Datasheet

FlowProbe 4x100GbE

Monitor networks in real-time to diagnose issues, detect anomalies and maintain security with the ultra high performance FlowProbe

The Telesoft FlowProbe provides detailed un-sampled traffic statistics in the form of flow records from large scale networks up to 4 x 100GbE per high performance 1U appliance.

Un-sampled flow based monitoring gives network analysts detailed and accurate information about each and every communication session, including the end point identities, the session start and end times and the volume of traffic transmitted. TCP session timing information allows detection of anomalies and classification of traffic. This gives complete traffic visibility for analysis, Network Performance Monitoring and Diagnostics (NPMD) and compliance.

In addition the Telesoft FlowProbe can identify Layer 7 protocols, and extract key information into flow records:

- HTTP flows are detected on any port, and the host, uri, method and status fields extracted and included in the flow record.
- SSL flows have the server name extracted and included in the flow record.
- DNS flows are detected, and the CNAME and host addresses added to the flow record.
- BGP correlation of IP address to AS is added to the flow record.

The probe does not affect the monitored traffic and typically connects to monitoring infrastructure such as packet brokers or taps. Flow records are exported for analysis and storage to the scalable Telesoft Data Analytics Capability (TDAC) collection, retention and analysis application or to another IPFIX/NetFlow compatible collector.

Automatic detection of tunnelled traffic (GRE,GTP, MPLS, IPinIP) and de-tunnelling gives visibility of encapsulated traffic found on national ISP and telco carrier networks, making the Telesoft 4x100GbE FlowProbe ideal for large scale national network deployments, peering links or data centre backbone. When de-tunnelling is selected, the FlowProbe will create flow records for the individual flows within a tunnel (including all the layer 7 details), and also identify the outer tunnel that is carrying it giving another layer of visibility and protection.

Key Features

Instruments up to 300 Million concurrent flows at a churn rate of 5M sustained, 7M peak flows/s	Monitor large scale network traffic for cyber security analysis, NPMD and compliance
Passively monitors 4x100GbE	Connect to large scale monitoring infrastructure, peering links, national xSP, large data-centre
De-tunnels GTP, GRE, MPLS and IPinIP traffic	Monitor large scale/national ISP and telco networks
Duplicate packet detection and removal	De-duplication improves monitoring tools efficiency, accuracy and storage requirements
Enhances records with BGP, SSL, DNS, HTTP host and HTTP URI	Layer 7 visibility and control for granular user management
Exports flow records to Telesoft TDAC or other compatible IPFIX collector	Quickly deploy accurate, large scale network visibility and analysis

Technical Specifications

Physical	• 1RU 19-inch rack mount • 1.7x17.2x30.6 in (4.3x43.7x77.7 cm)
Monitoring Interface	• 4 x 100GBASE-LR4 QSFP28
Tunnelling Support	• Configurable to automatically detect and de-tunnel: MPLS, IPinIP, GRE, GTP
Flow Export Interface	• 10GbE Fibre Interface with swappable transceivers • Up to 32 IPFIX collectors
Throughput	• 5M flow/s sustained, 7M flow/s peak • 300M simultaneous flows
Flow Record Format	• IETF RFC7011/RFC7012 IPFIX • Export formats: IPFIX, Netflow • Supported Collectors: Telesoft TDAC or other IPFIX/Netflow compatible collector
Enhanced flow data	• HTTP Host and URI: Rapidly know which IP addresses have visited which websites without any additional lookup, check for abnormal behaviour and look for connections to rogue URIs • HTTP Return Code: Check for abnormalities, such as machine initiated attacks indicated by a high level of 404 • Server Name from SSL certificate exchange: Check for abnormal behaviour or investigate specific servers of interest • DNS query name, response name, address: Detect suspicious and rogue DNS servers • Correlation of IP address to autonomous systems (AS), to map network infrastructure • TCP session timing (SYN / SYN-ACK): Detect anomalies and classify traffic
Power Stats	• 320W typical, and 350W peak

Order Options

Part Number	Description
500003074	400G FlowProbe, 1U, QSFP28, 4x100GbE
500003082 (Note 1)	100G QSFP28 LR4 Transceiver
500002852 (Note 2)	10GBase-LR optical SFP+ transceiver 1310nm, Single-mode LC
500003012 (Note 2)	10GBase-ER optical SFP+ transceiver 1550nm, Single-mode LC
500002853 (Note 2)	10GBase-SR optical SFP+ transceiver 850nm, Single-mode LC

note 1 - Four QSFP28 required for each FlowProbe
note 2 - Optional collector interface transceivers
Other transceivers may be used but must be on approved list. Contact Telesoft for more information.

Headquarters
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
t. +44 (0)1258 480880
f. +44 (0)1258 486598
e. sales@telesoft-technologies.com

Americas
Telesoft Technologies Inc
430 National Business Parkway
Suite 480, Annapolis Junction
MD 20701
USA
e. salesusa@telesoft-technologies.com

Asia
Telesoft Technologies Ltd
Tapasya Corp Heights
Ground Floor, Sector 126
Noida, 201301
t. +91 120 612 7725
e. salesindia@telesoft-technologies.com