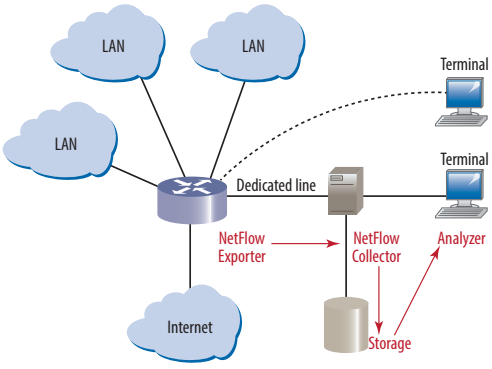
Improving the Effectiveness of Flow-Based Monitoring and Troubleshooting

Increasingly, network operators adopt flow-based technologies such as NetFlow, sFlow, J-Flow, and IPFIX to gain visibility into their network switches, routers, and other network devices. However, flow-based solutions alone are often insufficient to solve specific end-user problems, and they may even strain networks with the additional data they generate. Flow-level data is great for trending, high-level analysis, and some troubleshooting. However, access to packet data is required for detailed visibility into application performance, capacity planning, security threats, and end-user experience.

Flow Technology

Flow-based solutions consist of network equipment with embedded flow agents and flow collectors. Flow agents gather information about traffic on interfaces and forward it to flow collectors using the UDP protocol. A flow collector is a software application, running on a workstation or server, that collects the traffic data from a number of flow agents, stores the data, analyzes it, and presents the analysis to the network administrator in a variety of ways such as charts, dashboards, and thresholds. Many agents can send data to the same collector. Flow collectors may be incorporated with other systems which provide congestion control and troubleshooting, route profiling, audit trail security analysis, and accounting for billing.

Currently, there are a number of common flow implementations. NetFlow is the most common. Supported by Cisco® on its routers and switches, NetFlow sends information about completed traffic flows to a central collector. The device decodes every IP packet, maintains tables of active flows, and forwards flow records periodically or when they complete to a network management application. NetFlow has recently become adopted by the IETF Flow Information Export (IPFIX) standard as an approach that allows non-Cisco devices to send data to a NetFlow collector in a NetFlow-recognized format.



sFlow is an open standard based on RFC-3176. It was created by InMon® which provides sFlow collectors. sFlow uses statistical sampling to copy packets from the network stream and sent them to a collector/analyzer. Another common implementation is J-Flow by Juniper Networks.

Limitations of Flow-Based Implementations

Flow-based solutions involve a number of issues that can prove problematic.

Network Blind Spots — Flow is typically implemented only in higher-end switches and routers. Many enterprise remote branch office routers may not include the capability or require costly, specialized versions. Inconsistent implementations between products often result in large blind spots.

Overtaxing Infrastructure — Sending flow data may overtax routers and switches. More frequent sampling rates and a high number of agents may adversely impact packet-processing performance.

Lack of Content Awareness — Packet-level information in addition to flow information is required to isolate application-affecting parameters such as TCP window problems, application calls, and response codes. Adding deep packet inspection (DPI) functionality to existing network devices is both costly and complex.

Costly and Complex External Appliances — standalone flow-monitoring probes introduce additional hardware, setup, and maintenance costs, while potentially introducing additional points of failure.

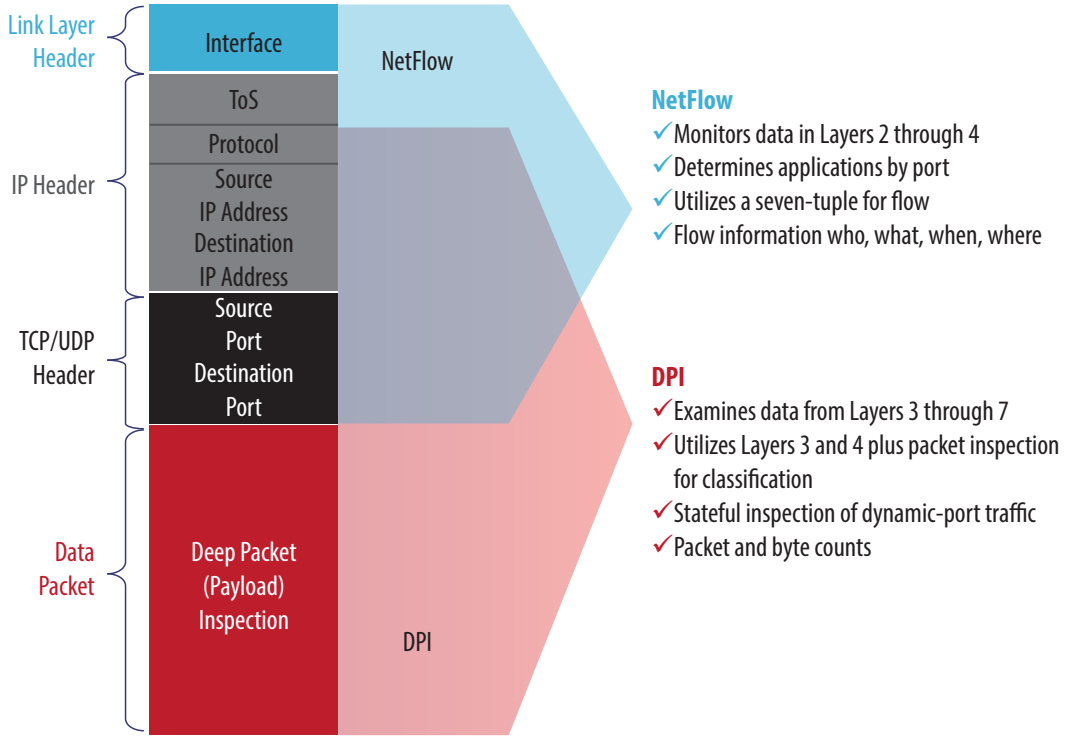


Figure 1. Characteristics of NetFlow and deep packet inspection packet processing

PacketPortal™ Complements and Enhances Flow-Based Solutions

PacketPortal complements flow-based reporting strategies by providing packet-level visibility, extending visibility to blind spots at the network edge such as remote offices, where implementing flow reporting may not be possible. PacketPortal overcomes the impracticalities—the cost, reliability and complexity—of using dedicated network probes while providing in-line content level visibility. PacketPortal can make any network device flow-capable, while also adding deep-packet and content intelligence, providing consistent access to key information for monitoring and troubleshooting. By offloading flow sampling, PacketPortal frees the network device to do what it does best: process and forward packets, thereby simplifying the deployment, planning, and engineering of flow within existing networks. As part of an overall flow-based monitoring strategy, PacketPortal helps reduce the time it takes to identify, diagnose, and resolve complex performance issues. PacketPortal minimizes the traffic load on the network by only sending filtered data and adds no additional processing tax on network devices which support PacketPortal-enabled SFProbes™.

Example Applications and Use Cases

PacketPortal complements flow capabilities embedded in network devices, and in combination with flow-analysis software tools, can enable a variety of solutions including:

Application Aware Policies and Congestion Control — By monitoring traffic flows on all ports continuously, flow can highlight congested links and identify traffic sources and associated application-level conversations. PacketPortal can filter data used on aggregated TCP ports, such as port 80, forwarding this to network and flow-analysis tools. Network operators can determine effective controls such as application-specific policies

Security and Audit Trail Analysis — A comprehensive security strategy involves protecting the network from external and internal misuse and protecting information assets from theft. This requires complete network surveillance with alerts to suspicious activity. PacketPortal can enhance basic flow-provided information to enable network-wide surveillance and route-tracing information. Upon detecting anomalies using Flow, PacketPortal can enable users to drill down to isolate specific issues.

Route Profiling and Capacity Planning — Since flow contains forwarding information, it can be used to profile the most active routes and the specific flows carried by these routes. PacketPortal helps isolate application details within flows. Understanding routes, flows, and details within flows makes it possible to optimize route performance by improving connectivity and performance and by choosing the most cost-effective peering partners based on a highly-granular basis.

Accounting and Billing for Usage — Detailed network usage information is needed to fairly charge for network services and to recover the costs of providing value-added services. Flow data can be used to account and bill for network usage by customer. PacketPortal enables transaction, content, and message-level billing which can also be used to provide customers with an itemized breakdown of their total traffic, highlighting top users and applications.

The combination of flow and PacketPortal allows network operators to implement network-wide monitoring with deep content intelligence, extending capability to remote locations where previously no detailed monitoring may have been possible. PacketPortal augments the capability of flow-capable network routers and switches, providing critical information for capacity planning, historic data collection and traffic analysis, network performance analysis, and unified visibility across networks.

Test & Measurement Regional Sales

NORTH AMERICA	LATIN AMERICA	ASIA PACIFIC	EMEA	www.jdsu.com/test
TOLL FREE: 1 855 ASK-JDSU 1 855 275-5378	TEL:+1 954 688 5660 FAX:+1 954 345 4668	TEL:+852 2892 0990 FAX:+852 2892 0770	TEL:+49 7121 86 2222 FAX:+49 7121 86 1222	