus on performance, usability and flexibility. Not many other products within network sniffing and deep packet inspection offers the same high performance while capturing, analyzing and forwarding extracted data in one turn without loss of packets.

The ability to real-time processing of network packets on fully utilized duplex network links, and what's even so important at any realistic packet size, on a single platform, enables the customer to create reliable network retention and monitoring solutions which are less complex, easier to maintain and offers the highest work flow visibility in the industry.

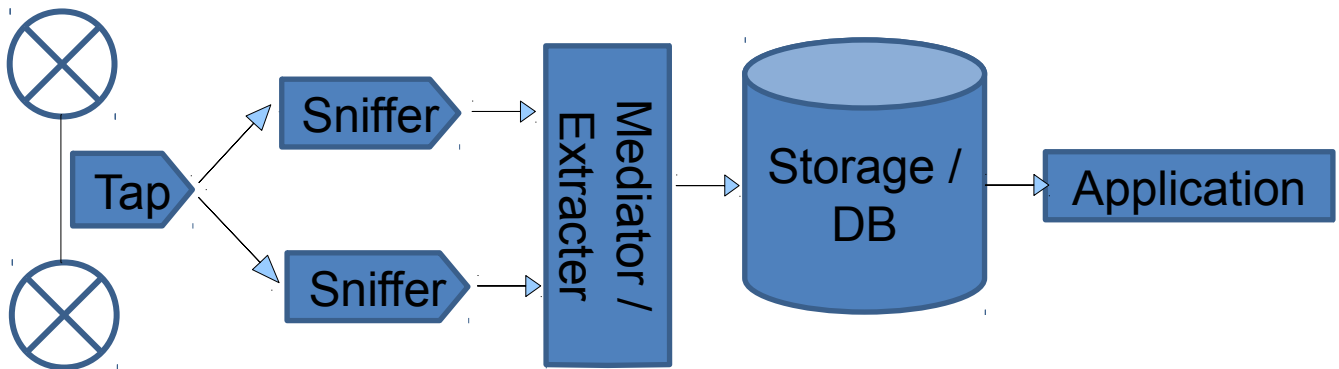


Illustration 10: Standard approach to Network retention and analytics

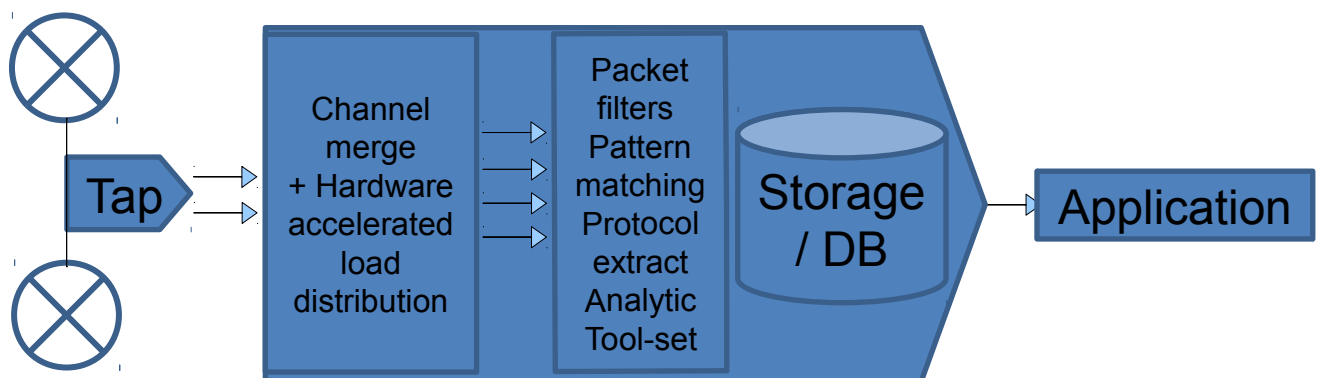


Illustration 11: Unispeed Netlogger tm - Single platform duplex device

5.2 Flexibility = Productivity

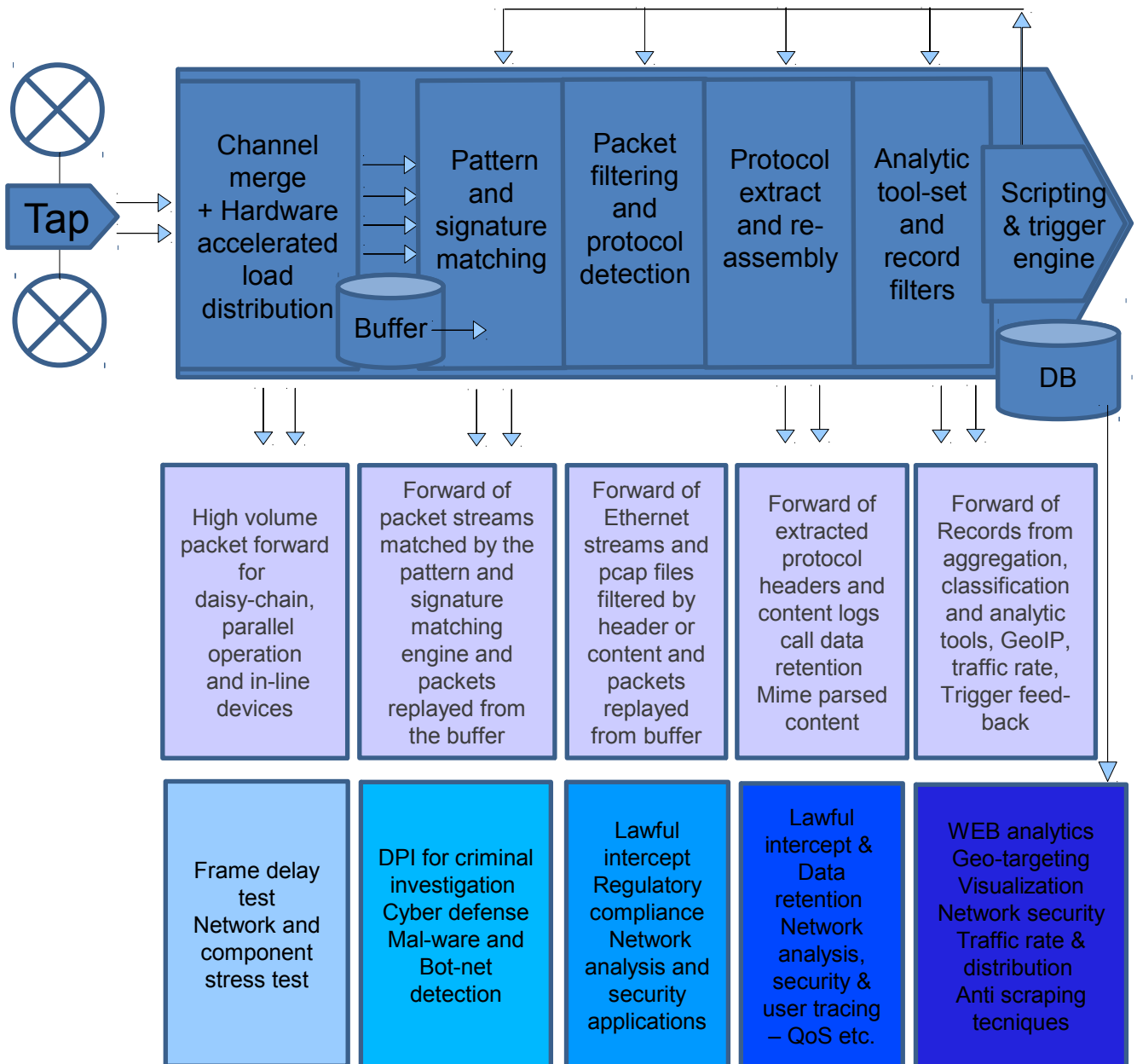
The Unispeed Netlogger™ is customized and specialized into a portfolio of products.

The Unispeed LI probes, the Unispeed Interceptor and Unispeed Bluegate are all build on the basic Netlogger FT design.

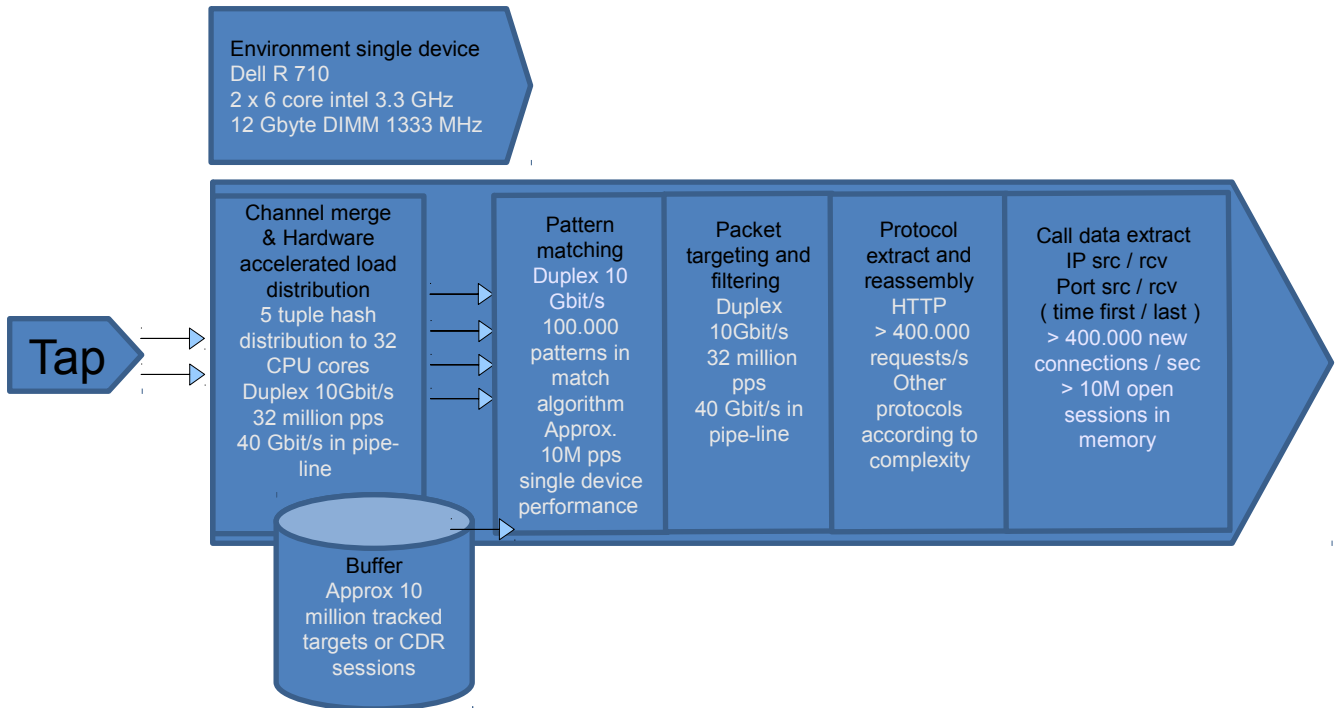
The FT framework which is the core engine is a high performance Linux based framework which takes full benefit of modern multi core hardware platforms and hardware accelerated capture interfaces.

No matter for which purpose the device was purchased - the customer is allowed to take full benefit of the flexibility the FT frame work offers.

The logic tool-chain architecture in the FT frame work assures that data can be drawn from the device at any point in the chain. Like wise can data from internal or external sources (files, binaries, data bases etc.) be joined into the chain at any given time.

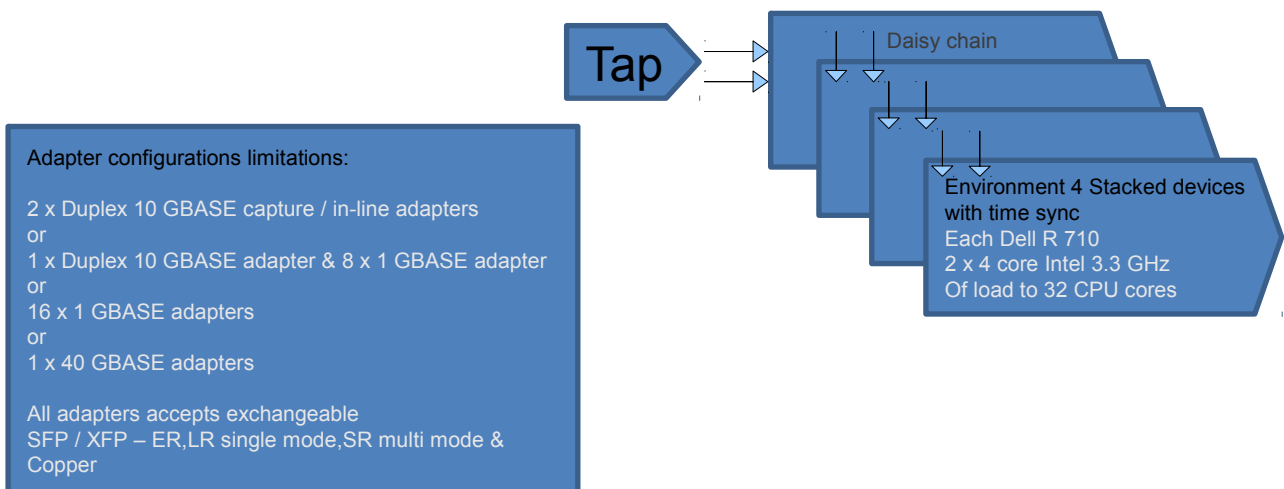


5.1 Performance



5.1 Scalability

For performance intensive operations maximum scalability is achieved by either daisy-chain stacked servers or by means of regeneration tabs. Each device will calculate a hash value for each frame using 5 tuple sorted hash algorithm - ensuring each complete session is directed to the same CPU thread. The remaining load is either dropped or chained to the next server in the stack.



5.2 Other technical differentiators

There are several features build into the Netlogger that distinguish it from ordinary packet sniffers.

First of all the Netlogger is build on a Zero-copy subsystem -the Unispeed K-sniffer. The ability to read packets from a Duplex network, filter, extract and reassemble protocols, and analyse the data without copying it makes the Netlogger by far the fastest and most versatile packet sniffer on the market - with multiple 1 Gbit/s, 10 GBit/s or 40Gbit/s duplex configurations available.

As the Netlogger performs real-time extraction/parsing and filtering/analysis of the collected data before storage, it is unlike most other system seldom limited by the speed data can be written to storage and retroactively accessed.

This is mainly due to the real time removal of overhead from packet headers, retransmission and irrelevant packets and protocols as Ethernet frames passes through the system. The Netlogger can log to several different file formats and databases simultaneously. The ability to collect and analyse data in one process also allows it to react on the data it captures in real-time and change the configuration of firewalls and IPS as things are happening or even change it's own configuration.

Secondly the Netlogger unlike most other packet sniffers can read data from almost all data sources including raw-packet-files (PCAP) and log-files (Netlogger format or common log files format, like CSV).

This valued feature enables the Netlogger to perform post-processing and data-mining of files previously stored, and even do this while it keeps capturing from the monitored network.

Another valued feature of the Netlogger is the way it fully integrates data from data-bases or static lookups and merges it into the data-stream. In this way it can join known information about costumers eg. User ID, AS-numbers or GEO- location data with real-time collected data. These lookups are cached in memory to avoid slowdown arising from data-base performance.

Derivatives of the Netlogger includes the Unispeed Interceptor which provides string / pattern and signature matching throughout the packet content before frames are delivered to the post processing tools. For each session the pattern match module forwards the post processing module receives a unique target ID. A geographical lookup can now be performed and the distribution of targets are easily depicted on a map

Unispeed Data Retention and LI probes provides extended functionality for targeting and remote data mining of Call data and LI capture files. In fact the Unispeed DR and LI probes are the only devices on the market which can fulfil any task associated with regulatory data retention and content intercept from capture, through mediation and forward of data for ETSI XML compliance and CALEA encapsulated content delivery.

6 Netlogger Commercial and Security Application Areas

The Netlogger™ device can be used for many different purposes. In the following we describe six different areas, where the Netlogger™ is often applied. The Netlogger™ can, however, be applied in many other areas. Therefore we recommend that you discuss your exact requirements with Unispeed (or a Unispeed partner) – then we will help you to find the solution, which is right for your organisation.

6.1 Web Analysis and business intelligence

Good service has always been a key factor to success. Today the customer's perception of your company starts even before you know the customer, namely when he first meets your web site. Most traditional web analysis is done by analysing historic data about customer behaviour. For optimum service more and more companies are moving into real-time web optimization. Unispeed Web analysis technology allows you to identify and track the customer in real-time and respond to his needs when he clicks through your web site. For extensive Business Intelligence solutions Unispeed has partnered with companies specialised in BI solutions which in combination with Unispeed data collectors brings you fast and accessible business intelligence for timely decision making.

The Unispeed Blue Shield Management system has its own graphic reporting system that will provide most users with a flexible and easy to use graphic data presentation system.

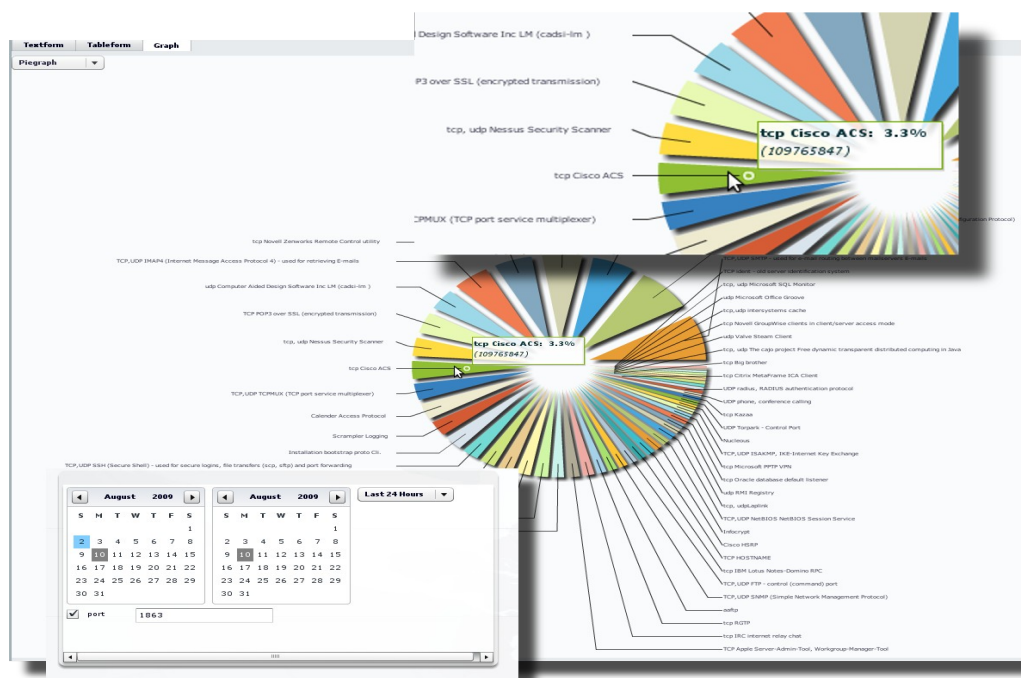


Illustration 12: Unispeed blue shield – Graphic reporting module

Web / HTTP analysis Key features

- Conversion rate The conversion rate is the key element for analysing a successful advertising campaign. In addition, it shows how effective specific search engines or partner sites are.
- Transition: Discover how costumers clicks through your web site, analysing if the costumer meets your success criteria in the shortest way, where costumers tend to drop out and why.
- Double coverage: Analyse the habit patterns of your costumers to fine tune your campaigns an optimise the flow through your web site
- Page entry: From where did the costumer enter your site, which affiliated sites or search engines are generating more costumers.
- Micro optimisation: real-time analyse how changes to the web site effects sales completion and a smooth conversion through you web site
- Costumer profiling: React to costumers need geographically, bandwidth, screen resolution, return rate of costumer
- Availability: Alert maintenance and sales functions if server or network response time exceeds desired limits (SMS, E-mail or sys log)
- Unispeed Netlogger™ eliminates the need for tagging the web pages and the need for processing vast amount of log files, thereby significantly increasing the performance and speed of both the network and the analysis.

The following features are all readily available in the standard Netlogger™

- Sniff all TCP & HTTP traffic on networks.
- Extract and reassemble HTTP traffic into streams of records, which describe client requests and server responses.
- Detect if a given URL is a page.
- Trace clients by a combination of HTTP fields.
- Detect user preferences on a web site.
- Derive agent information from the agent string, including agent name, agent version and client platform.
- Map client IP addresses to country, city, region.(GEO Targeting).
- Map client IP addresses to second level domain names (e.g. "domain.com").
- Map client IP address to AS-number
- Measure bandwidth of clients in real-time.
- Aggregate data in user-defined forms – e.g. client IP country distribution per minute, average server response time per hour, distribution of client agents per day etc.
- Aggregate data for click- stream analysis, transition and double coverage
- Generate statistics based on arguments in args or cookie
- Generate web log files.
- Log encrypted (SSL) traffic.
- Eliminate unwanted entries by applying custom filters on the data before it is written to log files.
- Learn unique geographical information about your clients.
- Generate customized server responses based on client connection properties.

6.2 Traffic and Content Billing

Unispeed traffic and content billing solutions can help service providers capture new revenue streams for a variety of high-value, high-margin content services. Installing a single Netlogger™ to your network will enable you to make intelligent billing solutions based on any combination of content, download time, volume and service.

Netlogger easily differentiates whether the traffic is inbound, outbound or internal and billing can be differentiated for different network layers, users and services.

The Netlogger™ device makes it easy to create and deploy applications for customer- and advertise billing.

Billing data is retrieved directly from the Ethernet stream and merged with the clients data. The Netlogger™ continuously extracts DHCP requests and Option 82 information in order to dynamically correlate the client ID and assigned IP-address

Some common usages are:

- **Per volume:** Netlogger will track the customers traffic volume aggregated over time. Advanced rules like traffic direction, price differentiating with respect to peakhours, maximum allowed band with or flat rate exceeds is easily configured into the Netlogger.
- **Per Application:** Netlogger will bill according to the application layer
- **Per download:** Netlogger will automatically identify whether the service is a downloaded picture, video, game etc. and bill accordingly
- **Per click:** Netlogger will bill-back content providers for each time the customer click on an advertisement
- **Per Location:** Netlogger can track the destination of each transmission and bill accordingly This feature enables the service provider to compensate for high amounts of international traffic arising from file sharing networks ect.

The Netlogger billing options is easy integrated with a variety of billing and CRM systems.

Quality of Service

Netlogger can track the quality of each transmission with respect to errors and retransmissions, thereby significantly improve customer satisfaction, and even alert maintenance and sales functions if server or network response time exceeds desired limits (SMS, E-mail or sys log)

6.3 Network Performance and optimisation

Unispeed Network performance and optimization solution can help service providers monitor the traffic flow across their network

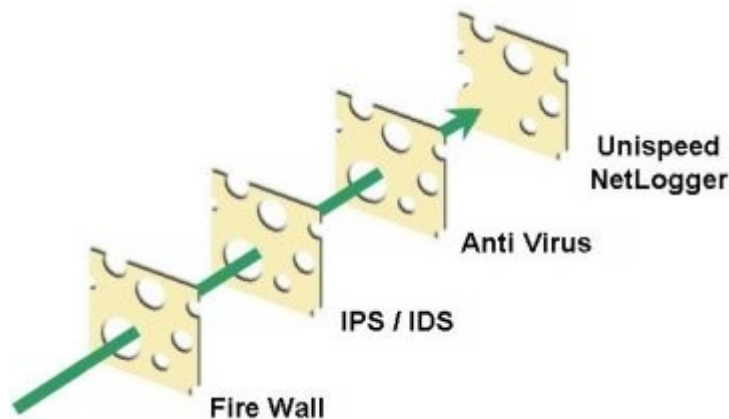
- **Traffic composition monitoring** is a key factor in controlling the usage across your network. Using deep packet inspection, Netlogger will provide you the most clear view of what is flowing through your network.
- **Quality of service** is best monitored from the customer point of view. Netlogger is doing this by checking each transmission for errors and retransmissions. It also monitors the response time and the integrity of the content being transmitted from each of your web servers. Even when web servers are responding erroneously or not responding at all, or your customer leaves a page before it is fully transmitted, Netlogger will log these events and give you a much more comprehensive performance analysis than relying on server monitor logs only.
- **Optimize** your network Unispeed Netlogger gives you precise information of the traffic composition and load distribution on your network. Without installing a single piece of software onto your web servers you will be able to enhance the performance and availability of your network and resources by analysing traffic patterns and server behaviour - either in real-time, or from recorded data. This will allow you to identify bottlenecks in the network topology, as well as faulty or overloaded equipment.
- Analyse and real-time visualise traffic composition across the network
- Deep packet inspect a number of protocols, including HTTP, DNS, FTP, SMTP, POP3, IMAP, IM , Telnet and Syslog.
- Direct policy enforcement server to prioritise or block undesired traffic based on layer 3 to 7 information or patterns and signatures matched in the full packet content
- Determine and real-time visualise
 - traffic amounts exchanged between servers.
 - latency and server response
 - traffic content composition
- Build and upgrade of data warehouses.
- Import of data from existing data sources (e.g. databases) to be used in network analysis.

6.4 Network Security

The Unispeed Netlogger™ is commonly used as last defence network security.

As illustrated by the "Swiss cheese model" any network, no matter how well protected, is susceptible to intrusion. Lots of systems such as IDS, IPS firewalls and anti virus programs provide protection against known vulnerabilities.

The unispeed Netlogger™ has the ability to match pattern and signatures when bot-nets are created and zombie PC's are recruited and map relationships between nodes, control- and dump-servers.



When an attack penetrates these systems there is however little chance that the source and effect of the attack is discovered timely.

The Unispeed Netlogger™

- Constantly monitors the traffic composition on the network and initiates logging when abnormalities are detected
- Rule based detection of floods, DoS and DDoS, classified by origin, content and intensity
- Detection of excessive streams of legitimate and expected type of traffic (service level attacks)
- Detection of which areas of a network is in trouble – allowing administrators to selectively block out internet traffic.
- or automatically direct firewall to block attacking IP- ranges for a time period
- Real-time email/sms notification system, so that when a security breach occurs, administrators can react promptly.
- Continuous dump of large amounts of traffic for post attack forensic analysis and data recovery.

6.5 Business critical data protection

Protecting your corporate data and intellectual properties is a vital task for any corporation linked to the internet. No matter if data is leaked from the inside or your company is a victim of automated scraping, Netlogger can help you

Intellectual Property protection

Netlogger can protect your documents and files from being mailed or uploaded to the internet. Netlogger will generate hash key/checksum from intercepted files (Video, pictures, documents etc.) and compare the result with data bases listing the hash key/checksum for such sensitive files.

Furthermore the Netlogger can search for strings in the content or packet headers that would indicate a undesired data transfer

Data Scraping

Scraping data from a web site is a growing problem for companies with on-line business, like travel agencies, dating sites or on-line directories. Several airlines are using data scraping to automatically

compare their prices with competing carriers, making your own campaign ineffective.

If not protected any information that you post on your web site could easily be scraped and available on a competitors site in a few minutes.

Since scraping by nature is accepted by your network as a legal action, your protective measures will be unable to detect the malicious traffic. Adding to the damage arising from loss of data, many scraping techniques whether distributed or not consume large amount of band with and cause excessive delays for legitimate users. In consequence this could lead to unnecessary investments in more band with and server capacity.

Unispeed Netlogger monitors your traffic without being detectable on the network. The advanced rule based classifier distinguish normal traffic from scraping. Thresholds can be set to determine the level and sort of countermeasures desirably for each attack. When values for these thresholds are exceeded Netlogger will issue alarms and generate SNMP messages to block the malicious traffic.

No matter how your network is attacked, Netlogger will remain unaffected and enable you to review the exact chain of events. This will enable you to refine the rule based classifier for even more precise threat mitigation.

Corporate policy enforcement

Most companies have set policies for their employees use of their corporate network and external connections, but very few have the equipment to control this traffic. Except from the large amount of time some employees spend writing private mails, instant messages or surfing the Internet, critical data and information could easily be disclosed via these channels.

Furthermore certain web sites contain material which most companies would have little interest in having their employees viewing from their position at work.

One way to restrict this traffic is to block access to certain ports and services, however this method is neither effective nor desirable Using the hash key / checksum method described above transfers of undesired material can be disclosed (Child porn pictures, training manuals etc.)

Adding deep packet inspection to your outside lines will enable you to apply smart filters onto the content level and disclose unauthorized access to your company's critical data or financial information or disclosure of such information.

When Netlogger intercepts a violation of your corporate policy it will retain a copy of the original data flow to ensure the data is valid from a legal aspect.

6.6 Cyber defense

Unispeed has developed solutions for lawful interception since year 2000. The Unispeed Blue Shield solution addresses Government Organisations and Communication Service Providers with a legal requirement to deliver data to Law Enforcement Agencies. However more and more countries are seeing the need to introduce network surveillance to their governmental and public networks in order to counter growing concerns about cyber attacks often launched from other countries.

With Unispeed data retention probes strategically positioned in the network infrastructure governments and GOV-Cert functions can receive early warning about such attacks.

Unispeed data retention probes can real-time track and Geo-target millions of packets per second and provide a highly sophisticated intelligence to decision makers.

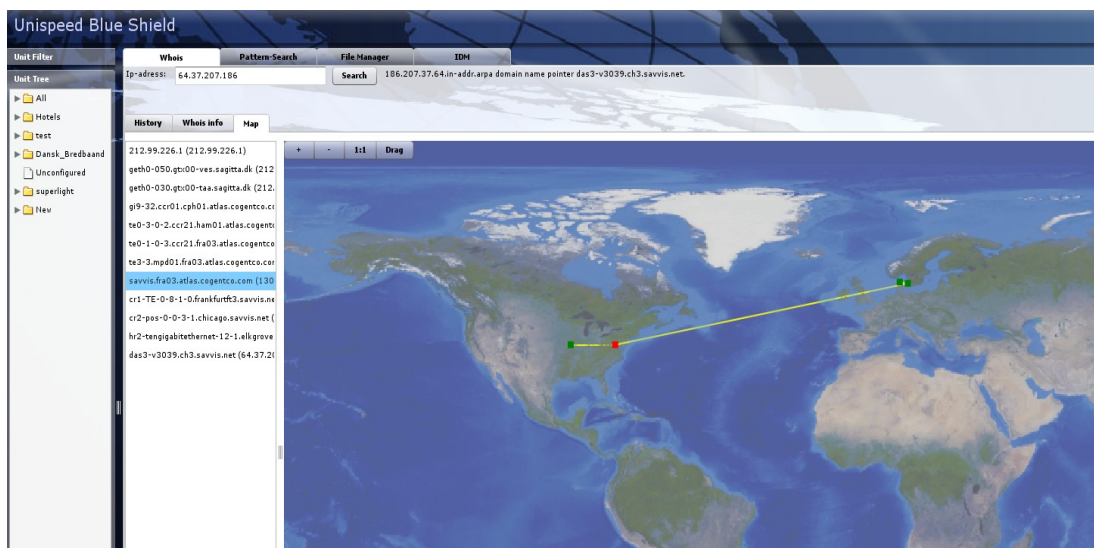


Illustration 13: Trace route depiction

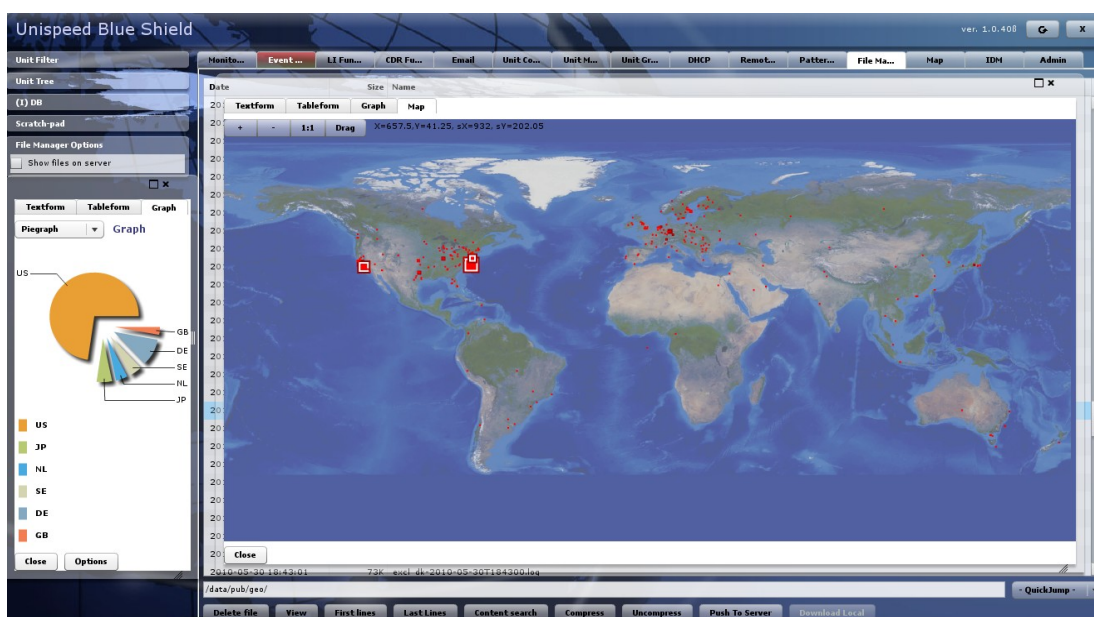


Illustration 14: GEO Lookup reporting