



## Unispeed Netlogger™ 3.0 White paper

Version 1.2, 26. April 2007

©2007 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](http://www.unispeed.com)

**Unispeed Inc.**  
255 E. Campbell Avenue  
Campbell, CA 95008  
USA

# Table of Contents

<b>1. Introduction.....</b>	<b>3</b>
<b>2. What is Unispeed Netlogger™?.....</b>	<b>4</b>
<b>2.1 Unique features.....</b>	<b>5</b>
<i>Return on Investments.....</i>	<i>5</i>
<b>3. Netlogger™ Application Areas.....</b>	<b>6</b>
<b>3.1 Web Analysis and business intelligence.....</b>	<b>6</b>
<i>Key features.....</i>	<i>6</i>
<b>3.2 Traffic and Content Billing.....</b>	<b>8</b>
<i>Key features.....</i>	<i>8</i>
<b>3.3. Network Performance and optimisation.....</b>	<b>9</b>
<i>Optimize your network.....</i>	<i>9</i>
<b>3.4. Network Security.....</b>	<b>10</b>
<b>3.5. Business critical data protection.....</b>	<b>11</b>
<i>Data Scraping.....</i>	<i>11</i>
<i>Corporate policy enforcement.....</i>	<i>11</i>
<b>3.6. Lawful interception.....</b>	<b>12</b>
<i>Unispeed Anti terror solution.....</i>	<i>12</i>

## 1. Introduction

During the last Decade, the interest in network traffic analyses has been constantly growing. Companies have realized the importance of knowing the activities on their networks, and have thus dedicated considerable resources to decipher network trends.

However, at first sight the amount of available network traffic data is overwhelming. Companies with busy networks have several servers, which makes network analyses both frustrating and time-consuming. Just looking at the log files of each individual server is enough to take your breath away!

And the problems do not stop here, since many questions arise:

- How do you store the data?
- How do you process the data?
- How do you deal with security threats?
- How do you detect bottlenecks during peak traffic hours?
- How do you build and upgrade your data warehouse?
- How do you secure your data and intellectual properties?

As you probably know, there is virtually no end to this list of questions. One answer is frequently followed by ten new questions – or at least: that was the way it used to be! With Unispeed Netlogger™, processing of network data is taken to a whole new ballgame.

The classic approach to log, analyse and decipher network traffic has lead to multiple software installations and ad-ons to the network servers and a large increase of net-flows on the network. This has lead to complicated network structures and overloaded servers, not to mention the vast amount of software licenses that has to be maintained.

Basically, with Unispeed Netlogger™ you have access to the hole story in real-time, allowing you to deep packet inspect your network traffic, 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 reporting suites. This will give you a thorough business overview and help your company to meet future challenges.

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.

## 2. What is Unispeed Netlogger™?

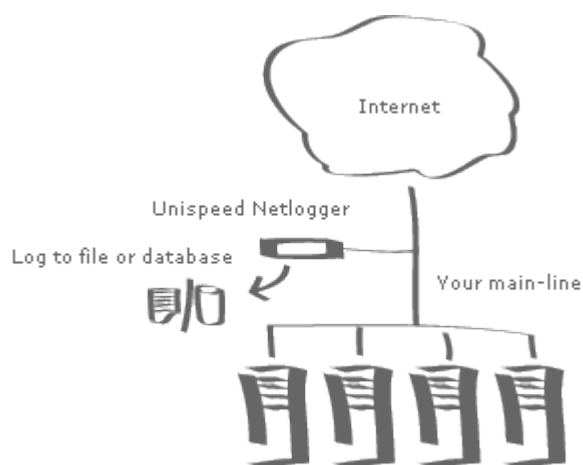
Without going into details, this white paper will present you with a quick overview of the various application areas that can be addressed by the Unispeed Netlogger™. This will help you to realize the many great features, which are directly usable in your day-to-day routines.

Basically, Unispeed Netlogger™ is a passive network sniffer, traffic analyser and data center, which you mount on your network. The enterprise version is designed for mounting in a standard 19" rack and equipped with up to 8 x 1Gbit network interfaces.

Netlogger Light versions are designed for office and mobile needs, wherefore they are fan-less and offered with wire-less network cards

The exact hardware configuration of the Netlogger™ box depends on the amount of traffic on your network and your data processing demands. Before setting up the Netlogger™ box, Unispeed (or a Unispeed partner) will discuss these issues with you.

Figure 2.1 demonstrates a normal set-up of the Netlogger™ box. Here, the Netlogger™ is logging network traffic to a NAS or database, but this could also be done exclusively on the Netlogger™ box, depending on the amount of data.



*Fig. 2.1: Normal set-up of the Netlogger™ box.*

A number of tools are present on the Netlogger™ box. A tool is an object with either an input and/or an output. We will discuss this in detail in chapter five. Normally the input is some data, while the output is some modified version of the input, after one or several operations have been performed.

The number of tasks the Netlogger™ box can perform depends on which tools are installed on it. More than 50 tools are currently available. Exactly which tools are present on your Netlogger™ box depends on which Netlogger™ solution you have purchased.

## 2.1 Unique features

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 called the Unispeed K-sniffer. The ability to read packets from a network, filter and analyse the data without copying it makes the Netlogger by far the fastest packet sniffer on the market (up to 6-8 Gbit/s depending on the amount of analysis it has to perform).

As the Netlogger performs real-time extraction/parsing and filtering/analysis of the collected data it is not limited by the speed the data can be written to memory. In fact the Netlogger can log to several files 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 and log-files (netlogger format or common log files format). This feature enables the netlogger to perform post-processing and data-mining of files previously stored, and even do this while it keeps sniffing the network.

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

### Return on Investments

Having a Netlogger™ attached onto your network performing consolidated logging relieves servers and routers from secondary logging funktions and can easily increase the network performance by 10 to 15%.

Furthermore the easy access to logdata generated by a simple reconfiguration of the Netlogger™, facilitates that future needs for network analysis, business intelligence and security can be added to the same platform without spending money on costly integration and software licences.

### 3. Netlogger™ Application Areas

The Netlogger™ box 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 company.

#### 3.1 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 behavior. 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 Targit. The Targit Suite in combination with Unispeed data collectors brings you fast and accessible business intelligence for timely decision making.

##### Key features

*Conversion rate* The conversion rate is the key element for analyzing a successful advertising campaign. In addition, it shows how effective specific search engines or partner sites are.

*Transition:* Discover how customers click through your web site, analysing if the customer meets your success criteria in the shortest way, where customers tend to drop out and why.

*Double coverage:* Analyse the habit patterns of your customers

*Page entry:* From where did the customer enter your site, which affiliated sites or search engines are generating more customers.

*Micro optimisation:* real-time analyse how changes to the web site effects sales completion and a smooth conversion through your web site

*Customer profiling:* React to customer's need geographically, bandwidth, screen resolution, return rate of customer

*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.
- Parse 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 extension (e.g. “com”, “dk” or “de”).
- Map client IP addresses to second level domain names (e.g. “domain.com”).
- 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.

## 3.2 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 and volume

The Netlogger™ box makes it easy to create and deploy applications for billing and analytical setups. Some common usages are:

- Port monitoring based on customer IP addresses.
- Billing based on user login.
- Customized user specific identifiers.
  - Per volume: Netlogger will track the costumers traffic volume aggregated over time. Advanced rules like price differentiating with respect to peak hours, maximum allowed band with or flat rate exceeds is easily configured into the Netlogger.
  - Per download: Netlogger will automatically identify whether the service is a download and bill accordingly
  - Per click: Netlogger will bill-back content providers for each time the costumer click on an advertisement
  - Quality of service: Netlogger can track the quality of each transmission with respect to errors and retransmissions, thereby significantly improve costumer satisfaction, and even alert maintenance and sales functions if server or network response time exceeds desired limits (SMS, E-mail or sys log)

The billing options can easily be fully integrated with a variety of billing systems.

Other approaches might be:

- Calculate used kilobit levels on connections and place the results in databases for quick billing.
- Different billing policies for different types of services (e.g. \$X per E-mail or \$X per KB, etc.).
- Merge billing files with real-time files.

### Key features

The Netlogger™ can be positioned on the network so as it receives a copy of all traffic flowing on the network simultaneously, without creating additional traffic on the network itself. This logically approach eliminates the risk of erroneous data arising from dublets and packets being dropped by routers and other network equipment in high load situations.

The advanced functionalities build into the Netlogger™ traffic measurement tools easily distinguish between inbound, outbound and internal traffic and delivers precise billing information to the accounting database.

### 3.3. 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

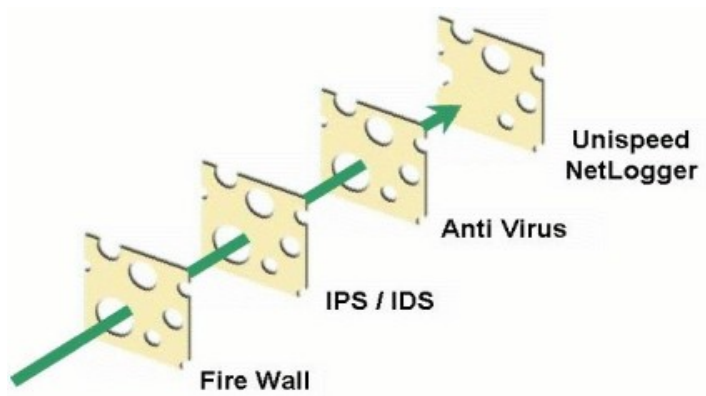
Unispeed Netlogger gives you precise information of the traffic composition and load distribution on your network. Without installing a single piece of software onto your web servers you will be able to enhance the performance and availability of your network and resources by analyzing traffic patterns and server behavior - 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, POP 3, IM, Telnet and Syslog.
- Direct policy enforcement server to prioritise or block undesired traffic based on layer 3 to 7 information or strings extracted from 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.

### 3.4. 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.



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.

### **3.5. 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

#### **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. 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.

### **3.6. Lawful interception**

Unispeed has developed solutions for lawful interception since year 2000.

Netlogger offers unmatched flexibility in terms of tracking criminal activity on the network. Filters and thresholds can be applied at any protocol level including searching for strings in attachments, instant messages, file transfers etc.

The generic trigger functionalities adds intelligence to the netlogger, as it allows the user to expand or redefine search patterns automatically.

The Netlogger can either work as a stand alone data acquisition device or perform post-processing of data streamed from the Unispeed Interceptor, DPI pre-filter device ( 8 GBit/s line speed capable).

With the Unispeed Netlogger you can

- Analyse, filter and classify traffic with respect to type, content or origin
- Extract traffic containing specific words, phrases, numbers or other rule based filtering
- Trigger a new set of rules and filters when records matches a filter
- Apply thresholds and double coverage logic to limit the risk of false positives

The Netlogger will real-time extract most common protocols and near real-time visualise the collected sessions in the build in the viewers.

### **Unispeed Anti terror solution**

For Companies and Internet service providers susceptible to Danish and European Anti terror laws Unispeed has developed an affordable solution based on the Netlogger that scales to any size network.

Costumers are offered full flexibility in terms of storing data to indexed logfiles on a network attached storage or into their existing databases.

The Unispeed solution is independent from existing infrastructure as it relies on mirrored traffic instead of netflows.

The solution can separate log data from the network to ensure that logdata is never compromised in case the network should be attacked.

Unique user identification is merged with captured data by retrieving the users mac. nr. or option 82 identification

A user friendly web interface allows the user to schedule session and content logging (HI2 data) and search database or logfiles for datasets that needs to be forwarded to the authorities.