

Next-Generation Ethernet Monitoring

Enschede (NL), Brno (CZE), 7. 7. 2011

Researchers from the University of Twente monitor Ethernet networks with FlowMon Probes - a solution of INVEA-TECH - and obtained interesting and surprising results, which are currently being published at major conferences.

The Design and Analysis of Communication Systems (DACS) research group from the University of Twente (The Netherlands), lead by professor Aiko Pras, focuses on research in the area of Next-Generation Ethernet monitoring. SURFnet, the Dutch academic backbone network operator, is currently investigating the deployment of a Next-Generation Ethernet network. FlowMon Probes from the Czech university spin-off company INVEA-TECH are used for practical measurements for the new SURFnet network.

INVEA-TECH prepared a special plugin for their FlowMon Probe platform, in order to support Ethernet-layer monitoring at the University of Twente. Thanks to this customized plugin, the probes monitor traffic at the Ethernet-layer and use a modified process of flow creation (source and destination MAC addresses, VLAN ID and Ethernet type are used as key-fields, among others; non key-fields statistics provided are Ethernet header length, Ethernet payload length etc.) The measured statistics are exported to IPFIX collectors for storage and analysis.

The new type of flow data offers a completely new insight into the network. While other flow monitoring technologies, such as NetFlow, provide flow data at the IP-layer (by means of IPv4 and IPv6), Ethernet-layer flow data provides an overview of all the traffic protocols operating on top of Ethernet. Among these protocols are Address Resolution Protocol (ARP), Link-Layer Discovery Protocol (LLDP), Novell IPX, DECnet Phase IV protocols, Spanning Tree Protocol (STP) and Wake-on-LAN Magic Packets.

“The special FlowMon Probe plugin from INVEA-TECH enables us to profile network traffic, but also to detect misconfigurations and security issues, which would not have been visible at the IP-layer. We are currently publishing first results of measurements at academic conferences,” said Aiko Pras, Associate Professor at the University of Twente.

Researchers of the University of Twente are joining INVEA-TECH’s community program, which will enable them to prepare their own FlowMon Probe plugins in the future and to use the probes for upcoming research experiments. *“We are glad that experts from the University of Twente are joining our community program and look forward to continuing this close and very productive cooperation,”* said Petr Springl, FlowMon Product Manager. *“The FlowMon community program is open to every research and academic organization focused on network monitoring and security based on flow technology.”* For more information about FlowMon Community program please contact us at www.invea-tech.com/contacts.

About the University of Twente:

The University of Twente (UT) is located in the Netherlands, and has some 3,300 scientists and other professionals working together on cutting-edge research, innovations with real-world

relevance and inspiring education for more than 9,000 students. The Design and Analysis of Communication Systems (DACS) group has around 20 researchers, who investigate the design and implementation of dependable networked systems, as well as methods and techniques to support the design and dimensioning of such systems, such that they are dependable, in all phases of their lifecycle. Important topics within DACS are network management and measurements, with a focus on flow-based techniques for the purpose of security and configuration management.

About INVEA-TECH:

INVEA-TECH develops and markets comprehensive network solutions for networks from 10 Mbps to 100 Gbps. The core idea of the company is to provide a complete range of innovative products and services for network security, network monitoring, traffic analysis and hardware-accelerated application development. The flagship product is FlowMon – a complete NetFlow/IPFIX monitoring and security solution which enables flow monitoring in each network and provides efficient network management, increased network security (NBA - network behavior analysis), LAN & WAN & Internet monitoring, users and application monitoring, data retention law fulfillment and more. The next products are FPGA boards with 10GE interfaces, the NetCOPE platform for rapid development of network applications or NIFIC - wire-speed filter for lawful interception, and others. For more information, visit www.invea-tech.com.